International Telecommunication Union

ITU-T

NGN FG Proceedings

Part II

2005

ITU-T
NGN FG
Proceedings

Part II

International Telecommunication Union

TABLE OF CONTENTS

Part I – Next Generation Networks Framework

Part II – NGN Focus Group Deliverables*

NGN Focus Group deliverables status, as indicated by FGNGN at its 9th meeting, 14-17 November 2005

Section 1 – Release Independent Deliverables

Working Group 2 deliverables – Functional architecture and mobility

Working Group 3 deliverables – Quality of Service

---

* *Legend*

P *Already passed to ITU-T Study Group 13; one already published as Q.Supplement 51*

A *Sufficiently mature to be considered by ITU-T Study Group 13 for publication*

S *Mature but would require further consideration in ITU-T Study Group 13*

D *Not yet mature, requires discussion and technical input to complete development*

Section 2 – Release 1 Deliverables

Working Group 1 deliverables – Service Requirements

A	2.1	NGN Release 1 scope
A	2.2	NGN Release 1 requirements

Working Group 2 deliverables – Functional Architecture and mobility

A	2.3	Functional Requirements and Architecture of the NGN
A	2.4	Mobility management capability requirements for NGN
A	2.5	IMS for Next Generation Networks
A	2.6	PSTN/ISDN emulation architecture

Working Group 3 deliverables – Quality of Service

P	2.7	A QoS control architecture for Ethernet-based IP access network
S	2.8	Multi service provider NNI for IP QoS
D	2.9	Requirements and framework for end-to-end QoS in NGN
D	2.10	The QoS Architecture for the Ethernet Network
D	2.11	Functional requirements and architecture for resource and admission control in NGN
D	2.12	A QoS framework for IP-based access networks
A	2.13	Performance measurement and management for NGN
P	2.14	Algorithms for achieving end to end performance objectives

Working Group 4 deliverables – Control and Signalling Capability

P	2.15	Signalling requirements for IP QoS (published as ITU-T Q-series Supplement 51)

Working Group 5 deliverables – Security Capability

A	2.16	Security requirements for NGN – Release 1
D	2.17	Guidelines for NGN-security for Release 1

Working Group 6 deliverables – Evolution

A	2.18	Evolution of networks to NGN
A	2.19	PSTN/ISDN evolution to NGN
A	2.20	PSTN/ISDN emulation and simulation

Section 3 – Beyond Release 1 Deliverables

Working Group 2 deliverables – Functional Architecture and mobility

D	3.1	Softrouter requirements
D	3.2	Converged services framework functional requirements and architecture

Working Group 7 deliverables – Future Packet-based Bearer Networks

P	3.3	Problem statement
A	3.4	FPBN requirements
A	3.5	FPBN high-level architecture
D	3.6	FPBN candidate technologies

NGN Focus Group deliverables status

Status

At its 9th meeting in London, 14-17 November 2005, the Focus Group on NGN has provided a view on the status of the documents.

Deliverables that are marked "P" in the sixth column of tables 1, 2 or 3, have already been passed to ITU-T Study Group 13, and one has been published, as shown.

The FGNGN considers that the deliverables that have given the status "A" have been developed to a sufficiently mature state, as technical reports, to be considered by ITU-T Study Group 13 for publication.

The FGNGN considers that those deliverables that have gained the status of "S" have reached a mature state but would require further consideration in Study Group 13 before publication.

The FGNGN considers that all other deliverables shown as status "D", are not yet mature, requiring discussion and technical input to complete their development.

ITU-T FGNGN deliverables

as approved at the FGNGN Plenary meeting 17 November 2005

Table 1 – List of Release Independent Deliverables

WG	Deliverable Title	Current Draft	Target Date	Cat.	Stat	Target SG*
2	Framework for Customer Manageable IP Network	FGNGN-OD-00194	August 2005	0/2/1	P	13
2	Terms, definitions and high level terminological Framework for Next Generation Network (TR-TERM)	FGNGN-OD-00261	4Q05	N/A	D	13
3	General Aspects of Quality of Service and Network Performance in the Next Generation Networks (TR NGN.QoS)	FGNGN-OD-00166	4Q05	0/1/1	D	13/12
3	Network performance of non-homogeneous networks in NGN (TR-NGN.NHNperf.)	FGNGN-OD-00240	4Q05	0/1/1	A	13/12

Table 2 – List of Release 1 Deliverables

WG	Deliverable Title	Current Draft	Target Date	Cat.	Stat	Target SG*
1	NGN Release 1 Scope	FGNGN-OD-00253	4Q05	1/1/1	A	13
1	NGN Release 1 requirements	FGNGN-OD-00252	4Q05	1/1/1	A	13
2	Functional Requirements and Architecture of the NGN (FRA)	FGNGN-OD-00244r2	4Q05	1/2/1	A	13
2	Mobility Management Capability Requirements for NGN (FRMOB)	FGNGN-OD-00246r1	4Q05	1/2/1	A	13/19
2	IMS for Next Generation Networks (IFN)	FGNGN-OD-00245r1	4Q05	1/2/1	A	13/19
2	PSTN/ISDN emulation architecture	FGNGN-OD-00247r1	4Q05	1/2/1	A	13
3	A QoS control architecture for Ethernet-based IP access network (TF 123.qos)	FGNGN-OD-00106	Mar. 2005	1/2/1	P	13
3	Multi Service Provider NNI for IP QoS (TR msnniqos)	FGNGN-OD-00205	4Q05	1/2/1	S	13
3	Requirements and framework for end-to-end QoS in NGN (TR e2eqos.1)	FGNGN-OD-00204	4Q05	1/2/1	D	13
3	The QoS Architecture for the Ethernet Network (TR enet)	FGNGN-OD-00202	4Q05	1/2/2	D	13
3	Functional Requirements and Architecture for Resource and Admission Control in Next Generation Networks (TR racf)	FGNGN-OD-00241	4Q05	1/2/2	D	13
3	A QoS Framework for IP-based access networks (TR ipaqos)	FGNGN-OD-00113	4Q05	1/2/1	D	13
3	Performance measurement and management for NGN (TR pmm)	FGNGN-OD-00239r1	4Q05	1/2/1	A	12

Table 2 – List of Release 1 Deliverables

WG	Deliverable Title	Current Draft	Target Date	Cat.	Stat	Target SG*
3	Algorithms for Achieving End to End Performance Objectives (TR apo) (#=From the September 2005 FGNGN meeting, this deliverable has been transfereed (via parent SG13) to continue further work in SG12.)	FGNGN-OD-00200	3Q05	1/2/2	P	12
4	Signalling requirements for IP QoS (TRQ.IP.QoS. SIG.CS1)	Q Series Supplement 51	Dec. 2004	1/2/2	P	11
5	Security Requirements for NGN Release 1	FGNGN-OD-00255	4Q05	1/2/1	A	13
5	Guidelines for NGN-Security for Release 1	FGNGN-OD-00254	4Q 05	TBD	D	13
6	Evolution of Networks to NGN	FGNGN-OD-00257	4Q05	1/2/1	A	13
6	PSTN/ISDN evolution to NGN	FGNGN-OD-00258	4Q05	1/2/1	A	13
6	PSTN/ISDN emulation and simulation	FGNGN-OD-00259	4Q05	1/2/1	A	13

Table 3 – List of beyond Release1 Deliverables

WG	Deliverable Title	Current Draft	Target Date	Cat.	Stat	Target SG*
2	Softrouter Requirements	FGNGN-OD-00043	TBD	2/2/1	D	13
2	Converged Services Framework Functional Requirements and Architecture (TR-CSF)	FGNGN-OD-00248r1	4Q05	2/2/1	D	13
7	Problem Statement	FGNGN-OD-00158	Apr. 2005	2/1/1	P	13
7	FPBN Requirements	FGNGN-OD-00268	4Q05	2/1/1	A	13
7	FPBN Architecture	FGNGN-OD-00269	4Q05	2/2/1	A	13
7	FPBN Candidate Technologies	FGNGN-OD-00180	4Q05	2	D	13

Explanation of Table Columns

The columns in the table are explained in this section.

WG: Working Group responsible for progressing the deliverable.

Deliverable Title: Title of the deliverable.

Current Draft: Output Document containing the draft text of the deliverable agreed to represent the deliverable by the Working Group.

Target Date: This is the date that the working groups are using as a target for Focus Group approval.

Category (Cat.): A tuple (x/y/z) indicating the intended release, stage and depth of the deliverable. The stage and depth description are taken from Recommendation I.310 with the deletion of "from a user's perspective" from the stage 1 definition and a simplification of the depth (step) indication. The categorisation is as follow:

Release

0 Generic Document; Contains Information That Is Not Release Specific

1 Release 1 document; all of the contents is applicable to ITU-T NGN release 1; unless stated otherwise in the document it is expected that it will remain in force beyond release 1

2 Release 2 document; specifies additional capabilities and interfaces as part of ITU-T NGN release 2

3 etc.

Stage and depth

1 overall service description

- /1 service prose definition and description
- /2 formal service description using attributes and/or graphic means

2 overall description of the organisation of the network functions to map service requirements into network capabilities

- /1 derivation of a functional model
- /2 information flow diagrams and possibly further details e.g. SDL

3 definition of switching and signalling/protocol capabilities needed to support services defined in stage 1.

- /- no further depth indicator

***Target Study Group (SG)**: The Focus Group's expectation of the ITU-T Study Group that will take the deliverable and further progress the work to Recommendation or other ITU-T published Document.

SECTION 1

RELEASE INDEPENDENT DELIVERABLES

WORKING GROUP 2
DELIVERABLES

FUNCTIONAL ARCHITECTURE AND MOBILITY

1.1 Framework for customer manageable IP network (*Status P*)

1.2 Terms, definitions and high level terminological framework for NGN (*Status D*)

1.1 – Framework for Customer Manageable IP Network*

Summary

Technical Report TR-CMIP specifies the framework for customer manageable IP network.

Key words

Customer, Manageability, Information Value Chain, Next General Network (NGN), Global Information Infrastructure (GII), protocol reference model.

Table of Contents

* Status P: This deliverable has already been passed to ITU-T Study Group 13.

Page

1.1 – Framework for Customer Manageable IP network

Introduction

This document contains the advanced IP network architecture especially in views of end-user functions for control and management. The future IP network is not just focused into the provider provisioned single network. It equally considers the integrated environments of fixed/wireless network elements to accommodate computer systems, home peripherals and intelligent appliances. The future IP network may compromise of heterogeneous requirements of service quality and physical interface from network and computer and consumer equipments.

A IP network guarantees real-time service quality and supports multimedia applications. It also provides bandwidth reservation and various service models for present and future business needs. A IP network has the following general features.

- Support business model for differentiated service concept
- Support usage-based billing and charging model
- Stable and secure with reliability performance of 99.999 %

To support these features, the network operator provides network connectivity services to its end users. A service level agreement (SLA) is a formal definition of the contractual relationship between service provider and its end user [14]. It specifies what the end user wants and what the supplier commits to provide. It defines the level for the quality of services provided, setting performance objectives that the supplier must achieve. It also defines the procedure and the reports that must be provided to track and ensure compliance with the SLA.

In this service environment defined by a SLA, the IP network should be reliable and manageable. The end-to-end connectivity should meet the negotiated SLAs according to various application types and equipment types. The users may want to include their specific performance requirements in terms of bandwidth, delivery time, and loss performance for each application. But, some users may not want SLA like the existing Best Effort IP service which means no guarantee of delivery time and loss performance.

The SLA for an IP network assures performance and availability of the network to an end user. Until now, the network performances including reliability and availability are the key parameters that network operator could control. The network offers a set of SLAs to the end user. The network capabilities which are defined in SLA may be activated by the request-based or subscription-based manners. By negotiating with the end user, the network operator has to control and manage network resources of the IP network.

1 Scope

The scope of this document covers:

- Definition of and requirements for the service capabilities offered to an end user of a NGN, implemented with IP.
- Reference architecture, from the end user perspective, of a manageable IP network
- Functional capabilities, from the end user perspective, of a manageable IP network
- Applications scenarios and procedures used by the end user of a manageable IP network

Details of the mechanisms to support these capabilities are out of the scope.

2 References

2.1 Normative References

ITU-T

[1] ITU-T Recommendation Y.100 (1998), General overview of the global information infrastructure standards development

[2] ITU-T Recommendation Y.110 (1998), Global information infrastructure principles and framework architecture

[3] ITU-T Recommendation Y.1001 (2000), A Framework for Convergence of Telecommunications Network and IP Network technologies.

[4] ITU-T Recommendation Y.1241 (2000), IP transfer capability for support of IP-based services

[5] ITU-T Recommendation Y.1221 (2001), Traffic Control and Congestion Control in IP Networks

[6] ITU-T Recommendation Y.1311 (2001), IP VPNs – Generic Architecture and Service Requirements

[7] ITU-T Recommendation Y.1311.1 (2001), Network Based IP VPN over MPLS Architecture

[8] ITU-T Recommendation Y.1541 (2000), Network performance objectives for IP-based services

[9] ITU-T Recommendation Y.1720 (2001), Protection Switching for MPLS Networks

[10] ITU-T Recommendation Y.2001, General overview of NGN functions and characteristics

[11] ITU-T Recommendation Y.2011, General reference model for Next Generation Networks

[12] ITU-T Recommendation M.3010, Principles for a Telecommunications management network

[13] ITU-T Recommendation M.3400, TMN Management Functions

[14] ITU-T Recommendation M.3050, Enhanced Telecommunications Operations Map

[15] ITU-T Recommendation Y.1711, Operation & Maintenance mechanism for MPLS networks

[16] ITU-T Recommendation Y.1291, An Architectural Framework for Support of Quality of Service (QoS) in Packet Networks

2.2 Informative References

[17] TR-059 DSL Forum, “DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services,” September, 2003

[18] R. Braden, “Requirements for Internet Hosts - Communication Layers,” RFC 1122, October 1989

[19] IETF, Cisco Systems NetFlow Services Export Version 9, RFC3954, October 2004

[20] IETF, LDP Specification, RFC3036, January 2001

[21] IETF, Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering, RFC3477, January 2003

[22] IETF, Detecting MPLS Data Plane Failures," Internet Draft draft-ietf-mpls-lsp-ping-08.txt, February 2005

[23] IETF, LSR Self Test, “draft-ietf-mpls-lsr-self-test-04.txt, February 2005

[24] Ian Foster, The Grid: Computing without Bounds, Scientific American, April 2003.

3 Terms and Definitions

- Customer Manageable IP

  It defines user manageability of resources parameters and network capabilities on an IP network. Users can allocate, configure, control, and manage the resources of IP network elements.

- End-to-End Transparency

  The seamless connectivity without change of information content between end users, while away from original location with the relevant terminal equipments and applications.

- Information Navigation

  moving from one source of information to other, related, sources of information

- Information Query

  requesting and defining ways of looking for information

- Auto-Discovery

  The end users or the network elements find their neighbors automatically by using solicitation and advertisement messages.

- Auto-Configuration

  The end user gets its interface address automatically that creates a link-local address and verifies its uniqueness on a link. It should be obtained through the stateful or stateless mechanism.

4 Abbreviations

AAA	Authentication/Authorization/Accounting
CDR	Connection Detail Record
CoS	Class of Service
CPE	Customer Premises Equipment
C-Plane	Control Plane
DNS	Domain Name Service
ftp	File Transfer Protocol
M-Plane	Management Plane
MPLS	Multi-Protocol Label Switching
P2P	Point to Point
P2MP	Point to Multipoint
PABX	Private Automatic Branch Exchange
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
QoS	Quality of Service

SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLS	Service Level Specification
VPN	Virtual Private Network
VTR	Video Tape Recorder
UNI	User Network Interface
U-Plane	User Plane
UPC	Usage Parameter Control
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XML	Extensible Markup Language

5 Service Definitions and Requirements for Customer Manageable IP Network

5.1 Service Definitions

The customer manageable IP service is defined from the users' point of view. It is clearly different from the service concept of the existing network provider. Figure 1/TR-CMIP shows the service concept of the customer manageable network. The network providers construct the network, but they may not be responsible for developing services. The end users can create and develop their own networking services with help of the network provider. The network capabilities offered to the end users include how to control and manage network elements and their resources. The network capabilities can be classified into a set of menus. A set of menu of network capabilities are specified in terms of a number of SLA parameters. The customer manageable IP service is defined as follows:

- An end user could choose his customers which may be human, terminal equipments, or applications.
- The end user could create their own services and network configurations (e.g. virtual private networks (VPN)) with relevant network resources provided by network providers.
- The end user could choose some control and management functions over his own network. In order to carry out these functions, the end user could choose from the sets of control and management functions, offer and negotiate service level agreements with network providers on QoS and network performance including security capability.

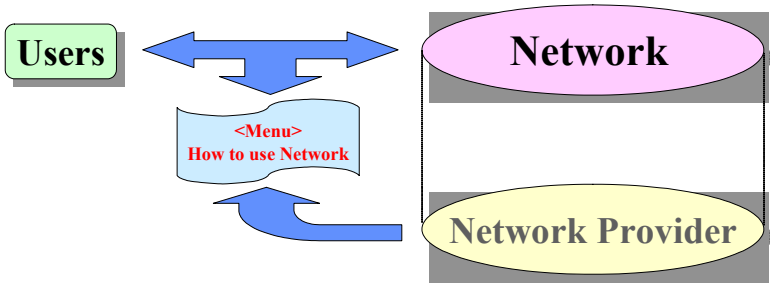


Figure 1/TR-CMIP – Service concepts of the Customer Manageable IP Network

From the information value chain model of global information infrastructure (GII), the 'end user' may be an individual, information agents/brokers, information providers or information service providers [1],[2].

The menus of network capabilities can be chosen through individual functional blocks or service blocks and their combinations. A functional block can be divided into entities of network resources. Examples of transport resources may be storage, bandwidth, processing time, etc. Examples of service block resources might be distance learning, telecommuting, electronic commerce, telemedicine, on-line entertainment, etc. Some resources dedicated to a group of users such as VPN are available. Also, some resources are combined with associated technologies and service architectures such as databases, secure networks, WWW, or Java, etc.

5.2 Level of Manageability

The network capability sets are classified into various levels of manageability. They depend upon the points of views of both the end user and the network operator. The detailed means of customer manageability are beyond the scope.

The level of manageability can be divided as shown in Table 1/ TR-CMIP.

Table 1/TR-CMIP – Levels of Manageability

Levels	Descriptions	Features	Remarks
0	**No Management**	No monitoring, No Resource Control	• No mechanism to detect network fault and congestion. • No mechanism to control network resources
1	**Overall Network Resource Management**	Overall monitoring, No Resource Control	• Notify overall network fault and resource status by network provider • No resource control by the end user
2	**Group level Resource Management**	Group level Resource Monitoring and Control	• Notify group level network fault and resource status by network provider • End user manages the group level resources
3	**Individual Resource Management**	Individual level Resource Monitoring and Control	• Notify individual network fault and resource status for end-to-end connectivity • End user manages the end-to-end resources

The group level manageability manages the same level of network resources for a set of user groups according to service/application types. It is applicable to the group of virtual private network users. For resource management, the multiple sets of individual resources that are normally dedicated to a single user can be grouped into a single entity of manageability. A single resource entity can also be shared within the same group of users. The same resources can also be shared by different user groups.

(Notes) The accuracy or granularity of manageability of resource parameters is beyond the scope since it depends upon the nature of implementation.

5.3 Service Requirements

The requirements for IP services are divided into end user service requirements, network provider requirements, VPN requirements, and application provider requirements. According to information value chain model, the network providers are responsible for communication and networking of information, for which information processing and storage capability are required. The VPN is to provide the dedicated network resources for a group of users. The application providers include information service brokers and information service providers.

5.3.1 End-User Service Requirements

The end user service requirements include as follows:

- Availability (e.g., 99.999 %)
- Response time (example, less than 5 ms to download a file of 1 Mbytes)
- Service blocking probability including network access blocking
- Service priority and QoS/CoS

5.3.2 Network Provider Requirements

From viewpoints of customer manageability, the network provider requirements can be specified in terms of network performance parameters between one or more interface points which are in the administrative domain of network operator [8]. They also include the parameters relating to network connectivity, Authentication/Authorization/Accounting (AAA), access filtering, end user service and troubleshooting.

Depending on service and application types, network providers may have the relevant processing and storage capabilities as well as intelligent telecommunication service capabilities. They can provide the add-on capabilities such as information query and navigation and name/number/address portability. Then, the network provider requirements are described as follows:

- Network capabilities for customer manageability
  - Create/update/delete user profiles including user name, number, subscripted services, etc.
  - Advertisement/solicitation of name, address and number
  - Assignment of network addresses and address filtering
  - Authorization/authentication to identify user (e.g., query for user identifier, password, certification, etc.)
  - End user service and troubleshooting of network access problems
  - End-to-end transparency
  - Name/number/service portability, navigation, name notification and name database management
  - Accounting of user's service utilizations for billing
- Network performance parameters
  - Packet error rate, packet loss rate
  - Round trip delay, one way delay and delay variance
  - Availability (system uptime, mean time to failure, mean time to repair, etc.)
  - Peak bandwidth, available bandwidth, minimum bandwidth
  - Round trip delay of location identification for mobility
  - Access blocking probability and service completion probability
  - Traffic monitoring and statistics (e.g., number of packets to be received or transmitted, number of packets discarded or received in error, etc.)

5.3.3 VPN Service Requirements

VPNs over IP networks can provide diverse configurations based upon necessary service features at customer premises. One network provider may configure a different VPN separately, using physically different links and routers. Then, the VPN service requirements are basically the same as those of the network provider. Additionally, the following service requirements can be specified:

- Configuration and operation of VPNs

- Security including VPN authentication and authorization

In order to configure VPNs with intelligent features, the active configuration mechanism will be helpful to provide user controllable services among VPN users via IP network. In addition, the following features will be necessary to support diverse VPN services over IP networks:

- VPNs with multiple dimensioned virtual networking
- VPN QoS/Resource negotiation with Policy Server
- IPv4/IPv6-based VPN services with mobility
- routing/forwarding functions for IPv6 VPN over MPLS

Furthermore, if IPv6 VPN is applied to IP network, the interworking functions are necessary.

5.3.4 Application Provider Requirements

The application provider may utilize a same infrastructure owned by the network provider to those subscribers whose IP addresses are assigned and managed by the network provider. For example, an application provider may offer gaming, video on demand, filtered Internet access via IPsec or various IP tunneling scheme. It is envisioned that the service environments of the application provider will be user-level rather than network level. Network elements used by the application provider can include application servers and directory servers as well as switches/routers.

The functional requirements of application providers are similar with network provider requirements. They include authenticating users, assignment of user profiles with preference, end user service and troubleshooting of network access and application-specific problems. They also have the ability to determine traffic usage for accounting purposes and billing.

The performance requirements of application provider depend upon specific applications. They are specified according to the number of application clients as well as the capacity of the application servers. The performance requirements of application provider are as follows:

- Transfer priority and QoS/CoS
- Security including access control and authentication
- Performance monitoring
- Identification of user, service, and terminal type
- Redundancy of servers (or reliability of servers)
- Clustering of servers
- Round trip delay of naming and identification
- Service completion probability
- Name/number/address/service portability
- Name/service advertisement and solicitation
- Information query and navigation including database management

6 Reference Model of Customer Manageable IP Network

6.1 Introduction

This section provides the reference model of customer manageable IP network. The user network interfaces (UNIs) are the demarcation points between the user domain and the network domain. Also, their functions

are identified at the User-Plane (U-Plane), the Control-plane (C-Plane), and Management-Plane (M-Plane). The detailed functional specifications at each interface are beyond the scope.

6.2 Reference Architecture

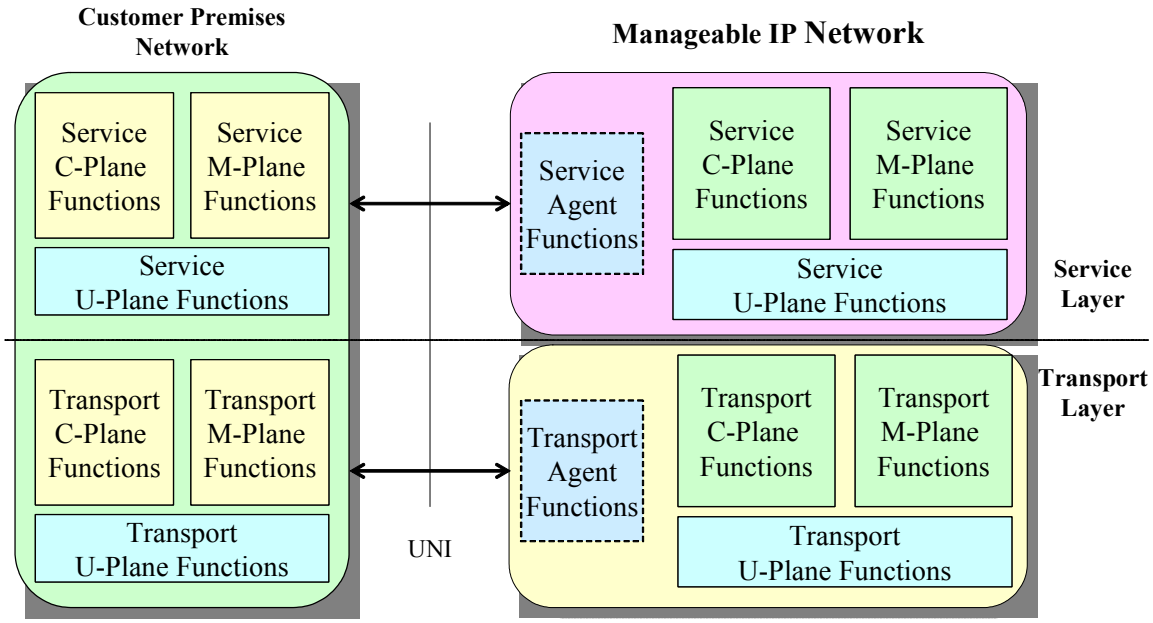


Figure 2/TR-CMIP – Reference architecture of customer manageable IP network

Figure 2/TR-CMIP shows the reference architecture of customer manageable IP network. According to the general reference model of Y.2011, the IP network is divided into service layer and transport layer. The functions of each layer are divided into the User-Plane functions, the Control-Plane functions, and the Management-Plane functions. The customer manageable functions at the interfaces between end user and network are guided by transport agent functions and service agent functions. The detail transport agent and service agent functions are beyond the scope.

The business processes in M.3050 and the FCAPS Management Functional Areas in M.3400 should be considered along with the manageability of IP-based networks and services.

6.3 Capability Sets of Manageability

The functional capabilities are provided by the network which is operated by network providers, VPN providers or application providers. The end users choose a set of functions according to their desired services and applications. At the transport layer, the functional capabilities of the IP network are controlled by end users. The end user also controls the service sets at the service layer.

The depth of manageability can be classified into implementation stage or control level of the network. Depending on services and application types, a number of capability sets of manageability could be offered to the users. For example, since the current router-based IP network could not provide any manageable capability, the end user experiences some difficulties to control the IP network elements for their specific applications. The source routing or the destination option in IPv6 can give a kind of manageability since the routing path can be selected by the end user. Also, the existing telephone network does not provide customer manageability since end users could not choose the QoS parameters.

A number of capability sets could be defined according to end user applications. The manageability sets can be classified into the following categories:

- Telco-based services and applications (e.g., fixed/wireless telephony, PABX, various access/trunk/home gateways, intelligent call centers and servers, etc.)
- Broadcast-based services and applications (e.g., interactive TV, video conference, satellite TV, etc.)
- Computer-based services and applications including Web services
- Home applications (e.g., PDA, VTR, consumer electronics, game box, etc.)

The detailed creation of capability sets also depends on technical feasibilities. The following technologies are classified from the viewpoints of customer manageability:

- Fixed and wireless transport technologies
- Switching and routing technologies
- Network control and management technologies
  - robustness, resilience, redundancy, and intelligence, etc.
  - Mobility management including location identification and authentication
- QoS and Traffic Engineering technologies
  - differentiated priority, aggregate QoS, and end-to-end QoS
  - Admission control, traffic shaping, re-routing, and congestion avoidance, etc.
- Network-based security and PKI technologies
- Navigation/Search/Query technologies including naming and directory services

The capability sets of manageability depend upon network scale, ownership, control accuracy, and service profile, etc. Table 2/TR-CMIP shows the examples of capability sets of manageability.

Table 2/TR-CMIP – Examples of Capability Sets of Manageability

Classifications	Capability Sets	Features	Descriptions
Public Networks	**P0**	No Management	– subscription by offline
	P1	Overall Resource Control	– basic OAM including network failure – monitoring of traffic activity and network status-
	P2	Group level Resource Control	– support a group of users and VPN subscribers – satisfy the group or VPN QoS/SLA including billing options
	P3	Individual Resource Control	– handle individual users – satisfy the negotiated QoS/SLA including billing options
Private Networks	**C0**	No Management	– configured by system operators
	C1	Overall Resource Control	– basic OAM including system faults – monitoring of traffic activity and system status
	C2	Group level Resource Control	– support a group of users – maintain the QoS/SLAs for a group of users
	C3	Individual Resource Control	– handle individual users – maintain the predictable QoS/SLA

(Note) It notes that the public network and private network can be classified according to ownership, administrative domain, and charging option, etc.

The example scenarios for manageability sets on existing IP networks are as follows:

- 1st stage: priority-controlled IP networks
  - priority and routing path control according to source and destination IP address pairs
- 2nd stage: application-based manageable IP networks
  - a number of bandwidth, metering, billing and security options based on application types
- 3rd stage: fully customized IP networks
  - fully customized or personalized controls on end-to-end resources

The possible scenarios or stages of manageability on the IP network could be chosen from business demands of end user.

6.4 Trade-off Analysis of Capability Sets in Scalability, Complexity, and Provisioning Costs

The functional sets for manageability can be chosen by end users after trade-off analysis versus their provisioning costs. The functional capabilities which require the trade-off analysis could be as follows:

- QoS option: guaranteed, acceptable and best effort,
- Security options including authentication, and
- Billing options including advice of charge, etc.

Some capabilities may have a set of granularities depending on implementation. They can be chosen with different weighing factors and end user preferences. First, QoS option refers to mechanisms to differentiate performance. It also means providing predictable or guaranteed performance to applications, sessions or traffic aggregates. As regards regional areas, the end user can choose their acceptable QoS option by comparing with their provisioning cost. Normally, users do not want to pay high service costs for their applications. In a case, the full sets of QoS capability are used without economic analysis. For the issues of authentication, it is also often called 'the identity problem.' Like spam, this is more of a user issue, but it should be solved over the network architecture since it may require scalable and hierarchical trust models. From information value chain model, the IP services could be offered with various billing options such as flat rate or usage-basis. The advice of charging may be used before retrieving some video content materials. Also, differentiated billing option can be offered when guaranteeing the delivery time of information materials. A group of users like companies or organizations could be charged for the usages of their VPNs including fixed and wireless applications.

7 Functional Capabilities for Manageable IP Network

7.1 Overview

The functional capabilities of the IP network are divided according to end user perspectives and provider perspectives. The manageable functional sets provided by the network provider are offered to the end users. The end users use their functional sets in order to construct their own IP network.

The manageable functional capabilities are classified into those of the User-Plane, the Control-Plane and the Management-Plane. The relationships of manageable functional sets between end user and network provider are given in Table 3/TR-CMIP. The manageable objects are divided into the managing entities as an active object and the managed entities as a passive object. It assumes that the managing entities are intended to create, initialize, set, and write the corresponding functional capabilities and the managed entities are to receive, read, and release the functional capabilities. The control accuracy of the manageable objects depends upon implementation level and control parameters of those entities.

Table 3/TR-CMIP – Relationships between manageable functional sets in terms of the U-Plane, the C-Plane and the M-Plane

(Note) The meaning of "x" notation indicates the active management entities which include creation, initialization, write, or remove operations on those management objects. The meaning of "o" notation indicates the passive management entities which include receive, read, process, monitor, and release operations.

Capabilities	End user Perspectives			Network Provider Perspectives		
	U-plane	C-plane	M-plane	U-plane	C-plane	M-plane
Naming			x			o
Addressing	o			x		
User Grouping			x			o
Application Clustering			x			o
End User/Service Registration			x			o
End User/Service Identification			x			o
Information Navigation and Query			x			o
Auto-Discovery			o			x
Auto-Configuration			o			x
Information Access Control	x			o		
Information Security	x			o		
End-to-End Transparency	x			o		
Connection Configuration		x			o	
Routing and Forwarding Control	x			o		
Alternative Path Selection	x			o		
Multi-homing	x			o		
Mobility Control		x			o	
Mobility Management			x			o
Traffic Measurement	x			o		
Usage Parameter Control	x			o		
Bandwidth Assignment	x			o		
SLA Negotiation			x			o
End-to-End QoS Provisioning	x			o		
Priority Assignment	x			o		
Information Storage	x			o		
Directory Processing	x			o		
Segment OAM and End-to-End OAM	x			o		
VPN Configuration			x			o
Billing and Charging Option			x			o
Client/Server Management			x			o
Agent Management			x			o

7.2 Naming and Addressing Capability

If an end-user moves continuously, its connectivity would be manageable and controllable at any time. It may frequently bring the binding procedure between permanent address (that is home address) and temporary address (that is care-of-address). The temporary care-of-address may be used to identify the visiting location and it does not play the same role as the fixed home address. The home address looks like a kind of user identifier such as an existing telephone number.

To support the IP network, the existing Domain Name Service (DNS) functions based on IP address would be extended to allow user controllability. The real-time address translation and dynamic mapping between address and domain name server are required to support mobility. The following requirements for naming and addressing are necessary to support the customer manageable IP services.

- End user and terminal identification by number and its naming service
- Dynamic update and automatic configuration of name service database
- Translations between private naming/addressing and global naming/addressing for end-to-end connectivity

In the customer manageable IP network, name information is managed and transferred by end user.

7.3 User Grouping and Application Clustering Capability

User grouping is mainly used for multicast and VPN service. The IP network requires proper registration and membership distribution mechanism for user grouping. Flexible grouping mechanism is also needed to control a number of user groups simultaneously. Therefore, to give the customer manageability, end users have a right to select, join, and leave a group actively.

Clustering is the common term for distributing a service over a number of servers in order to increase fault tolerance or to support load sharing among a number of servers. It is often used for large scale and mission critical applications where there can be no downtime. The application clustering can be applied to efficiently manage the future very large scale network**.**

In the customer manageable IP network, end user can trigger application clustering by turning multiple computer servers into a cluster. Each of the servers maintains the same information and they perform administrative tasks such as load balancing, determining node failures, and assigning failover duty.

7.4 End User/Service Registration and Identification Capability

The end user can be identified by his name, address, and/or number. The physical attachment point like MAC address is also used to identify him. The relevant binding mechanisms among name, address, number and physical attachment point are needed to allow user manageability. End users can dynamically update and change their registration information in the IP network.

When the end users move other location, their physical locations have to notify at the corresponding registration servers or the destination users being active.

7.5 Information Navigation and Query Capability

In the IP network, all information will be available in digital form, which can be used to describe various types of multimedia information. This description shall be associated with the content itself to allow fast and efficient searching for material of a user’s interest. All the information and applications stored in the network should be addressed and managed by their name and keyword. To handle large volumes of storage information, the database may be searched and sorted with relevant directory structure.

For information navigation and query capability, it specifies a standard set of descriptors that describe various types of multimedia information and identify its contents. The description of "information material" provides the means to encode audio-visual material as objects having certain relations in time and space.

To help information acquisition, it requires short descriptions for raw information contents. In principle, any type of information materials may be retrieved by means of any type of query material. The search engine to match the query data and the information description may be needed. To help information acquisition, information processing and storage platform may be needed (e.g., servers for messaging, retrieval, and distribution, etc.)

7.6 Auto-Discovery and Auto-Configuration Capability

Auto-discovery and auto-configuration capabilities are the key technologies that enable the IP network to be quickly customized to the environments that they are intended to manage. In order to deploy new services at a rapid pace, it is essential that the discovery methodologies be implemented in an extensible manner, so that new discovery capabilities can be added step-by-step to the IP network.

The IP network should support the auto-discovery capability that dynamically conveys location information of end user. It can be useful for service scalability. Its advantages are as follows.

- Reduce downtime by eliminating the process of identifying the IP address and manually adding it in the replacement unit
- Increase safety in the automation system by eliminating the potential for erroneous IP configurations
- Increase security by monitoring all devices on the network
- Reduce the added costs in both equipment and support. Eliminating the complexity from modification of switch configuration firmware and/or hardware

7.7 Information Access Control and Security Capability

End users may at times take network paths with certain level of security. For securing data traffic, it should construct a secure channel to their home networks. It provides the access control technique and cryptographic techniques during registration and activation time. The IP based VPN services are mandatory to provide the security with appropriate policy. The set of administrative policies determine both connectivity and QoS for VPN customers.

The packet filtering capability can provide reasonable protection and access control at the user network interface. It is applied to various gateway routers or intermediate network equipments between end users and network. The packet filtering and security functions can be combined with specific protocols like SIP, H.323, ftp, or Email, etc.

7.8 End-to-End Transparency Capability

One of the critical requirements is seamless connectivity when away from original location. Also, the end-to-end transparency should be maintained during handover. The transparencies are essential for applications independent of the supporting infrastructure. The network provider should support the following three transparencies.

- Location transparency

  With distributed computing technology, third party service providers can access from anywhere regardless of the actual physical location of such server.
- Network transparency

The application server executes the corresponding control process independent of specific network types and user terminals.

- Protocol transparency

  It achieves protocol transparency by providing a standardized protocol interface, realizing independent service control processes, shielding complex network technical details from the service provision platform, and developing open communication network interfaces.

The existing IP network cannot support network transparency due to firewall, network address translation (NAT) and so forth. To support the customer manageable IP network, these three transparencies should be manageable by end user. If the end user wants end-to-end transparency, network providers could check whether they could support the end-to-end transparency. The network provider will restrict other functions such as NAT or disguised traffics which can disrupt the transparencies. It should be verified which functions disrupt location, network and protocol transparencies.

7.9 Connection Configuration Capability

The connection configuration specifies who communicates with whom (e.g., end user, information service broker, and information broker, etc. Entities (e.g. sets of users, object entities, sets of processors, etc.) geographically distributed across an open communications environment can communicate with one another.

There are three basic connection configurations such as point-to-point, multicast, and broadcast. Multicast and broadcast services are configured by point-to-multipoint connections.

Point-to-point connection may provide unidirectional and bidirectional, symmetric and asymmetric paths. For the point-to-point connection the manageable IP network can support the following features.

- established, modified, or released by two participating users' request
- established with unicast addressing/naming capability

Broadcast connection may provide unidirectional communication between one user and the others. This connection is the one-to-many (all) during a particular initiated session. Sending the broadcast information everywhere is a significant wastage of network resources if only a small group is actually interested in its' contents.

Multicast connection is the one-to-many relationship continues for duration of a given initiated session. In this connection, one user is root and other users are leaves that are not all users in network. The root can send one copy of each packet and address it to the group of leaves that want to receive it.

7.10 Routing and Forwarding Control Capability

The proper routing paths between the source and the destination are decided according to traffic contract and overall network traffic condition. The routing path could be chosen by the end user with a definite routing policy. The routing paths between the source and the destination are decided by end users in the IP network. For connectionless transfer, the router forwards the IP messages with their respective QoS information and end user requirements along a selected routing link.

In general, the routing algorithm could be classified according to routing decision processes which are generally applied to end-to-end or hop-by-hop connections. For network scalability and robustness, some combinations of routing decision processes may be used for the specific connections or message flows. In particular, robust and efficient operation in mobile IP networks is to be supported by incorporating routing preferences of mobile IP hosts.

The following routing requirements are necessary in IP networks:

- Capability to support the QoS enabled path

The QoS enabled path is needed to support the user's specific requirements (mobility, VPN, security, policy, and QoS level, etc.).

- Capability to provide alternate path

  To cope with a failure of routing path, the alternate routing paths should be provided.

- Capability to exchange routing information for internetworking situations

  negotiate and select the QoS parameters with the multiple network providers to support the end-to-end QoS requirements.

- Capability to support scalable routing

  A trade-off introducing a limited amount of routing database information in IP network elements could be considered at the large scale IP network.

- Capability to support broadcast routing

  The network is able to copy packets that allow sources to send packets to all receivers.

- Capability to support multicast routing

  The network is able to build packet distribution trees that allow sources to send packets to all receivers that are bound to the multicast spanning tree. The multicast tree is built according to network policies.

7.11 Alternative Path Selection and Multi-homing Capability

To deliver reliable service, the user can require a set of procedures to provide protection of the traffic carried on different paths and to support the selection of its' physical/logical interface. To support this requirement, an alternative path selection and multi-homing capability is needed.

Alternative path selection capability guarantees seamless service by avoiding service degradation when network faults occur. For selection of the backup path, the IP network maintains its' route information along the same original path and proceeds to setup the alternative path. There are following requirements to support alternative path selection capability:

- Alternative path discovery
- When a network fault occurs, the user traffic is automatically routed to the alternative path according to the alternative path selection policy that is set by the end user. The network provider must furnish tools and network information to enable end user in setting policy and provisioning alternative paths. The alternative path is provided by the network provider policy, administration considerations, and traffic requirements to several network entities such as users, network equipments, service providers, etc. Alternative path comparison (optional)

  When discovering various alternative paths by network provider, user can determine what the best selected path is.

There are some advantages of providing multi-homing capability. The first advantage is redundancy. This is similar to alternative path effect. Network entities such as users, hosts, routers and subnets should be able to insulate it from certain failure modes within one or more network providers. The network with this capability should accommodate continuities in connectivity during failures. The other advantage is to support better performance. By multi-homing, a network entity should be able to protect itself from performance degradations between the entity's transit providers. Multi-homing provides multiple interfaces that are connected to different networks.

7.12 Mobility Control and Management Capability

While most end users are assumed to move continuously, their connectivity should be manageable and controllable at any time. The efficient mobility management procedures should be developed in a

combination with security procedures. The users and terminals in mobility should be able to dynamically update their location database. It is continuously checked by the mobile users' database. It establishes the mechanisms that enable a mobile host to maintain and use the same IP address as it changes its point of attachment to the network. It has the relevant registration protocol to authenticate the mobile IP nodes and users. The location resolution and seamless handover procedures are enforced while the IP users or terminals are in motion. To support mobility control, the following capabilities are necessary:

- Capability to allow a mobile node to be reachable by having a permanent address
  - Address management function
  - Registration function
- Capability to know where a mobile node is
  - Network information advertising/detecting function
  - Registration function
  - Paging function
- Seamless handover capability
  - Regional mobility management function
  - Multicast function
- Capability to provision proper resources during handover
- Capability to support inter-domain mobility
- Capability to find the optimal routing path
- Capability to support commonly AAA and security

7.13 Traffic Measurement and Usage Parameter Control Capability

Usage Parameter Control (UPC) is the set of actions the network takes to monitor and control traffic. This includes the validity of the connection. The operation of the UPC is to check whether input traffics conform the QoS objectives of a compliant connection or not. However the excessive policing actions on a compliant connection are part of the overall network performance degradation and so safety margins should be engineered to limit the effect of the UPC. Conforming traffic means performance guarantees as contracted. Traffic exceeding the conformance test will receive an excess treatment. The forwarding process can further be associated with service priority, and service reliability parameters.

Flow control of UPC guarantees that sources behave as agreed upon during the call setup phase, after a call is accepted and a decision made to penalize or not penalize traffic or connection when its arrival triggers an overflow. It takes actions (such as tagging or discarding) if a source does not obey its contract. Violation of its contract takes place when there are malfunctioning equipments, malicious users or delay jitters.

The IP network has to support directly traffic measurement and usage parameter control functions. End user can negotiate the UPC parameters with a network provider. The user can control the QoS level based on these UPC parameters. For example, NetFlow describes to provide access to observations of IP packet flows in a flexible and extensible manner [19].

7.14 Bandwidth Assignment and SLA Negotiation Capability

The IP networks would be manageable, reliable and seamless to satisfy the negotiated SLAs. In addition, end users may choose their service profiles and performance characteristics.

The network provider must negotiate and agree with the end user on the technical details of specific instances of the service products being offered. The QoS parameters may be the same as those offered or

customized to a specific service instance. There are always two SLAs, one for each direction. The SLA specification requires extensive testing of the available infrastructure.

The IP network will provide the end user services with the provisioned SLA. The end user could dynamically negotiate SLA with the network provider. The end user can change the SLA to the maximum extent the network provider could provide.

7.15 End-to-End QoS Provisioning and Priority Assignment Capability

For the applications to work to the satisfaction of end users it needs performance guarantees on the resources they use. The end-to-end QoS provisioning is required for many applications, such as the upper bound for packet loss and the maximum transmission delay in real-time audio streaming applications.

The IP network will allow the end user to select end-to-end QoS. The network provider should guarantee end-to-end QoS as the contract with end user.

7.16 Information Storage and Directory Processing Capability

Networks generate a large amount of information. Compiling and managing this information manually is nearly impossible. Directory processing plays an important role in providing information access across networks. It is involved with many directory operations that require access to information such as end user preferences, patient information, student records, and public records.

From a service provider's perspective, it requires the capability to manage both user profiles (e.g., phone number, address, and subscribed service lists) and network/service profiles (e.g., network configuration, topology, and server lists). If a service provider grants a user the capability to manage the user's profile, the user can manage personal information like password, friends' address lists, etc.

The service layer at the IP network may provide information storage services for clients. Grid networks are one popular application environment which can provide these services in a secure, flexible, dynamic manner [24].

7.17 Segment OAM and End-to-End OAM Capability

As the network converges onto an IP-based infrastructure, the requirements for both segment and end-to-end OAM capability become more pivotal in order to maintain SLA contracts. To construct segment and end to end OAM flows from the perspective of an end system, the MPLS OAM and MPLS Ping/Trace could be applicable [15],[22].

7.18 Virtual Private Network Configuration Capability

The VPN can be configured on multiple dimensioned service provider networks. In these multiple dimensioned network environments, VPN requires its specific routing and forwarding. For the IP networks, policy based control functions to provide VPN configuration individually and dynamically are also required. VPN has multiple sub-VPNs for voice, on-demand streaming data, secure information, etc. The sub-VPNs can be interconnected through different Service Provider Networks according to the required QoS and service features.

In order to provide service dependent routing/forwarding features for VPNs, the IP network will provide virtual networking. For demanding QoS satisfactions of VPNs, the resource virtualization function is needed along with virtual networking functions to accommodate VPN service features efficiently.

To provide intelligent and dynamic configurations in VPNs, the following functions are needed in the IP network.

- For dynamic re-configuration on a VPN node, intelligent features will be necessary to select tunnel(s) for each end system that has to be connected to the VPN.
- The firewall policies can be chosen to ensure a high degree of security which controls incoming/outgoing unauthorized packets.
- For QoS-capable VPNs it is important to provide a tailored communications services that could be differentiated in terms of performance, monitoring, accounting, security and privacy. As an example, the ingress node in a IP network performs the aggregate flow scheduling based on multiple individual flows for VPN channels.
- Hierarchical mobility management (e.g., micro/macro mobility) could be necessary for provisioning mobility among VPN groups.
- The ingress nodes of a VPN provide dynamic configuration filtering rules with levels of granularity ranging from a single node to an entire VPN.

7.19 Billing and Charging Capability

If the IP network provides the relevant traffic control and management functions to some user services and applications, traffic monitoring functions to measure the effects of traffic control may be needed. In addition, the mechanism for charging of service rates may be needed for audio/video applications.

The billing and charging capabilities are based on collections of the charging parameters. The following charging parameters could be considered:

- Connection mode
- Connection establish and release time
- QoS class and priority
- Traffic parameters including constant bit rate (CBR) and variable bit rate (VBR)
- Connection detail records (CDR) including number of packets to be delivered, tagged and discarded

For end user manageability, some charging parameters could be selected during the SLA negotiation.

7.20 Client/Server Management and Agent Management Capability

The fast growth of network, service and content providers has led to a complex service delivery environment. Therefore, client/agent/server management are required to support scalable and efficient deployment of services. The following features could be supported in the IP network:

- A service portal as a broker for services is able to manage the complex service provider relationships.
- Separation of service control from service transport, allowing the control of multiple and heterogeneous networks using a common control plane and providing a path to simpler and cheaper network devices.
- Support of multiple network technologies is also achieved by abstracting the service QoS requirements from the underlying technology.
- A scalable and flexible architecture enables both service and network plug and play (i.e. dynamic registration of new service and network providers through agent collaboration).
- User mobility enhancement, i.e. users can access the system from multiple Customer Premises Equipments (CPEs) as the CPE agents collaborate with the service portal agent to provide location information of the user.
- Relatively simple distributed software entities (agents) are able to cooperate to implement the complex trading model of the service supply chain

The IP network allows end users to get client/agent/server management on demand of the end user. There are two kinds of end users: service providers and service clients. If the service provider wants agent management for clients, the network supports agents of the service provider for provisioning clients. These agents are located at the proper places all over the network and act like the service provider to clients. If the service client wants agent management, the network substitutes the client to perform tasks as an agent. This agent acts as a server of a service provider to a client of a service end user and vice versa simultaneously. Clients will release the agent resources of the network once their concerned tasks are executed.

8 Service Procedures and Applications Scenarios

In this section, the protocol procedures for customer manageable IP services and applications are described. The applicable scenarios of manageable IP service can be given as follows, but their lists are not exhausted.

- manageable naming and personal directory services
- manageable access control services
- manageable QoS services
- end user manageable location monitoring services manageable home networking services
- client networking Service with QoS and security

8.1 Manageable Personal Directory Services

Manageable personal directory service is a service intended to provide users with access to various personal directory-related information. Directory databases are repositories for information about network-based entities, such as applications, files, printers and people. In customer managed IP network environments, the user has his customized directory database in the network and can access the directory any time even if the user moves to a different location. The user can also get the information of other users such as the user's telephone number and location information using query procedures with directory service.

8.1.1. Objectives of Manageable Personal Directory Services

One of the main objectives for supporting personal directory service in IP networks is to have the customized personal directory for the management of user data. For each user a personal set of data has to be stored somewhere in the network and this user profile has to be accessible from every point in the network the user can move around. For supporting this objective, the user profile should be modifiable. Another objective is for the network operators to build specialized directory services into their applications.

8.1.2. Functional Model of Manageable Personal Directory Services

The basic functions to access and manage the directory service are described. Figure 3/TR-CMIP shows the functional model for the manageable personal directory service. This model includes agents, managers and database to support directory service in manageable IP networks as follows.

- Directory User Agent (DUA) and Directory Service Agent (DSA)

  The directory service is described as a highly distributed client server system. This may be characterized by a typically small number of hosts (servers, DSA) providing callable services to the other hosts (users, DUA).

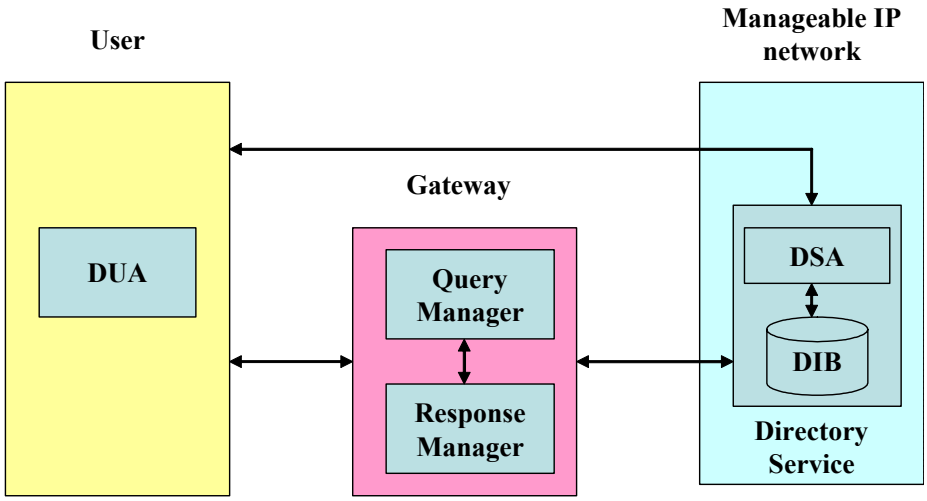
- Directory Information Base (DIB)

  The DIB is a single, logical, global directory database. The DIB stores information on directory objects such as user profile, and location data etc.

- Query Manager and Response Manager

Query Manager and Response Manager are responsible for processing the query and response message between DUA and DSA.

In this model, the user can directly access his own directory service to update and manage directory information for customized directory services.



Note) DUA: Directory User Agent, DSA: Directory System Agent
DIB: Directory Information Base - user profile, location data etc

Figure 3/TR-CMIP – Functional model for manageable personal directory services

The personal directory services offer the following functionalities.

- Creation and deletion of user information in a distributed database maintained in the IP networks
- Download and removal of information copies into network elements
- Modifications to information in user management database and network elements
- Retrieval of information contents from any network site
- Retrieval of object identifiers for users based on properties of their information
- Reconfiguration of information allocation when user changes his or her home site

8.1.3. Service Scenarios and Procedures of Manageable Personal Directory Services

In general, a directory service has to provide four types of services:

- Mapping name → information

  For example, an object's name may be mapped on its network address. Actually, this is exactly the service provided by a phone book or through telephone enquiries.
- Mapping information → set of names

  This service establishes a "Yellow pages" function.
- Mapping name → set of names

  A set of objects is identified by one single name.
- Secure communication

  Authentications as well as mechanisms for electronic signatures are provided.

In manageable personal directory services, the following scenarios are considered.

- Directly accessing user's own directory between DUA and DSA

- Retrieval of the directory service through gateway

First, the service procedures for accessing user's own directory are shown in Figure 4/TR-CMIP. The user directly communicates with his or her directory in IP networks. After the authentication procedure is completed, the user can always modify and get his or her user information in his or her directory. User's location information is updated in the directory in order to always find users in case that the user moves to another location.

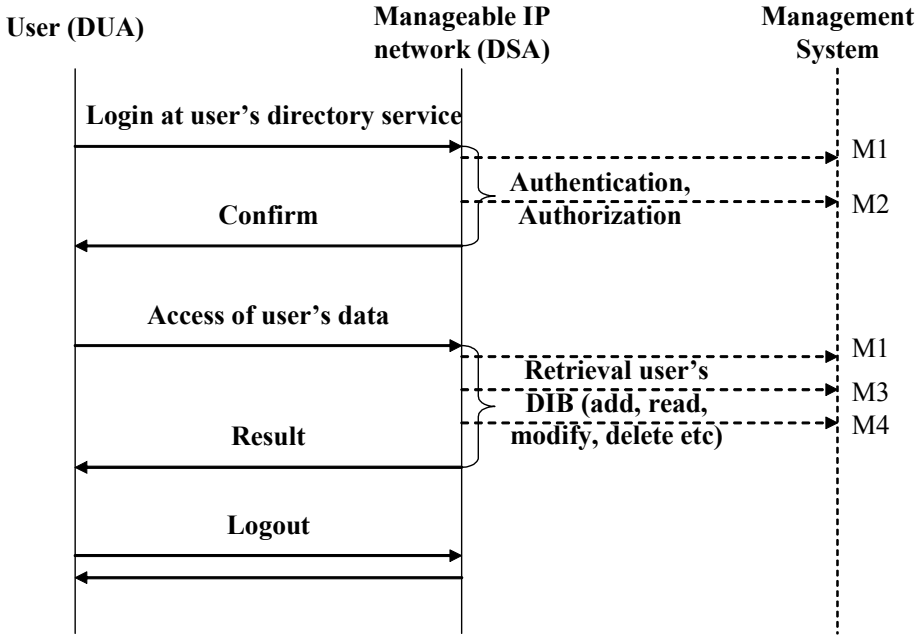


Figure 4/TR-CMIP – Message flow for accessing user own directory

For example, when accessing user own directory, sample fault management events that are sent to the management system for potential fault scenarios are considered as follows.

- M1) Directory service unavailable; this could be due to a communication or a database problem
- M2) Authentication failure; the event might be sent when fraud is suspected, for example, based on a repeated pattern of failed login attempts within a relatively short period of time
- M3) Unauthorized user; two common cases are as follows.
  - User information in the message does not match the user information for the existing authorization. This event is also important for fraud detection
  - The user does not have sufficient authority to retrieve, modify, or delete requested information
- M4) Unable to update the database in case of modify and delete operations.

Second, the service procedures for retrieval the directory service through gateway are shown in Figure 5/TR-CMIP. The user sends the query to gateway with the information (name, etc.) that he or she wants to find. The gateway searches the directory service system in the network by Query Manager and sends the information request to the designated directory service system. After retrieval of DIB of the directory service, the gateway is returned the corresponding information (address, number etc) and sends the response to the user through the Response Manager.

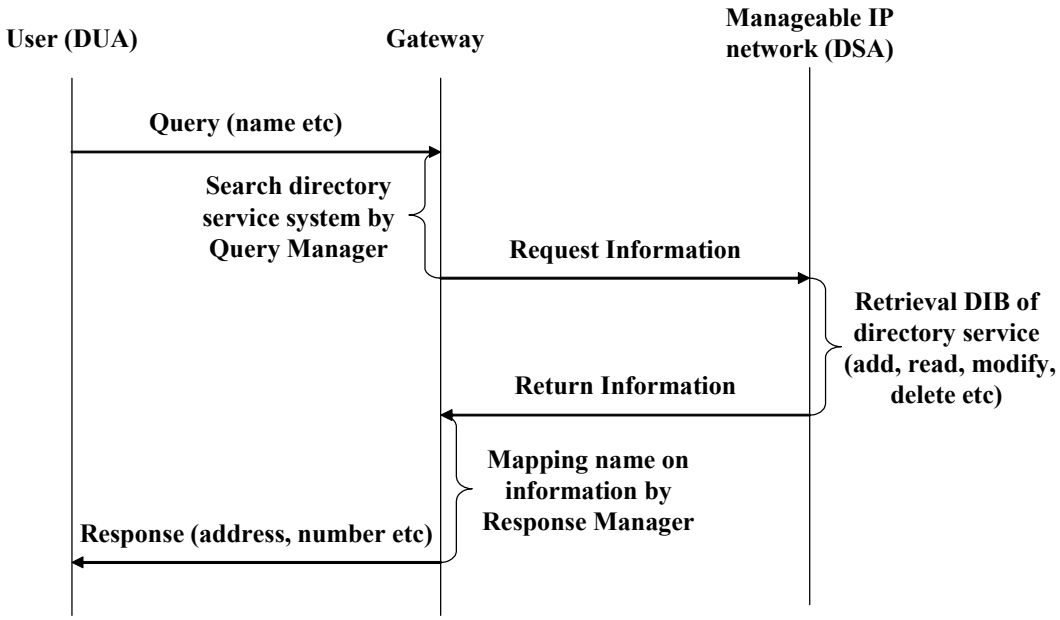


Figure 5/TR-CMIP – Message flow for retrieval the directory service

8.2 Manageable Access Control Services

Manageable access control is to provide that the end user has some controllability while accessing his own service profiles and the transport capabilities including VPN.

Manageable access control is developed with business model of service provisioning in mind. It gives an insight to provide the end user with superior content retrieval and access. An access gateway functional block supports the concept of service driven access control in IP networks. It shows how it can be used to describe procedures to maintain reliable and resilient service provisioning in the context of roaming, integration and internetworking of different domains.

8.2.1. Objectives of Manageable Access Control Services

Reserving a service profile driven access control mechanism for traffic aggregates is one of the key features for manageable IP networks. This is because the user requests may contain application data of different contents and bandwidth requirements. From the perspectives of commercial viability, the end user wants to pay for the networking services only if his or her desired level of content retrieval is satisfied. The existing access control mechanisms of the existing IP networks do not take into consideration the feature of dynamic service profile provisioning to accommodate multiple requests of an end user for multivariable content access. This is the key driving factor of a service profile driven mechanism for access control.

8.2.2. Functional Blocks of Manageable Access Control Services

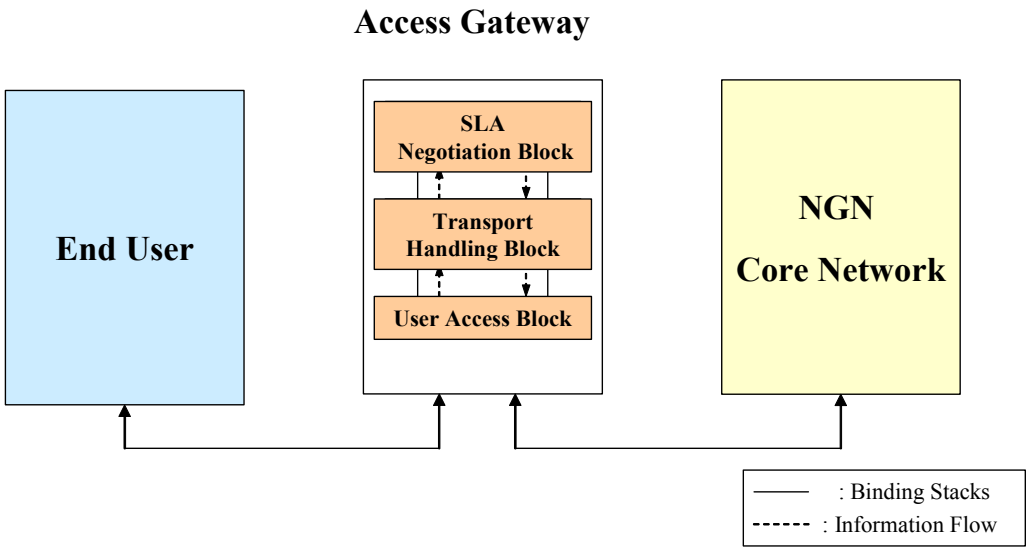


Figure 6/TR-CMIP – Functional block diagram of manageable access control services

Figure 6/TR-CMIP shows the functional blocks of an access gateway for a manageable IP network that enables service provisioned access control to users. There are three major aspects from the end user manageable access points of view, which are described as follows:

- User Access Block

  The User Access Block is where the primary data reduction functions reside and where the user's request information gets logged first. Information that is deemed critical to manage the network is translated into a standard object format and forwarded to the Transport Handling Block.

- Transport Handling Block

  The Transport Handling Block provides communications paths with relevant transport management between the User Access Block and the SLA Negotiation Block. All information forwarded from the User Access Block is utilized by the Transport Handling Block to provide information to network operators. The Transport Handling Block adheres to open standards to provide ubiquitous information access. This allows the Transport Handling Block to share management information stored in distributed database. These databases provide common data storage so that new information contents can be easily inserted into the access handling environment. This is one of the key concepts in manageable access from the end users' point of view where enforcement of service level agreements must be robust and reliable.

- SLA Negotiation Block

  The SLA Negotiation Block performs the function of presenting the user's information to the network provider. It has the functionalities for requested SLA negotiation with the network operator based on the user's profile for access control in IP networks. Charging and billing procedures also form an important part of the functionality of the SLA Negotiation Block. It acts as the 'front-end' interface for user-network communications and completes the binding for direct communication with the user once the requested service negotiation and authentication with the network provider is complete. Once this is done, it updates its' reference database about the established session and keeps a tag for billing and accounting processes.

This architecture has two important benefits:

1. It is easy to design and independence of data flow and control information maintenance can be ensured to a very high degree.

2. It involves minimum overhead in communications and is secure in terms of established sessions.

An important feature of the SLA Negotiation Block in manageable access control is the ability to update easily if the end user's service requests change during an ongoing established session. The SLA Negotiation Block needs only to update its' internal records and communicate the change to the network provider about the change in request. An entirely new session establishment is not necessary. Billing information is passed onto the user once its' session is completed.

8.2.3 Service Procedures for Manageable Access Control Services

- Dynamic negotiation of service profile information:

  Dynamic negotiation of service profile information takes place in the SLA Negotiation Block of the access gateway to which the end users are linked with. Network access can thus be partitioned dynamically using the functional blocks of the access gateway for manageable access control.

- Service procedures for manageable access by the user:

  Figure 7/TR-CMIP shows an example of protocol flow diagram for end user driven access control in IP networks. The user sends in a request to the access gateway with service provisioning requests, whereby the User Access Block looks up the network conditioning database and passes the request on to the Transport Handling Block and thence to the SLA Negotiation Block. The SLA Negotiation Block must provide application multiplexing. There should be a provision to accommodate changes in end users' service level agreements dynamically in an ongoing established session, and to admit the user profile while roaming. It negotiates the session requirements with the network provider while maintaining a set of default requested objects in its internal database. This is another key feature which enables service provisioning negotiation for manageable access control. Based on the user's requests, the presentation manager opens a session control session with the network provider and informs the request of services, negotiates about the policy management with the network provider about directory, access control and security issues based on the default stored values and opens the sessions pertaining to bandwidth management and transport.

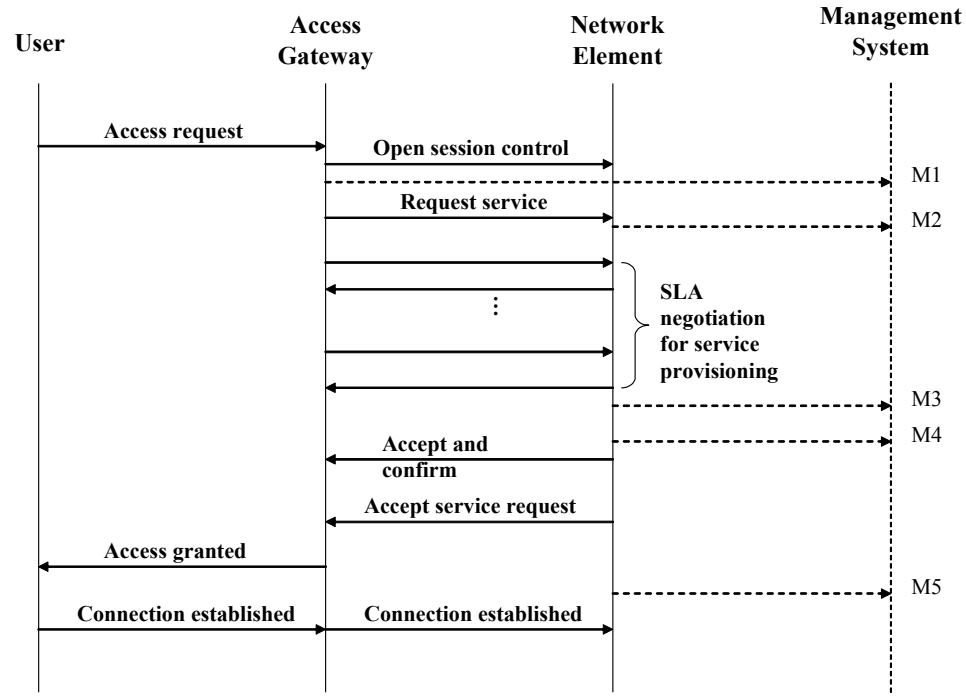


Figure 7/TR-CMIP – Example of flow diagram for manageable access control services

For example, during session initiation, SLA negotiation, and connection establishment, sample fault management events that are sent to the management system. The potential fault scenarios are considered as follows.

M1) Session initiation failure

M2) Service request processing failure

M3) SLA negotiation failure; SLA negotiation failure could occur as a result of fault in the service layer or the transport layer in a rather complex message flow between a number of network elements such as access gateway, bandwidth managers and policy managers. Therefore further investigation is required to breakdown of this event.

M4) SLA provisioning failure on the access gateway

M5) Connection establishment failures; the significant of this event is on determining management requirement for the connection (or connections) associated with a session.

- Billing and accounting procedures:

  The SLA Negotiation Block updates its reference database after the session is initiated and starts the system log module once the session is initiated. This is needed for billing and accounting purposes. The logs are important for collection and distribution of the user's preferences, application requirements, network device capabilities on network operator side and availing the accounting policy information from network operator. Once a successful connection with network provider is done upon authentication and verification of the user profile, it informs the User Access Block and the user starts receiving his service requests.

- Support of mobility and seamless connectivity based on manageable access control:

  Since the manageable access control scheme provides gateway access using IP address awareness, it is also important to support cross network policy management for mobile users during roaming. This functional component provides the required policies governing users who access third party networks and cross geographical boundaries. It keeps in constant contact with other cross network location registers of the geographically dispersed but inter-connected networks, exchanging accounting, service feature profile and control data for local and roaming subscribers. If within an established session, there is a change in the user’s service requests, or profile, the SLA Negotiation Block updates its internal database and starts negotiating with the network operator without creating a new session or disrupting the flow in the established one. If the network operator does not entertain this new request, the SLA Negotiation Block informs the user about the unavailability of resources while continuing to service the earlier request. The user has the choice to either go along with or terminate the ongoing session. After the user has terminated the session, the SLA Negotiation Block makes a final write to its internal database about the session statistics and makes a note of the accounting tag. It releases the session and passes on the information to the User Access Block and thence to the user.

8.3 Manageable end-to-end QoS Services

Manageable QoS service is a concept designed to keep in mind the versatility of customer manageable IP networks. A key feature of manageable IP networks is providing the end user with greater flexibility of managing their QoS access requests with minimal changes in conditioning. It provides the end user with superior QoS management and service guarantee while maintaining the economies of scale for the network provider and the end user alike. It supports the service driven end-to-end QoS provisioning and how it can describe procedures to maintain reliable and resilient service provisioning in the application service scenarios thereof.

8.3.1 Objectives of manageable end-to-end QoS service

Manageable end-to-end QoS service intends to provide users with access and control to satisfy their multiple type service requests in IP networks. The end user negotiates with network how to get network resource for end-to-end QoS, handle faults and bottlenecks which may hinder end-to-end QoS. The end user is able to negotiate with the network operator dynamically on the service level provisioning. The network provider may consider that one specific QoS mechanism is not enough to satisfy end-to-end QoS and many different QoS mechanisms may be needed to support end-to-end QoS.

Target objectives of manageable end-to-end QoS service are to

- provide user the control of QoS parameters to setup end-to-end connection,
- provide user the status of end-to-end QoS,
- provide network provider to support various end-to-end QoS request,
- provide network provider to manage QoS in non-homogeneous QoS network.

Manageable end-to-end QoS services offer the following requirements:

- Creation, modification and removal of manageable end-to-end QoS service profiles
- Notifying the end user about negotiation of manageable end-to-end QoS services dynamically.
- Monitoring the network and ascertaining whether end-to-end QoS can be satisfied
- Provision of network to satisfy end-to-end QoS based on service profile.

8.3.2 Functional model and procedure for manageable end-to-end QoS service

User regards manageable end-to-end QoS service as an agent like private network operator. Network considers manageable end-to-end QoS service as manager like provisioning and managing network operator.

The basic functional blocks to access and manage end-to-end QoS service are described in this section. Figure 8/TR-CMIP shows the functional model for manageable end-to-end QoS service. This model includes a service managing block which is responsible for handling user requests and data and an agent which negotiates on the provisioning with the network operator to satisfy end-to-end QoS.

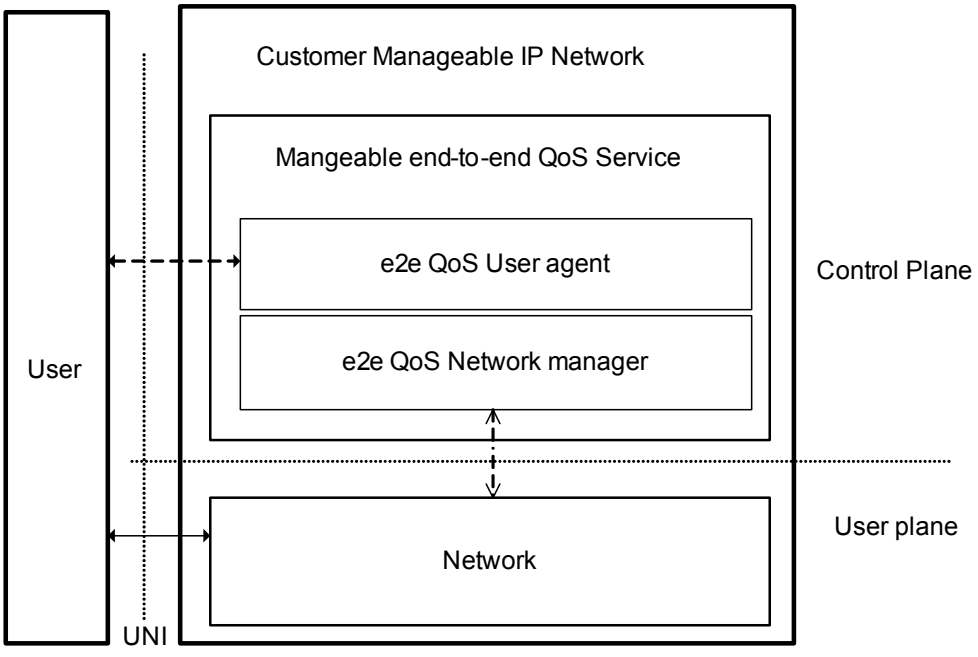


Figure 8/TR-CMIP – The functional model for manageable end-to-end QoS service

- Manageable end-to-end QoS User Agent (QUA)

  The QUA consists of the request function block and the negotiation function block. The request manager receives the user's request, verifies if the request is valid within network resources across the network. The negotiation manager receives notifications from the manageable end-to-end QoS network manager(QNM), determines if the user's end-to-end QoS request is guaranteed and renegotiates with the user about handling end-to-end QoS exceptions, if any.

- Manageable end-to-end QoS Network Manager (QNM)

  The QNM receives instructions from the QUA. It is notified about bandwidth, delay, jitter, packet loss and other QoS guarantee mechanisms. It resolves QoS request mismatches while negotiating with the network according to the nominal values of user requests pertaining to allocation and increment of bandwidth, change of QoS mechanisms, tuning QoS parameters to network supported provisioning, rerouting and protection, etc.

In procedures of manageable end-to-end QoS service, user creates and registers manageable end-to-end QoS service with his initial requirements for end-to-end QoS. The QUA can poll or obtain a notification about QoS performance from an access node and edge router of a network. Bandwidth, delay, jitter and packet loss are the basic parameters for manageable QoS performance. When the end-to-end QoS performance falls below the threshold level requested by the user, the QUA takes appropriate actions based on its stored default values to recover from the service level degradation. If the QUA is unable to negotiate with network operator, the end user can negotiate again and ensure the guarantee of different QoS levels.

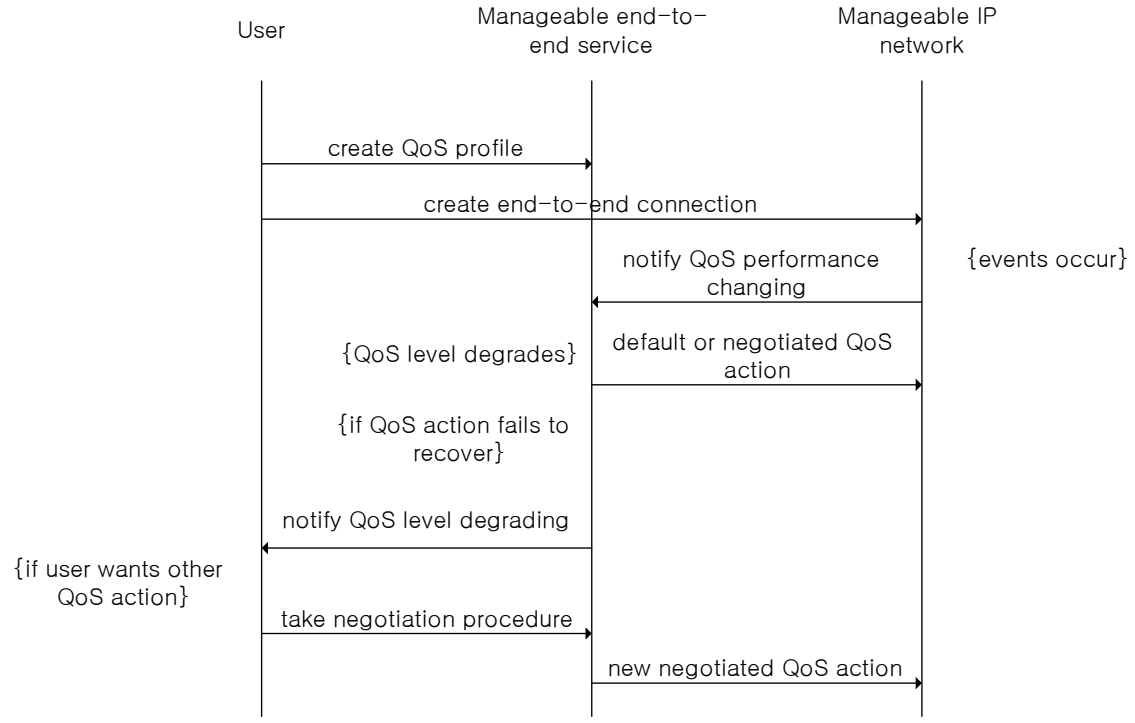


Figure 9/TR-CMIP – Message flow for manageable end-to-end QoS service scenario

The interface between user and manageable end-to-end QoS function provides messages to:

- create and delete QoS profile in manageable end-to-end QoS function
- notify QoS level degrading to user
- make compromise between user and QF when user's requests can not be satisfied

The interface between manageable end-to-end QoS function and IP network provides messages to:

- notify QoS performance changing to manageable end-to-end QoS function

- take QoS action on the network

8.3.3 Service scenario of manageable end-to-end QoS service

In the IP network, a user requests the network an end-to-end connection with his/her QoS requirements. The manageable end-to-end QoS service will take place of the user to get end-to-end QoS connection. It examines the path of end-to-end connection and makes end-to-end connection. If there is QoS degrading, the manageable end-to-end QoS service will consider the following actions;

- provide more network resources or reroute for end-to-end connection
- renegotiate QoS parameters for end-to-end connection with user

When network does not consist of homogeneous equipments to satisfy same QoS level, the manageable end-to-end QoS service should know the different capabilities and select proper QoS mechanism.

The following three scenarios are considered;

- Scenario 1 (Selection of TE Capability)

  Let's assume a user want guaranteed a specific bandwidth for peer-to-peer connection like VoIP network. First, the user sends his connection request to the network. The network receives this request and checks the status of available resources. Then the network responses the user with two options; best-effort delivery with admission control and TE available end-to-end communication path.

- Scenario 2 (Priority Assignment with Cost Option)

  In this scenario, the end-to-end QoS service offers priority scheduling. When there is congestion on end-to-end path, it can take higher priority. When the status of path becomes normal, the priority provisioning returns the normal condition to save cost.

- Scenario 3 (Re-Negotiation of TE Capability)

  When QoS is degraded and all options are not applicable, it notifies the users and renegotiates with the user how to satisfy end-to-end QoS.

8.4 End User Manageable Location Monitoring Services

End user manageable location monitoring service is a service to manage other end users' location information wherever they are at any time. In IP networks, the end user's location information is originally managed by the network provider or service provider. Then, an end user requests other end users' location information to the network and monitors their location information after retrieving their location information. In this mode of service, an end user could be located at the fixed or wireless/mobile network.

8.4.1 Objectives of End User Manageable Location Monitoring Service

The main objective feature of end user manageable location monitoring service is that an end user retrieves other end users' location information from the location information database of IP networks and maintains and manages other end user's location information to monitor other end users' location. In many cases, users are interested to communicate with a certain set of their interested peers. Another objective is to provide basic information support to other services such as emergency services and connectivity services.

8.4.2 Functional Model for End User Manageable Location Monitoring Services

The following functions are required to support end user manageable location monitoring service.

- Functions required on the end user side
  - requests about other end users' locations to the IP network
  - managing monitored end users' location information

- Functions required on the IP network side
  - managing their respective end users' location information
  - responding to end user location requests

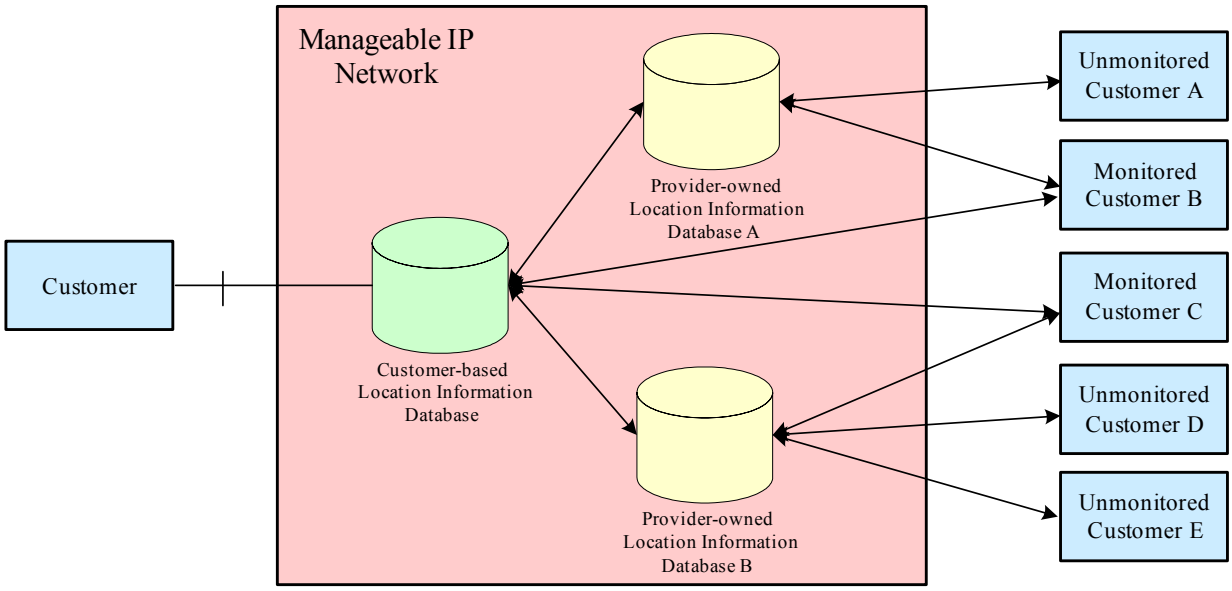


Figure 10/TR-CMIP – Functional model for end user manageable location monitoring service

Manageable IP networks have two types of databases to support end user manageable location monitoring service. One is provider-owned location information database that has raw location information of network end users. This database is an original network location information database such as Home Location Register/Visitor Location Register, Domain Name System, and Home Agent/Foreign Agent binding cache. Another is end user-based location information database that contains processed location information of network end users. This database is service dependent location information database, such as GPS location information and location information combined with other end user information such as availability and connectivity.

- Provider-owned Location Information Database

  This functional block is to maintain and manage location information of all its' respective network end users.

- End user-based Location Information Database

  This functional block is to request, update, add, delete other end user location information to Provider-owned Location Information database of other end user and respond to the requested location information.

8.4.3 Service Scenarios and Procedures of End User Manageable Location Monitoring Services

An end user is interested to know the location information of its peers. The IP network maintains their location information at all places and times. An end user requests their location information to the IP network in the general case. In this scenario, security issues such as authentication and authorization and accounting issues are out of the scope.

There are two scenarios in this case:

- End user to End user-based Location Information Database to Provider-owned Location Information Database

This scenario is a single-mode operation. An end user requests for the other user's location information once. If the end user based location information database does not have the other location information, it sends a request to the provider-owned location information database.

- End user to End user-based Location Information DB to Monitored End user

  This scenario is a continuous-mode operation. An end user requests for the other user's location information continuously. After the single-mode operation, the end user-based location information database contains the monitored end user's location information. Therefore, end user-based location information database issues a request to the monitored end user directly.

In these two scenarios, the end user-based location information database may not need to share its network resources directly with an end user since the provider-owned location information may be proprietary to the network provider. The provider-owned location information database should manage all their respective end users' location information.

The first scenario is single-mode operation scenario whose service procedure is shown in Figure 11/TR-CMIP. In this scenario, an end user requests other end user's location information to the end user-based location information database with a single-mode start message. In the case the end user-based location information database does not have the corresponding requested end user's information, it issues a request to the provider-owned location information database to this effect. After receiving the request message, the provider-owned location information database responds with its proprietary location information to the end user-based location information database. This information is processed by the end user-based location information database and it provides this processed information to the end user who requested it.

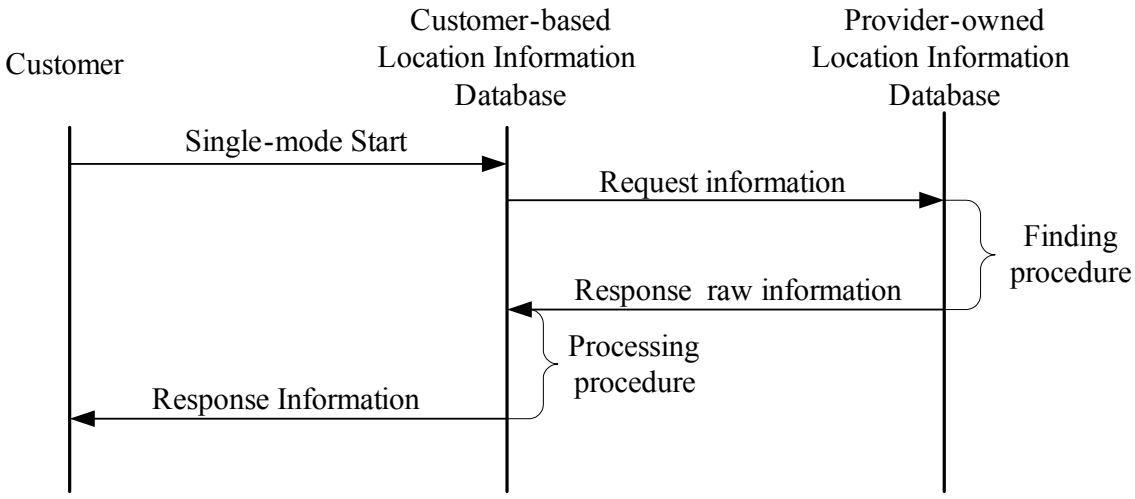


Figure 11/TR-CMIP – Service Procedure of single-mode operation service scenario

The second scenario is the continuous-mode operation scenario whose service procedure is shown in Figure 12/TR-CMIP. In this scenario, an end user requests a monitored end user's location information from its information database with a continuous-mode start message. The first operation is almost the same as the single-mode operation service scenario. However, the end user-based location information database continuously adds other monitored end users to the user list. The end user-based location information database periodically provides the processed information to the end user. If the end user-based location information database receives a stop message, this process stops and the end user-based location database deletes the monitored end user's information from its list.

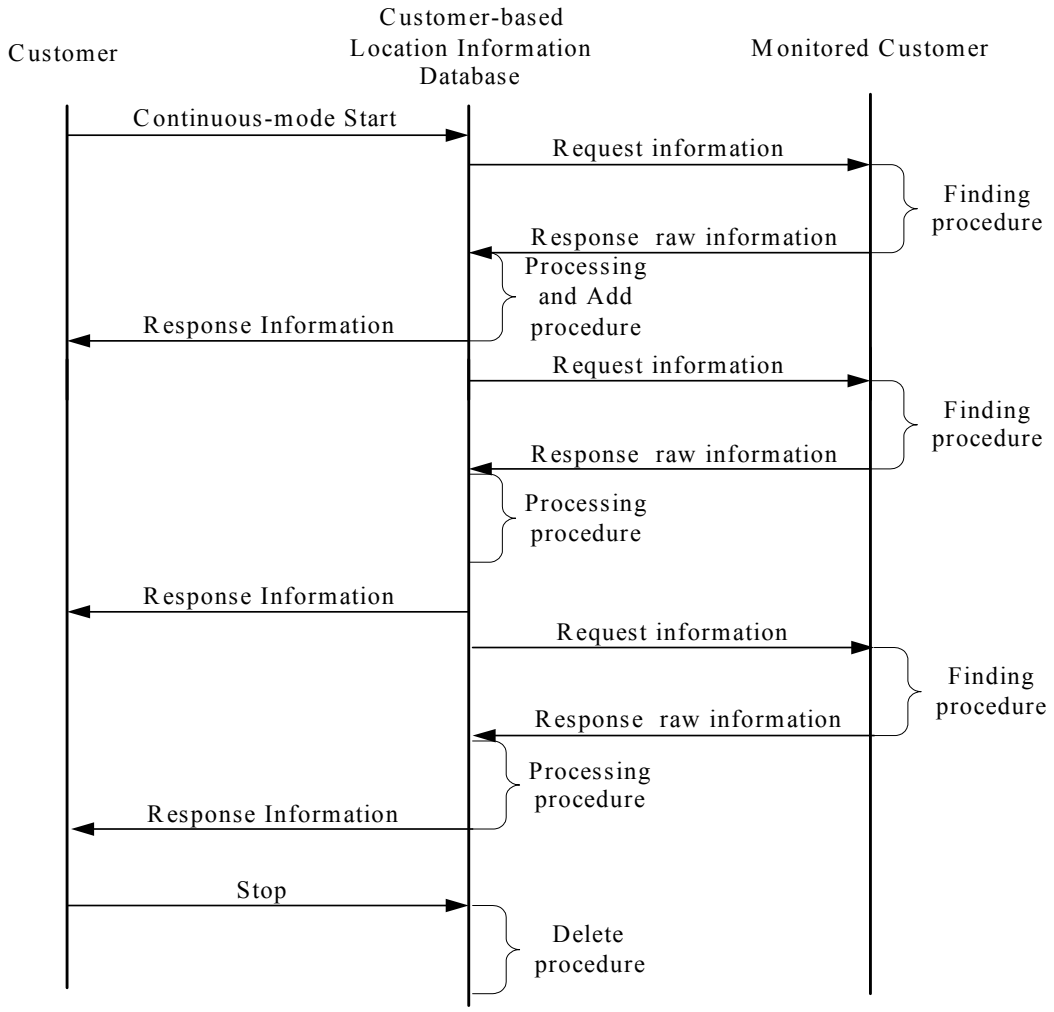


Figure 12/TR-CMIP – Service Procedure of continuous-mode operation service scenario

8.5 Manageable Home Networking Services

8.5.1 Objectives of the Manageable Home Networking Services

Home networking services can be defined as providing home automation services, home entertainment services, security services, and internet service to the home. Home automation services are to control lighting, appliances, and climate control in home. Home entertainment services allow user to access audio, video, and theater services in home. In addition, ubiquitous services will be extended to support the interconnection among various devices with radio frequency identifier (RFID) tags and increase the scale of network connections in comparison with home networking services.

8.5.2 Functional Model of Manageable Home Networking Services

There are two modes of operations for home networking services. One is the local service access inside the home or within home area network, which is starting service invocation from inside the home. The other is the remote service access from external networks.

In Figure 13/TR-CMIP, it can be seen that the Service Gateway within the manageable IP network acts as the portal to allow remote access and control from external network to home network. Service Gateway enables the remote end user to manage home networking services and devices via the Residential Gateway. The following functions and capabilities are provided by Service Gateway to support home networking services in the IP network;

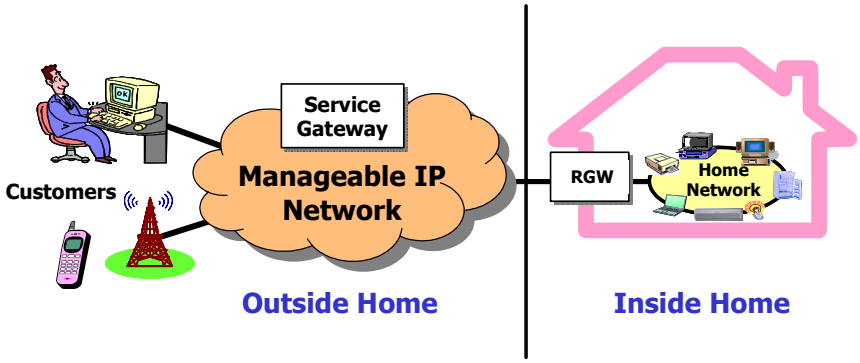


Figure 13/TR-CMIP – Architecture for home networking service in manageable IP network

– User authentication and authorization
– Service management
– Service usage measurement
– Secure connection/session establishment
– Firewall function to protect against the possible threats
– Home directory service function that collects and presents the instances of home equipment, equipment services, and contents, to the user
– Remote control function
– Remote configuration, management function
– Web service-based interface to have access and control
– Policy decision function to manage QoS

A Residential Gateway is a device that interconnects various home networking devices and acts as a mediator between the end user of the devices and the Service Gateway. The Residential Gateway allows intelligent end-user services, not just simple network connections, to be created and managed within the home network as well. The details of the Residential Gateway are not addressed here.

8.5.3 Service Scenario and Procedures related to Manageable Home Networking Services

Figure 14/TR-CMIP shows an example of information flows of home networking service to enable an end user to "turn on the lights" at remote site. It is assumed that SIP, HTTP, and SOAP can be used for delivering control messages to communicate between Gateways and home devices. The following procedures show the information flows required for a "turn on the lights" home networking service.

1. A remote end user is trying to login Service Gateway to have access and control to home networking services
2. If an end user is successfully authenticated and authorized, then Service Gateway returns an OK message to the end user
3. End user sends a control message, say, "turn on the light in living room" to a device via Service Gateway
4. The Service Gateway then requests the session establishment between Service Gateway and Residential Gateway, and a home device to send a control message
5. If a session is successfully established, the Service Gateway sends "turn on the light in living room" control message to a home device via the Residential Gateway
6. The response from a home device is acknowledged
7. The OK control message is delivered to end user

8. The end user logs off to quit the home networking service
9. The session is terminated between Service Gateway and Residential Gateway, and a home device
10. The session is ended between end user and Service Gateway

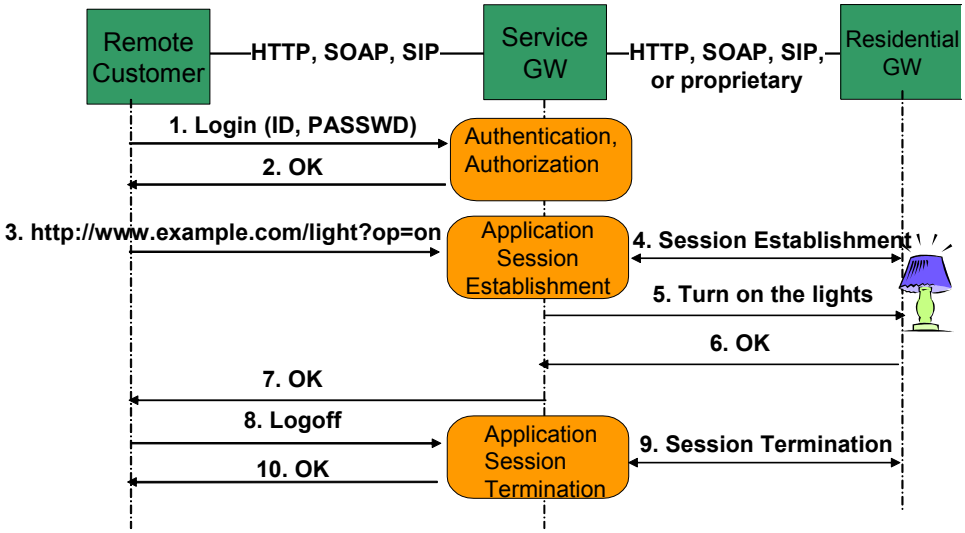


Figure 14/TR-CMIP – Example of information flows of home networking service to "turn on the light"

8.6 Client Networking Services with QoS and Security

8.6.1 Objectives of Client Networking Service with QoS and Security

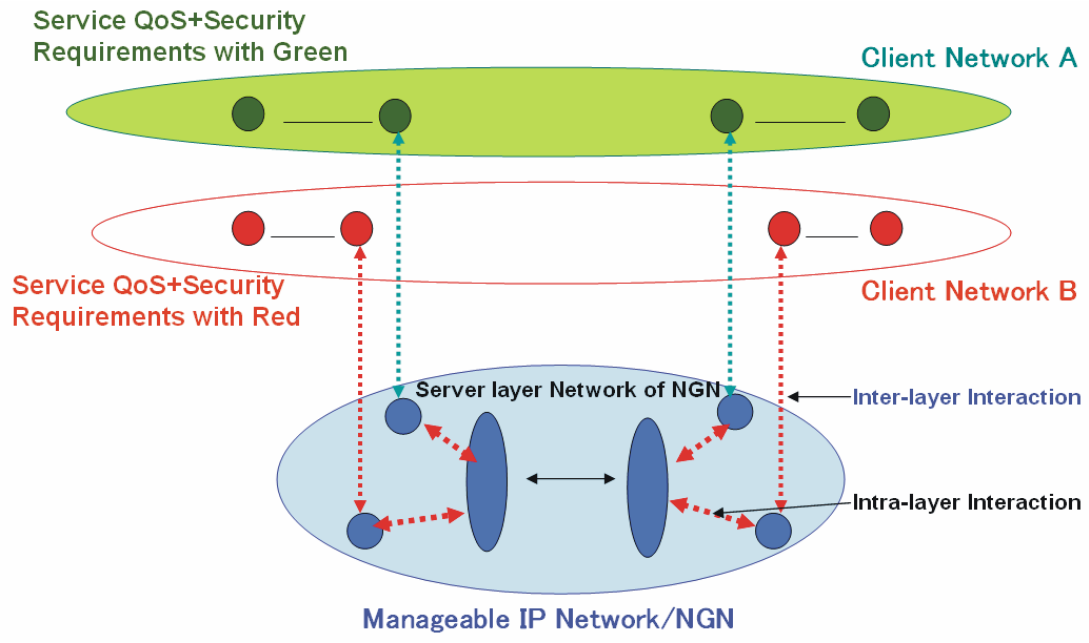


Figure 15/TR-CMIP – Example architecture for client networking service with QoS and security

The IP network provides such functions to control QoS and security capabilities simultaneously or partly as end users request. The network expects that in many types of services a secured path is tightly associated

with QoS provisioning. Therefore, it will be necessary to classify networking service features in QoS and security with on-line as well as off-line procedures.

The objective of client networking service with QoS and security is to protect two types of threat. An example is to provide authentication mechanisms at the level of aggregates of packets such as channels or flows so that these checks need not be done on individual packets. This suggests that an architecture where authentication and other resource management decisions are initially processed to reduce the cost of subsequent decisions. Consequently, a multilayered architecture to provide QoS and security procedures may be needed, as shown in Figure 15/TR-CMIP.

8.5.2 Overlay Model of Client Networking Services with QoS and Security

Figure 16/TR-CMIP shows the overlay model of client networking services with QoS and security. It shows an example of overlayed virtual networking. The virtual networking is applied to the model based on independently multilayered architecture, in which incoming packets are classified at edge level and the packets for secured QoS service are forwarded to policy based overlay networks. Thus, it provides secured networking and QoS managed functions through admission control and other control mechanisms. Based on functional architecture, a networking feature is necessary to adopt QoS and security features efficiently.

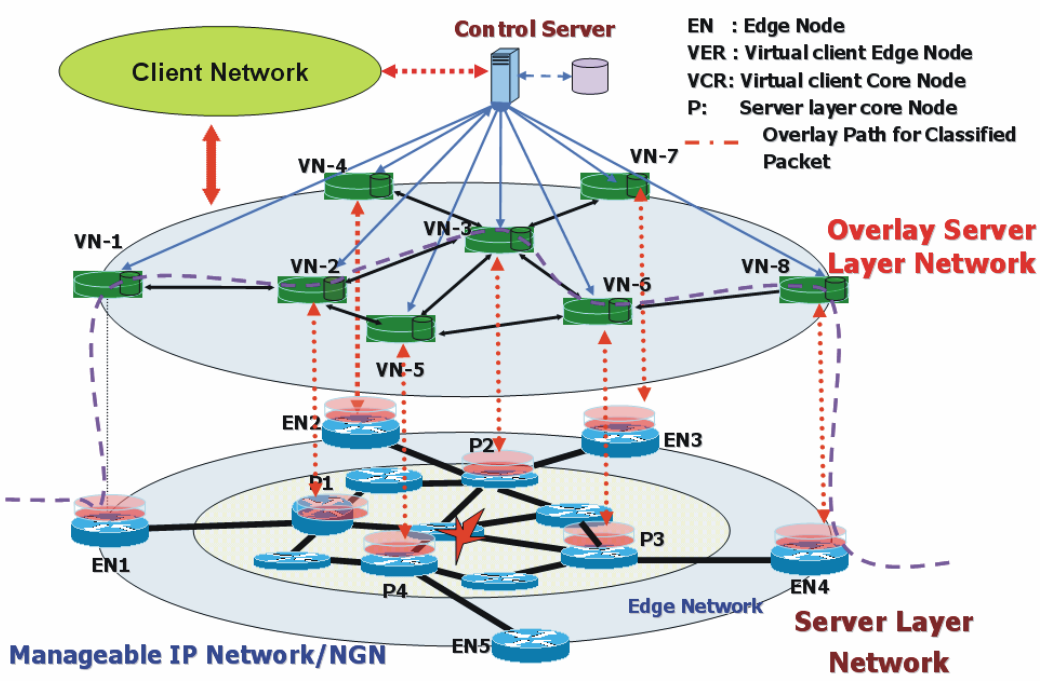


Figure 16/TR-CMIP – Overlay model of client networking services with QoS and security

An example of routing management algorithms of the overlay model is shown in Figure 17/TR-CMIP. This figure shows the procedure for VNF (Virtual Networking Function) table construction. The control information is classified according to the incoming end user information, and the control server will make its own networking table in procedures (c), (d), and (e). The multiple virtual networking tables constructed according to security level and required QoS level is applied to perform the routing functions over the overlay network. The primary goal of VNF provisioning on overlay network is to provide multiple secured QoS paths at each level. The VNF routing function is performed independently of other VNF domain in the network.

In order to make a forwarding information base from information of routing and policies, advanced control mechanisms are needed to supply multilayered virtual client networking associated with end user manageable networking features.

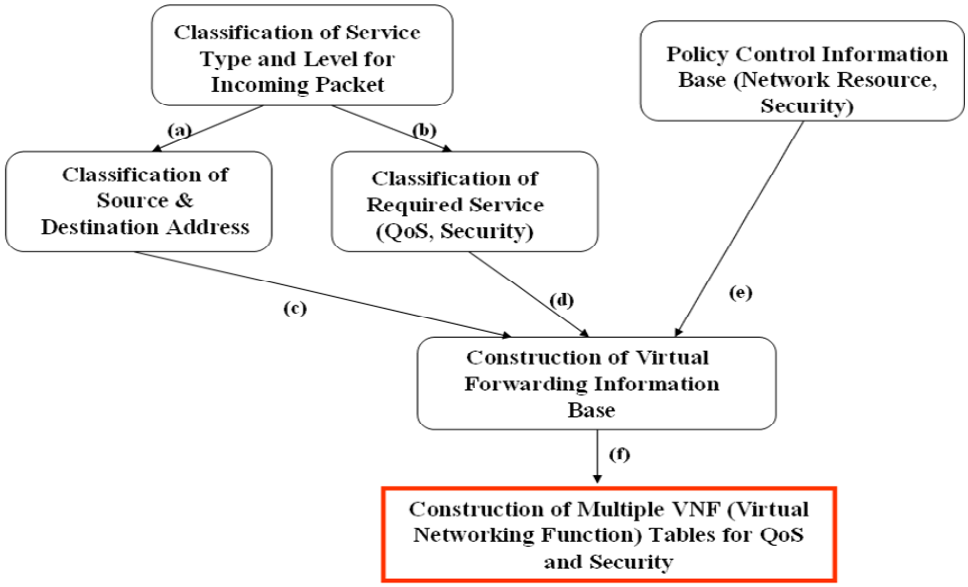


Figure 17/TR-CMIP – Examples of table construction of virtual networking function in overlay model

9 Security Considerations

It has become evident that security is a major element that should be considered for most applications. The Internet is becoming more and more popular in using many applications, such as business transactions, banking, government departments, and so on. The proliferation of such applications has raised the need for more security. This capability is needed in the IP network. For the secure use of IP network, the following items need to be considered.

- Authentication: This is required to verify claimed identity.
- Authorization: enables certain action s after authentication. This ensures that only authorized person or device can be allowed to access to network elements, services and applications.
- Confidentiality: Data should not be handled by unauthorized entities.
- Integrity: Ensures the data is not modified in transition.
- Non-repudiation: Ensures that the origin of the received data should not be denied by the sender.
- Communication security: This function ensures that information flows only between the authorized end points.
- Availability: This function ensures that there is no denial of authorized access to network elements, services, applications, and so on.
- Privacy security: This function provides data protection from disclosure to an authorized entity.

For the case of mobility, there are inherent security risks. To be able to use the customer manageable IP concept avoiding some or all of the security risks associated with mobility, the specific threats need to be identified. The following lists are some weak points and potential solutions, related to mobility.

- Using binding updates: The binding update in IPv6 protocol may be used to redirect route from source to destination. If it is not used carefully, some detrimental results can be caused in the case of mobile communications.
  - Stealing data: If a rogue user knows a mobile node's permanent address, he can send a binding update to a correspondent node or a database maintaining the binding update to change the route for the original mobile node's data into his.

  - Reflection and flooding attacks: When a sender and a destination are communicating, it is perfectly acceptable that the sender sends a packet to the destination, which results the destination replying back to the sender. However, if the sender sends a packet to the destination that causes the destination to reply to any other person, it is called a reflection attack. In this case, the attacker can flood the another person's link by using the reflection attack.
  - Man-in-the-middle attacks on the binding update: This attack can be used on the communication path between two nodes by an attacker. The obvious method is to change the contents of a packet to cause some results that were not intended by the original sender of the packet. When the attacker is located on the path between a mobile and a correspondent node, he can modify the content of the binding update, possibly bringing a refection attack or hijacking of ongoing connection between the mobile and correspondent nodes.
- Attacks using packet header information: The packet includes destination information. Therefore, if an attacker is communicating with a mobile node, he may put another address in the header information field, causing the mobile node to forward his packets to another node, which can cause reflection or flooding attack.

There can be many requirements on security. Among them, we first consider some points as mentioned above and introduce some points to enhance security as follows.

- Securing communication between mobile node and correspondent node: Messages between a mobile node and a correspondent node are needed for binding cache and binding update list management especially in the mobility management. The binding update is acting as a redirection request. Therefore, it is important that a correspondent node trusts the mobile node to be able to accept this request.
  - Message integrity: It is needed that an attacker can not modify the contents of the binding update message as well as the binding acknowledgment message.
  - Avoiding denial of service attack: In order to avoid this attack, correspondent nodes must ensure that they do not maintain state per mobile node until the binding update is accepted.
- Securing messages in the database for the binding update: the same attacks on the binding update to correspondent nodes are relevant when a mobile node is communicating with its binding update database. The database impersonation could be detrimental to the mobile and correspondent nodes. So, it is important that mobile node's communication is secured using authentication.

Appendix I

An example of functional architecture and service creation scenario for end user manageable VPN services

The VPN will be one of the most promising services in NGN according to rapid increase of VPN service demands. The framework for dynamic creation of VPN service based on intelligent/active networking will promote a variety of VPN application services. In network based on service negotiation, a node with intelligent/active features is able to represent a solution in order to manage the whole amount of different requests coming from consumers.

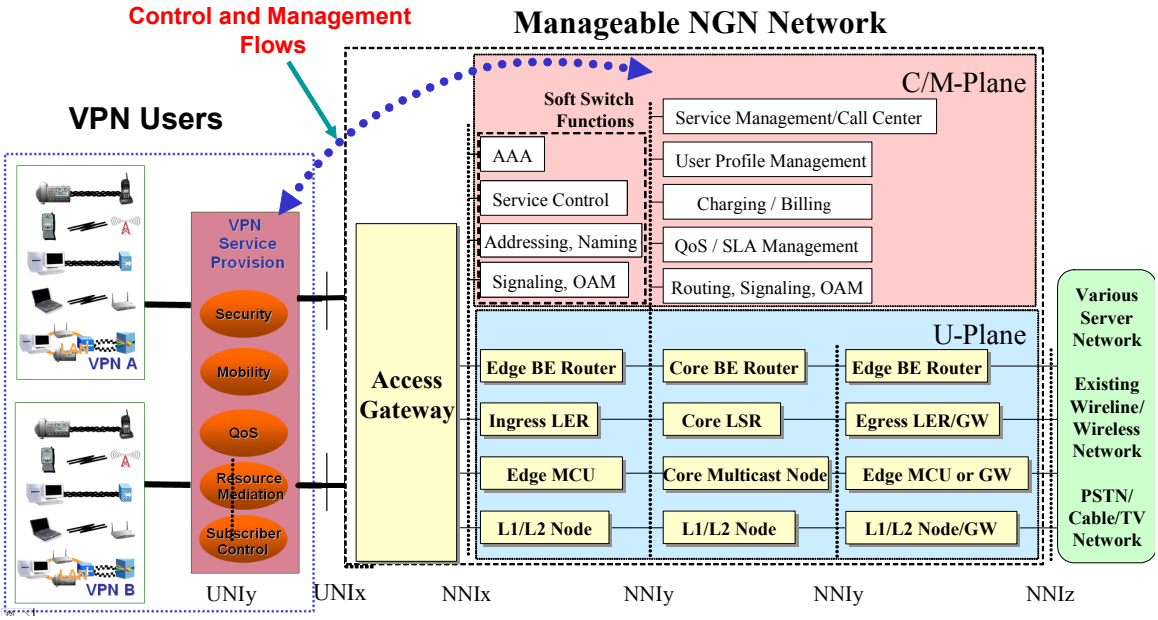


Figure I-1/TR-CMIP – An example of functional architecture for end user manageable VPN services

The security is definitely one of the key issues in VPN scenario. An intelligent and active feature in VPN networking will take an important role to provide flexible means to customize services appropriately. The intelligent/active features for security in VPNs are exploited for adaptive secure routing and service capability. The security capability of VPN is negotiated with C/M-Plane of IP network, and its service level will be assigned to VPN users.

As shown in Figure I-1/TR-CMIP, control and management functions of customer manageable IP network, a control flow between a service provision module of VPNs and C/M-Plane Module of customer manageable IP network is established to deliver networking service capabilities from/to VPNs. The C/M-plane of IP network will have to be characterized to provide the above networking capabilities to VPNs.

In addition to the above features, the following capabilities are characterized to provide intelligent/active VPN services in IP network.

- Mobility
- Static/Dynamic QoS provisioning

- Resource Mediation for VPN services
- Subscriber Control on VPNs service capabilities
- Security negotiation/provisioning

From a functional standpoint in intelligent VPN of IP network, the VPN is as an active flow that is activated by appropriately customizing additional intelligent/active features of VPN access node. This is achieved via one underlying program and their injected programs, each associated to one of the intelligent/active VPN functions. The activation process is appropriately invoked with respect to the external topology, an internal topology and its routing table of VPNs (with multiple virtual routing tables). By applying these parameters a number of different VPNs are characterized by their own topology and management strategy.

Figure I-2/TR-CMIP indicates an example of functional architecture to implement manageable VPN. If we consider VPNs are interconnected at different operators or ISPs in the IP network, implementation architecture for manageable VPN may be shown in this figure. For example, the manageable VPN service needs the following threes functions of Service Mediator, SLA mediator, and Access Mediator.

- Service Mediator Function
  - AAA
  - Presentation
  - Subscription
- SLA Mediator Function
  - Dynamic negotiation and re-negotiation of the SLA
  - Synchronization with other SLA Mediator
  - Communication with resource manager in customer manageable IP network
- Access Mediator Function
  - AAA
  - Directory transactions
  - Preference lists handling
  - Service menu
  - User profile Processing
  - Terminal types and mapping

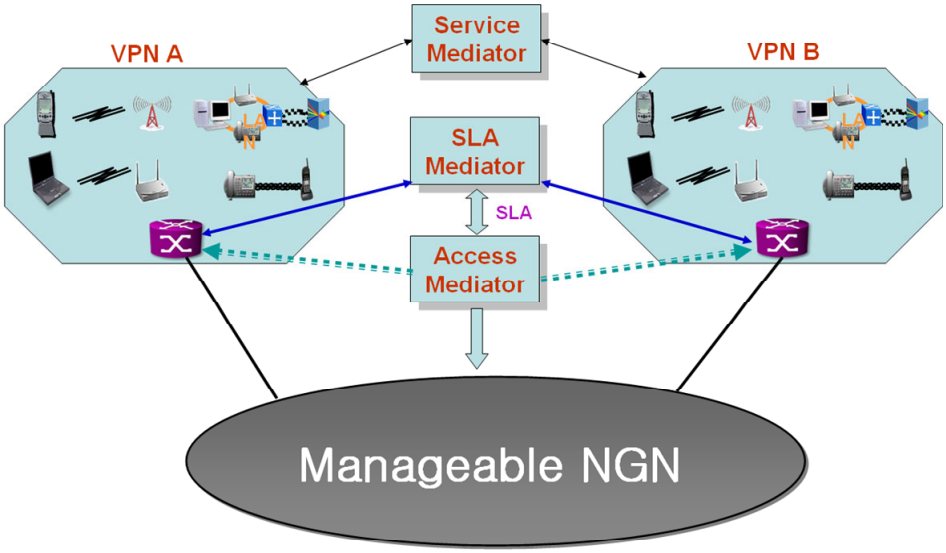


Figure I-2/TR-CMIP – An example of implementation scenario for end user manageable VPN

1.2 – Terms, definitions and high-level terminological framework for Next Generation Networks*

Abstract

This draft has been produced to capture the set of terms which frame the key NGN concepts and to show the relationships among them.

For the most part, this document uses terms and definitions that have already been defined elsewhere and which are considered particularly suitable, applicable or adaptable to NGNs.

The current contents are intended to provide a starting point for further development, and an on-going basis for development.

Temporary Note:

This document has been based on material from many sources. In particular, the following materials have been examined in the course of its production so far:

a) The ITU-T SANCHO database

b) Recommendations from various study groups (e.g. SG11, SG13, SG15, etc)

c) ETSI TISPAN (ETSI TR 00004 V0.0.6 (2005-07)).

e) Existing FG NGN Documents

The intent is to facilitate consistent use of terms within the FG and coherency among NGN activities.

Consistency checks need to be continued, and when completed an major editorial clean up will be necessary.

Table of Contents

* Status D: The FGNGN considers that this deliverable is not yet mature, requiring discussion and technical input to complete development.

1.2 – Terms, definitions and high-level terminological framework for Next Generation Networks

1 Scope

This document contains terms and definitions and a framework relevant to providing a general understanding of Next Generation Networks and a guide for NGN specification development.

This document is not exhaustive, and does not replace the terms and definitions used in other organizations.

This document is not simply a compendium of terms and definitions. The primary purpose of this document is to provide a context for the use of certain terms and definitions to avoid mis-understandings in NGN activities. Thus, the definitions are arranged in a specific order and certain necessary relationships are illustrated. Additionally, explanatory notes are also included where deemed appropriate.

For the most part, this document uses terms and definitions that have already been defined elsewhere and which are considered particularly suitable and applicable to NGN work.

Terms that are thought to be universally understood are simply referenced where appropriate.

2 References

Boilerplate required

[1] ITU-T Recommendation Y.101: GII terminology: Terms and definitions

[2] ITU-T Recommendation Y.1231, IP Access Network Architecture

[3] ITU-T Recommendation Y.2001 (2004), General overview of NGN

[4] ITU-T Recommendation Y.2011 (2004),

[5] ITU-T Recommendation Y.FRA Functional requirements and architecture of the NGN

[6] ITU-T Recommendation G.805 (2000), Generic Functional Architecture of Transport Networks

[7] ITU-T Recommendation X.200 (1994), Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model

[8] ITU-T Recommendation G.809 (2003), Functional Architecture of Connectionless Layer Networks

[9] ITU-T Recommendation G.902 (), Framework Recommendation on functional access networks (AN) - Architecture and functions, access types, management and service node aspects

[10] ITU-T Recommendation G.993.1 (2004), Very high speed digital subscriber line transceivers

[11] ITU-T Recommendation G.8080/Y.1304 (2001), Architecture for the automatically switched optical network (ASON)

[12] ITU-T Recommendation E.651 (), Reference connections for traffic engineering of IP access networks

[13] ETSI TISPAN TS 01018 V0.0.2, TISPAN-NGN, NGN Terminology

[14] ITU-T Recommendation Q.1761 (2004), Principles and requirements for convergence of fixed and existing IMT-2000 systems

[15] ITU-T Recommendation Y.1001 (), IP Framework - A framework for convergence of telecommunications network and IP network technologies

[16] Draft TR-Signalling requirements for IP-QoS (FGNGN-OD-00030)

[17] Requirements and framework for end to end QoS architecture in (FG-NGN-OD-00204)

[18] Draft TR-NGN.NHNperf (FG-NGN-OD-00201)

[19] Algorithms for Achieving End to End Performance Objectives (TR-apo) (FGNGN-OD-00200)

[20] Functional requirements and architecture of the NGN (FGNGN-OD-00223)

[21] Evolution of networks to NGN (FG-NGN-OD-00217)

[22] PSTN/ISDN evolution to NGN (FG-NGN-OD-00218)

[23] PSTN/ISDN emulation and simulation (FG-NGN-OD-219)

[24] Draft FGNGN-IFN (IMS for Next Generation Networks) (FG-NGN-OD-00224)

[25] TR-CMIP (Framework for Customer Manageable IP Network) (SG13 TD PLEN)110)

[26] Softrouter requirements (FG-NGN-OD-0043)

[27] Future Packet Bearer Network requirements (FG-NGN-OD-00209)

[28] Future Packet Bearer Network Architecture (FG-NGN-OD-00210)

[29] Release 1 Scope (FG-NGN-OD-00229)

[30] Release 1 Requirements (FG-NGN-OD-00230)

[31] Tr-enet (FG-NGN-OD-00202)

[32] TR-RACF (FG-NGN-OD-00203)

[33] TR-msnniqos (FG-NGN-OD-00205)

[34] TR-NGN.NHNperf (FG-NGN-OD-00206)

[35] TR-CSF (FG-NGN-OD-00226)

[36] TR-PIEA (FG-NGN-OD-00227)

[37] ITU-T Recommendation Z.100 Supplement 1 (05/97) SDL+ methodology: Use of MSC and SDL (with ASN.1)

[38] ITU-T Recommendation M.3050, Enhanced Telecommunications Operations Map

[39] ITU-T Recommendation Q.833.1, Asymmetric digital subscriber line (ADSL)

[40] ITU-T Recommendation E.164

[41] 3GPP TS 23.271 V6.6.0 (2003-12), “Functional stage 2 description of Location Services (LCS)”.

[42] 3GPP TS 23.141 V6.2.0 (2003-03), “Presence Service – Architecture and Functional Description”.

[43] 3GPP TS 22.141 V6.4.0 (2003-09), “Presence Service (Stage 1)”.

[44] 3GPP TS 22.340 V6.1.0 (2003-09), “IP Multimedia System (IMS) Messaging (Stage 1)”.

[45] 3GPP TS 22.140 V6.4.0 (2004-01), "Multimedia Messaging Service (Stage 1)".

[46] 3GPP TS 22.174 V6.2.0 (2003-03), "Push Service-Service aspects (Stage 1)".

[47] 3GPP TS 23.875 V5.1.0 (2002-03), "Support of Push Service".

[48] 3GPP TS 23.877 V1.0.0 (2003-12), "Architectural Aspects of Speech Enabled Services".

[49] 3GPP TS 22.977 V6.0.0 (2002-09), "Feasibility Study for Speech Enabled Services".

TBC

3 Fundamental NGN Definitions

3.1 Basic Definitions

The following three definitions define the fundamental nature of an NGN.

Next Generation Network (NGN) [3]: a packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

NGN service stratum [4]: that part of the NGN which provides the user functions that transfer service-related data and the functions that control and manage service resources and network services to enable user services and applications.

NGN transport stratum [4]: that part of the NGN which provides the user functions that transfer data and the functions that control and manage transport resources to carry such data between terminating entities.

Visual representation of the relationship between these definitions is shown below in figure 1:

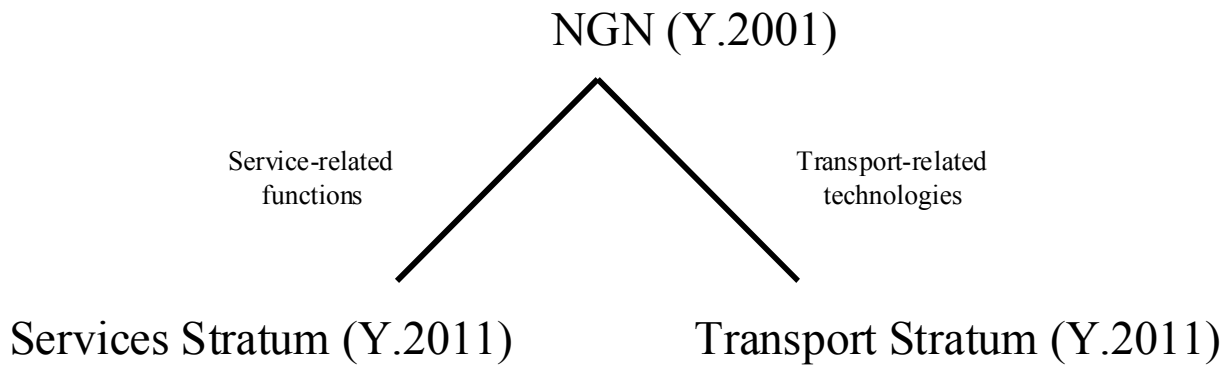


Figure 1 – Defined Fundamental Components of an NGN

3.2 NGN Release Concept

NGN Release: A set of NGN specifications covering a defined set of services and capabilities for implementation in a timely manner. A given specification of a given NGN Release can be categorized using the 3-stages methodology defined in Recommendation I.130, i.e. service aspects (Stage 1), functional network aspects (Stage 2) and network implementation aspects (Stage 3). All services and capabilities

defined in a given NGN Release must be specified to Stage 3 level to ensure that the release is fully implementable.

An NGN Release Description document will define the aspects given above related to that release and reference the documents providing the required information details.

Release completion: An NGN release is completed as soon as the related NGN Release Description document is approved by the ITU-T and all documents referenced in that document are approved by the responsible body.

4 Modes of Communication

The layering principles of ITU-T Recommendation X.200 (1994), Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model 0 apply.

In this respect, any (N)-layer may offer a connection-mode service, a connectionless-mode service, or both, to the (N+1)-layer, using the service or services provided by the (N–1)-layer.

4.1 connection-mode service [7]

A connection is an association established for the transfer of data between two or more peer-(N)-entities. This association binds the peer-(N)-entities together with the (N–1)-entities in the next lower layer. The ability to establish and release a connection and to transfer data over it is provided to the (N)-entities in a given (N)-layer by the next lower layer as a connection-mode service. The use of a connection-mode service by peer-(N)-entities proceeds through three distinct phases:

a) connection establishment;

b) data transfer; and

c) connection release.

Notes:

1 In the context of some of the NGN documents, the phrases “session” or session-based services may be encountered for this mode of operation.

Session-based services: A network controlled session is established before the content is transferred. In general, session based services are peer-to-peer communications, broadcast and multicast type communications. Examples of the session based services are not limited to, conversational services, interactive videophone, etc.

2 The abbreviation CO may also be encountered.

4.2 connectionless-mode service [7]

Connectionless-mode transmission is the transmission of a single unit of data from a source service-access-point to one or more destination service-access-points without establishing a connection. A connectionless-mode service allows an entity to initiate such a transmission by the performance of a single service access.

Notes:

1 In the context of some of the NGN documents, the phrases “non-session-based services may be encountered for this mode of operation.

Non-Session based Services: There is no network controlled session established before the content is transferred. In general, non-session based services are of short duration.

2 The abbreviation CL may also be encountered.

5 The Transport Stratum

The transport stratum has both vertically layered and horizontal dimensions.

5.1 Vertical aspects

The following terms and definitions of G.805 [6] apply to the vertical layering principles for “connection-mode” operation [7].

5.1.1 Connection mode

layer network: A "topological component" that represents the complete set of access groups of the same type which may be associated for the purpose of transferring information.

client/server relationship: The association between layer networks that is performed by an "adaptation" function to allow the link connection in the client layer network to be supported by a trail in the server layer network.

trail: A "transport entity" which consists of an associated pair of "unidirectional trails" capable of simultaneously transferring information in opposite directions between their respective inputs and outputs.

Note: This could be regarded as a “connection” trail to distinguish it from the “connectionless trail defined in G.809.”

path layer network: A "layer network" which is independent of the transmission media and which is concerned with the transfer of information between path layer network "access points".

transmission media layer network: A "layer network" which may be media dependent and which is concerned with the transfer of information between transmission media layer network "access points" in support of one or more "path layer networks".

transport: The functional process of transferring information between different locations.

transport entity: An architectural component which transfers information between its inputs and outputs within a layer network.

transport network: The functional resources of the network which conveys user information between locations.

Note: In accordance with G.805, the NGN context of the NGN transport stratum, the term transport has the wider scope than “transmission” or “first mile” access networks.

5.1.2 Connectionless mode

The following terms and definitions of G.809 0 apply to the vertical layering principles for “connectionless” 0 layer networks.

layer network: A “topological component” that represents the complete set of access groups of the same type which may be associated for the purpose of transferring information.

client/server relationship: The association between layer networks that is performed by an “adaptation” function to allow the “flow” in the client layer network to be supported by a trail in the server layer.

connectionless trail: A “transport entity” responsible for the transfer of information from the input of a flow termination source to the output of a flow termination sink. The integrity of the information transfer may be monitored.

transport: The functional process of transferring information between different locations.

transport entity: An architectural component which transfers information between its inputs and outputs within a layer network.

transport network: The functional resources of the network which conveys user information between locations.

With the exception of "trail" it can be seen that certain definitions apply equally well to connection mode as well as to connectionless mode.

Notes:

1 A client is the user or consumer of services.

2 A server the provider of services.

3 A client may in turn be a server to another higher layer client.

5.1.3 Visual illustration of client and server layer networks

The figure below illustrates the relationship between client and server layer networks.

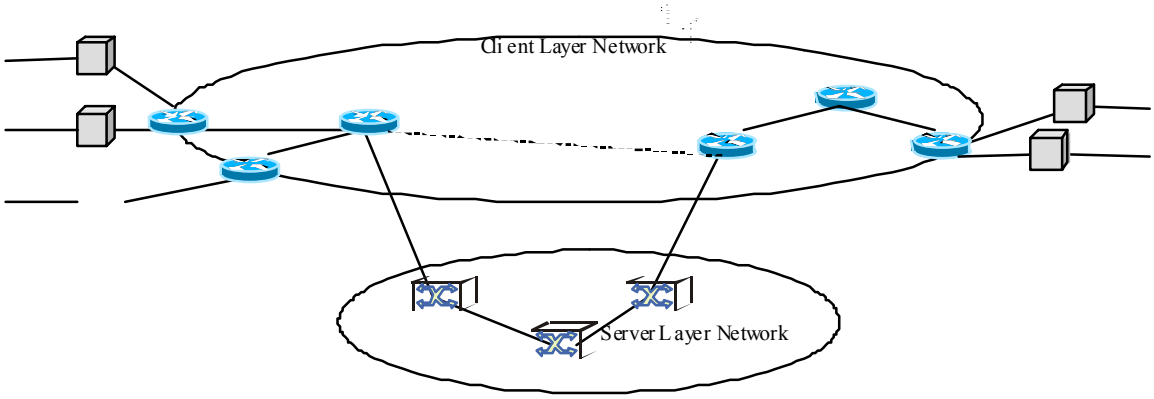


Figure 2 – Illustration of client and server layer networks

Note: As indicated in Recommendation Y.2011 [4], the NGN transport stratum is implemented by a recursion of multiple layer networks as described in Recommendations G.805 and G.809. From an architectural perspective, each layer in the transport stratum is considered to have its own user, control and management planes.

5.1.4 User, control and management planes

From Recommendation G.993.1 [10]:

Plane: A category that identifies a collection of related objects, e.g. objects that execute similar or complementary functions; or peer objects that interact to use or to provide services in a class that reflects authority, capability, or time period.

Transport plane: The Transport Plane provides bidirectional or unidirectional transfer of user information, from one location to another. It can also provide transfer of some control and network management information. The Transport Plane is layered; it is equivalent to the Transport Network defined in ITU-T Rec. G.805.

User plane: A classification for objects whose principal function is to provide transfer of end-user information: user information may be user-to-user content (e.g. a movie), or private user-to-user data.

Notes:

1 In the case of client/server layer networks the client is the "user".

2 In some cases the term data plane is also used instead of user plane

3 This usage should not be confused with "transport plane" as defined in Recommendation G.8080 [11] as follows:

Transport plane: The Transport Plane provides bidirectional or unidirectional transfer of user information, from one location to another. It can also provide transfer of some control and network management information. The Transport Plane is layered; it is equivalent to the Transport Network defined in ITU-T Rec. G.805.

From Y.2011 [4]:

Control plane: the set of functions that controls the operation of entities in the stratum or layer under consideration, plus the functions required to support this control

Management plane: the set of functions used to manage entities in the stratum or layer under consideration, plus the functions required to support this management

5.2 Horizontal

The Transport Stratum comprises the horizontal components shown below:

Figure 3 – General horizontal components

Note: Not all components may be involved in any given communication instance.

Network: A horizontal segment within the transport stratum that its own specific protocols, and which provides communication between two or more defined points to facilitate NGN transport service between them.

For general definitions the following terms from Y.101 [1] and Q.833.1 [ ] apply:

NGN access network: Implementation comprising those entities (such as cable plant, transmission facilities, etc.) which provide the required transport capabilities for the provision of telecommunications services between a Service Node Interface (SNI) and each of the associated User-Network Interfaces (UNIs).

The following corresponding term for core network is offered:

NGN core network: Implementation comprising those entities (such as cable plant, transmission facilities, etc.) which provide the required transport capabilities for the provision of telecommunications services between Service Node Interfaces (SNIs).

Segment (Network Segment): A horizontal partition within the transport stratum provides communication between two or more defined points. [new]

Access segment: The network segment from the interface on the customer's side of the CE to the interface on the customer side of the first Gateway Router

[NOTE: this definition needs to be aligned with the NGN FRA definition finally settled on].

Core Network segment: A core network segment is between Gateway routers, including the gateway routers themselves. The network segment may include some number of interior routers with various roles

Editor's Note: Not sure about term "Gateway".

For service node the following definitions from G.902 [9] apply:

Service Node (SN): Network element that provides access to various switched and/or permanent telecommunication services. In case of switched services, the SN is providing access call and connection control signalling, and access connection and resource handling.

Service Node Interface (SNI): Interface which provides customer access to a service node.

Service Platform (SP): Equipment which allows users to gain access and systems to communicate to the NGN through networks, used to describe the terminal device (i.e., TEs : PC, Telephone, Mobile Phone, etc.) and the server (i.e., Application Server, Media Server, etc.) employed by the service application. [206]

Customer network [21]: A telecommunications network belonging to the customer and located in the customer premise(s).

Customer Premises Equipment (CPE) [17]: End-user system including private network elements connecting the customer applications to the access line.

Customer Premises Network (CPN) [17]: A private network administrated by the user, that may be individual, home or enterprise.

Terminal equipment (TE): Represents the customer's access equipment used to request and terminate network associated connectivity services. [OD-00204]

Off-path [27]: Off-path in a co network means it is using a separate trail. Off-path in cl-ps network means it is using a separate server layer trail.

6 IP related Capabilities

From Y.1001 [15]

IP Transfer Capability: The set of network capabilities provided by the Internet Protocol (IP) layer. It may be characterized by the traffic contract as well as performance attributes supported by control and management functions of the underlying protocol layers. Examples of IP Transfer Capability include basic best effort IP packet delivery and the capability provided by Intserv, and Diffserv framework defined by the IETF.

Auto-Configuration [25]: The end user gets its interface address automatically that creates a link-local address and verifies its uniqueness on a link. It should be obtained through the stateful or stateless mechanism.

Auto-Discovery [25]: The end users or the network elements find their neighbors automatically by using solicitation and advertisement messages.

Control Element (CE) [26]: The CE is a logical entity providing layer 3 control functionality for the purpose of packet forwarding. A CE controls one or multiple FEs belonging to the same NE. A CE is associated with exactly one NE. However, an NE may have one or more CEs. A CE may consist of multiple, distributed, redundant sub-components (PCEs) to implement the control functionality.

Control Link [26]: Control links interconnect CEs with FEs. Direct control links connect CEs with FEs without any intermediate FEs or NEs. Indirect control links span intermediate FEs and NEs.

External Link [26]: External links are layer 3 packet-forwarding links that leave the packet-forwarding plane of an NE to connect with neighboring NEs. In other words, enternal links are Inter-NE links.

From softrouter document, is this still appropriate to be included?

Flow [IP flow] [17]: A sequence of packets sent from a particular source to a particular destination to which the common routing is applied. If using IPv4, a flow is identified by IPv4 5-tuple including source/destination IP addresses, protocol ID, source/destination port numbers. If using IPv6, a flow is identified by IPv6 3-tuple including source/destination IP addresses, flow label.

Forwarding Element (FE) [26]: The FE is a logical entity providing layer 3 packet forwarding functionality. An FE can only be associated with exactly one NE at a given point of time. The FE's control may be migrated to a different CE, if needed. An FE must be able to process protocols for communication with its CE and for FE discovery. An FE may utilize fractional, whole or multiple PFEs. IP TTL and IP options may be modified on a per FE granularity.

Internal Link [26]: Internal links are layer 3 packet-forwarding links that interconnect FEs of the same NE. In other words, the internal links are Intra-NE links. The link between FEs and CE are not considered internal links.

From softrouter document, is this still appropriate to be included?

IP Service Endpoint [16]: A functional entity which includes one type of IP Signalling Endpoint and the User (of that endpoint).

IP Signalling Endpoint [16]: The termination point of an IP signalling path.

IP Transport Packet Size [16]: Length of the payload of a IP Transport Protocol contained in a IP packet.

(IP) Network Element [26]: The NE is a logical entity performing the traditional layer 3 routing functionality. It consists of one or more CEs and FEs. FEs and CEs of the same NE may be separated by multiple hops. IP TTL and IP options may be modified on a per FE granularity. This means that the data plane sees a NE as multiple hops whereas the control plane sees a NE as a single hop.

From softrouter document, is this still appropriate to be included?

Network Entity [16]: The network element responsible for terminating the IP Signalling Protocol.

Physical Control Element (PCE) [26]: A hardware platform that implements layer 3 router control functions. A PCE may host partial CEs (CE sub-components) or multiple CEs.

Physical Forwarding Element (PFE) [26]: A hardware platform that implements layer 3 packet forwarding functionality. A PFE may host multiple FEs but not partial FEs.

Post-Association Phase [26]: Period of time during which FEs and CEs know their mutual bindings and establish communication over a protocol.

Pre-Association Phase [26]: Period of time during which the CE and FE discover each other's existence and attempt to bind themselves. It includes the determination of which CE and which FE can be part of a given NE (This, obviously, is preceded by the determination of which PCEs/PFEs are part of a given CE/FE).

From softrouter document, is this still appropriate to be included?

Customer Manageable IP Network [25]: defines user manageability of resources parameters and network capabilities on an IP network. Users can allocate, configure, control, and manage the resources of IP network elements.

Information Navigation [25]: moving from one source of information to other, related, sources of information.

Information Query [25]: requesting and defining ways of looking for information

Auto-Discovery [25]: The end users or the network elements find their neighbors automatically by using solicitation and advertisement messages

Auto-Configuration [25]: The end user gets its interface address automatically that creates a link-local address and verifies its uniqueness on a link. It should be obtained through the stateful or stateless mechanism

7 Mobility

A number of base terms have been adopted. Relationship between basic terms used for mobility is shown in the figure below.

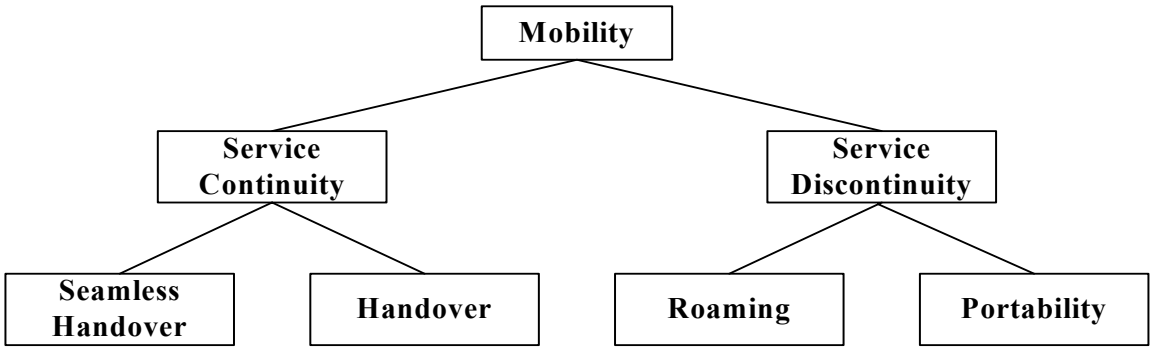


Figure 4 – Relationship between mobility terms

Mobility [3]: the ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment.

Notes:

1 The degree of service availability may depend on several factors including the Access Network capabilities, service level agreements between the user's home network and the visited network (if applicable) etc. Mobility includes the ability of telecommunication with or without service continuity. [Y.2001].

2 In Y.2001 this is called Generalized Mobility.

Service continuity: The ability for a mobile object to maintain ongoing service, including current states, such as user's network environment and session for a service.

Service discontinuity: The inability for a mobile object to maintain ongoing service, including current states, such as user's network environment and session for a service.

Network mobility: The ability of a network, where a set of fixed or mobile nodes are networked to each other, to change, as a unit, its point of attachment to the corresponding network upon the network's movement itself. [224]

Seamless handover: It's one special case of mobility with service continuity, when it's preserved the ability to provide services without any impact on their service level agreements to a mobile object during and after movement. [Same as ETSI]

Handover: The ability to provide services with some impact on their service level agreements to a mobile object during and after movement. [Same as ETSI] [224]

Roaming: This is the ability of the users to access services according their user profile while moving outside of their subscribed home network, i.e. by using an access point of a visited network.

This is usually supported by a roaming agreement between the respective network operators.

Roaming agreement: A business arrangement between a pair of operators in which it is agreed that the one operator will provide service to the customers of the other operator. Among other issues, a roaming agreement may address the level or type of service to be provided to the roaming customers as well as arrangements for compensation for the use of the roamed-to operators resources. [224]

Nomadism: Ability of the user to change his network access point on moving; when changing the network access point, the user's service session is completely stopped and then started again, i.e., there is no session continuity or hand-over possible. It is assumed that normal usage pattern is that users shutdown their service session before moving to another access point. Source *ITU-T Q.1761 (04). And [224]*

Mobility management (MM): The set of functions used to facilitate the mobility. These functions include authentication, authorization, location updating, paging, download of user information and more. [224]

Terminal Mobility: This is the mobility for those scenarios where the same terminal equipment is moving or is used at different locations. The ability of a terminal to access telecommunication services from different locations or while in motion, and the capability of the network to identify and locate that terminal.

Personal mobility: This is the mobility for those scenarios where the user changes the terminal used for network access at different locations. The ability of a user to access telecommunication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile. [224]

Service Mobility: This is Mobility, applied for a specific Service, i.e. the ability of a mobile object to use the particular (subscribed) service irrespective of the location of the user and the terminal that is used for that purpose. [Same as ETSI]

Network mobility [Q.1703] :

The ability of a network, where a set of fixed or mobile nodes are networked to each other, to change, as a unit, its point of attachment to the corresponding network upon the network's movement itself. [224]

Portability: Mechanism that allows a user to retain the same directory number, regardless of the subscribed-to service provider. Number portability may be limited to specific geographical areas. In the context of the All-IP network, the term "number portability" refers specifically to ITU-T E.164 numbers used for telephony. (Q.1742.1 (02), 3.30; Q.1742.2 (03), 3.30; Q.1742.3 (04), 3.30)

Regional mobility: When a mobile object changes its location, the mobility could be completed within a region covered by a system that is responsible for the mobility in its region. This is defined as regional mobility.

Home Network: The network associated with the operator/service provider that owns the subscription of the user. [224 and 229]

Visited Network: The network that is local to the user in a roaming configuration (REL1). [224 and 229]

8 Roles, players, value-added chain, etc

Taken from Y.110 [ ]:

Role: A role is a business activity which fits in a value chain. The role is constrained by the smallest scale of business activity which could exist independently in the industry and so a marketplace will exist for every relationship between roles.

Player: A player is an organization, or individual, which undertakes one or more roles. The player can be a commercial company, a government agency, a non-governmental organization, a charity or an individual.

Value chain, complete value chain, and primary value chain: A "tree" of roles are connected together to make an end good/service. The total set of roles involved in producing an end good/service are and the way they pass intermediate goods/services between the roles is called the complete value chain. The set of roles which form the only principle activity of a generally recognized industry which produces the end good/service are the primary value chain. All the other roles in the complete value chain will be providing support goods/services for roles in the primary value chain.

9 User, customer, subscriber, client, provider, etc.

In a service context is usual to consider the party supplying the service and the party using the service. Unfortunately we have a number terms in common use, some of which can be regarded as synonyms depending on the context in which they are used. Further, unlike many previous environments where it was clear where there was only one simple relationship between these two parties, the NGN environment enables an arbitrary recursion of these relationships.

The following definitions form M.3050.1, Enhanced Telecom Operations Map (eTOM) – The business process framework, have been adopted:

Customer: The Customer buys products and services from the Enterprise or receives free offers or services. A Customer may be a person or a business.

Source: M.3050.1

Note: there could be many users per customer.

Subscriber: The person or organization responsible for concluding contracts for the services subscribed to and for paying for these services. [M.3050]

Note: there could be many users per subscriber.

End User: The End User is the actual user of the Products or Services offered by the Enterprise. The end user consumes the product or service. See also Subscriber below.

Source: M.3050.

The following may also be helpful:

User, End user: A human being, organization, or telecommunications system that accesses the network in order to communicate via the services provided by the network.

Source: ETSI AT ES 202 488-2

In most cases we use the term “user” in the FGNGN documents to mean the entity physically using the service at the interface to the network, at the UNI, or associated with the device at the UNI. The user represents the entity actually receiving the subscribed services and physically associated with the delivery point, where the actual service interactions take place, typically the UNI.

In the contractual sense we need to be able to distinguish between a subscriber/customer who is the actual user (1:1 relationship), and a subscriber/customer that is an organization with a number of delegated users (1:N relationship).

For most intents and purposes, the terms “customer” and “subscriber” may be regarded as synonyms.

Note: Extreme care needs to be taken over the term “end” which may be relative rather than absolute depending on the point where the recursion stops.

Network provider [17]: The organization that maintains and operates the network components to support services. A network provider may also take more than one role, e.g. also acting as Service Provider**. [204]**

Service provider [17]: A general reference to an operator that provides NGN telecommunication services to Customers and other users either on a tariff or contract basis. A Service Provider may or may not operate a network. A Service Provider may or may not be a Customer of another Service. [204]

Terminal equipment (TE) [17]: Represents the customer's access equipment used to request and terminate network associated connectivity services. [204]

User Network Interface (UNI): An interface between the user equipment and a network termination at which interface the access protocols apply. Note: This interface is not constrained to a single protocol.

Network Node Interface (NNI): The interface of a network node (node as defined in Rec. E.351) which is used to interconnect with another network node. Note: This interface is not constrained to a single protocol. In the case of interconnection between an NGN network and a legacy network it will also depend on the type of network connecting to NGN and where the mediation is performed if any.

Customer Premises Network (CPN) [17]: A private network administrated by the user, that may be individual, home or enterprise. [204]

or

Customer network: A telecommunications network belonging to the customer and located in the customer premise(s). The customer network is connected to the user side of an access network [217]

(General) Domain: A collection of physical or functional entities which are owned and operated by a player and can include entities from more than one role. The extent of a domain is defined by a useful context and one player can have more than one domain~~; however, a domain should not include more than one service provisioning platform.~~

Source: minor change from ITU-T Y.110

***Editor's note**: The last sentence is no longer valid and should be removed: a single operator may own for example an ISDN/PSTN emulation platform and offer presence service from an entirely different platform within the same domain*

Administrative domain: collection of physical or functional entities under the control of a single administration.

Source: ETSI TIPHON TR 101 878, SPAN TS 102 261; very similar to definition in ITU-T X.115 (95)

User domain: collection of physical or functional entities under the control of an end-user that share a consistent set of policies and common technologies.

ETSI TIPHON TR 101 878, SPAN TS 102 261

Service domain: collection of physical or functional entities offering IP based services under the control of an NGN Service Provider which share a consistent set of policies and common technologies.

Source: adapted from ETSI TIPHON TR 101 878, SPAN TS 102 261

Private domain: Those parts of a private NGN that belong to a private entity and which are usually located on that private entity's premises.

Source: minor adaptation from ETSI CN EG 201 026

***Explanation**: This and the following term are used in the context of corporate networks. They refer to the fact that a corporate network (private NGN) can rely partly or wholly on services offered by a public network.*

Public domain: Those parts of a private NGN that are provided using the public network infrastructure of another NGN.

Source: minor adaptation from ETSI CN EG 201 026

Demarcation Point - Generally a point which separates two domains, here the separation between the access and transit networks.

10 Telecommunications, Services, Applications, etc

Basic Terms

Service: A set of functions and facilities offered to a user by a provider.

NOTE - In this definition, the "user" and "provider" may be a pair such as application/application, human/computer, subscriber/organization (operator). The different types of service included in this definition are data transmission service and telecommunications service offered by an operating agency to its customers, and service offered by one layer in a layered protocol to other layers.

Complementary Definition

Service: Task or set of tasks performed by the provider(s) of that telecommunication service for the user of the service in an NGN environment.(editor's notes: NGN environment need to be defined) Created from service capabilities. [check reference]

Telecommunication service: a service which implies automated processing, storage and providing of the information (including voice, data, image and video) via telecommunication networks. (editor's notes: this definition is from **T05-SG13-050425-D-0174**. Added at the May SG 13 meeting.)

Telecommunication: Any transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire ,radio, optical or other electromagnetic systems.

(as defined in the ITU Constitution provision 1012 and in the International Telecommunication Regulations ITR)

Application [21]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface. [217]

Application Server (AS) [21]: A unit that supports service execution, e.g. to control Call Servers and NGN special resources (e.g. media server, message server). [217]

Application Network Interface: provides a channel of interactions and exchanges between "3rd Party Application Providers" and NGN elements offering needed capabilities and resources for realization of value added services. [229]

Call server (CS) [21]: A unit which controls set-up, maintenance, modification and release of a call.

Connection-oriented network service [17]: A network service that establishes logical connections between end users before transferring information.

Connectionless service [17]: A service, which allows the transfer of information among service users without the need for end-to-end logical connection establishment procedures.

Session (1): A temporary relationship among a group of objects that are assigned to collectively fulfill a task for a period of time. A session has a state that may change during its lifetime. The session represents an abstract, simplified view of the management and usage of the objects and their shared information. Sup. 27 to Q-Ser. (99), 3.7

or

Session (2): A period of communication between two terminals which may be conversational or non-conversational (for example, retrieval from a database). H.245 (05), 3.24; H.246 (98), A.2.6; H.310 (98), 3.27

- ***Session-based services***: A network controlled session is established before the content is transferred. In general, session based services are peer-to-peer communications, broadcast and multicast type communications. Examples of the session based services are not limited to, conversational services, interactive videophone, etc.
- ***Non-Session based Services***: There is no network controlled session established before the content is transferred. In general, non-session based services are of short duration.

IP multimedia application: An application that handles one or more media simultaneously such as audio, video and data (e.g. chat, shared whiteboard) in a synchronised way from the user's point of view. A multimedia application may involve multiple parties, multiple connections, and the addition or deletion of resources within a single IP multimedia session. A user may invoke concurrent IP multimedia applications in an IP multimedia session.

Source: ETSI 3GPP TS 122 228

IP multimedia session:

An IP multimedia session is a set of multimedia senders and receivers and the data streams flowing from senders to receivers. IP multimedia sessions are supported by the NGN and are enabled by IP connectivity bearers. A user may invoke concurrent IP multimedia sessions.

Source: ETSI 3GPP TS 122 228

Specific Services (Editor's note: this section needs discussion wrt its suitability)

Location Service (LCS): network provided enabling technology consisting of standardised service capabilities, which enable the provision of location applications. The application(s) may be service provider specific. A Location Service is specified by all the necessary network elements and entities, their functionalities, interfaces, as well as communication messages to implement the positioning functionality in a cellular network.

Source: 3GPP TS 23.271 V6.6.0 (2003-12), "Functional stage 2 description of Location Services (LCS)".

Generally there are four categories of usage of the Location Service. These are: Commercial LCS, Internal LCS, Emergency LCS and Lawful Intercept LCS.

- **The Commercial LCS:** an application that provides a value-added service to the subscriber of the service, through knowledge of the UE location and if available, and at the operator's discretion, the positioning method used to obtain the location estimate. This may be, for example, a directory of restaurants in the local area of the UE, together with directions for reaching them from the current UE location.
- **The Internal LCS:** use of the location information of the UE for Access Network internal operations. This may include; for example, location assisted handover and traffic and coverage measurement. This may also include support for certain O&M related tasks, supplementary services, IN related services, bearer services and teleservices.
- **The Emergency LCS:** a service provided to assist subscribers who place emergency calls(place calls to emergency services). In this service, the location of the UE caller and, if available, the positioning method used to obtain the location estimate is provided to the emergency service provider to assist them in their response. This service may be mandatory in some jurisdictions. In the United States, for example, this service is mandated for all mobile voice subscribers.

- **The Lawful Intercept LCS**: a service to provide the location information to support various legally required or sanctioned services.
- Source: 3GPP TS 23.271 V6.6.0 (2003-12), "Functional stage 2 description of Location Services (LCS)".

Location Based Service (LBS): service provided either by teleoperator or a 3rd party service provider that utilizes the available location information of the terminal. Location Application offers the User Interface for the service. LBS is either a pull or a push type of service (see Location Dependent Service). [3]

Source: 3GPP TS 23.271 V6.6.0 (2003-12), "Functional stage 2 description of Location Services (LCS)".

Location Dependent Service (LDS): service provided either by teleoperator or a 3rd party service provider that is available (pull type) or is activated (push type) when the user arrives at a certain location. It requires no advance subscription, but the push type activation must be confirmed by the user. The offered service itself can be any kind of service. [3]

Source: 3GPP TS 23.271 V6.6.0 (2003-12), "Functional stage 2 description of Location Services (LCS)".

Presence Services

Presence Services provide the ability for the home network to manage presence information of a user's device, service or service media even while roaming. A user's presence information may be obtained through input from the user, information supplied by network entities or information supplied by elements external to the home network. Consumers of presence information (i.e., "watchers") may be internal or external to the home network. [4]

Source: 3GPP TS 23.141 V6.2.0 (2003-03), "Presence Service – Architecture and Functional Description".

The presence service results in presence information of a user and information on a user's devices, services and services components being managed by the network. This service capability enables the creation of enhanced fixed and mobile multimedia services comparable to those currently present on the Internet. Presence is an attribute related to, but quite different from mobility information, and is a service that can be exploited to create additional services. The types of services that could be supported by the presence service may include:

New communications services

– The presence service will enable new multimedia services to exploit this key enabler to support other advanced multimedia services and communications. These new services may infer the context, availability and willingness of a user to accept or participate in particular types of communications by accessing the presence information for the user's devices and services. Examples of such new multimedia services that could potentially exploit the presence service include "chat", instant messaging, multimedia messaging, e-mail, handling of individual media in a multimedia session etc.

Information services

– The presence service may also be exploited to enable the creation of services in which abstract entities are providing the services to the mobile community. The presence service may be used to support such abstract services as cinema ticket information, the score at a football match, motorway traffic status, advanced push services etc. [5]

Resource: 3GPP TS 22.141 V6.4.0 (2003-09), "Presence Service (Stage 1)".

Messaging Services

The material currently in TD12 (WP1/13) is not currently suitable?.

Messaging Services incorporate one or more of the following messaging types: Immediate messaging, Deferred delivery messaging and Session based messaging. With Immediate messaging the sender expects immediate message delivery in what is perceived as real time compared with Deferred messaging where the sender expects the network to deliver the message as soon as the recipient becomes available. With Session based messaging a communications association is established between two or more users before communication can take place. In the simplest form Session based messaging maybe a direct communication between two users. Messaging services may be single- or multimedia-based, enabling a unified application which integrates the composition, storage, access, and delivery of different kinds of media, e.g. text, voice, image or video.

Immediate messaging: Typically, the sender is aware of the availability of the recipient(s) (possibly through the use of the Presence service) before sending this type of message as, if the recipient is not available, the message may be discarded or deferred. An immediate message may be deferred by the recipient's network based on the message filtering settings defined by the recipient or by the recipient's service provider.

Session based messaging: The sender and recipient expect near real time message delivery. Typically, recipients of the session based messaging that are not joined to a group or are not available will not receive the messages. Typically, a sender may send a message to all participants in the messaging session without addressing them individually.

Source: 3GPP TS 22.340 V6.1.0 (2003-09), "IP Multimedia System (IMS) Messaging (Stage 1)".

Deferred delivery messaging: The sender expects message delivery as soon as the recipient becomes available. Deferred delivery messaging must support storage of messages or message elements until delivered to the recipient's terminal, until they expire, or until they are deleted by the user.

Source: 3GPP TS 22.140 V6.4.0 (2004-01), "Multimedia Messaging Service (Stage 1)".

10.1 Push Services

Push service: a service capability used by a Push Initiator in order to transfer push data (e.g. data, multimedia content) to the Push Recipient without a previous user action. The Push Service could be used as a basic capability or as component of a value added service.

Push initiator: the entity that originates push data and submits it to the push function for delivery to a Push recipient. A Push initiator may be, for example, an application providing value added services.

Push recipient: the entity that receives the push data from the Push function and processes or uses it. This may include the UE with which the network communicates, the user agent with the application level address, or the device, machine or person which uses the push data. A Push recipient is controlled by an individual user.

Push Data: data sent by the push initiator to the push recipient, of a format known to the receiver (push recipient).

Source: 3GPP TS 22.174 V6.2.0 (2003-03), "Push Service-Service aspects (Stage 1)"

Editor's Note: Is the following text necessary???

Push Services introduce a means to transmit push data from a *push initiator* to a *push recipient* (e.g. a UE) without a previous user action. The push concept, as provided by the SMS teleservice, has been very successful, both for text messaging (for user viewing) and for other data. The Push Service should therefore be understood as a building block (network capability), which can be used for new services, both public and private.

In the normal client/server model, a client requests a service or information from a server, which then responds in transmitting information to the client. This is known as the "pull" technology; the user pulls information from the content provider. The World Wide Web is a typical example of pull technology, where a user enters a URL (the request) that is sent to a server and the server answers by sending a Web page (the response) to the user. In contrast to

this there is also the "push" technology where there is no explicit request from the user before the content provider (push initiator) initiates an information transfer to a user. Whereas "pull" transactions of information are always initiated from the user, "push" transactions are content provider initiated. Push services may be used to implement high level services such as IP multimedia services, MMS, etc., and new services including public safety, government, corporate IT, transfer of push data to machines and devices, in addition to infotainment type services.

*Source: 3GPP TS 22.174 V6.2.0 (2003-03), "Push Service-*Service *aspects (Stage 1)"*

To offer a push service to a user through a delivery network, there are two approaches depending on type of contents to be delivered. One content type can be delivered directly to the user with single message and does not require a dedicated IP connection. Another content type requires a sequence of messages (e.g. a movie clip that streams for some period) and requires a dedicated IP connection for communication between the application server and the user.

Source:3GPP TS 23.875 V5.1.0 (2002-03), "Support of Push Service"

Speech-Enabled services

Speech-enabled Service: (or Automated Voice Service) is a voice application that provides a voice interface driven by a voice dialog manager to drive the conversation with the user in order to complete a transaction and possibly execute requested actions. It relies on speech recognition engines to map user voice input into textual or semantic inputs to the dialog manager and mechanisms to generate voice or recorded audio prompts (text-to-speech synthesis, audio playback). It may also rely on additional speech processing (e.g. speaker verification). Telephony-based automated voice services also typically provide call processing and DTMF recognition capabilities. Examples of traditional automated voice services are traditional IVR (Interactive Voice Response Systems) and VoiceXML Browsers. Examples of Automated Voice Services include:

- Communication assistance (Name dialling, Service Portal, Directory assistance)
- Information retrieval (e.g., obtaining stock-quotes, checking local weather reports, flight schedules, movie/concert show times and locations)
- M-Commerce and other transactions (e.g., buying movie/concert tickets, stock trades, banking transactions)
- Personal Information Manager (PIM) functions (e.g., making/checking appointments, managing contacts list, address book, etc.)
- Messaging (IM, unified messaging, etc…)
- Information capture (e.g. dictation of short memos)

Editors Note: Is the following text necessary????

Automatic Speech Recognition (ASR) platforms tend to perform the following sequence of operations: *echo cancellation, feature extraction* and *interpretation*. The echo cancellation process is used to permit a person to send commands to the ASR platform while the ASR platform is still playing voice announcements. (Without echo cancellation, the ASR platform cannot distinguish between its own "voice" and the voice of the user!) The feature extraction process extracts phonemes from the input speech signal and transforms them into words using acoustic models. The speech recognition engine then performs a search of the uttered words in the grammar created by GSL (Grammar Specific Language). The interpretation process is used to extract the semantic interpretation from the word sequence. [10]

Source: 3GPP TS 23.877 V1.0.0 (2003-12), "Architectural Aspects of Speech Enabled Services".

Speech-enabled services may utilize speech alone for input and output interaction, or may also utilise multiple input and output modalities leading to the multimodal services. As the name implies, speech-only services utilise only the speech modality for both user input and output. These services are especially suited to the smaller size wireless devices in the market today. Multi-modal interfaces combine the use of multiple interaction modes, such as voice, keypad and display to improve the user interface to services. These services exploit the fact that different interaction modes are good at different things - for example, talking is easier than typing, but reading is faster than listening. [11]

Source: 3GPP TS 22.977 V6.0.0 (2002-09), "Feasibility Study for Speech Enabled Services".

11 Functional aspects

The following definitions from Y.FRA apply:

Functional Entity [20]: An entity that comprises a specific set of functions at a given location. Functional entities are logical concepts, grouping of functional entities are used to describe practical physical realizations. [223]

Functional architecture [20]: A set of functional entities which are used to describe the structure of a NGN. These functional entities are separated by reference points and thus they define the distribution of functions. These functional entities can be used to describe a set of reference configurations. These reference configurations identify which of the reference points are visible at boundaries of equipment implementations and between administrative domains.

Reference point [20]: A conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing between these functional entities. A reference point may or may not correspond to one or more physical interfaces between pieces of equipment.

Gateway [21]: A unit that interconnects different networks and performs the necessary translation between the protocols used in these networks.

Interface: A shared boundary between networks and between SP and network. An interface supports various characteristics pertaining to the functions, physical interconnections, signal exchanges and other characteristics as appropriate. [206]

12 Evolution to NGN, PSTN/ISDN simulation, emulation, and other related terms

Evolution to NGN [21]: A process in which parts of the existing networks are replaced or upgraded to the corresponding NGN components providing similar or better functionality, while maintaining the services provided by the original network. In addition, evolution to NGN will provide extra capabilities to the existing networks. [217]

PSTN/ISDN Emulation [23]: Provides PSTN/ISDN service capabilities and interfaces using adaptation to an IP infrastructure.

Note: Not all service capabilities and interfaces have to be present to provide an emulation. [219]

PSTN/ISDN Simulation [23]: Provides PSTN/ISDN-like service capabilities using session control over IP interfaces and infrastructure.

Note: This definition allows for the possibility of simulation providing a complete mapping of the PSTN / ISDN service set (complete simulation). [219]

Media Server [22]: A network element providing the Media Resource Processing Function for telecommunication services in NGN. [218]

Remote User Access Module (RUAM) [22]: A unit that physically terminates subscriber lines and converts the analogue signals into a digital format. The RUAM is physically remote from the Local Exchange.

User Access Module (UAM) [22]: A unit that physically terminates subscriber lines and converts the analogue signals into a digital format. The UAM is collocated with a Local Exchange (LE), and is connected to the Local Exchange.

Interworking: This term is used to express interactions between networks, between end systems, or between parts thereof, with the aim of providing a functional entity capable of supporting an end-to-end communication. The interactions required to provide a functional entity rely on functions and on the means to select these functions. [OD-00204 and 219]

Interoperability: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged. [OD-00204]

Gateway: A unit that interconnects different networks and performs the necessary translation between the protocols used in these networks. [217]

Access Gateway (AG): A unit that provides subscribers with various service access (e.g. PSTN, ISDN, V5.x, xDSL, LAN etc.) and connects them to the packet node (IP or ATM) of an NGN. [217]

Signalling Gateway (SG) [22]: A unit that provides signalling conversion between the NGN and the other networks (e.g. STP in SS7). [217]

Transit Gateway (TG) [21]: A unit that provides an interface between the packet nodes of the NGN and the circuit switched node of the PSTN for bearer traffic. The TG provides any needed conversion to the bearer traffic. [217]

Call Server: The core element of a CS-based PSTN/ISDN emulation component, which is responsible for call control, gateway control (Access GW, Media GW, and Packet GW), media resource control, routing, user profile and subscriber authentication, authorization and accounting. [217]

Node: A network element (e.g. switch, router, exchange) providing switching and/or routing capabilities. [217]

Accounting: See Recommendation X.462 [4]. For convenience the definition is repeated here: "The action of collecting information on the operations performed within a system and the effects thereof." [217]

Billing: See Recommendation Q.825 [5]. For convenience the definition is repeated here: "Administrative function to prepare bills to service customers, to prompt payments, to obtain revenues and to take care of customer reclaims." [217]

Charging: See Recommendation Q.825 [5]. For convenience the definition is repeated here: "The set of functions needed to determine the price assigned to the service utilization." [217]

13 Quality of Service

Absolute QoS [17]: This term refers to a traffic delivery service with numerical bounds on some or all of the QoS parameters. These bounds may be physical limits, or enforced limits such as those encountered through mechanisms like rate policing. The bounds may result from designating a class of network performance objectives for packet transfer.

QoS Class (?): Identifies the category of the information that is received and transmitted in the U-plane.

Relative QoS [17]: This term refers to a traffic delivery service without absolute bounds on the achieved bandwidth, packet delay or packet loss rates. It describes the circumstances where certain classes of traffic are handled differently from other classes of traffic, and the classes achieve different levels of QoS.

Unidirectional QoS Path (?): A unidirectional QoS Path is a path along which the user data packets flow in the same direction.

Aggregate Loss Ratio: The loss aggregated along a path across multiple provider's networks.

Apportionment [19]: Method of portioning a performance impairment objective among segments.

Allocation [19]: Formulaic division or assignment of a performance impairment objective among segments.

Importance [27]: Importance is the survivability of a given packet compared to all other packets when the network has insufficient resources to service all the traffic. The importance of a given packet is independent of the delay requirements (urgency) of that packet. [209]

Measurement point: A point in the network containing functionality that may initiate or respond to measurements with other measurement points. (located at peering points, demarcation points, PEs, CEs and Landmark customer premise equipment).

Media Flow: A unidirectional or bidirectional media stream of a particular type, which is specified by two endpoint identifiers, bandwidth and class of service. OD-00203

Media: One or more of audio, video or data. [223]

Media stream: A media stream can be of type audio, video or data or a combination of any of them. Media stream data conveys user or application data (payload) but no control data H.235 (03), 3.12. [223]

Stream: A flow of real-time information of a specific media type (e.g. audio) and format (e.g. G.722) from a single source to one or more destinations. T.137 (00), 3.22 [223]

Gate: Packet filter for a media flow OD-00203

Gate Control: Enable or disenable packet filter for a media flow OD-00203

Flow [IP flow]: A sequence of packets sent from a particular source to a particular destination to which the common routing is applied. If using IPv4, a flow is identified by IPv4 5-tuple including source/destination IP addresses, protocol ID, source/destination port numbers. If using IPv6, a flow is identified by IPv6 3-tuple including source/destination IP addresses, flow label. OD-00204.

Path Unavailability: The period of time from when losses exceed a threshold until they drop below another threshold, a measure of bursty loss.

Period Path Unavailability: The total period of unavailability during a customer reporting period (typically one month).

Urgency [27]: Urgency is how fast a packet must get processed in the up-state to meet the requested QoS requirements. The urgency of a packet is conveyed in terms of the performance (delay) it requires and a packet's urgency is independent of the survivability (importance) of that packet. [209]

14 Identification and Location (including Numbering, Naming, Addressing, Routing, etc)

Address: An identifier used for routing a communication to an entity [209 modified]

Note: The following definition from SG2 is considered to be too restrictive with respect to what is being identified. **Address:** A string or combination of digits and symbols which identifies the specific network termination points of a connection and is used for routing. [Sup. 3 to E.164 (04), 3.1.1; Sup. 4 to E.164 (04), 3.1.1; E.191 (00), 3.1.]

Name: An identifier (that may be resolved to an address) that uniquely identifies an entity within a particular identification domain. [210]

Identifier: A string of digits and/or symbols.

Note: An identifier may two forms, an abstract syntax for human readability, and real syntax for protocol encoding and/or machine readability purposes.

User* Identifier [NGN Rel1req]: A type of password, identity, image, or pseudonym associated with a user, assigned by and exchanged between operators and service providers to identify a user, to authenticate her/his identity and/or authorize the use of service. Examples are biometric identifiers such as a user eye image, a finger print, a SIP URI, etc. [230)

*user was added, as result of e-mail discussion

Identity: The attributes by which an entity or person is described, recognized or known. [230]

Identity Provider: A service provider that creates, maintains, and manages identity information for subscribers/users, and can provide an authentication assertion to other Service Providers within a circle of trust. [230]

NGN* User Identity Module: An entity that can be used to store, transport, process, dispose of, or otherwise handle user identity information. [230]

[Is the word "NGN" appropriate here? Too restrictive?]

Single Sign ON: The ability to use an authentication assertion from one network operator/service provider to another operator/provider for a user either accessing a service or roaming into a visited network. [230]

User Attribute: A characteristic that describes the user (e.g., user identity's life time, user status as being "available", "don't disturb", etc.). [230]

WORKING GROUP 3
DELIVERABLES

QUALITY OF SERVICE

1.3 General aspects of Quality of Service and network performance in the NGN (*Status D*)

1.4 Network performance of non-homogeneous networks in NGN (*Status A*)

1.3 – General aspects of quality of service and network performance in the NGN*

Table of contents

* Status D: The FGNGN considers that this deliverable is not yet mature, requiring discussion and technical input to complete development.

1-3 – General aspects of quality of service and network performance in the NGN

1 Scope

This Draft has been developed to:

- provide descriptions of NGN Quality of Service, Network Performance and Quality of Experience;
- illustrate how the Quality of Service, the Network Performance, and Quality of Experience concepts are applied in NGN environment;
- describe performance aspects of the Next Generation Network (NGN) including performance of service and transport stratum;
- provide a basis for common understanding of performance concepts useful to users and to the industries that compose the NGN (e.g., Fixed & mobile telecommunications, broadcasting, etc.);
- define the application QoS classes of the NGN.

2 References

The following ITU-T Recommendations contain provisions which, through reference in this text, constitute provisions of this Draft. At the time of publication, the editions indicated were valid. All Recommendations are subject to revision; all users of this Draft are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations listed below. A list of the currently valid ITU-T Recommendations is regularly published.

- Rec. E.800 Terms and definitions related to quality of service and network performance including dependability
- Rec. G.1000 Communications quality of service: A framework and definitions
- Rec. G.1010 End-user multimedia QoS categories
- Rec. I.350 General aspects of quality of service and network performance in digital networks, including ISDNs
- Rec. I.356 B-ISDN ATM layer cell transfer performance
- Rec. X.800 Security Architecture for Open Systems Interconnection for CCITT applications
- Rec. X.805 Security Architecture for systems providing end-to-end communications
- Rec.Y.1540 Internet protocol data communication service - IP packet transfer and availability performance parameters
- Rec.Y.1541 Network performance objectives for IP-based services
- Rec. Y.1560 Parameters for TCP connection performance in the presence of middleboxes
- Rec. Y.1561 Performance and Availability Parameters for MPLS Networks
- Rec. Y.2011 General principles and general reference model for NGNs

3 Abbreviations

This Draft uses the following abbreviations:

AN	Access Network
ATM	Asynchronous Transfer Mode
B-ISDN	Broadband Integrated Services Digital Network
CN	Core Network
CPN	Customer Premise Network
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
ISDN	Integrated Services Digital Network
MP	Measurement Point
MPLS	Multi-Protocol Label Switching
NGN	Next Generation Network
NP	Network Performance
PDH	Plesiochronous Digital Hierarchy
QoE	Quality of Experience
QoS	Quality of Service
RTP	Real-time Transport Protocol
SDH	Synchronous Digital Hierarchy
SP	Service Platform
TCP	Transmission Control Protocol
TE	Terminal Equipment
UDP	User Datagram Protocol

4 Description of Quality of Service (QoS), Network Performance (NP) and Quality of Experience (QoE)

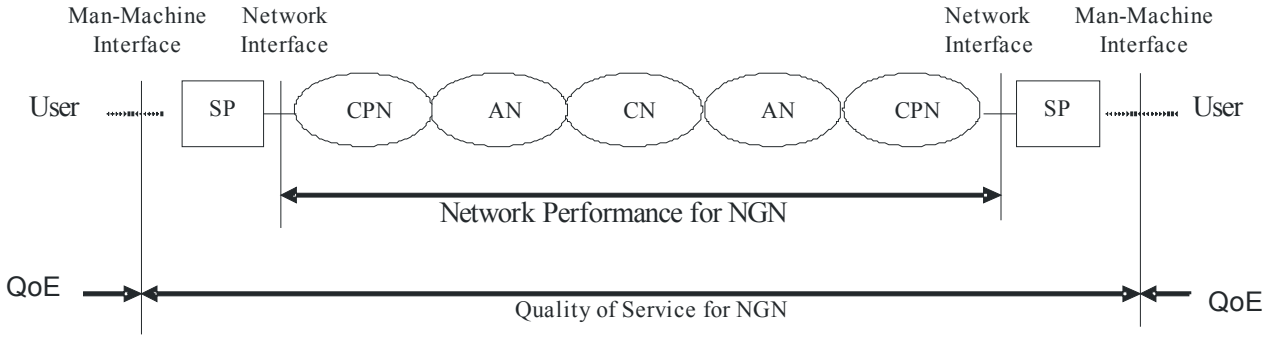
QoS is defined in Recommendation E.800 as follows: "Collective effect of service performance which determine the degree of satisfaction of a user of the service".

The definition of QoS in Recommendation E.800 is a wide one encompassing many areas of work, including subjective user satisfaction. However, within this Draft the aspects of QoS that are covered are restricted to the identification of parameters that can be directly observed and measured at the point at which the service is accessed by the user.

Recommendation I.350 defines Network Performance as the "NP is measured in terms of parameters which are meaningful to the network provider and are used for the purpose of system design, configuration, operation and maintenance. NP is defined independently of terminal performance and user actions".

QoE is defined as the overall acceptability of an application or service, as perceived subjectively by the end-user. Quality of Experience includes the complete end-to-end system effects (client, terminal, network, services infrastructure, etc). Overall acceptability may be influenced by user expectations and context.

Figure 1 illustrates how the concepts of QoS, NP and QoE are applied in the NGN environment.



- CN : Core Network
- SP : Service Platform
- AN : Access Netw-ork
- CPN : Customer Premise Network

Note 1: The definitions of each network are based on existing telecommunication terminologies. In order to include the functions for radio communication and broadcasting, those definitions may be changed. This is FFS.

Note 2: User-to-user communication is the basic consideration in this figure. In order to cover the broader view of NGN, the connectivity of NGN should facilitate:

- user-to-user connectivity (MMI-to-MMI);
- user-to-services platform connectivity (MMI-to-MNI);
- services platform-to-services platform connectivity (MNI-to-MNI)

Figure 1/Draft TR-NGN.QoS – General reference configuration for NGN QoS, NP and QoE

5 Distinction among QoS, NP and QoE

QoS provides a valuable framework for network provider, but it is not necessarily usable in specifying performance requirements for particular network technologies (i.e. ATM, IP, MPLS, etc.). Similarly, NP ultimately determines the (user observed) QoS, but it does not necessarily describe that quality in a way that is meaningful to users.

QoE is subjective in nature, i.e. depend upon user actions and subjective opinions.

The definition of QoS, NP and QoE should make mapping clear in cases where there is not a simple one-to-one relationship among them.

Table 1 shows some of the characteristics which distinguish QoS, NP and QoE.

Table 1/Draft TR-NGN.QoS – Distinction between quality of experience, quality of service and network performance

Quality of Experience	Quality of Service	Network Performance
User oriented		Provider oriented
User behaviour attribute	Service attribute	Connection/Flow element attribute
Focus on user-expected effects	Focus on user-observable effects	Focus on planning, development (design), operations and maintenance
User subject	Between (at) service access points	End-to-end or network elements capabilities

6 Measurability of QoS, NP and QoE parameters values

Due to separating QoS, NP and QoE, a number of general points should be noted when considering the development of parameters;

– the definition of QoS parameters should be clearly based on events and states observable at service access points and independent of the network processes and events which support the service;

– the definition of NP parameters should be clearly based on events and states observable at network element boundaries, e.g. protocol specific interface;

– the definition of QoE parameters[1] is out of scope of this Draft.

7 Layered Model of QoS and NP for NGN

Figure 2 illustrates the layered nature of QoS and NP of NGN.

Recommendation Y.2011 describes the layered model of NGN as follows:

NGN service stratum: That part of the NGN which provides the user functions that transfer service-related data and the functions that control and manage service resources and network services to enable user services and applications. User services may be implemented by a recursion of multiple service layers within the service stratum. The NGN service stratum is concerned with the application and its services to be operated between peer entities. For example, services may be related to voice, data or video applications, arranged separately or in some combination in the case of multimedia applications. From an architectural perspective, each layer in the service stratum is considered to have its own user, control and management planes.

NGN transport stratum: That part of the NGN which provides the user functions that transfer data and the functions that control and manage transport resources to carry such data between terminating entities. The data so carried may itself be user, control and/or management information. Dynamic or static associations may be established to control and/or manage the information transfer between such entities. An NGN transport stratum is implemented by a recursion of multiple layer networks as described in Recommendations G.805 and G.809. From an architectural perspective, each layer in the transport stratum is considered to have its own user, control and management planes.

– The transport stratum that provide connection-oriented or connectionless transport supporting the service stratum. This stratum may involve different types of technologies, for example, IP, ATM, Frame Relay, SDH, PDH, ISDN, and leased lines. There may be several layers of protocols and services below the IP layer that is dominant protocol in NGN.

---

[1] ITU-T SG12 had specified MOS (Mean Opinion Score) parameter and R-rating approach for voice applications. Q.11/SG12 intends to produce non-voice E-model value for data and multimedia applications.

– The service stratum, supported by the transport stratum, that may include, for example, TCP, UDP, FTP, RTP, and HTTP. The service stratum will modify and may enhance the end-to-end performance provided at the transport stratum.

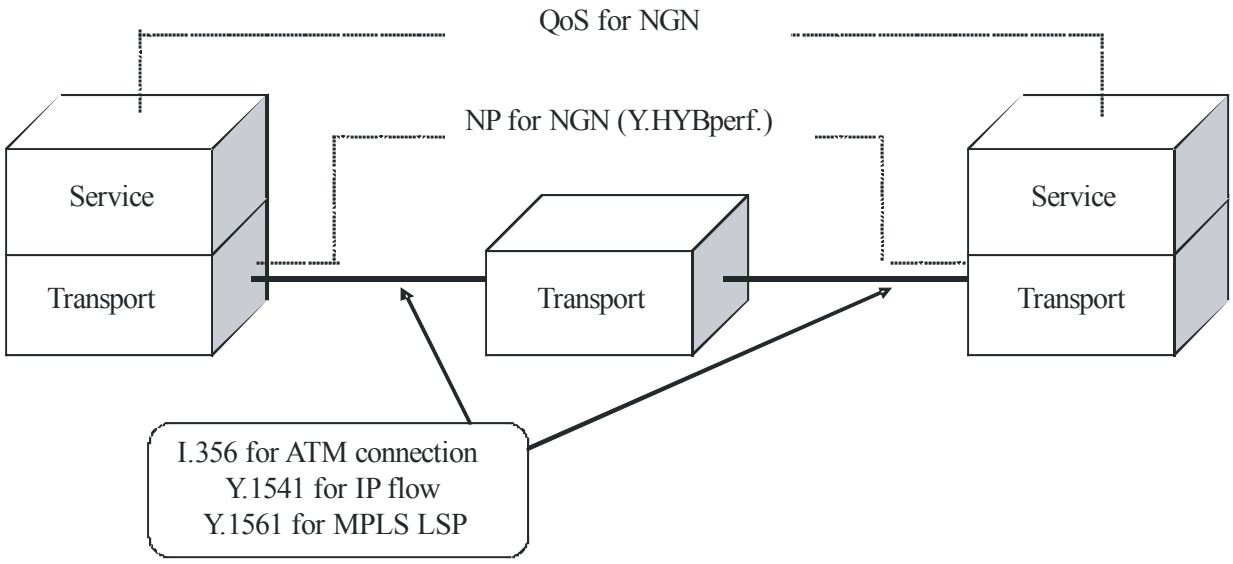


Figure 2/Draft TR-NGN-QoS – Layered model of QoS and NP for NGN

In the case of service stratum, the interface between the user and the service provider may be a man-machine interface. In the case of transport stratum, this interface corresponds to the network interface card of Service Platform (SP). As a result, some of parameters for describing the QoS of the service stratum will be different from those that describe the QoS of a transport stratum.

The parameters and objectives for the performance of service stratum are specified in other Recommendations, i.e. G.1000 and G.1010. For the transport stratum, Draft TR-NGN.NHNperf. specifies the performance of non-homogeneous networks environment.

8 Application QoS classes

ITU-T has developed well-defined Network QoS classes based on the specific technology and network, which are ITU-T Recommendation Y.1541 for IP performance, I.356 for ATM performance, etc. The coverage of those Recommendations focuses on UNI-to-UNI (Y.1541) and S/T reference points (I.356). It is important to note that, specifications for CPN (Customer Premise Network), user's terminal and user-to-user connection are beyond the scope of these Recommendations.

In ITU-T Recommendation Y.2011, NGN service should be supported by user-to-user connectivity and CPE is encompassing into the portion of interest for this purpose.

From this sense, the scope of the end-to-end NGN QoS should encompass CPN and Service Platform and describes in the figure 1 of this Draft.

NGN has to support different types of access networks. The harmonization of these specifications is needed to be able to manage end-to-end QoS in a non-homogeneous network. But different network and various Network QoS classes make a complex to the mapping when those networks are interconnected.

Application QoS provides guidance on the key factors that user-to-user connectivity from the perspective of the end-user. By considering the performance requirement of applications involving the media of voice,

video, image and text, and the parameters that govern end-user satisfaction for these applications, Application QoS is determined.

Application QoS classes will be categorized by a user's QoS requirement range and may insist of performance parameters (as in the Network QoS Classes of ITU-T Rec. Y.1540 for IP service offers).

8.1 Classification of Application QoS

A typical user is not concerned with how a particular application is supported. However, the user is interested in comparing the same service offered by different quality in terms of various ranges. This implies that Application QoS should be classified as follows;

1) Based on end-to-end user expectation of impairments and is therefore not dependent on any specific technology (network as well as application) for its validity. But the classification should be easily applied to the Network QoS classes for the purpose of implementation and operation.
2) Provides an indication of the upper and lower boundaries for applications to be perceived as essentially acceptable to the user.
3) Shows how the performance parameters (delay, delay variation, loss, etc.) and their objectives can be grouped appropriately, with implying that one class may "better" than another.

8.2 Relationship between Application QoS classes and Network QoS classes

Application QoS classes are used as the basis for deriving Network QoS classes and associated QoS control mechanisms/signalling for the underlying transport networks

The following points should be regarded to negotiation and control of NGN QoS.

1) Application needs can certainly be specified in terms of QoE/user expectations or other appropriate measures. However, provision must also be made for the request of basic (homogeneous or heterogeneous) network transport supported by a specific QoS class, with a specific traffic descriptor.
2) Network QoS classes are specified in terms of those network performance parameters that the network is able to substantially influence in the course of performing specific network functions (e.g., access, information transfer, or disengagement).
3) ITU-T has used the approach of specifying Network QoS classes. For ATM in Recommendation I.356, for Frame Relay in Recommendation X.146, for UMTS in 3GPP TS29.207 and for IP in Recommendation Y.1541.
4) In order for the above considerations to mesh in a successful delivery of Quality to the end-user – across NGN - there should be classes of application QoS that are mapped into specific Network QoS classes.

The below table shows some of the characteristics, which distinguish Application QoS classes and Network QoS classes.

Table 2/Draft TR-NGN.QoS – Distinction between Application QoS classes and Network QoS classes

Application QoS classes	Network QoS classes
Service acceptability	Network capability
Network technology independent	Network technology dependent
NGN service stratum	NGN transport stratum
Requested/selected by user: the end-to-end service	Supported by service/network provider: the end-to-end network
User-required performance	Network-supporting performance

8.3 Framework for end-to-end QoS control

Framework for end-to-end QoS service control and network QoS control describes a frame for QoS control at different levels; call control, QoS control, network control and traffic management. More detailed technologies like related protocols, procedures and functions are specified in different documents (TR-RACS, TR-e2eqos, etc.)

8.3.1 Call control

End-to-end QoS service control is negotiated/communicated end-to-end at the call control level. For this purpose, a set of Application QoS classes, and signalling requirements and flows are able to be defined. The idea is that call control protocols are enhanced with a generic end-to-end QoS service control mechanism to negotiate these Application QoS classes and associated parameters (for example, maximum delay, maximum delay variation, maximum information loss, etc.) in the service stratum of NGN strata model. Such a generic end-to-end QoS service control mechanism should be defined independent of the underlying technology (ATM or IP) and operate across network domains and including terminal characteristics to negotiate/communicate the requested application quality that will be perceived by the end-users (i.e. "mouth-to-ear"). These Application QoS classes need to be mapped to specific network (IP, ATM, and FR) QoS classes, and these mappings be made available to the appropriate QoS control elements.

8.3.2 QoS control

QoS service control is also negotiated/communicated at the vertical control level. The idea is that vertical control protocols are enhanced to negotiate/communicate the QoS parameters (for example, maximum delay, maximum delay variation, maximum information loss, etc.) in the transport stratum of NGN strata model. These QoS parameters should be defined independent of the underlying technology (ATM or IP) of the transport stratum. Vertical visibility is the point of the mappings of Application QoS classes into Network QoS classes. There must be visibility of these network QoS classes all the way up to the service stratum.

8.3.3 Network control

Network QoS is negotiated/communicated at the network control level. The idea is that network control protocols are enhanced with a mechanism to negotiate the network QoS by using corresponding network technologies (Y.1541 IP QoS classes and Y.1221 IP transfer capabilities for IP based network, I.356 ATM QoS classes and I.371 ATM transfer capabilities for ATM based network).

8.3.4 Traffic management

Network QoS is negotiated/communicated at the network level, i.e. as part of the protocols associated with the traffic transfer in the network stratum. The idea is that network QoS technologies (network QoS classes and network transfer capabilities) are used to differentiate between different types of traffic. In IP-based network stratum, IP QoS classes and IP Transfer Capabilities may be used to enhance existing IP mechanisms like DiffServ, IntServ/RSVP and MPLS/LDP.

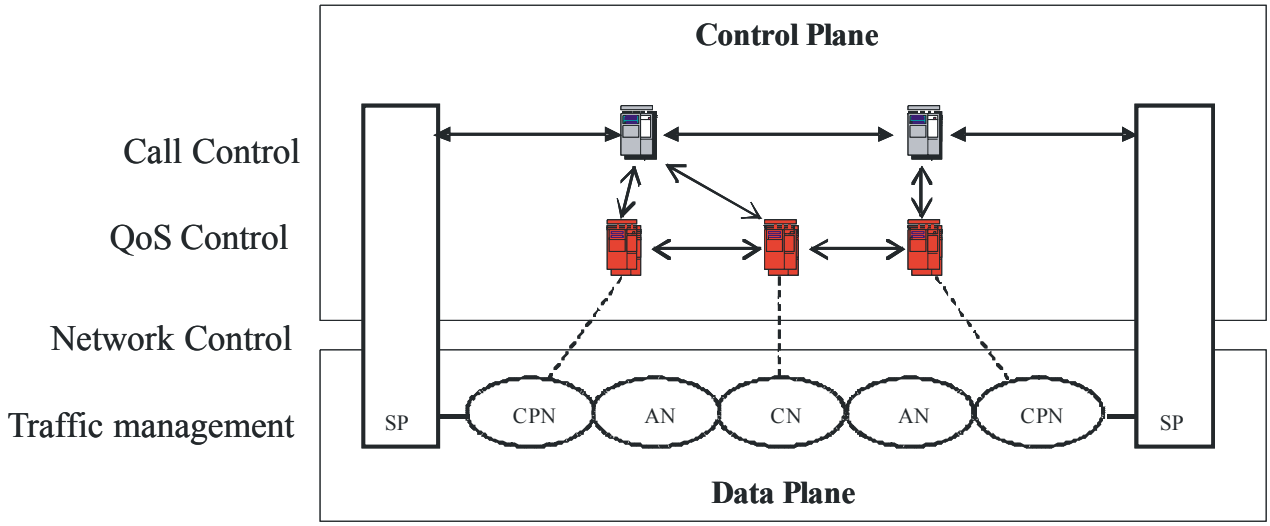


Figure 3/Draft TR-NGN-QoS – Overall configuration for end-to-end QoS control on NGN

Note : This figure shows the relationships and roles of the four components of QoS control. More details (i.e. reference points, interfaces, implemenationioal configuration, etc.) will be introduced in other documents.

8.4 Application QoS

The end-to-end communication procedure on NGN is separated into two parts; control procedure and user data transfer procedure. In order to specify Application QoS, those two aspects should be considered.

8.4.1 Control performance

Control performance covers performance aspects of two functions as follows;

- call set-up
- call disengagement

The call set-up function begins upon issuance of a set-up request signal or its implied equivalent at the interface of interest among three connectivity (MMI-MMI, MMI-MNI and MNI-MNI). It ends when either:

1) a ready for data or equivalent signal is issued to the calling participant; or

2) at least one bit of user information is input to the interface of interest (after call set-up).

It includes all activities traditionally associated with physical circuit establishment (e.g. dialling, switching, and ringing), control activities during call set-up completion (QoS control and Network control in figure 3/Draft TR-NGN.QoS) as well as any activities performed at higher protocol layers (ATM signalling, MPLS LSP signalling, etc.).

The call disengagement function is associated with each participant (among three connectivity; MMI-MMI, MMI-MNI and MNI-MNI) in a communication session: each disengagement function begins on issuance of a disengagement request signal. The disengagement function ends, for each participant, when the service/network resources dedicated to that each participation in the communication session have been released. Disengagement includes both physical circuit disconnection (when required) and higher-level protocol termination activities.

8.4.2 User data transfer performance

The user information transfer begins on completion of the call set-up function, and ends when the "disengagement request" terminating a communication session is issued. It includes all formatting,

transmission, storage, error control and media conversion operations performed on the user information during this period, including necessary retransmission within data plane.

It includes all performance aspects of NGN components; the performance of Service Platform, Customer Premise Network, Access Network and Core Network.

The parameters and objectives for the performance of user data transfer are specified in other Recommendations, i.e. G.1000 and G.1010.

9 Performance Parameters

The 3x3 performance matrix may be extended to address QoS and NP of the NGN. The performance criterion: speed, accuracy, and dependability might be supplemented with criteria such as ease-of-use. The communications functions: access, user information transfer, and disengagement might be supplemented with information storage, information translation, and brokerage functions.

Editor's Note: Figure1/G.1000 shows the extended matrix between criteria and function to facilitate identification of communications QoS criteria.

Draft NGN-MAN introduces Manageable Network concept.

Addition of billing for functions as well as reliability and security for criteria on the matrix may be considered, but those functions should be quantifiable.

Appendix I

The impact of QoE to clarify NGN QoS

I.1 User acceptability for NGN service

A service acceptability that is experienced by a user depends on the expected value from the service. When this user is using the service to take a high value and perceives the high QoS, this service can be classified as the acceptable level.

Case 1. E-mail service

Recommendation G.1010 introduces a well-defined QoS requirement for the specific service itself as follows;

> *"E-mail is generally thought to be a store and forward service which, in principle, can tolerate delays of several minutes or even hours"*

For the user who is trying to let someone know how he is, delays of hours may be acceptable. But, when this user should be required urgent information for the business purpose, the acceptable delay will be less than several seconds.

Case 2. Voice service

An acceptable target value for conversational voice prefers delays of less 150 ms in Table I.1/G.1010. Also Table 2/Y.1541 gives some guidance for the applicability and engineering of IP-based network QoS classes, and voice service (VoIP) is aligned for QoS class 0 and 1. These two classes specify delays of 100 ms and 400 ms respectively.

Voice has been traditionally considered one of the high quality-required services. But, when the user communicates a very long distance international call by Internet telephony for free, delay of 150 ms is not expected and delays of 1 second may be acceptable.

I.2 Network/service provider's viewpoint for user acceptability

QoS target value is supported by a provider should depend on the user acceptability. When the user requests the service to give a high value and expects the high QoS value, this service should be supported by the acceptable level.

For the purpose to meet user acceptability, a provider should transfer e-mail in several seconds when there is a requirement for the fast and reliable service of e-mail from a user.

The user who doesn't pay for voice service like Internet telephony, the provider doesn't need to support a high quality for that voice service. It may be dealt with the lowest quality service from provider's viewpoint.

1.4 – Network performance of non-homogeneous networks in NGN*

Summary

This draft identifies the relationship of performance aspects of the transport stratum on NGN, and specifies the mapping among IP, ATM, Frame Relay and UMTS networks' QoS classes. This mapping is intended to be the basis for engineering of networks and for agreements among network providers, and between end users and their network providers, in the NGN environment.

Table of Contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

1.4 – Network performance of non-homogeneous networks in NGN

1 Scope

This Draft has been developed to:

– describe performance aspects of the transport stratum in the Next Generation Network (NGN)

– identify general performance principles and frameworks that can be applied to the development of specific performance descriptions (e.g., methods and methodologies for performance specification, allocation, and validation);

– define the relationship among individual networks' performance which may be observed at physical interfaces between a specific network and associated service platform, and at physical interfaces between networks.

– specify the mapping among IP, ATM, Frame Relay and UMTS QoS classes, where multiple networks co-operate to realise the end-to-end connectivity desired, but the underlying network technologies differ.

2 References

The following ITU-T Recommendations contain provisions which, through reference in this text, constitute provisions of this Draft. At the time of publication, the editions indicated were valid. All Recommendations are subject to revision; all users of this Draft are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations listed below. A list of the currently valid ITU-T Recommendations is regularly published.

– Rec. E.800 Terms and definitions related to quality of service and network performance including dependability

– Rec. I.350 General aspects of quality of service and network performance in digital networks, including ISDNs

– Rec. I.356 B-ISDN ATM layer cell transfer performance

– Rec. I.610 B-ISDN operation and maintenance principles and functions

– Rec. O.181 Equipment to assess error performance on STM-N interfaces

– Rec. O.191 Equipment to measure the cell transfer performance of ATM connections

– Rec. O.211 Test and measurement equipment to perform tests at the IP layer

– Rec. X.200 Information technology - Open Systems Interconnection - Basic Reference Model: The basic model

– Rec.Y.1540 Internet protocol data communication service - IP packet transfer and availability performance parameters

– Rec.Y.1541 Network performance objectives for IP-based services

– Rec. Y.1560 Parameters for TCP connection performance in the presence of middleboxes

– Rec. Y.1561 Performance and Availability Parameters for MPLS Networks

– Rec. Y.1711 Operation & Maintenance mechanism for MPLS networks

– Rec. Y.1730 Requirements for OAM functions in Ethernet-based networks and Ethernet services

– Rec. Y.2011 General principles and general reference Model for NGNs

– Draft TR-NGN.QoS General Aspects of QoS/NP on NGN

– IETF RFC 2011 SNMPv2 Management Information Base for the Internet Protocol using SMIv2

3 Abbreviations

This Draft uses the following abbreviations:

ATM	Asynchronous Transfer Mode
B-ISDN	Broadband Integrated Services Digital Network
BRM	Basic Reference Model
CER	Cell Error Ratio
CMR	Cell Misinsertion Rate
CLP	Cell Loss Priority
CLR	Cell Loss Ratio
E-LSP	EXP-inferred-PSC LSP
FDJ	Frame Delay Jitter
FEC	Forwarding Equivalence Class
FID	Frame Identification
FLR	Frame Loss Ratio
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPDV	IP Packet Delay Variation
IPER	IP Packet Error Ratio
IPLR	IP Packet Loss Ratio
IPTD	IP Packet Transfer Delay
L-LSP	Label-only-inferred-PSC LSP
MIB	Management Information Base
MP	Measurement Point
MPE	Measurement Point E
MPN	Measurement Point N
MPLS	Multi-Protocol Label Switching

NG	Network Group
NGN	Next Generation Network
NP	Network Performance
OAM	Operation, Administration and Maintenance
OSI	Open System Interconnection
PDU	Protocol Data Unit
PHB	Per-Hop-Behaviour
PSC	PHB Scheduling Class
QoS	Quality of Service
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SECBR	Severely Errored Cell Block Ratio
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SP	Service Platform
SPR	Spurious Packet Rate
TCP	Transmission Control Protocol
TE	Terminal Equipment
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
3GPP	Third Generation Partnership Project

4 NGN Transport Network components

NGN Transport Network: In this Draft, the NGN transport network interconnects service platforms. It consists of various networks to support the transport stratum functions of NGN layered model and has user data transport functions, control functions and management functions.

Service Platform (SP): Equipment which allows users to gain access and systems to communicate through the NGN such as the terminal device (i.e., TEs : PC, Telephone, Mobile Phone, etc.) and the server (i.e., Application Server, Media Server, etc.) employed by the service application.

Network: A horizontal segment within the transport stratum that has its own specific transport protocols, for communication between two or more defined points. Networks are generally interconnected as described in Figure 1 and can be operated by different providers respectively.

Interface: A shared boundary between networks and between SP and network. An interface supports various characteristics pertaining to the functions, physical interconnections, signal exchanges and other characteristics as appropriate.

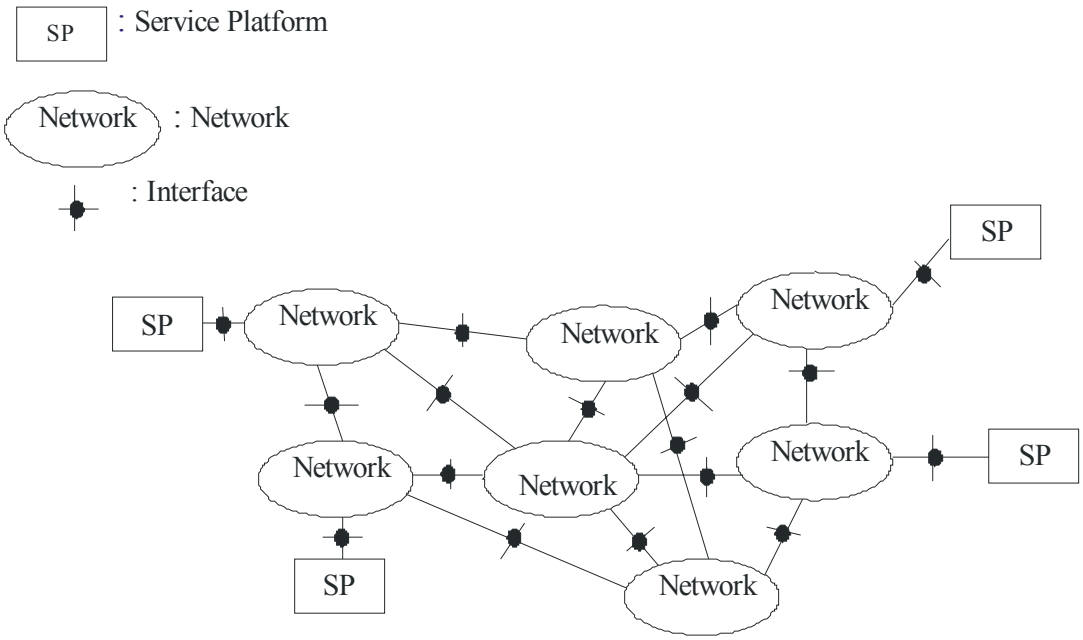


Figure 1/TR-NGN.NHNperf. – NGN Transport Network Components

5 Measurement points and measurable sections

The end points of interest for the end-to-end network performance of NGN transport network segment will be located between the SPs. For the purpose of practical measurement, the physical interface which is connected to transport function of the SP may be used as the measurement point (MP) for network performance. The ideal measurement point is an issue for further study.

Measurement point (MP): The boundary between a SP and a network or between networks at which performance reference events can be observed and measured. A network or a set of networks is measurable if it is bounded by a set of measurement points.

There are two types of MPs. MPEs are measurement points near network interface and thus are at terminal equipment. MPNs are measurement points established at the network node before and after the link cross the network.

Measurement point E (MPE): A measurement point E is located at an interface that separates a SP from an attached network component.

Measurement point N (MPN): A measurement point N is located at an interface between networks. The exact location of the MPN depends on the network type and is specified, for each network type, in the associated Recommendation (for example, I.356 for ATM, I.353 for ISDN, Y.1540 for IP, Y.1561 for MPLS, etc.)

Figure 2/TR-NGN.NHNperf. – Measurement Point E and N

In this Draft, the following sections are measurable.

Basic network portion: A network which is delimited by two MPs.

The performance of any network is measurable relative to any given unidirectional transfer of a protocol data unit (PDU). A PDU is corresponding to a specific protocol format, i.e., the cell for ATM, the packet for IP, the frame for Frame Relay or Ethernet, etc.

The ingress MP is the MP crossed by PDUs as they enter that basic network portion. The egress MP is the MP crossed by PDUs as they leave that basic network portion.

End-to-end NGN transport network: The set of networks that provides the transport of PDUs transmitted between SPs. The MPs that bound the end-to-end NGN transport network are the MPs at the SPs.

The end-to-end NGN transport network performance is measurable relative to any given unidirectional transfer of PDUs.

Network group (NG): An NG refers to any concatenation of networks.

The performance of any given NG is measurable relative to any given unidirectional transfer of PDUs. The ingress MP is the MP crossed by PDUs as they enter that NG. The egress MP is the MP crossed by PDUs as they leave that NG.

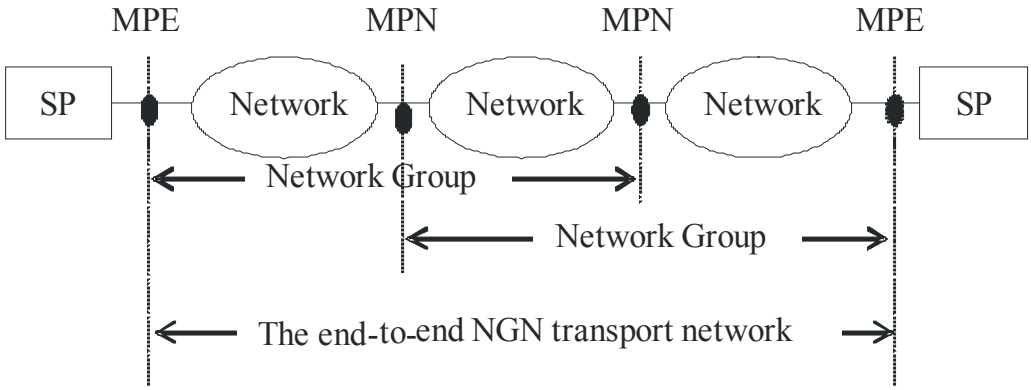


Figure 3/TR-NGN.NHNperf. – Relationships among measurable sections

6 Vertical layered model of the NGN transport network

Figure 5 shows a relationship between OSI BRM (ITU-T Recommendation X.200) and the layered protocol stack of NGN general reference model (ITU-T Recommendation Y.2011). The NGN transport network consists of many protocols to support a set of transport stratum functions of NGN layered model.

In this figure the end of the transport stratum protocol stack is denoted by the datum at layer 3 and the beginning of the service stratum protocol stack by the datum at layer 4. So, for example, in an IP-based transport network, layer 3 would be the IP layer, and layer 4 would be the TCP or UDP layer. A variety of underlying layers, layer 1 and 2, will exist depending on the underlying technologies used to support IP (e.g. ATM over SDH over Optical, Ethernet over Optical or SDH over Optical, etc.).

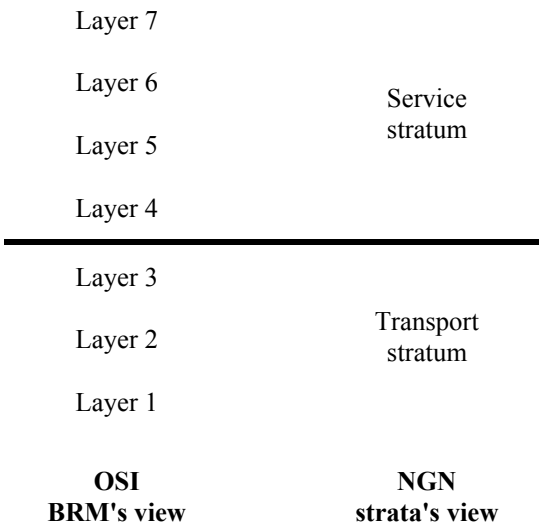


Figure 4/TR-NGN.NHNperf. – Generic layered protocol stack architecture

7 Horizontal reference configuration of the NGN transport network

Scenario 1 – Homogeneous protocol on two MPs

The same protocol is used at each end. Network performance between MPs can be evaluated by a protocol-specific performance criterion that has an end-to-end significance, even when different network types are included.

If there isn't an end-to-end significant protocol between two MPs, scenario 2 on behalf of scenario 1 should be considered.

Figure 5/TR-NGN.NHNperf. – General configuration of homogeneous protocol in MPs

NOTE – Performance for homogeneous protocols will be outside of the scope of Draft TR-NGN.NHNperf. A main target for this Draft will be cases where heterogeneous protocols are used at the two MPs.

Scenario 2 – Heterogeneous protocols on two MPs

Different protocols are used at each end. These different protocols may interwork by protocol mapping or encapsulation.

Figure 6/Y.NGN-NHNperf. – General configuration of heterogeneous protocols in MPs

8 Reference events

Reference events must be defined for the transfer of user information or control information across the measurement points. The dominant PDU of the NGN are expected to be IP packets, but each network's unique PDUs create reference events at their MPs.

Two classes of reference events are distinguished: exit events and entry events.

Exit event: An exit event occurs when a unit of user or control information crosses the MP exiting the network component or SP into the attached network component.

Entry event: An entry event occurs when a unit of user or control information crosses the MP entering the network component or SP from the attached network component.

9 Performance objectives

Scenario 1 – Homogeneous protocols

In a scenario where two interfaces of the same type are used at the involved MPs, the performance objectives and parameters can be applied to support a specific network performance without parameter mapping.

Scenario 2 – Heterogeneous protocols

In a scenario where two interfaces of different types are used at the involved MPs, the intervening networks need to be engineered to meet the performance objectives. Where performance at each interface is described in terms of its own specific parameters, parameters mapping may be used such as the mapping between cell loss ratio in ATM network and frame loss ratio in Frame Relay network defined in X.144.

10 Performance measurement

There are two basic approaches to performance measurement defined in ITU-T Recommendation M2301 (for IP performance measurement). These are "intrusive" and "non-intrusive" which equate to the terms "active" and "passive" used by the IETF (formerly, "out-of-service" and "in-service" by ITU-T Recommendation O.181, O.191, etc.).

10.1 Intrusive performance measurement

Intrusive performance measurements are made by inserting test PDUs (IP test packet of Recommendation O.211, ATM test cells of Recommendation O.191, STM test signal structure of Recommendation O.181, etc.) interleaved with the normal traffic flows/connections between two MPs. This kind of measurement allows more detailed investigation of specific performance parameters e.g. one-way delay using time stamped PDUs, effect of PDU size and number of PDUs on performance.

It should be noted that intrusive performance measurement causes additional traffic through the network so care must be taken to ensure that the use of this test does not cause congestion and the subsequent loss of customer's PDUs (IP packet, ATM cell, Ethernet Frame, etc.). Intrusive performance measurement estimates the performance seen by the existing traffic and predicts the performance that will be seen by additional traffic within limits.

The test PDU stream and the measurement period should be appropriate to the application service to be supported. The test PDU length and characteristics, and the intervals between measurement periods are separately specified in other Recommendations as follows:

– For IP performance measurement, ITU-T Recommendation O.211 "Test and measurement equipment to perform tests at the IP layer"
– For ATM performance measurement, ITU-T Recommendation O.191 "Equipment to measure the cell transfer performance of ATM connections"
– For STM performance measurement, ITU-T Recommendation O.181 "Equipment to assess error performance on STM-N interfaces"

10.2 Non-intrusive performance measurement

The performance can be assessed by interrogating all the network nodes (IP router, ATM switch, and Ethernet switch, etc.) for performance statistics and thus obtaining a real time view of the effect of the network on the traffic passing through that network.

It can also be used for maintenance purposes and/or to check the OAM procedures or MIB monitoring by SNMP applications. This kind of measurement has the advantages of minimizing impact on customer's traffic and testing every route/connection through the network.

Problems on links or network nodes can also be quickly identified. It should be noted, however, that non-intrusive measurements will sometimes be restricted to one domain or one network that has its own specific protocol.

The details of OAM PDU format, functions and monitoring methods are separately specified in other Recommendations as follows:

– For ATM OAM, ITU-T Recommendation I.610 "B-ISDN operation and maintenance principles and functions"
– For MPLS OAM, ITU-T Recommendation Y.1711 "Operation & Maintenance mechanism for MPLS networks"
– For Ethernet OAM, ITU-T Recommendation Y.1730 "Requirements for OAM functions in Ethernet-based networks and Ethernet services"
– For IP MIB monitoring, IETF RFC 2011 "SNMPv2 Management Information Base for the Internet Protocol using SMIv2"

11 Homogeneous network QoS classes

ITU recommends using on the concept of QoS classes for the network and the application level. For the network, ITU prefers the approach of QoS classes instead of individually specified performance parameters. A QoS class creates a specific combination of bounds on the performance parameters and objectives.

11.1 IP network QoS classes

ITU-T Recommendation Y.1541 introduces six (0 ~ 5) QoS classes of IP-based services in table 1/Y.1541.

The below table 1 shows IP performance values to be achieved internationally for each of the performance parameters defined in ITU-T Rec. Y.1540, with these added QoS classes.

Table 1/TR-NGN.NHNperf. – IP network QoS class definitions and network performance objectives (ITU-T Recommendation Y.1541)

Network performance parameter	IPTD	IPDV	IPLR	IPER
QoS Class 0	100 ms	50 ms	1×10^{-3}	1×10^{-4}
QoS Class 1	400 ms	50 ms	1×10^{-3}	
QoS Class 2	100 ms	U*	1×10^{-3}	
QoS Class 3	400 ms	U*	1×10^{-3}	
QoS Class 4	1 s	U*	1×10^{-3}	
QoS Class 5 (Unspecified)	U*	U*	U*	U*

U*: unspecified

11.2 ATM network QoS classes

ITU-T Recommendation I.356 specifies 5 (1 ~ 5) QoS classes of ATM-based network in table 2/I.356. It defines parameters and performance objectives for quantifying the ATM cell transfer performance of a broadband ISDN connection as below;

Table 2/TR-NGN.NHNperf. – ATM network QoS class definitions and network performance objectives (ITU-T Recommendation I.356)

Network Performance Parameter	CTD	2-pt. CDV	CLR_{0+1}	CLR_0	CER	CMR	SECBR
QoS Classes:							
Class 1 (stringent class)	400 ms	3 ms	3×10^{-7}	None	Default	Default	Default
Class 2 (tolerant class)	U	U	10^{-5}	None	Default	Default	Default
Class 3 (bi-level class)	U	U	U	10^{-5}	Default	Default	Default
Class 4 (U class)	U	U	U	U	U	U	U
Class 5 (stringent bi-level class)	400 ms	6 ms	None	3×10^{-7}	Default	Default	Default

11.3 Frame Relay network QoS classes

ITU-T Recommendation X.146 defines 4 (0 ~ 3) QoS classes of Frame Relay-based network in table 1/X.146. It defines parameters and performance objectives for quantifying the Frame Relay frame transfer performance of switched virtual connection (SVC) or permanent virtual connection (PVC) as below;

Table 3/TR-NGN.NHNperf. – Frame Relay network QoS class definitions and network performance objectives (ITU-T Recommendation X.146)

Class	FLR_c	FTD	FDJ
0	No upper bound specified on FLR_c. But FLR_c will have a practical upper bound and will not be arbitrarily bad.	No upper bound specified on FTD. But delay will have a practical upper bound and will not be arbitrarily large.	Not Applicable
1	Value < 1×10^{-3}, and 95th percentile of weighted 15-minute values < 3×10^{-3}.	95th percentile < 400 ms.	95th percentile < 52 ms
2	Value < 3×10^{-5}, and 95th percentile of weighted 15 minute values < 1×10^{-4}.	95th percentile < 400 ms.	95th percentile < 17 ms
3	Value < 3×10^{-5}, and 95th percentile of weighted 15-minute values < 1×10^{-4}.	95th percentile < 150 ms	95th percentile < 17 ms

11.4 UMTS QoS classes

3 GPP document TS 23.107 specifies UMTS QoS classes as below

Table 4/TR-NGN.NHNperf. – UMTS network QoS class definitions and network performance objectives (3GPP TS 23.107)

Traffic class	Conversational class	Streaming class	Interactive class	Background class
Maximum bitrate (kbps)	<= 16 000	<= 16 000	<= 16 000 - overhead	<= 16 000 - overhead
Delivery order	Yes/No	Yes/No	Yes/No	Yes/No
Maximum SDU size (octets)	<=1 500 or 1 502	<=1 500 or 1 502	<=1 500 or 1 502	<=1 500 or 1 502
SDU format information				
Delivery of erroneous SDUs	Yes/No/-	Yes/No/-	Yes/No/-	Yes/No/-
Residual BER	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$ (7)	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$ (7)
SDU error ratio	10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-1}, 10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-3}, 10^{-4}, 10^{-6}	10^{-3}, 10^{-4}, 10^{-6}
Transfer delay (ms)	100 – maximum value	300 (8) – maximum value		
Guaranteed bit rate (kbps)	<= 16 000	<= 16 000		
Traffic handling priority			1,2,3	
Allocation/Retention priority	1,2,3	1,2,3	1,2,3	1,2,3
Source statistic descriptor	Speech/unknown	Speech/unknown		
Signalling Indication			Yes/No	

12 Relationships between the homogeneous network performance classes

12.1 ATM network performance support of IP QoS

This clause presents an analysis of mapping IP performance parameters on top of the ATM QoS Class objectives as specified in ITU-T Rec. I.356. The purpose of this analysis is to estimate IP level performance obtained when ATM is used as the underlying transport. Because there are no routers considered in this analysis, the IP performance numbers shown here are the best that can be expected. In scenarios where intermediate routers exist, the IP performance will be worse.

Table 5/TR-NGN.NHNperf. – IP Packet Loss Ratio (IPLR) values corresponding to ATM QoS service classes 1 and 2 (IP packet size 40 bytes; all errored packets are assumed lost)

ATM QoS Class	Delivered ATM CER	Delivered ATM CLR	Resulting IPLR
1	4.00 E-06	3.00 E-07	4.30 E-06
2		1.00 E-05	1.40 E-05

Table 6/TR-NGN.NHNperf. – IP Packet Transfer Delay (IPTD) values for a flow over a national portion and an end-to-end flow

Network Portion	IPTD resulting from ATM QoS Class 1 (no delay from IP routers)
National Portion	~27.4 ms
End-to-End	400 ms

Note that Class 0 and Class 2 mean IPTD cannot be met on the 27 500 km reference connection of I.356.

The value of the Cell Error Ratio (CER) in the ATM classes is 4×10^{-6}. If IP packets are long (1500 bytes) and errored cells cause errored IP packets, the value of IP packet error ratio will be about 10^{-4}.

Cell Misinsertion Ratio (CMR) is currently specified as 1/day. The implication of CMR on SPR requires more study.

12.2 IP-based network to UMTS

The QoS translator would map Y.1541 class 0 to the UMTS conversational class, selecting the 10^{-4} value for the SDU error ratio attribute. The UMTS SDU transfer delay value (100 ms maximum) might or might not meet the example objective for the UMTS network portion (50 ms mean), depending on the SDU transfer delay distribution. The UMTS SDU error ratio value (10^{-4}) would meet the Y.1541 IPLR and IPER objectives assumed for the UMTS network portion ($5x10^{-4}$, $5x10^{-5}$), since the former parameter definition combines the Y.1541 packet loss and packet error outcomes. The UMTS conversational class requirement to "preserve time relation (variation) between information entities of the stream" would relate qualitatively to the Y.1541 IPDV objective, but the end-to-end objective would not be assured since the UMTS specification does not currently limit IPDV.

Y.1541 class 1 would be mapped to the UMTS streaming class, again selecting the 10^{-4} SDU error ratio value. The UMTS SDU transfer delay value (280 ms maximum) might or might not meet the example objective for the UMTS network portion (200 ms mean), depending on the delay distribution. The UMTS SDU error ratio value would meet the example Y.1541 IPLR and IPER objectives as described for class 0 above. The Y.1541 IPDV objective would be addressed qualitatively but without end-to-end assurance as noted above.

Y.1541 classes 2-4 could be mapped to the UMTS interactive class with a 10^{-4} SDU error ratio. The three Y.1541 classes could be mapped to different UMTS interactive class priority levels to reflect their different IPTD objectives; but these relative priorities would not provide assured quality levels. If more assured IPTD values were required, Y.1541 classes 2-4 could be mapped to the UMTS conversational or streaming class. The SDU transfer delay limit of the UMTS conversational class (100 ms maximum) might or might not meet the example IPTD objective of class 2 (50 ms mean); it would definitely meet the assumed IPTD objectives of classes 3 and 4 (200 ms and 500 ms mean, respectively). Similarly, the SDU transfer delay limit of the UMTS streaming class (280 ms maximum) might or might not meet the assumed IPTD objectives of classes 2 and 3 (50 ms and 200 ms mean respectively), but would definitely meet the assumed IPTD objective of class 4 (500 ms mean).

Y.1541 class 5 would be mapped to the UMTS background class.

The mappings suggested above are probably the most reasonable ones for the stated example, and they could meet the postulated IPLR and IPER requirements for all of theY.1541 classes. The suggested mappings would not meet the end-to-end delay requirements for some classes, and as noted, would place no quantitative bounds on end-to-end IPDV.

For comparability between Y.1541 and TS 23-107 (3GPP), the SDU should be defined to correspond to an IP packet in 3GPP specifications of QoS requirements for IP-based services. An evaluation interval of 1 minute should be used in assessing both mean delay and delay variation. Payload sizes of 160 and 1500 octets should be used in specifying and evaluating performance values.

12.3 Frame Relay network performance and ATM network performance

This description is derived from Annex C of ITU-T Recommendation X.144 “User information transfer performance parameters for public frame relay data networks”

12.3.1 Frame Loss Ratio and Cell Loss Ratio

Consider the probability of frame loss due to independently occurring cell losses. Take the probability of a single cell's loss to be as given by the CLR. The probability that a frame F_{cells} in length does not experience a lost cell is:

$$(1-CLR)^{F_{cells}}$$

The FLR due to this mechanism is the logical complement of this, namely the probability that such a frame does experience one or more cell losses, which is:

$$FLR_{CLR} = 1-(1-CLR)^{F_{cells}}$$

12.3.2 Frame Loss Ration and Cell Misinsertion Rate

Consider the probability of frame loss due to a randomly occurring misinserted cell. If the Cell Misinsertion Rate (CMR) and the Peak Cell Rate (PCR) applicable to the ATM connection are known, then the fraction of received cells that are misinserted is CMR/PCR. Take this fraction to be the probability that a single cell is misinserted. The probability that a frame F_{cells} in length does not experience a misinserted cell is:

$$(1-CMR/PCR)^{F_{cells}}$$

The FLR due to this mechanism is the logical complement of this, namely the probability that such a frame does experience one or more cell losses, which is:

$$FLR_{CMR} = 1-(1-CMR/PCR)^{F_{cells}}$$

12.4 IP QoS and MPLS QoS

12.4.1 Relationship between IP and MPLS technologies to support QoS-related aspects

IETF discussed how to support DiffServ in MPLS to provide IP QoS in RFC3270. Since DSCP is in the IP header of the packet and invisible in the MPLS forwarding process, the PHB to which the packet belongs cannot be decided by the DSCP of the packet. To tackle this problem, a method is to map the packet's PHB by the EXP field in the MPLS shim header. The EXP field can only support 8 PHBs, since it has only 3 bits. In this method, PHB is inferred according to the EXP field value, therefore, the LSP(s) set up by this method is denoted as E-LSP（EXP-Inferred-PSC LSP）.

To forward a packet, the LSP path is determined by the label, the scheduling treatment and drop priority are determined by the PHB, which is mapped by the value of the EXP field. The mapping relationship between the values of the EXE fields and the PHBs are pre-defined, and the value of the EXP field in the MPLS shim header is set by the network provider or based on the DSCP in the IP header of that packet, which does not need any additional signaling.

If more than 8 PHBs are needed or there is no MPLS shim header in the MPLS packet, the PHB to which the packet belongs can not be determined by the value of the EXP field, thus, the label of the packet is required. The LSP(s), which is set up by this method, is denoted as L-LSP (Label-Only- Inferred-PSC LSP). The PHB of the packet can be determined by both the label and the value of the EXP/CLP field. For example, the label is used to determine the LSP path and the scheduling treatment, which means, the PSC is determined by the label. When MPLS shim header is used, the EXP field of 3 bits length can establish 8 drop priorities. When ATM based MPLS is used, the CLP (cell loss priority) field of 1 bit length in the cell header can establish 2 drop priorities. This method can be used to configure the AF PHBs. Moreover, the PHB can also be solely determined by the label, which means, the label determines not only the LSP path but also the scheduling treatment and the drop priority of the packet. This method can be used to configure the EF PHB. When L-LSP is used, the mapping relationship between the labels (may also include EXP/CLP) and the PHBs is configured by the network provider or based on the DSCP in the IP header of the packet. Since the label includes both the path and PHB/PSC information, the label distribution protocol need to be extended to bind the label with both a Forwarding Equivalence Class and a PHB/PSC together, carrying the PHB/PSC information during the LSP path set up process.

12.4.2 Difference between E-LSP and L-LSP

The following table summarizes the difference between E-LSP and L-LSP:

Table 7/TR-NGN.NHNperf. – The comparison of E-LSP and L-LSP

E-LSP	L-LSP
PHB determined by the value of the EXP	PHB determined by the label, or by both the label and the value of the EXP/CLP
Need not any additional signalling to map the EXP to PHB	Use signalling to bind the label with the PHB/PSC during the LSP set up process
Use the MPLS Shim header	Use the MPLS Shim header or link layer header
Support up to 8 PHBs, all these PHBs can be used in the same LSP	Support arbitrary number of PHBs, one LSP can use only one PHB/PSC
Label only carry the path information, increase the utilization of labels resource and simplify the states maintained	Label carries both the path and the scheduling treatment information, use more labels and maintain more states

Since E-LSP can support more PHBs, it can reduce the total number of LSP in the network. E-LSP can also reduce the resource of labels, since the PHB information is not included in the labels, it can simplify the structure of the label. Moreover, the PHB of the packet is solely determined by the value of the EXP field, which is just like the tradition DiffServ mechanism in which the PHB is determined by the DSCP, so the E-LSP is easy to be realized and does not need any additional signalling or extend the existing signalling.

The advantage of L-LSP is that it can be used in the network environment which does not support the MPLS Shim header and support arbitrary number of PHBs. Since each LSP just adopts only one PHB/PSC, Different PHB can use different LSP path to forward and so to provide better granularity of QoS control ability. For example, the L-LSP forwarding the EF traffic can be routed through the links which have low delay, and the L-LSP forwarding the AF traffic can be routed through the links which have rich bandwidth resource but relative high delay.

In a word, the specific network environment needs to be considered carefully to choose E-LSP and L-LSP or use both of them.

13 Heterogeneous network QoS classes

13.1 QoS class mapping rationale

For each of the most relevant technologies a small yet versatile set of QoS classes has been standardised (Frame Relay, ATM, UMTS and IP).

– It is stipulated that these network QoS classes are specific for a network technology, i.e. there are different sets of QoS classes for ATM, for UMTS, for Frame Relay and for IP.

– Each set consists in an intentionally small number of classes to facilitate broad support by and easy interworking between network providers.

– Each set is sufficiently versatile to support a broad range of applications. Each set of classes includes at least one QoS class which commits to a low loss, low delay and low delay variation, which is expected to be of interest for interactive real-time applications; QoS class 1 & 0 of Y.1541, QoS class 1 of I.356, QoS class streaming & conversational of 3GPP TS 23.107 and QoS class 3 & 2 of X.146. Each set also includes an unspecified (best-effort) class; QoS class 5 of Y.1541, QoS class 4 of I.356, QoS class background of 3GPP TS 23.107 and QoS class 0 of X.146.

The defined QoS classes, as currently defined, also support paths which are a concatenation of network sections which use a same technology but are under the responsibility of different network providers. The specified end-to-end network performance objectives are fully applicable. It is to the network provider's discretion how and with which technology that section is realised. For example an IP path for which an IP QoS class has been agreed, may be implemented using ATM; the IP QoS class performance objectives still apply.

Where different domains use different technology (with different network interfaces) which are concatenated by means of interworking functions, is strictly not covered by the QoS classes as currently defined.

Nevertheless an end-to-end network performance bound may be obtained. It is expected that the realised performance on such a concatenated path is not worse than if the end-to-end path were implemented as a single technology path in IP. In other words, the IP network performance objectives provide an upper bound for the mixed-technology case.

It is expected that interworking between different technologies does not to require significant additional delay allocation. Care should be taken when interworking between a packet technology and ATM; the additional shaping delay can be limited for small packets and suitable settings (e.g. PCR) for the ATM connection.

13.2 Mapping among IP, ATM, Frame Relay and UMTS QoS classes

The section treats the case where multiple networks co-operate to realise the end-to-end connectivity desired, but the underlying network technologies differ.

In principle, the ingress-to-egress node performance and capacity information may be available regardless of the underlying network technology, whether it is IP, ATM, UMTS, Frame Relay, etc. QoS Classes may best be mapped among these networking technologies as follows:

Table 8/TR-NGN.NHNperf. – Mapping among QoS Classes

IP QoS Class	ATM QoS Class	FR QoS Class	UMTS QoS Class
0	1(note 1)	3	Conversational
1	1(note 1)	2	Streaming
2	2 & 3(note 2)	1(note 2)	Interactive
3			
4			
5	4	0	Background

Note 1: ITU-T Recommendation I.356 has developed to specify QoS classes and network performance objectives for ATM cell transfer performance. The most stringent ATM cell transfer delay objective (400 ms) is achievable on the long distance ATM connection (i.e., 27,500 km covering international connection). And ITU-T Recommendation Y.1541 defines 100 ms IP packet transfer delay on the QoS class 0 and 400 ms on the QoS class 1.

In the case that IP QoS class 0 & 1 are mapped into ATM QoS class, ATM QoS class 1 is easily selected for both classes to support the required delay objectives. On the other hand, when ATM QoS class 1 is mapped into IP QoS classes, an appropriate class should be introduced for each. IP QoS class 1 IPTD (400ms) is the same of ATM QoS class 1 CTD (400ms). But, obviously, 100 ms IPTD requirement of IP QoS class 0 cannot always be met on the 27,500 km.

From this sense, it should be noted that the delay objectives of a class do not preclude a network provider from offering services with shorter delay commitments. Any such commitment should be explicitly stated.

Every network provider will encounter these circumstances (either as a single network, or when working in cooperation with other networks to provide the UNI-to-UNI path in IP-based network), and the mapping of QoS classes between ATM and IP in this table provides and is selected achievable IP QoS classes as alternatives

Note 2: These QoS classes have the performance objectives which is more tolerable than the stringent QoS classes, especially on delay variation- and loss-related performance parameters. It is not certain that an individual QoS class should be mapped to each other (IP QoS classes 2, 3 & 4 and ATM QoS classes 2 & 3). This is for further study.

14 Security considerations

This Draft does not specify a protocol, and there are limited areas where security issues may arise. Most of the issues are related to performance measurement and are identified in the security considerations section of ITU-T Draft TR-PMM. However, imperfect QoS class mapping can result in promotion or demotion of the QoS class intended, which may have unanticipated consequences.

SECTION 2

RELEASE 1 DELIVERABLES

WORKING GROUP 1
DELIVERABLES

SERVICE REQUIREMENTS

2.1 NGN Release 1 scope (*Status A*)

2.2 NGN Release 1 requirements (*Status A*)

2.1 – NGN Release 1 Scope*

Summary

This document provides a high level description of NGN Release 1 and its scope in terms of supported services and capabilities. This document describes high level objectives, in terms of the services and capabilities. Further documents provide the detailed requirements for NGN Release 1.

Key words

NGN, NGN Release 1 Scope, NGN Release 1 environment, NGN services, NGN Release 1 services, NGN Release 1 Capabilities, Service Support Capabilities, Service Enablers, open service environment, Use Cases

Table of Contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

2.1 – NGN Release 1 Scope

Introduction

NGN Focus Group has adopted a release-based approach for the production of NGN Technical Specifications/Reports, with the scope of each release clearly defined and with clear deadlines for completion.

NGN Focus Group develops stage 1 and 2 of NGN Release 1 specifications.

This document gives a description of Release 1 in terms of the overall requirements and high level overview of the functional features to be addressed.

In order to fulfil the general goals, objectives and principles of an NGN, identified in particular in Recommendations Y.2001 [Y.2001] and Y.2011 [Y.2011], this document focuses on key capabilities, while ensuring an architectural flexibility to support future enhancements and releases with minimum impact. Release 1 is the first step towards a comprehensive framework of services, capabilities and network functions that constitute an NGN, as described in [Y.2001].

This framework is expected to deliver services tailored to all user's and service provider's requirements so that they satisfy a wide range of needs and human capabilities. There is strong pressure to design the NGN to enable everyone to use it.

Specific realisations of NGN Release 1 may extend beyond the services and capabilities described in this document. Service provider requirements may drive a particular set of services and capabilities to be supported in a particular network.

The document is organised as follows:

– section 2 provides references;
– section 3 provides terms and definitions;
– section 4 provides the scope of NGN Release 1 in terms of environment and key aspects;
– section 5 provides a list of NGN Release 1 services;
– section 6 provides a list of NGN Release 1 service capabilities

1 Scope

This document provides a high level description of NGN Release 1 and its scope in terms of supported services and capabilities.

This document describes high level objectives, in terms of the services and capabilities. Further documents provide the detailed requirements for NGN Release 1.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Specification. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Specification are therefore encouraged to investigate the possibility of applying the most recent edition of the

Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[E.351] TU-T Recommendation E.351, Routing of multimedia connections across TDM-, ATM-, and IP-based networks

[M.3050] TU-T Recommendation M.3050, Enhanced Telecommunications Operations Map

[X.805] ITU-T Recommendation X.805, Security architecture for systems providing end-to-end communications

[Y.2001] ITU-T Recommendation Y.2001: General overview of NGN functions and characteristics

[Y.2011] ITU-T Recommendation Y.2011: General Reference Model for Next Generation Networks

[Y.101] ITU-T Recommendation Y.101: GII terminology: Terms and definitions

[Y.110] Global Information Infrastructure principles and framework architecture

[Z.100] ITU-T Recommendation Z.100, Specification and Description Language (SDL)

[ETSI-TSPN] ETSI TISPAN NGN Release 1 Definition

[FGNGN-FRA] ITU-T FGNGN deliverable FGNGN-OD-244 “Functional requirements and architecture of the NGN”

[FGNGN-IFN] ITU-T FGNGN deliverable FGNGN-OD-245, Draft FGNGN-IFN (IMS for Next Generation Networks)

[FGNGN-RACF] ITU-T FGNGN deliverable FGNGN-OD-241, Resource and admission control functions

[FGNGN-REQ] ITU-T FGNGN deliverable FGNGN-OD-252, NGN Release 1 Requirements

[FGNGN-SEC] ITU-T FGNGN deliverable FGNGN-OD-254, Guidelines for NGN security

[FGNGN-TERM] ITU-T FGNGN deliverable FGNGN-OD-261, Terminological framework for NGN.

3 Terms and definitions

3.1 Definitions

This document uses the following terms:

Application network interface: provides a channel of interactions and exchanges between “3rd Party Application Providers” and NGN elements offering needed capabilities and resources for realization of value added services.

Customer: The Customer buys products and services from the Enterprise or receives free offers or services. A Customer may be a person or a business. Source for definition is [M.3050].

Home network: The network associated with the operator/service provider that owns the subscription of the customer.

Internet: A collection of interconnected networks using the Internet Protocol which allows them to function as a single, large virtual network. Source for definition is [Y.101].

Mobility: The ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment. The degree of service availability may depend on several factors including the Access Network capabilities, service level agreements between the user's home network and the visited network (if applicable), etc. Mobility includes the ability of telecommunication with or without service continuity. Source for definition is [Y.2001]

Network node interface: The interface of a network node (node as defined in Rec. E.351) which is used to interconnect with another network node. Note: This interface is not constrained to a single protocol. In the case of interconnection between an NGN network and a legacy network it will also depend on the type of network connecting to NGN and where the mediation is performed if any.

Nomadism: Personal or Terminal mobility without service continuity.

Personal mobility: His is the mobility for those scenarios where the user changes the terminal used for network access at different locations. The ability of a user to access telecommunication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile. Source for definition is [FGNGN-TERM].

Service: A set of functions and facilities offered to a user by a provider. Source for definition is [Z.100].

Service continuity: He ability for a user to maintain an ongoing service during mobility.

Subscriber: The person or organization responsible for concluding contracts for the services subscribed to and for paying for these services. Source for definition is [M.3050]. Note: See also definition of customer.

Terminal mobility: his is the mobility for those scenarios where the same terminal equipment is moving or is used at different locations. The ability of a terminal to access telecommunication services from different locations and while in motion, and the capability of the network to identify and locate that terminal.

User: The user is the actual user of the products or services offered by the Enterprise. The user consumes the product or service. Note: See also definition of end user from [M.3050].

Visited network: he network that is local to the customer in a roaming configuration.

3.2 Acronyms and Abbreviations

This document uses the following abbreviations and acronyms:

ANI Application network interface

API Application Programming Interface

ATM Asynchronous Transfer Mode

BBC Basic Bearer Capability

CUG	Closed User Group
DM	Device Management
DRM	Digital Right Management
DVB	Digital Video Broadcast
EBC	Enhanced Bearer Capability
ENUM	TElephone NUmber Mapping
FTTH	Fiber to the Home
GPS	Global Positioning System
HDTV	High Definition Television
IM	Instant Messaging
IMS	IP Multimedia Subsystem
IN	Intelligent Network
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
ISDB	ISDN Digital Broadcast
MMS	Multimedia Message Service
MOD	Music on Demand
NAAF	Network Access Attachment Functions
NAPT	Network Address Port Translation
NGN	Next Generation Network
NNI	Network node interface
OAM	Operation, Administration, Maintenance
OMA	Open Mobile Alliance
OSA	Open Service Access
OTA	Over the Air
OTN	Over the Network
OSE	OMA Service Environment
PBX	Private Branch Exchange
PDA	Personal Digital Assistant
P-NNI	Private Network node interface
PoN	Push to talk over NGN
PSTN	Public Switched Telephone Network
QoS	Quality of Service

RACF	Resource Admission Control Functions
RFID	Radio Frequency Identification
SCF	Service Capability Features
SCS	Service Capability Servers
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
TDM	Time Division Multiplex
URL	Uniform Resource Locator
VOD	Video on Demand
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
xDSL	Various types of Digital Subscriber Line

4 NGN Release 1 environment overview

The NGN framework shall support advanced architecture objectives [FGNGN-FRA] for the offer of a comprehensive set of services over a unifying IP layer network. The transport stratum should support a multiplicity of access transport functions and a variety of mobile and fixed terminal types. Services are separable from the transport stratum into a service stratum and are not limited to those provided by the "home network", but may be obtained from multiple service providers and third parties. Services shall be able to traverse multiple providers' networks.

The functions that are supported by NGN release 1 specifications are illustrated in figure 1. This document provides an overview of some major components from this figure. The details of this figure, including the interfaces between NGN and user functions, between NGN and network nodes, and between NGN and 3rd party Application providers, are described in [FGNGN-FRA].

In Release 1 all services are carried over IP although IP itself may in turn be carried over a number of underlying technologies, such as ATM, Ethernet, etc. Release 1 assumes IPv4 or IPv6 networking at packet interconnection points and packet network interfaces and therefore focuses on the definition of IP packet interfaces.

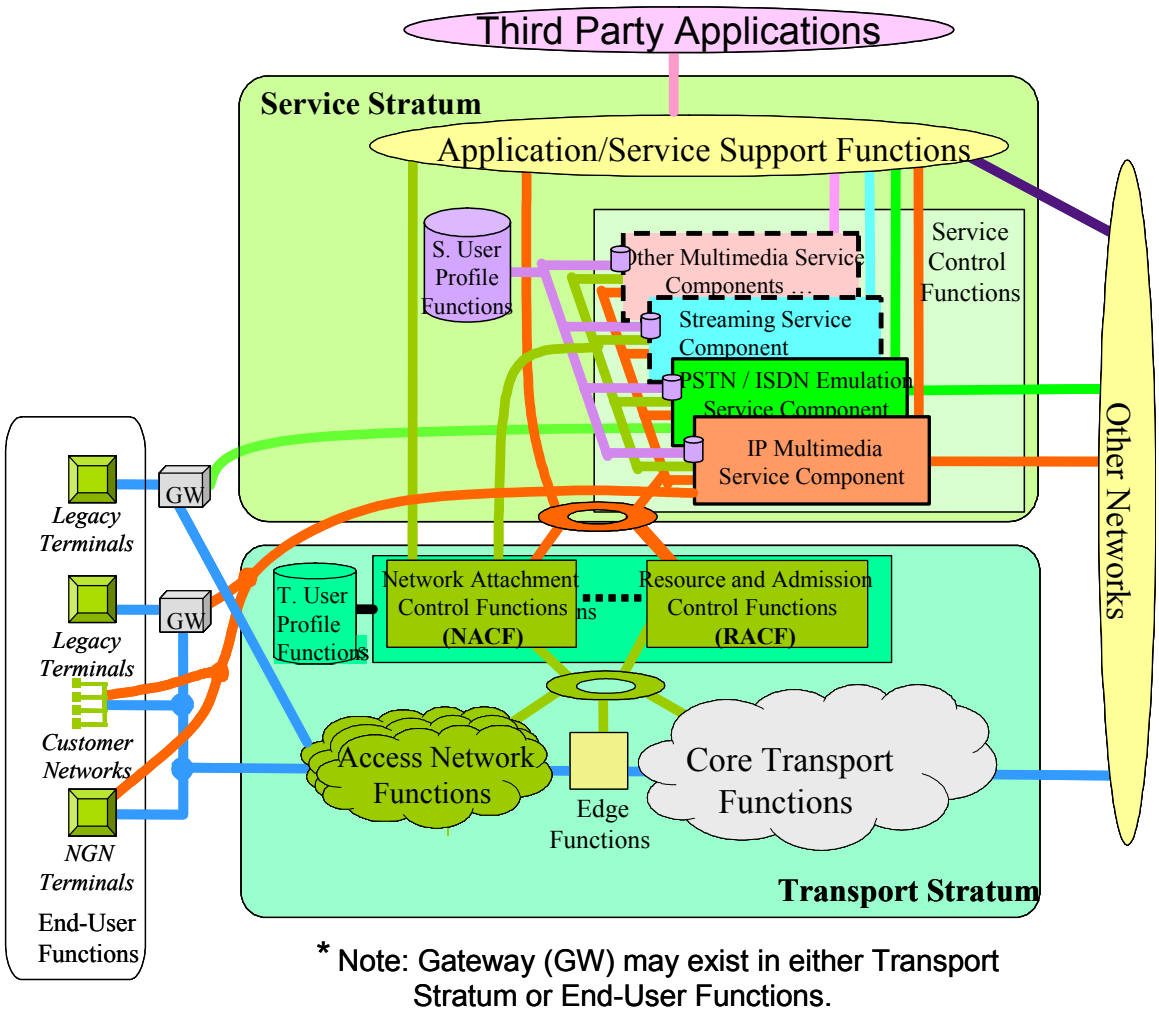


Figure 1 – Transport and Service Configuration of the NGN

4.1 Service Stratum

4.1.1 IP Multimedia Service Component

IP Multimedia Service Component is a service component within the Service Stratum based on the capabilities of the IP Multimedia Subsystem (IMS) [23.228, TIA-873]. It has been a starting point for the definition of Release 1 to leverage the capabilities of the IMS. To support the heterogeneous access transport environment of Release 1 the capabilities of the IMS need to be extended. The IMS functionality for NGN Release 1 employs SIP based service control [FGNGN-IFN].

NGN Rel.1 shall maintain full compatibility with 3GPP/3GPP2 IP connectivity access transport functions (e.g. IP-CAN) and terminals.

4.1.2 PSTN/ISDN Emulation Service Component

Release 1 defines a service component to support PSTN/ISDN replacement scenarios, with full interoperability with existing (legacy) PSTN/ISDN networks. This component fully supports legacy (PSTN/ISDN) interfaces to customer equipment and provides the user with identical services and experience to that of the existing PSTN/ISDN.

4.1.3 Service Framework and Application Support

NGN will help in the creation and offering of new services. As the number, sophistication, and degree of interworking between services increases, there will be a need for providing more efficiency and scalability for network services. Therefore, NGN applications and user services should be able to use a flexible service and application provisioning framework.

Such a framework should enable application providers, both NGN internal and 3rd party, to implement value added services that make use of network capabilities in an agnostic fashion. Network capabilities and resources that are offered to applications are defined in terms of a set of capabilities inside this framework and are offered to 3rd party applications through the use of a standard application network interface (ANI). This provides a consistent method of gaining access to network capabilities and resources and application developers can rely on this consistency when designing new applications.

The internal NGN application providers may make use of the same network capabilities and resources that are used by 3rd party Application Providers.

NGN Release 1 should support the following three classes of value added service environments:

- IN-based service environment – Support for Intelligent Network services. Examples of ANI specific protocols for this environment include IN Application Protocol [Q.1236], Customised Application for Mobile network Enhanced Logic (CAMEL) [Q.1200][22.708] and Wireless Intelligent Network (WIN) [TIA-771];
- IMS-based service environment – Support for IP Multimedia Subsystem based service environment. Examples of ANI specific interfaces include ISC, Sh, Dh, Ut, Ro, Rf, Gm, and Mb [23.228].
- Open service environment – Support for open service environments. Examples of this environment using ANI include OSA/Parlay, Parlay X, OMA [OSA-Parlay-4] [OSA-Parlay-5] [OSA-Parlay-X] [OMA-OSE].

4.2 Transport Stratum

4.2.1 Access Transport Functions

NGN Release 1 supports access transport functions of diverse technologies and capabilities. NGN communications and services are available to all qualified users requesting those services regardless of the type of access transport function technology.

An access transport function provides IP connectivity, at the transport stratum, between the End-user functions and the NGN core transport functions as described in [FGNGN-FRA]. An access transport function for Release 1 has capabilities to provide IP connectivity to NGN core transport functions within the NGN Release 1 time frame. These access transport functions should support services identified for NGN Release 1. The following is a non-exhaustive list of candidate technologies to implement access transport functions for NGN Release 1.

– Wireline
  - XDSL: this includes ADSL [G.992.1] [G.992.3] [G.992.5], SHDSL [G.991.2] and VDSL [G.993.1] [G.993.2] transport systems and supporting connection/multiplexing technologies.
  - SDH dedicated bandwidth access. [G.707]
  - Optical access: this covers point to point [IEEE 802.3ah (100Base-LX/BX)] and xPON transport systems such as BPON [G.983 series], GPON [G.984 series], EPON (Gigabit EPON is sometimes called GEPON) [IEEE 802.3ah (1000Base-PX)]
  - Cable networks: cable networks based on PacketCable Multimedia specifications [5] as another type of access transport function. [J.179]

- LANs: LANs using either coaxial or twisted pair cable, including 10Base-T Ethernet [IEEE 802.3], Fast Ethernet [IEEE 802.3u], Gigabit Ethernet [IEEE 802.3z], 10 Gigabit Ethernet [IEEE 802.3ae].
- PLC(Power Line Carrier) networks: the PLC network transmits and receives data over the power line.

– Wireless

- IEEE 802.X Wireless networks [WLAN][BWA].
- The NGN transport stratum should support 3GPP/3GPP2 PS domain with no modification to the access transport functions. In this sense NGN supports any 3GPP or 3GPP2 IP-CAN. NGN does not support the CS domain as an access transport technology.
- Broadcast networks (3GPP/3GPP2 Internet Broadcast/Multicast, DVB, ISDB-T) [BDCST]

4.2.2 NGN core transport functions

NGN core transport functions provide IP connectivity, at the transport stratum, across the core network. For a more detail description, see [FGNGN-FRA].

4.2.3 Network Attachment Control Functions

The Network Attachment Control functions (NACF) provide registration at the access level and initialization of end-user functions for accessing the NGN services. The functions provide network-level identification/authentication, manage the IP address space of the access network functions, and authenticate access sessions.

4.2.4 Resource and Admission Control Functions

Application functions supporting different NGN services interact with the Resource and Admission Control functions (RACF) to provide capabilities for control of NGN transport resources, including QoS control and NAPT/FW traversal control.

The RACF interact with transport functions to control one or more of the following functionalities in the transport layer: packet filtering; traffic classification, marking and policing; bandwidth reservation and allocation; network address and port number translation; Anti-spoofing of IP addresses; Network Address and Port Translation (NAPT), firewall traversal; and usage metering.

The RACF interact with NACF, including network access registration, authentication and authorization, parameters configuration, to check user profiles and Service Level Agreement (SLA) held by them.

4.3 Network Node Interfaces (NNIs)

4.3.1 Interconnection and NNIs

As well as interconnection between multiple NGN administrative domains, the NGN is also required to support access to and from other networks that provide communications, services and content, including the secure and safe interconnection to the Internet.

NGN Release 1 provides support for services across multiple NGN administrative domains. Interoperability between NGN administrative domains shall be based on defined interconnect specifications.

4.3.2 NNIs to non-NGNs

Release 1 supports interconnection to other IP networks and by implication to any IP based network that complies to the NGN interconnection protocol suite.

Release 1 supports direct interconnection with the PSTN/ISDN by means of Interworking functions that are implemented within the NGN.

Interoperability between NGN and non-NGN shall be based on defined interconnect specifications.

Table 1 lists the candidate interconnection interfaces including a non-exhaustive list of protocols that may be supported in Release 1 and may also be applied as P-NNIs to Enterprise networks. The following is the list of candidate networks that will interconnect using NNIs to the NGN:

- Internet
- Cable Networks
- Enterprise Networks
- Broadcast Networks
- PLMN Networks
- PSTN/ISDN Networks

Table 1 – Release 1 (P-)NNIs for interconnect to other networks

Type of Networks	Signaling Interface	Bearer Interface
Circuit-based Networks	ISUP	TDM
IP–based Networks	SIP (session control), IPv4, IPv6, MIPv4, MIPv6, BGP, HTTP	IPv4, IPv6, MIPv4, MIPv6, RTP, RTCP

4.3.3 NNIs between NGNs

NGN release 1 allows for the partition of the NGN into separate administrative domains. Interfaces on a trust boundary between domains need to support various functionalities to enable robust, secure, scaleable, billable, QoS-enabled, and service transparent interconnection arrangements between network providers. Some of the trusted domain's internal information may be removed across a trust boundary, for instance to hide the user's private identity or network topology information.

4.4 User Profile Functions

Release 1 defines the User Profile Functions, which provide capabilities for managing User Profiles and making the User Profile information available to other NGN functions. A User Profile is a set of attribute information related to a user. The User Profile Functions provide the flexibility to handle a wide variety of user information. Some of the user profile models which may inform the design of the User Profile Functions include:

- 3GPP Generic User Profile (GUP)
- 3GPP2 User Profile
- W3C Composite Capabilities/Preference Profile (CC/PP)
- OMA User Agent Profile
- 3GPP/ETSI Virtual Home Environment
- Parlay Group – User Profile Data

As shown in figure 1, the User Profile Functions support the identified Service and Control Functions in the Service Stratum, as well as the Network Access Attachment Functions in the Transport Stratum. This central role for the User Profile Functions is natural, since users and their service requirements are the driving forces behind the existence of the network itself.

4.5 End-User Functions

Customers may deploy a variety of network configurations, both wired and wireless, inside their customer network. This implies, for example, that Release 1 will support simultaneous access to NGN through a single network termination from multiple terminals connected via a customer network.

It is recognized that many customers deploy firewalls and private IP addresses in combination with NAPT. NGN support for user functions is limited to control of (part of) the gateway functions between the end user functions and the access transport functions. The device implementing these gateway functions may be customer or access transport provider managed. Management of customer networks is however outside of the scope of Release 1. As a result customer networks may have a negative impact on the QoS of an NGN service as delivered to user equipment.

Implications of specific architectures of customer networks on the NGN are beyond the scope of Release 1. Customer network internal communications do not necessarily require the involvement of the NGN transport functions (e.g., IP PBX for corporate network).

4.5.1 User equipment

The NGN should support a variety of user equipment.

This includes gateway + legacy terminals (e.g. voice telephones, facsimile, PSTN textphones etc.), SIP phones, soft-phones (program on PC), IP phones with text capabilities, set-top boxes, multimedia terminals, PCs, user equipment with intrinsic capability to support a simple service set, and user equipment that can support a programmable service set.

It is not intended to specify or mandate a particular NGN user equipment type or capability, beyond compatibility with NGN authentication, control and transport protocol stacks.

NGN supports a mobile terminal that is fully compliant with 3GPP specifications only when directly connected through a 3GPP IP-CAN. Release 1 may not support 3GPP mobile terminals when they are not directly connected through a 3GPP IP-CAN.

Release 1 should allow the simultaneous use of multiple types of access transport functions by a single terminal, however there is no requirement to co-ordinate the communication. Such terminals may therefore appear to be two or more distinct terminals from the network point of view.

The user equipment should enable interface adaptation to varying user requirements, including the needs by people with disabilities, for connection with commonly provided user interface devices.

5 NGN Release 1 services

It has to be noted that compliance of a given network environment to NGN Release 1 does not mean support of all possible combinations of services (as well as capabilities and network configurations) described in this document. It is recognized that a specific realisation of NGN may be constituted by an arbitrary set (or superset) of the above services (as well as capabilities and network configurations).

The services listed in this section are provided as examples of the types of services supported by NGN Release 1.

5.1 Multimedia services

NGN Release 1 supports both real time conversational communications (beyond voice) and non-real time communications. This includes, but is not limited to, the end to end (user to user) delivery of

communications utilising more than one media. Non-real time services may be supported using one or many media streams or using other delivery protocols not directly related to multimedia sessions.

– Real-time Conversational Voice services (interoperable with the existing public-switched telephone network (PSTN) and with mobile networks).

– Messaging services such as IM, SMS, MMS, etc.

  • Instant messaging (IM) : A type of communications service that enables the user to create a kind of private chat room with another individual in order to communicate in real time, analogous to a telephone conversation but using text-based, not voice-based, communication, for example, through automatic transmission at short time intervals[T.140] or in a message-wise mode. Typically, the IM system alerts the user whenever somebody on his private list is online, the user can then initiate a chat session with that particular individual.

– Push to talk over NGN (PoN) – Push to talk services using an NGN core network that might be serving multiple types of access transport functions [OMA- PoC].

– Point-to-Point interactive multimedia services, e.g. interactive real-time voice, real-time text, real-time video (e.g. IP videotelephony (as per [F.724])), total conversation [F.703], voice telephony with text using [T.140], whiteboarding etc.

– Collaborative interactive communication services: support of low-latency multimedia conferencing with file sharing and application sharing, e-learning, gaming.

– Content delivery services: Delivery of video and other media streams to users, such as Radio and Video streaming, Music and Video on Demand, (Digital) TV Channel Distribution, financial information distribution, professional and medical image distribution, electronic publishing.

– Push-based services - Services provided via push capability (e.g., IP multimedia services, MMS, and new services including public safety, government, corporate Information Technology etc.)

– Broadcast/Multicast Services.– These types of services enable the optimization of network resources by using broadcast/multicast mechanisms for the delivery of content streams to multiple users and groups. Examples of such services are as follows: replays of scoring plays at sporting events to persons at the events or those unable to attend the event; concerts or other streaming audio or video programming, reporting of alert conditions for emergency community notification services; advertising of movie trailers in an area around the theater that is showing the movie. [22.146][BWA]

– Hosted and transit services for enterprises (IP Centrex, etc.)

– Information services, such as cinema ticket information, motorway traffic status, advanced push services, etc.

– Location-based services, such as tour guide service, user service, assistance service for disabled persons and emergency call.

– Presence and general notification services: The presence service provides access to presence information to be made available to other users or services. Presence is a set of attributes characterising the current properties (e.g., status, location, etc.) of an entity. An entity in this respect is any device, service, application, etc., that is capable of providing presence information. Availability, on the other hand, denotes the ability and willingness of an entity to communicate based on various properties and policies associated with that entity -- e.g., time of day, device capabilities, etc. The terms presence and availability are almost always used together to provide a complete set of presence information. NGN users shall be able to be both the suppliers of presence information (sometimes called presentities), as well as the requesters of presence information (watchers).

– 3GPP Release 6 and 3GPP2 Release A OSA-based services

5.1.1 General principles for codecs use in NGN

The NGN should support different types of codecs that include audio, text and video capabilities. It is recognized that some codecs play an important role in existing and emerging networks for audio and video services. A minimal list of codecs shall be supported by the NGN, but network support of additional codecs is not prevented.

Transcoding shall be performed to provide end-to-end service interoperability when needed and should be avoided wherever possible.

Codecs negotiation shall be supported between NGN entities (terminals, network elements).

5.2 PSTN/ISDN Emulation services

5.2.1 General aspects for PSTN/ISDN Emulation

PSTN/ISDN Emulation provides PSTN/ISDN service capabilities and interfaces using adaptation to an IP infrastructure.

It is anticipated that the NGN will support an orderly and market-driven evolution for the support of both legacy equipment and the PSTN/ISDN service set. Key scenarios of this feature are:

- PSTN/ISDN Replacement (in whole or in part)
- Support for legacy terminals connected to the NGN.

5.2.2 Terminals for PSTN/ISDN Emulation

PSTN/ISDN Emulation services should support legacy terminals. The user should have the identical experience as provided by the legacy PSTN/ISDN services.

Legacy terminal support includes connection via terminal adaptation and the access transport function.

5.2.3 Target services for PSTN/ISDN Emulation

The PSTN/ISDN service set is not re-defined by NGN. It is assumed that a PSTN/ISDN call server may provide an ISUP or other PSTN/ISDN call model, and NGN will provide packet-based signalling transport and interworking.

Not all service capabilities and interfaces have to be present to provide an emulation of a particular PSTN/ISDN network.

Although PSTN/ISDN Emulation supports all PSTN/ISDN services, individual service providers may choose to deploy PSTN/ISDN Emulation with support for only a sub-set of PSTN/ISDN services.

5.3 PSTN/ISDN Simulation services

5.3.1 General aspects for PSTN/ISDN Simulation

PSTN/ISDN Simulation provides PSTN/ISDN-like service capabilities using session control over IP interfaces and infrastructure.

PSTN/ISDN Simulation uses the capabilities of the IP Multimedia Service Component to provide these services.

It is not assumed that simulated services will be identical to those in the PSTN/ISDN, and they need not necessarily utilise PSTN/ISDN call models or signalling protocols. PSTN/ISDN Simulation is provided at the user interface, which may be different from PSTN/ISDN.

5.3.2 Terminals for PSTN/ISDN Simulation

NGN Release 1 should support a set of PSTN/ISDN-like services for advanced terminals such as IP-phones, or for terminal adaptations connected to legacy terminals.

5.3.3 Target services for PSTN/ISDN Simulation

ISDN bearer and supplementary services are described and defined in I.230 and I.250 series of ITU-T Recommendations.

When PSTN/ISDN simulation is performed, some of the PSTN/ISDN services may be provided though the services themselves may not necessarily have the full functionality as defined for PSTN/ISDN.

NOTE – "Simulation" is said to be "based on" PSTN/ISDN services in order to provide PSTN/ISDN-like services.

Additional services, e.g. SIP based, may also be available when PSTN/ISDN simulation is performed.

5.4 Internet access

An NGN should not inhibit user access to the Internet [Y.101] through existing mechanisms (e.g., ISP offering of Internet access to xDSL users.)

Support for Internet access through the NGN core network, that includes end to end transparency, peer to peer applications and some other Internet services, is in scope of NGN, but not required in Rel.1 (i.e., in Release 1, actions by the RACF or other NGN functions may impact Internet connectivity traversing the NGN.)

Examples of Internet services can be found in both the list of multimedia services and the list of other services as provided in this document.

5.5 Other services

The list of services in this section primarily addresses various data services common to packet data networks and provided by an NGN.

- Virtual Private Network (VPN) services: Multi-point controlled and secured communication services for the exchange of single or multimedia streams among restricted group of service endpoints and making usage of shared transport stratum resources. Note: VPN functionalities could be also act as service enabler for support of applications and user services.
- Data retrieval applications: such as tele-software.
- Data communication services: such as data file transfer, electronic mailbox and web browsing
- Online applications (online sales for consumers, e-commerce, online procurement for commercials)
- Sensor Network services: these services provide a user with information about a certain item (e.g., merchandise) upon the user's request. This can be realized by attaching an identifier to the item, accumulating the historical information of the item through the NGN and retrieving the accumulated information through the NGN. For example, the history of a piece of vegetable (e.g., harvest date, region of cultivation, name of the farmer, etc.) can be precisely recorded by using this identifier. This identifier could be realized in various ways, for example by an RFID chip (a small Integrated Circuit chip which can store information and can communicate using radio-wave), which can be attached to most of items.

- Remote control/tele-action services, such as home applications control, telemetry, alarms etc.
- Over-the-Network (OTN) Device Management –Device Management (DM) provides a mechanism for service providers and third parties (e.g., enterprise network operators and MVNOs) to configure devices on behalf of the user or to evaluate the status of devices (when such access has been permitted by the user either through service agreements statically configured or through interaction with the user.) DM relies on a network connection between a management server and an user terminal. Typical tasks carried out using DM are determining the nature of events and alarms generated by devices, servicing through software installation or upgrading, and configuration of terminals by setting of parameters. Over-the-air (OTA) DM of wireless devices is possible taking into consideration available bandwidth and latency in the network. An example of OTN DM is developed in Open Mobile Alliance (OMA). [OMA-DM][22.057]

5.6 Public Interest Services Aspects

The services listed in this section may be applicable to NGNs. The NGN provides these services in compliance with regional administrations and international treaties. Precise implementation of these services is beyond the scope of this document.

– Lawful Interception

Where required by regulation or law, an NGN transport provider and/or NGN service provider shall respond to Lawful Interception requirements. Therefore, an NGN shall provide mechanisms that make Lawful Interception possible. These mechanisms shall provide access to Content of Communication (CC) and Intercept Related Information (IRI) by Law Enforcement Agencies (LEA), as per the requirements of the administrations and International treaties.

– Emergency Communications

Where required by regulation or law, the NGN shall support priority capabilities and mechanisms for Emergency Communications using multimedia (e.g., voice, text, data and video). Emergency communications include:

- individual to authority communications, i.e., calls to emergency service providers, e.g., 911(USA), 110/119 (Japan), 112 (EU);
- authority to authority communications, e.g. Telecommunications for Disaster Relief (TDR) and Emergency Telecommunications Services (ETS); and
- authority to individual communications, e.g., community notification services. TDR and ETS may also be authority to individual communications.

Specifically, the design of the NGN shall include service and transport level capabilities to allow emergency communications to be supported using priority/preferential schemes. Call/session control of emergency communications and emergency communications bearer traffic shall receive priority treatment during congestion/failure conditions. Consideration shall be given to the necessary interworking and mapping of priority mechanisms between the various components of the NGN (e.g., between the access and the core network priority, and between the service stratum and the transport stratum priority) to assure end-to-end priority/preferential communication. As one method of offering individual-to-authority Emergency Communications, Release 1 of NGN should consider support for basic access to existing individual-to-authority Emergency Communications. The need to provide location data should be considered.

Scenarios for TDR service are included in [Y.1271].

– Users with disabilities

Where required by regulation or law, NGN Release 1 shall support users with disabilities (including but not restricted to those with hearing and speech disabilities). Services may include relay services for translation between different communication modes. Traditional relay services are text relay

service for translation between text and voice, video relay service for translation between sign language and voice with text, and speech-to-speech services supporting people with weak or hard-to-understand speech. NGN should consider mechanisms to support convenient invocation of such services.

– Network/service provider selection

  In order to urge competition among providers, regulation may order providers to allow users to choose user's favourite provider for each communication connection. NGN shall support the capability for provider selection, where required by regulation or law.

– Consumer Assistance Protection and Privacy

  Where required by regulation or law, NGN shall support measures intended to provide for consumer assistance protection and privacy. These may include:

  • Do Not Call; SPAM.

    These capabilities include support for reference lists or other mechanisms whereby subscribers indicate their preferences as to unwanted solicitations.

  • Malicious communication trace

    This functionality can be used to identify a malicious user, by tracing and determining information pertaining to the identity of the individual, the terminal and location of the originator of a communication.

  • User identity presentation and privacy

    Where required by regulation or law and where user identity is provided as part of session signalling, the NGN shall support mechanisms to provide user identity privacy, including network ability for presentation, restriction and override capability.

6 NGN Release 1 Capabilities

Based on the services identified in section 6 of this document, the following capabilities are listed as supporting the services.

It is important to highlight that the following list has essentially an informative purpose, without any ambition to be exhaustive and to identify the most appropriate level of functional aggregation for NGN Release 1 realisations. Basically, this list is to provide guidelines for the NGN architecture work so that the functional building blocks identified in the NGN architecture are able to support these capabilities.

The following classification is used:

– Basic Capabilities – underlying capabilities and/or capabilities which are of general usage by services and user applications

– Service Support Capabilities – capabilities which are accessed and/or used directly by services and user applications

6.1 Basic Capabilities

6.1.1 Connectivity Capabilities

6.1.1.1 Basic Connectivity Capability (BCC)

It provides basic point-point, or point to-multipoint, or multipoint-to-multipoint connectivity. Features of BCC include: best effort service, limited security, etc.

6.1.1.2 Enhanced Connectivity Capability (ECC)

Enhanced Connectivity Capability (ECC) provides connectivity as in BCC plus differentiating features such as QoS support, advanced level of security, and access to virtual private networking.

6.1.2 Media resource management

Media resource support mechanisms are traditionally used in conjunction with traditional voice processing services and user interactions via voice and DTMF. These are expanded in NGN in support of new data, video and content services. Release 1 NGN provides capabilities to handle various media resources in order to enable various applications.

6.1.3 Access Transport capabilities

Release 1 NGN provides capabilities to access NGN services by a variety of access transport functions. Users should be able to access services from anywhere at anytime.

6.1.4 Interoperability and Interworking

Release 1 NGN should interwork with various kinds of networks. Services shall operate seamlessly across the NGN infrastructure provided by one or more network providers. Release 1 NGN provides capabilities for security, OAM, resiliency, quality of service and, where needed, media (audio, video, etc.) transcoding support in interconnection scenarios with other networks in order to ensure seamless end-to-end operations and related accounting and charging support.

6.1.5 Routing

Release 1 NGN provides capabilities to use both static and dynamic routing schemes. It shall be possible to select the proper routing paths between the traffic originating node and the traffic receiving node according to the traffic contract.

6.1.6 QoS-based Resource and Traffic Management

End to end QoS typically involves combinations of networks of varying infrastructure technologies as well as of multiple operators. It may also involve endpoints of vastly different QoS capabilities. Release 1 will provide an initial set of high-level requirements, architectures, mechanisms and guidelines to address these diversities to enable end-to-end QoS for applications. In particular, Release 1 is aimed at providing QoS support (i.e., relative or absolute QoS) for an application through resource and admission control (as specified in [FGNGN-RACF]), including general coordination within and between NGNs.

6.1.6.1 QoS service level support

NGN Release 1 shall provide Quality of Service capabilities in order to ensure the required service level for users or applications. QoS service level support may include use of Resource and Admission control mechanisms (via RACF) as well as QoS signalling mechanisms.

6.1.6.2 Quality measurements and prediction

NGN Release 1 provides Quality measurements and Quality prediction functionalities.

Perceptual quality metrics for NGN services and performance metrics associated with NGN functions should be provided. Through the use of these metrics, services quality should be measured pro-actively for each service as required by that service. Mechanisms to predict the quality of the experience of NGN services perceived by the customer should be provided.

6.1.6.3 Classes and Priority Management

As one method for QoS management, NGN Release 1 provides capabilities for traffic class differentiation and priority management. NGN Release 1 shall support priority calling for emergency communications and national security services.

6.1.6.4 Processing/traffic overload management

In order to avoid traffic and processing overload and keep response times just low enough under such processing overload to preclude users abandoning their service requests, Release 1 NGN provides some form of overload detection and control (including expansive controls such as load balancing and resource replication).

6.1.7 Accounting, Charging and Billing

Charging and billing functions are supported in the NGN in order to provide accounting data to the network operator regarding the utilization of resources in the network. These functions support the collection of data for later processing (offline charging) as well as near-real time interactions with applications such as for pre-paid services (online charging).

Release 1 will include the functional entities and interfaces necessary to support these capabilities for services supported in Release 1.

6.1.8 Numbering, naming and addressing aspects

NGN is intended to provide an efficient, secure and trustworthy numbering, naming and addressing environment for users, network operators and service providers. Regulatory requirements as well as interoperability with PSTN/ISDN will be taken into account.

NGN should support:

- IP network addressing (IPv4 or IPv6 (or both));
- E.164 numbering
- E.164 numbering with ENUM-like support;
- At least SIP URI or TEL URI;
- Unicast, Broadcast and Multicast IP addressing.

Evolution to NGN shall ensure that the sovereignty of ITU Member States with regard to country code numbering, naming, addressing and identification plans is fully maintained, as described in Recommendation E.164 [E.164] and other relevant Recommendations.

6.1.9 Identification, authentication and authorization

6.1.9.1 Identification

NGN Release 1 provides capabilities for user identification, in order for network operators and service providers to identify the users of NGN services and use this information as required (e.g. for authentication and authorization procedures). Device identification should be enabled for devices in the following situations:

- when the device identification provides information regarding the capabilities of the device that might impact the delivery of services to the user;
- when the device identification provides for an ability to track stolen or misappropriated devices;

6.1.9.2 Authentication

NGN Release 1 provides authentication capabilities to gain access to both service-related and transport-related capabilities. Separate authentication may be required to the access network functions and to the service functions. These capabilities may be performed separately or combined. The user device may perform these functions transparently for the user, or direct user interaction may be required.

6.1.9.3 Authorization

NGN Release 1 provides capabilities in order to allow service access by authenticated users or devices according to their access rights.

6.1.10 Security and Privacy

NGN Release 1 networks will contain the typical security features incorporated in existing networks and will contain a number of incremental security features required so as to allow for secure interconnection with other NGNs or existing networks. The related requirements are based on the application of the ITU-T Recommendation X.805 to NGN and thus address the following dimensions of NGN security: Access control, Authentication, Non-repudiation, Data confidentiality, Communication security, Data integrity, Availability, and Privacy. For more details see [FGNGN-REQ] and [FGNGN-SEC].

6.1.11 Mobility management

In describing the mobility within a NGN, two distinct types of mobility are used: Personal mobility, and Terminal mobility.

No major new interfaces for mobility are proposed for Release 1. Existing interfaces between networks, users and terminals, users and networks, terminals and networks will be used. Release 1 continues to use existing signalling capabilities for all types of mobility as currently defined.

Nomadism shall be supported between different network termination points.

6.1.11.1 Personal Mobility

Personal Mobility in NGN Release 1 is based on a personal identifier (e.g. the UPT number or PUI (Personal User Identity)) , and the capability of the network to provide those services delineated in the user's profile [Q.1742]. Personal mobility involves the network capability to locate the terminal associated with the user for the purposes of addressing, routing and charging of the user's services.

For NGN Release 1, personal mobility exists where users can use registration mechanisms to associate themselves with a terminal that the network can associate with the user. Where interfaces between users and terminals, and users and networks for user registration exist, it is assumed these interfaces will be used for NGN Release 1.

6.1.11.2 Terminal Mobility

For NGN Release 1, terminal mobility exists within and among networks where registration mechanisms are used to associate the terminal to the network. Where existing mechanisms support terminal registration, it is assumed these mechanisms will be used for NGN Release 1. Where support for terminal mobility with service continuity exists, such support is expected to also be used for NGN Release 1.

6.1.12 OAM

NGN is formed by two separate strata, Transport and Service [Y.2011]. There are separate OAM functions for the Transport stratum (where the principles of [G.805] and [G.809] are applied, resulting in each layer network having its own OAM capabilities) and for the Service stratum.

Release 1 NGN provides OAM functions for both service and transport strata.

In order to offer reliable NGN services that can support the requirements of Service Level Agreements (SLA), it may be necessary that the NGN services have their own OAM capabilities

6.1.13 Other Basic Capabilities of Interest to Network and Service Providers

6.1.13.1 Critical Infrastructure Protection

NGNs shall be designed to minimize network attacks from within their own or outside networks. This may include reporting of outages and analysis of failures. (Note: critical infrastructure protection seems an essential capability that is required in most jurisdictions as well as by the ITU's own treaty instruments.)

6.1.13.2 Non disclosure of information across NNI interfaces

Where required by regulation or law, or by country or regional conditions, the NGN shall have capabilities to enable the service provider to not disclose internal or service users' information to other entities across NNI interfaces. Also, the NGN shall have capabilities to enable the network provider to not disclose internal network information to other entities across NNI interfaces.

6.1.13.3 Inter-provider and universal service compensation

When services are offered to the public, providers usually seek to be compensated on some bases for resources made available to other providers. In addition, national authorities may institute use-based compensation mechanisms. NGNs may be required through appropriate accounting mechanisms to support these requirements.

6.1.13.4 Service unbundling

In many national jurisdictions, it is required that service providers "unbundled" their offerings to allow customers a choice of providers for diverse services, as well as allow providers to competitively offer their services to customers.

6.1.13.5 Exchange of user information among providers

NGN should support standard interfaces to allow providers to exchange user information.

6.1.14 Management aspects

NGN management supports the monitoring and control of the NGN services and service and transport components via the communication of management information across interfaces between NGN components and management systems, between NGN-supportive management systems, and between NGN components and personnel of service providers and network operators. The NGN Management Focus Group is responsible for providing solutions to support the following aims of both the service support and basic management aspects for the NGN.

NGN management supports the aims of the NGN by:

- Providing the ability to manage, through their complete life cycle, NGN system components, both physical and logical. This includes resources in the transport stratum, service stratum, access transport functions, interconnect components and customer networks and terminals.
- Providing the ability to manage NGN service components independently from the underlying NGN transport components and enabling organizations offering NGN user services (potentially from different service providers) to build distinctive service offerings to customers.

- Providing the management capabilities which will enable organizations offering NGN user services to offer users the ability to personalize user services and to create new services from service capabilities (potentially from different service providers).
- Providing the management capabilities which will enable organizations offering NGN user service improvements including user self service (e.g. provision of service, reporting faults, online billing reports).
- Developing a management architecture and management services which will enable service providers to reduce the time frame for the design, creation and delivery of new services.
- Supporting the security of management information, including customer and end user information.
- Supporting the availability of management services any place any time to any authorized organization or individual (e.g. access to billing records shall be available 24/7).
- Supporting eBusiness Value Networks based upon concepts of business roles (Customer, Service Provider, Complementor, Intermediary, Supplier (e.g. Equipment Vendor)) [Y.110] [M.3050].
- Allowing an enterprise and/or an individual to adopt multiple roles in different value networks and also multiple roles within a specific value network (e.g. one role as a retail service provider and another role as a wholesale service provider) [M.3050].
- Supporting B2B processes between organizations providing NGN services and capabilities.
- Allowing the management of hybrid networks comprising NGN and non-NGN (e.g. PSTN, cable network) resources.
- Integrating an abstracted view on Resources (network, computing and application), which is hiding complexity and multiplicity of technologies and domains in the resource layer.
- Supporting the collection of charging data for the network operator regarding the utilization of resources in the network either for later use by billing processes (offline charging) or for near-real time interactions with rating applications (online charging).

6.2 Service Support Capabilities

6.2.1 Open service environment

Open service environment capabilities stem from the general characteristics of the NGN in supporting and establishing an environment for enhanced, flexible and open service creation and provisioning.

6.2.1.1 Services Coordination

Services coordination provides a means of coordinating identities, sessions, services, plus network and device resources to applications, either in a centralized way, or with support functions distributed across user devices, edge devices, etc. Service coordination for Release 1 will be supported where mechanisms already exist for service coordination, e.g., IN services, OSA/Parlay API and OMA service environment..

6.2.1.2 Application Service Interworking

This capability allows interworking of application services and network entities for service creation and provisioning.

6.2.1.3 Service discovery

Service discovery is often the first step to locate services for subsequent interaction. As such, NGN should support this capability. Service discovery is essential for supporting user mobility and user device independent access to services.

An example of service discovery capability is implemented in the Web services framework (Web services can be used to export network services and use the Universal Discovery, Description and Integration (UDDI) registry to implement service discovery [UDDI]).

6.2.1.4 Service Registration

This capability allows the registration of other capabilities in directories of the open service environment which are accessible by capabilities and/or applications and user services. Web services provide an example of service framework using such registration capability: when it is wished to expose a Web service, this one is registered in public Web service "registries" (a registry is a special directory that not only points users to a resource, but also lets them register services with it).

6.2.1.5 Developer Support

Developers are a key part of the service delivery chain. Needs of developers include collection and publishing of data, plus providing for a means for software developers to articulate and specify their needs, and to identify developer interfaces.

6.2.2 Profile Management

6.2.2.1 User Profile

The User Profile Functions provides capabilities for the full range of data management functions (creation, maintenance, deletion of individual User Profiles; access control, preferences, definition of attributes and the interrelationships among various attributes, etc.), in addition to handling the exchange of User Profile information with other NGN functions at both service and transport strata (such as Authentication, Authorization, Service Registration, Mobility, Location, Charging, language preferences and mode preferences).

Beyond simply acting as a data repository, the User Profile Functions provide a framework for evolving to support the emerging network-based identity management and advanced identity functions. The User Profile Functions include support for expressions of user preferences, and the ability to apply logical functions to determine which of multiple related profile elements, or related profiles, should be made available to other NGN functions.

The User Profile Functions provide features to enable support for a number of related capabilities including:

- Flexible control of how a user's presence and location information may be made available to other parties
- Privacy and security functions, based on the operator as one trust anchor among many

6.2.2.2 Device Profile

Release 1 NGN provides functionalities to manage information related to customer terminals. This includes terminal identification, address, name, static attributes such as supported media and protocols, transmission speed, bandwidth, and processing power, and dynamically changing attributes such as the user using the terminal, geographical location, running applications on the terminal.

6.2.3 Policy Management

Policies can be used to control access to enablers. An example of this capability is found in OMA service environment. It provides a policy-based management means to provide protection from unauthorized requests, and to support authorized requests with support for charging, logging, user privacy and user preferences. Release 1 NGN provides policy management capabilities in order to ensure service access, provisioning and management across a range of networks and technologies.

6.2.4 Service enablers

Service enabler capabilities support more specific or advanced services and enable access and/or handling of more specific information provided by these capabilities.

6.2.4.1 Group management

This capability provides functionalities related to the secure and efficient management of groups of network entities (terminals, users, network nodes etc.). It may be used by applications and services for different purposes, including VPN applications, video content distribution, over-the-network device management, network and service provisioning and management, emergency community notification services etc.

6.2.4.2 Personal information support/management

This capability provides management of customers' personal information and communication context related data. Such types of information (e.g. presence information, content access, Internet TV time information etc.), delivered by applications (e.g. presence, notification and information services) according to pre-defined user preferences and policy attributes, may be stored and managed by the personal information support/management on behalf of service users. This information may be also retrieved on behalf of the user through personal information support/management acting as an user proxy for the applications.

6.2.4.3 Message handling

This capability provides management of message-based data streams. Functionalities include real-time and non real-time messaging management as well as single and multimedia data stream management. Examples of real-time messaging are Instant Messaging and Chat, Email and SMS are examples of non real-time messaging.

6.2.4.4 Broadcast/Multicast support

This capability enables applications to deliver content to multiple users at the same time using broadcast or multicast type of content delivery mechanisms.

In addition to standard point-to-point unicast, broadcast and multicast mechanisms should be supported for efficient network resource usage and scalable content delivery.

For providing broadcast/multicast services, both transport and service stratums should provide related capabilities.

6.2.4.5 Presence

Presence is enabled by three capability groupings:

a) Presence Collection Capability. The network provides a capability to collect information describing the connectivity state of the device used by the user. This capability could be used, for example, to describe the subscriber's state of connectivity to the network. The user can also provide information, such as availability.

b) Presence Distribution Capability. This capability enables another user to be informed of current presence status of a particular user. The capability can also be used for another service to access the users' presence information.

c) Presence Management Capability. NGN Release 1 provides Presence Management, a set of capabilities to manage the presence information is managed in compliance with user privacy and access rules requirements. The Presence Management Capabilities enables the distribution capability to supply only part of the presence information. The Presence Management Capability collects requests from users to receive presence information for another user. This capability also

provides the user with the ability to determine the distribution of their presence information, e.g. to accept or reject a request for presence information on a per watcher basis.

6.2.4.6 Location management

Location is an enabling capability for provisioning of location applications, which use information regarding the location of users and devices within networks. The location of users and devices in networks can be related to positioning, hence enhancing applications with local context and relevance.

6.2.4.7 Push-based support

This concerns capabilities to transmit data from an initiator to a recipient without a previous user action, e.g., SIP-based Push mechanism. In the "normal" receiver/sender model (also know as client/server model), a recipient requests a service or information from a sender, which then responds in transmitting information to the recipient. This is known as "pull" technology where the recipient pulls information from the sender, e.g., browsing the World Wide Web. In contrast to this, there is also "push" technology, which is also based on the sender/receiver model, but where there is no explicit request from the receiver before the sender transmits information.

6.2.4.8 Device management

Device management (DM) defines management protocols and mechanisms that enable robust management during the entire life cycle of the device and its applications over a variety of bearers. One aspect of this is device provisioning by which a device is initially configured with a minimum of user interaction. Examples of DM are provided in OMA, which has specified an enabler for DM.

6.2.4.9 Session handling

NGN Release 1 provides capabilities to setup, manage, and terminate end-to-end service sessions that involve, for example, multiple parties, a group of endpoints associated with those parties, and a description of multimedia connections among the endpoints. These are session management capabilities in both fixed and mobile network environments in order to accommodate different service application requirements as well as to route session signaling to the appropriate application servers.

6.2.4.10 Web-based application support and content processing

Web browsing and content processing are important enablers which allow optimization of device capabilities and network characteristics, building on external standards such as those defined by W3C and OMA.

6.2.4.11 Data synchronization

Data synchronization allows devices and elements within the network infrastructure, e.g., servers to exchange data according to user or operator needs. As an example, SynchML common representation, synchronization and device management protocols. For example, the Open Mobile Alliance Data Synchronization V1.1.2 specification [OMA-DS], capable of synchronization networked data with many different devices, including handheld computers, mobile phones, automotive components, and desktop PCs is a synchronization service enabler for NGN.

6.2.4.12 Commerce & Charging

Commerce provides an increasingly important revenue stream for operators and service providers. A charging enabler gives support to an underlying NGN charging system. This enabler provides charging interfaces among service providers, content providers and network operators. It includes the facilitation of event/time/session/user charging for the various service types allowing differentiation between

communication, content and application. The Open Mobile Alliance Charging specification, Version 1.0.1, details such a charging enabler [OMA-CS].

6.2.5 PSTN/ISDN emulation support

These are specific capabilities to support the PSTN/ISDN emulation services.

NOTE – PSTN/ISDN Simulation services use the capabilities of the IP Multimedia Service Component and therefore do not require additional specific capabilities.

6.2.6 Other Service Support Capabilities of Interest to Network and Service Providers

6.2.6.1 Public Interest Services aspects

Where required by regulation or law, NGN Release 1 shall provide capabilities for the support of public interest services. Specific capabilities will depend on needs of regional administrations and international treaties.

6.2.6.2 Digital Rights Management

NGNs may be required to support the management and use of digital objects that are subject to copyright protection.

6.2.6.3 Fraud Detection and Management

NGNs may be required to support the detection and minimization of activities that misrepresent the identity of the parties, the nature of the services or transactions, or payments therefore. These capabilities will also be especially important for NGN operators in supporting roaming and other nomadic capabilities. (Note: fraud detection and management seems an essential capability that is required in most jurisdictions as well as by the treaty instruments, and by most operators among themselves.)

6.2.6.4 Number portability

Where required by regulation or law, number portability shall be supported. Number portability allows users to keep the same number when the customers change providers or service delivery technologies such as among wireline, cable or mobile.

Appendix I

Service Descriptions and Use Cases

(*informative*)

I.1 General Use Cases

1) Telephone Service among VoIP/IP Phone and Mobile Phone

Packet-based telephone service is similar to telephone service of circuit switched network. Mutual communication between fixed-terminal and mobile terminal and roaming service are provided. Also, the phone network traces the location of users using the user identification functionality. So one can be reached by one phone address regardless of where the person is and regardless of which terminal the person uses.

2) Video Telephony and Total Conversation

Video telephony service is basically point to point real time multimedia communication service between human users providing communication in video and voice. Total conversation is a similar service providing real time text in addition to video and voice. They can be enhanced with additional features such as multimedia messaging service (MMS) and interactive video responder. For example, when the called person is not available, video, picture or text messages can be shown on the calling person's terminal. And the calling person can select the action such as forwarding the call to mobile terminal, leaving video message or emailing to the person.

Also the quality of the video or voice is automatically adjusted depend on which access transport function is used. When the call connection is established, the network automatically detects the type and quality of the access connection (such as dial-up, xDSL, FTTH, WLAN etc.) of each end, and measures the end-to-end quality of the call connection, Notifying the quality information of the call connection to user terminals, each user terminals can adjust the bit rate of the video stream, and the video quality which each user sees can be optimized. When adjusting the video quality, the requirements of people requiring good flow of the video image for use in sign language and lip reading should be considered so that when conditions call for quality sacrifice, first spatial resolution is reduced and then as a last resort the temporal resolution.

3) Video on Demand (VOD) / Digital TV Channel Distribution

This service enables broadcasting of communication services in networks. Every pattern of communication as on demand (VOD) and TV channel distribution are assumed. We assume such broadband data communication as transmitting high-capacity data e.g. HDTV. Even if all the registered users' access occurs, quality of video should not be affected. Since needs for the service will be different for each users, service level should be agreed between the user and the service provider when the user subscribe the service, Size of the screen, frames per second and price will be different depend on the SLA, and even the same content should be delivered differently based on the each user's SLA. Moreover, if a user watches TV program using many kind of terminal such as fixed television, fixed PC, mobile terminal, and so on, the bit rate of the video should be automatically adjusted depending on the capacity of the terminal and access transport function. When a user changes terminals, the session management should be considered. For example, a user can suspend a video session on TV at home and then resume the session on PC at his/her office.

In order to provide the high bit rate and real time broadcasting service to all people throughout city or nation, a network needs to support an efficient data delivery mechanism. Since broadcasting is a one-to-many type communication, the delivery network should support that communication type which may need different

mechanism from one-to-one communication. Multicast type contents delivery will be one of the methods that support one-to-many type communication.

4) Multimedia Conference

The application that enables many users registered and authorized to join in a conference with terminals handling multimedia data as video, voice, image and real time text. It realizes interactive communication not only attending that meeting but also sending messages in any media. Users can specify other person with a user-friendly name like URL and domain name, network will translate the name into a network address or number to connect. That makes it possible that various media as voice, image and video are treated as well as text data like instant massage and displayed them in the suitable way according to condition of users. Also, value of ubiquitous is provided because users can receive services from everywhere and with every terminal connected to the networks. This multimedia conference can be used for a virtual community site.

Communication type of multimedia conference is many-to-many type communication which is different from one-to-one and one-to-many type, especially in terms of scalability. Technique like multicast could be applied to this type of communication also. Moreover, it is important to adjust the quality of media (bit rate) depending on the each user's condition or type of access transport function.

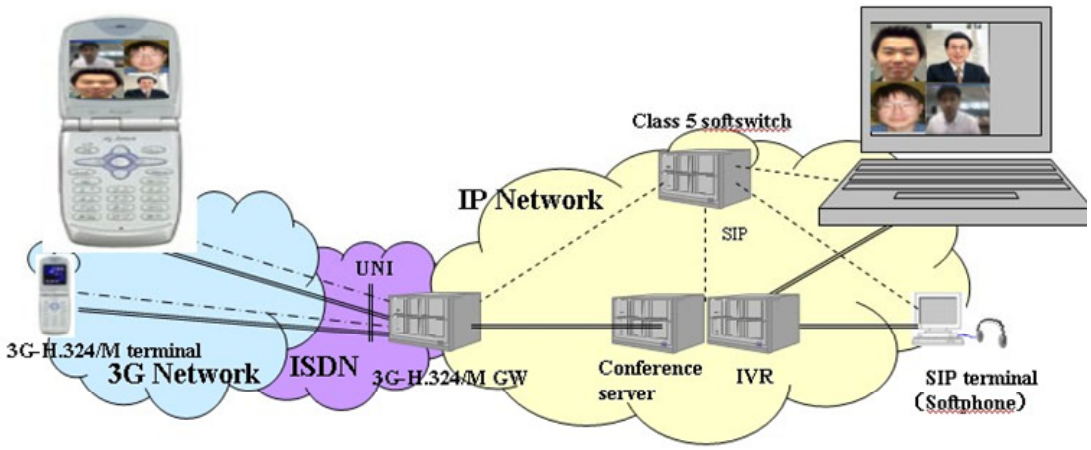


Figure I.1 – Example of Multimedia Conference

Figure I.1 is a an example of multimedia conference which, with a number of networks as mobile and fixed telephone worked together, users of each network can join. According to the profiles of users and/or terminals, text, voice and image can be transmitted in the suitable way. In so doing, regarding quality of service, the regular quality which provides stable services has to be guaranteed through the networks.

5) Online applications (e.g. Sales/Commerce, Gaming …)

A variety of commercial services, such as online sales for consumers, online procurement for commercials and information providing service will be deployed. It is supposed that more complicated services using web service or agent technology will be provided. For consumers, there are examples of service that recommend shops based on the user profile and the nearest shop according to user location. On the other hand, for business use, it is necessary that quality terms of network are guaranteed and reliability is ensured in order to carry out mission critical transactions without fail. At the same time, a function for security needs to be enough in order not to leak information.

6) Remote control of Home applications (Ubiquitous Network with Home electric appliances and Sensing devices)

It is assumed that home electric appliances, through the use of wireless technology such as Bluetooth, will become NGN enabled and thus can be integrated into networks. The term electrical appliances is to be interpreted in the most general sense and is intended to include such devices as security cameras, traffic observation cameras, observation devices for care and water meters. As a result, these home electric appliances and various sensors can be monitored and controlled from a distant place and will require an access control capability which allows for authentication of users.

7) Services utilizing location information

Considering mobility management on ubiquitous environment, NGN should consider mechanisms to manage location information of users and terminals. Location information will be from GPS, indoor positioning service, RFID and telecom positioning information (like cell station information). Location information is useful for NGN services like tour guide service, user service, assistance service for handicapped and emergency call.

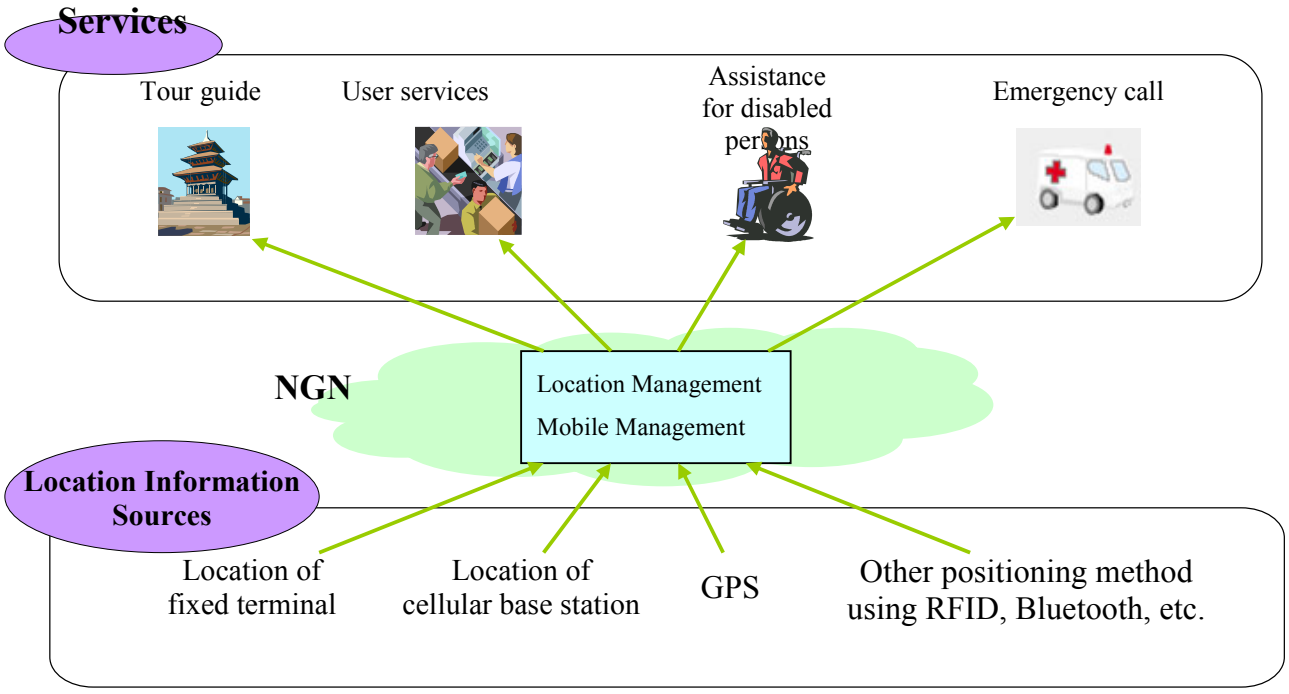


Figure I.2 – Services utilizing location information

8) Lawful interception

In NGN, capturing, monitoring and recording of a specific data stream within a network should be possible when requested by regulatory bodies. And also, the lawful interception of various means of communications, such as voice, video, e-mail, IM etc., is needed. Though link speed of the network is becoming more than a gigabit, routers should have a functionality to enable that interception.

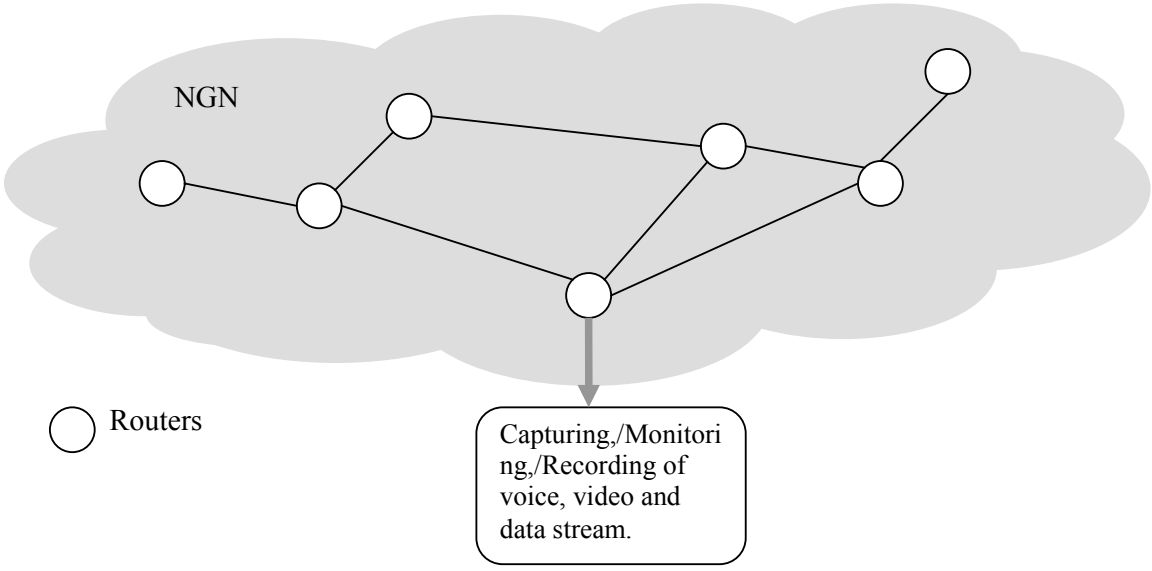


Figure I.3 – Lawful Interception

9) Prioritized communication/traffic handling

Considering NGN to become percolated through the whole society, urgent calls e.g. emergency call, criminal call need to be treated as a priority. It has to be possible for a computer and PDA as well as fixed and mobile phone to make such an urgent call (e.g. refer to E.106/draft F.706 Recommendations).

10) Presence Enhanced Services

The presence service provides access to presence information of a user, user's devices, and services to be made available to other users or services. The presence information might be from users who want to provide their presence information to others or network systems which care about the user's session or service status.

Use of this service will make the almost of NGN services currently present including real-time conversational voice/video services, instant messaging, messaging services such as SMS, MMS, push to talk over NGN and so on, much more enhanced and enriched. These enhanced services may infer the current status, availabilities, and preferences of a user to initiate the various kinds of communications by accessing the presence information for the user's devices and services.

Examples of such enhanced services are as follow,

– User A who wants to communicate with his friend B finds that B's phone is busy on A's buddy list, so A may send SMS message to him instead of phone call. (retrieve the call status information from presence server interworking with session controller)
– User A finds out on his buddy list a friend B is game on line and joins that game session by driving his game program. User A also may invite the other friends who use the game phones and in idle state to join the game, while sending SMS to the friend who is busy to hang up the phone and join the game. (retrieve the application service status information from presence server interworking with various application servers)
– User A is always provided the stock information that he is interested in by registering the CP agent as his buddy. When the price of stock matches the conditions preset, he is noticed by SMS message or by CP agent buddy status warning. (provided the information services by registering various 3rd party contents providers on the buddy list)

– User A initiates the conference call with his buddy members by just clicking the buddy icon of presence client on his device. The conference service initiates the conference call to the members who are idle states while sending SMS requesting joining the conference to the members whose call status are busy.(provided the enhanced application services requiring media to be converted and directed to specific devices based on presence information using enhanced easy to use presence client)

– User A is travelling to distant land. Upon connecting his or her computer to the network, User A sees in the buddy list that User B is online. User A initiates a videophone call to User B to discuss a future trip. User B had a stroke a couple of years ago that affected his speech. So, when User B wants to contribute to the discussion he types in the text area and the text appears in near real-time on the User A's terminal. User B shares his experience from an earlier trip to that distant land by sending photos, They discuss plans for future travel based on these pictures. Finally they decide upon the destination of the trip. User A establishes a link to a travel information site to request information for their continued planning after the current call.

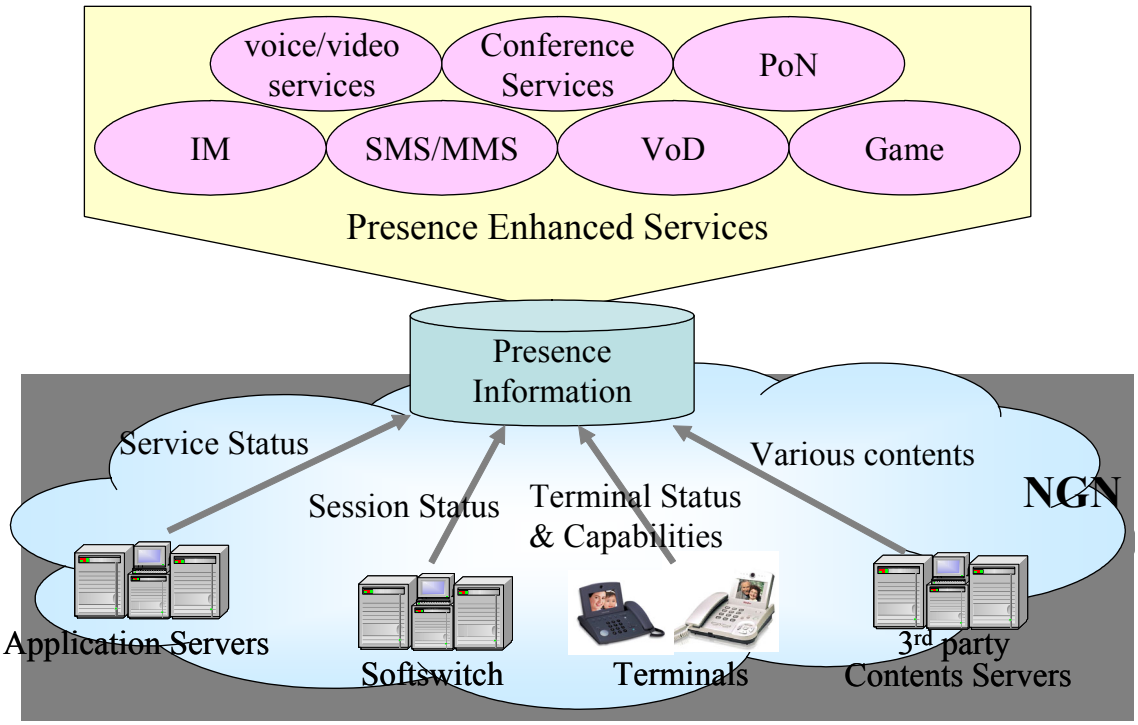


Figure I.3 – Presence enhanced Services

I.2 Business Use cases

Use cases:

1. business meetings through voice text, video telephony, total conversation and conferencing
2. secure access to the corporate network from outside the office (VPN)
3. access to email and the world wide web from laptop, handheld PC and cellphone
4. handover of applications (eg. VoIP) between enterprise or home wireless hotspots and WAN
5. roaming of terminals across network domains and operators
6. use of multimedia information sharing tools, such as 'whiteboarding'
7. route in-coming faxes and multimedia messages to particular terminal or network server
8. synchronization of work office with home office applications

9. cooperative product development from multiple remote locations
10. Device-management monitor/control services
11. Download the device management info through Over the Air Multicast and Broadcast
12. Customer Service Desk supporting deaf clients, through a video relay service or a real time text relay service for translation between sign language and voice or between real time text and voice.

Special considerations:

- secure mobile access from any location with wireless signal coverage
- support for a wide variety of device types and capabilities
- transcoding or adaptation of content according to network and/or terminal capabilities
- mobile location services

I.3 Medical Use Cases

Use Cases:

1. a doctor on the move requires storage and manipulation of patient data
2. immediate on-site video transmission to doctor as first aid
3. transmission of medical data to doctor or consultant
4. transmission of surgical treatment to remote medical staff
5. communication with older people in home care, who may need to see the person they are talking to and have text or lip-reading to compensate for hearing reduced by age.
6. Mobile Telemedicine System

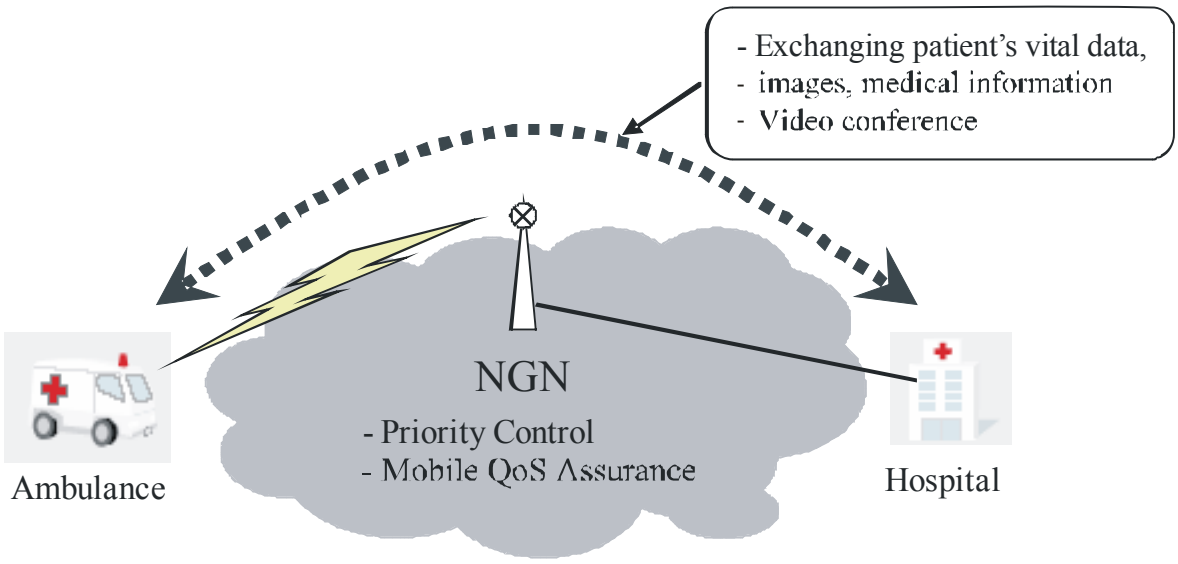


Figure I.4 – Mobile Telemedicine System

Mobile Telemedicine is a service for communication between ambulance and hospitals, and it enables to share medical data (real-time vital data from ambulance, medical care information and so on) of patient among medical experts in hospitals, and supports quick decision to save the patients life. Because this service manages life-threatening information, communication link should be highly reliable even though

wireless communication media will be used. NGN shall support priority management of emergency call and quality assurance of mobile communication.

NOTE – priority management of emergency calls is for further study.

Special considerations:

- large data volumes
- scalable data, including lossless data storage
- transcoding or adaptation of content according to network and/or terminal capabilities
- reliability
- privacy

Appendix II

Examples of categorization of Services

(*informative*)

II.1 Basic/Enhanced services versus Service/Transport stratum

Table II.1 – Basic/Enhanced services versus Service/Transport stratum categorization

	Service Stratum	Transport Stratum
Basic Services	E.g. Point to Point voice, Point to Point fax Point to Point text services Point to Point total conversation (video, text and voice) Point to Point video services	E.g. Bandwidth and circuit wholesaling
Enhanced Services	E.g. Multi-point voice, fax and video services Content Delivery services Presence Services Multi-media conferencing	E.g. Virtual Private connectivity

II.2 Unicast/Multicast/Broadcast versus Real-time/Non-real-time: General mapping

Table II.2 – General Unicast/Multicast/Broadcast versus Real-time/Non-real-time categorization

		Real time	Non-real time
Unicast	Peer-to-peer	**Single medium** - (voice) Telephony- Instant messaging / Chat - Gaming - File sharing - Voice conferencing - Push to talk -Push to view -Emergency messaging services	**Single medium** - e-mail - SMS - Fax
		Multi media - Video telephony - Text telephony - Total conversation - Video conferencing - White boarding - Emergency messaging services	**Multi media** - MMS
	Client-server	**Single medium** - Gaming- Voice conferencing- Radio (broadcast) streaming- websurfing	**Single medium** - Music on demand (MoD) - Video on demand (VoD)
		Multi media - Video conferencing - TV (broadcast) streaming - Video security	**Multi media**
Multicast		**Single medium** - Radio multicast - Gaming - Emergency alert	**Single medium** - OTA/OTN device management - cell broadcast SMS
		Multi media - Video multicast - Gaming	**Multi media** - cell broadcast MMS
Broadcast		**Single medium** - Radio broadcast	**Single medium**
		Multi media - TV broadcast	**Multi media**

II.3 Business Mapping

Table II.3 – Business Unicast/Multicast/Broadcast versus Real-time/Non-real-time categorization

		Real time	Non-real time
Unicast	Peer-to-peer	**Single medium** - Identity management (Personal, security inventory) - Location applications - Presence applications	**Single medium** -
		Multi media - 'Whiteboarding'	**Multi media** - Product marketing
	Client-server	**Single medium** - e-commerce - Stock trading - Business transactions - Product software updates - User portal personalization - Terminal software integrity checks - Remote monitoring of terminal radio capabilities	**Single medium** - Product database access
		Multi media - professional training - marketing tools	**Multi media** - e-Learning
Multicast		**Single medium** - Sales targeting - Traffic Alert	**Single medium** - Electronic publishing - Electronic Coupon - Traffic Alert
		Multi media - Traffic alert with route info.	**Multi media** - Traffic Alert with route info
Broadcast		**Single medium** - Radio broadcast	**Single medium** - Sales promotions
		Multi media - general news, financial and travel info	**Multi media** - Movie trailers

II.4 Medical Mapping

Table II.4 – Medical Unicast/Multicast/Broadcast versus Real-time/Non-real-time categorization

		Real time	Non-real time
Unicast	Peer-to-peer	**Single medium** - Medical sensor applications - Patient surveillance	- Medical sensor data applications
		Multi media - First aid assistance - Medical inspection relay	**Multi media** - Medical database transfer (large data size, lossless storage)
	Client-server	**Single medium** - Equipment data logging	**Single medium** - Equipment data processing or viewing
		Multi media - Home medecine - Telepresence	**Multi media** - Personal medical database (large data size, lossless storage) - Medical library / diagnosis
Multicast		**Single medium**	**Single medium**
		Multi media - Specialized medical training	**Multi media** - Targeted advertising of health products
Broadcast		**Single medium**	**Single medium** - Alerts by Center of Disease Control
		Multi media - Medical profession education	**Multi media** - Medical product information distribution

Appendix III

Mapping of Services and Service Enablers Capabilities

(*informative*)

This Appendix provides an example mapping of most of the services identified in Section 6 to selected "service enablers" capabilities in Section 6.1.4. The mapping is not meant to be exhaustive nor represent requirements for support. Since data communications, on-line services, and remote control services may be transparent to the service enablers identified in this table, they are not included in the services list. Also, PSTN/ISDN emulation is not included in the table since the services are prescribed and would not use the service enablers.

Table III.1 – Illustrative mapping of Services to Service Enabler Capabilities

Services\Service Enablers	Presence Support	Location Support	Group Support	Personal Information Support	Message Handling	Broadcast/ Multicast Support	Push-Based Support	Session Handling*
Real-time Conversational Voice services								X
Real- time Text								X
Messaging services	X		X		X			X
Push to talk over NGN	X		X					X
Point to Point interactive multimedia services			X					X
Collaborative interactive communication services		X	X					X
Content Delivery Services		X					X	
Push-based Services		X					X	
Broadcast/Multicast Services						X		
Hosted and transit services for enterprises			X					X
Information Services	X	X		X			X	
Presence and general notification services	X	X	X					
3GPP Release 6 and 3GPP2 Release A OSA-based services	X	X	X	X	X	X	X	X
Data Retrieval	X			X			X	
Sensor Network							X	
Over the Network Device Management	X			X			X	

Appendix IV

Bibliography of Informational References

(*informative*)

ITU-T Series of Documents

[E.164] ITU-T Recommendation E.164, The international public telecommunication numbering plan

[F.703] ITU-T Recommendation F.703, Multimedia Conversational Services Description

[F.724] ITU-T Recommendation F.724, Service description and requirements for Videotelephony services over IP networks

[F.733] ITU-T Recommendation F.733, Service description and requirements for Multimedia Conference Services over IP networks

[F.741] ITU-T Recommendation F.741, Service description and requirements for Audiovisual on Demand Services

[F.742} ITU-T Recommendation F.742, Service description and requirements for Distance Learning Services

[G.805] ITU-T Recommendation G.805, Generic Functional Architecture of Transport Networks

[G.809] ITU-T Recommendation G.809, Functional architecture of connectionless layer networks

[G.799.1] ITU-T Recommendation G.799.1, Functionality and interface specifications for GSTN transport network equipment for interconnecting GSTN and IP networks

[G.IP2IP] ITU-T Recommendation G.IP2IP, Functionality and Performance of an IP-to-IP Voice Gateway optimised for the transport of voice and voiceband data

[H.510] ITU-T Recommendation H.510

[H-supp1] ITU-T H-series Supplement 1 Low bitrate video quality requirement from Sing language and lip reading application

[M.3017] ITU-T Recommendation M.3017, Framework for the integrated management of hybrid circuit/packet networks

[M.3060] ITU-T Recommendation M.3060, Principles for the Management of Next Generation Networks

[M.1645] ITU-T Recommendation Q.1645, Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000

[I.230] ITU-T Recommendation I.230, Definition of bearer service categories

[I.250] ITU-T Recommendation I.250, Definition of supplementary services

[Q.833.1] ITU-T Recommendation Q.833.1, Asymmetric digital subscriber line (ADSL)

[Q.1200] ITU-T Recommendation Q.1200 Series, General series Intelligent Network Recommendation

[Q.1236] ITU-T Recommendation Q.1236, Intelligent Network Capabilities Set 3 – Management Information Model Requirements and Methodology

[Q.1702] ITU-T Recommendation Q.1702, Long-term vision of network aspects for systems beyond IMT-2000

[Q.1703] ITU-T Recommendation Q.1703, Service and network capabilities framework of network aspects for systems beyond IMT-2000

[Q.1761] ITU-T Recommendation Q.1761, Principles and requirements for convergence of fixed and existing IMT-2000 systems

[T.140] ITU-T Recommendation T.140, Protocol for Multimedia Application Text Conversation

[Y.110] ITU-T Recommendation Y.110, Global Information Infrastructure principles and framework architecture

[Y.1271] ITU-T Recommendation Y.1271, Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks

ETSI Series of Documents

[22.057] ETSI TS 122 057 V5.3.1, Mobile EXecution Environment (MExE) service description; Stage 1.

[22.708] ETSI TS 122 078 V3.3.0, Customised Applications for Mobile network Enhanced Logic (CAMEL); Service description, Stage 1.

[22.140] ETSI TS 122 140 V5.3.0, Multimedia Messaging Service (MMS);Stage 1.

[22.146] ETSI TS 122 146 V6.6.0, Multimedia Broadcast/Multicast Service (MBMS);Stage 1..

[42.033] ETSI TS 142 033 V6.0.0, Lawful interception - stage 1.

[22.127] ETSI TS 122 127 V5.5.0, Service Requirement for the Open Services Access (OSA); Stage 1.

[23.141] ETSI TS 123 141 V6.8.0, Presence service; Architecture and functional description; Stage 2.

[23.228] ETSI TS 123 228 V6.10.0, IP Multimedia Subsystem (IMS); Stage 2.

[26.235] ETSI TS 126 235 V6.4.0, Packet switched conversational multimedia applications; Default codecs

[101.331] ETSI/TS 101 331 Requirements of Law Enforcement Agencies

[133.106] ETSI/TS 133 106: UMTS; Lawful Interception requirements

Open Mobile Alliance Specifications

[OMA-DS] Open Mobile Alliance, Data Synchronizaton, Version 1.1.2

[OMA-DM] Open Mobile Alliance, Device Management, V1.1.2.

[OMA-CS] Open Mobile Alliance, Charging Specification, Version 1.0.1

[OMA-OSE] OMA-Service-Environment-V1_0_1-20050614-A

[OMA-PoC] Open Mobile Alliance, Push to talk over Cellular, Version 1

Open Service Access

[OSA-Parlay-X] Open Service Access (OSA), Parlay X Web Services, Parts 1-14, ETSI ES 202 391-[1-14] V1.1.1 (2005-03)

[OSA-Parlay-4] Open Service Access (OSA), Application Programming Interface (API), Parts 1-14, ETSI ES 202 915-[1-14] V1.3.1 (2005-03)

[OSA-Parlay-5] Open Service Access (OSA), Application Programming Interface (API), Parts 1-15, ETSI ES 203 915-[1-15] V1.1.1 (2005-04)

IN Services

[TIA-771] TIA/EIA/IS 771-1, Wireless Intelligent Network

[TIA-873] TIA/EIA 873.002, All IP Core Network Multimedia Domain - IP Multimedia Subsystem - Stage-2 (2003)

UDDI Specifications

[UDDI] UDDI Spec Technical committee, UDDI Specification, Version 3.0.2

References for Access Network technologies

Wireless Local Area Network [WLAN]

[802.11] IEEE 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999

[802.11a] IEEE 802.11a Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band, 1999

[802.11b] IEEE 802.11b Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, 1999

[802.11d] IEEE 802.11d “Specification for Operation in Additional Regulatory Domains”, 2001

[802.11e] IEEE 802.11e Draft - Medium Access Control (MAC) Quality of Service (QoS) Enhancements, 2004

[802.11f] IEEE 802.11f Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, 2002

[7802.11g] IEEE 802.11g Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band, 2003

[802.11h] IEEE 802.11h Spectrum and Transmit Power Management Extensions in the 5GHz band in Europe 2002

[802.11i] IEEE 802.11i Medium Access Control (MAC) Security Enhancements, 2004

[802.11j] IEEE 802.11j Draft - 4.9GHz-5GHz Operation in Japan, 2004

[802.1X] IEEE 802.1X IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control”, 2001

Broadband Wireless Access [BWA]

[802.16] IEEE 802.16-2001 Air Interface for Fixed Broadband Wireless Access Systems

[2802.16a] IEEE 802.16a-2003 Air Interface for Fixed Broadband Wireless Access Systems– Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 2-11 GHz

[802.16c] IEEE 802.16c-2002 Air Interface for Fixed Broadband Wireless Access Systems-- Amendment 1: Detailed System Profiles for 10-66 GHz

[802.16e] IEEE 802.16e-2002 Draft – Air Interface for Fixed Broadband Wireless Access Systems-- Amendment for Physical and Media Access Layers for Combined Fixed and Mobile Operation in Licensed Bands

Asymmetric Digital Subscriber Line (ADSL)

[G.992.1] ITU-T Recommendation G.992.1 series, Asymmetrical digital subscriber line (ADSL1)

[G.992.3] ITU-T Recommendation G.992.3 series, Asymmetrical digital subscriber line (ADSL2)

[G.992.5] ITU-T Recommendation G.992.5 series, Asymmetrical digital subscriber line (ADSL2+)

Single-pair High-speed Digital Subscriber Line (SHDSL)

[G.991.2] ITU-T Recommendation G.991.2, Single-pair high-speed digital subscriber line (SHDSL)

Very-high-speed Digital Subscriber Line (VDSL)

[G.993.1] ITU-T Recommendation G.993.1 series, Very-high-speed digital subscriber line (VDSL1)

[G.993.2] ITU-T Recommendation G.993.2 series, Very-high-speed digital subscriber line (VDSL2)

Synchronous Digital Hierarchy (SDH)

[G.707] ITU-T Recommendation G.707, Network node interface for the synchronous digital hierarchy (SDH)

Optical point-to-point

[802.3ah] IEEE 802.3ah 100Base-LX/BX and 1000Base-LX/BX

Broadband Passive Optical Network (BPON)

[G.983 series] ITU-T Recommendation G.983 series, Broadband passive optical networks, BPON

Gigabit-capable Passive Optical Network (GPON)

[G.984 series] ITU-T Recommendation G.984 series, Gigabit-capable passive optical networks, GPON

Gigabit Ethernet Passive Optical Network (EPON, GEPON)

[802.3ah] IEEE 802.3ah 1000Base-PX, Gigabit Ethernet passive optical network (EPON, sometimes called GEPON)

Broadcast [BDCST]

[DVB-S] ETSI EN 300 421 DVB-S: Framing structure, channel coding and modulation for 11/12 GHz satellite services

[DVB-S2] ETSI EN 302 307 DVB-S2: Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2)

[dvb-T] ETSI EN 300 744 DVB-T Framing structure, channel coding and modulation for digitalterrestrial television

[DVB-H] ETSI EN 302 304 DVB-H: Transmission System for Handheld Terminals (DVB-H)

[DVB-SI] ETSI EN 300 468 DVB-SI: Specification for Service Information (SI) in DVB systems

[DVB-Data] ETSI EN 301 192 DVB-Data: Specification for data broadcasting

[ATSC 53C] ATSC A/53C: ATSC Digital Television Standard, Rev. C

[ATSC 65B] ATSC A/65B: Program and System Information Protocol for Terrestrial Broadcast and Cable, Rev. B

[ATSC 90] ATSC A/90: Data Broadcast Standard

[ARIB B10] ARIB STD-B10 Service Information for Digital Broadcasting System

[ARIB B20] ARIB STD-B20 Transmission System for Digital Satellite Broadcasting

[ARIB B24] ARIB STD-B24 Data Coding and Transmission Specification for Digital Broadcasting

[ARIB B31] ARIB STD-B31 Transmission System for Digital Terrestrial Television Broadcasting (ISDB-T)

[J.160] Architectural framework for the delivery of time-critical services over cable television networks using cable modems

[J.178] IPCablecom CMS to CMS signalling

[J.179] IPCablecom support for multimedia

2.2 – NGN Release 1 Requirements*

Abstract

This document provides the update of the NGN Release 1 Requirements document generated as WG1 output of London, November 2005 FG NGN meeting.

Table of Contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

2.2 – NGN Release 1 Requirements

1 Scope

This document provides a set of general requirements of NGN Release 1, including requirements of the NGN capabilities identified in NGN Release 1 scope [FGNGN-R1-SCOPE]. It is also aligned with the general goals and objectives of Recommendation [Y.2001]. Detailed requirements for support of the capabilities identified in NGN Release 1 scope [FGNGN-R1-SCOPE] are outside the scope of this document and are specified in related documents.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Specification. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Specification are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this document does not give it, as a stand-alone document, the status of a Recommendation.

[FGNGN-R1-SCOPE] ITU-T FGNGN deliverable, NGN Release 1 Scope

[Y.2001] ITU-T Recommendation Y.2001, General overview of NGN functions and characteristics

[M.3050] ITU-T Recommendation M.3050, Enhanced Telecommunications Operations Map (eTOM)

[G.711] ITU-T Recommendation G.711, Pulse code modulation (PCM) of voice frequencies

[G.729] ITU-T Recommendation G.729, Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)

[G.729A] ITU-T Recommendation G.729 Annex A, Reduced complexity 8 kbit/s CS-ACELP speech codec

[H.263] ITU-T Recommendation H.263, Video coding for low bit rate communication

[H.264] ITU-T Recommendation H.264, Advanced video coding for generic audiovisual services

[Y.101] ITU-T Recommendation Y.101, GII terminology: Terms and definitions

[Y.1411] ITU-T Recommendation Y.1411, ATM-MPLS network interworking - Cell mode user plane interworking

[G.723.1] ITU-T Recommendation G.723.1, Speech coders: Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s

[T.140] ITU-T Recommendation T.140, Application protocol for text conversation

[Y.1541] ITU-T Recommendation Y.1541, Network performance objectives for IP-based services

[G.1000] ITU-T Recommendation G.1000, Communications Quality of Service: A framework and definitions

[G.1010] ITU-T Recommendation G.1010, End-user multimedia QoS categories

[ETSI-TISPAN-R1-REQ] ETSI TISPAN NGN, Service and Capabilities Requirements;Release 1

[Y.NGN-account] ITU-T Draft Recommendation, Requirements and framework allowing accounting, charging and billing capabilities in NGN

[E.164] ITU-T Recommendation E.164, The international public telecommunication numbering plan

[FGNGN-SEC] ITU-T FGNGN deliverable FGNGN-OD-254, Guidelines for NGN security

[FGNGN-SECREQ] ITU-T FGNGN deliverable FGNGN-OD-255, Security Requirements for NGN Release 1

[FGNGN-FRMOB] ITU-T FGNGN deliverable FGNGN-OD-246, Mobility Management Capability Requirements for NGN

[Y.1710] ITU-T Recommendation Y.1710, Requirements for Operation & Maintenance functionality in MPLS networks

[Y.1730] ITU-T Recommendation Y.1730, Requirements for OAM functions in Ethernet-based networks and Ethernet services

[I.610] ITU-T Recommendation I.610, B-ISDN operation and maintenance principles and functions

[G.808.1] ITU-T Recommendation G.808.1, Generic protection switching - Linear trail and subnetwork protection

[M.3060] ITU-T Recommendation M.3060, Principles for the Management of Next Generation Networks

[ATIS-NGN-FMWK] ATIS Next Generation Network (NGN) Framework – Part 1: NGN Definitions, Requirements and Architecture

[Y.1271] ITU-T Recommendation Y.1271, Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-witched and packet-switched networks

[E.106] ITU-T Recommendation E.106, International Emergency Preference Scheme (IEPS) for disaster relief operations

[ETSI-TISPAN-R1-DEF] ETSI TISPAN NGN Release 1 Definition

3 Definitions and Abbreviations

3.1 Definitions

This document uses the following definitions.

Accounting: The action of collecting information on the operations performed within a system and the effects thereof.

Address: An identifier used for routing a communication to an entity.

Billing: Administrative function to prepare bills to service customers, to prompt payments, to obtain revenues and to take care of customer reclaims.

Charging: The set of functions needed to determine the price assigned to the service utilization.

Customer: The Customer buys products and services from the Enterprise or receives free offers or services. A Customer may be a person or a business.

Home Network (as used in context of section 4.3)**:** A local area network (LAN) communications system designed for the residential environment, in which two or more devices, e.g. personal computer (PC) and household electric appliances and equipment with embedded computers or intelligent functionality (e.g. air-conditioners, audio/video equipment, bath equipment, gas fittings, lighting equipment, microwave ovens, refrigerators, television sets, and washing machines) exchange information under some sort of standard control.

Home Network (as used in context of section 4.11)**:** The network associated with the operator/service provider that owns the subscription of the user.

Identity: The attributes by which an entity or person is described, recognized or known.

Identity Provider: A service provider that creates, maintains, and manages identity information for subscribers/users, and can provide an authentication assertion to other service providers within a circle of trust.

NGN User Identity Module: An entity that can be used to store, transport, process, dispose of, or otherwise handle user identity information.

Priority Classification: Classification of traffic classes according to different levels of priorities.

Priority Enabling Mechanisms: The mechanisms by which appropriate treatment of traffic according to priority classes may be enabled in the network.

Priority Signalling: Part of the priority enabling mechanisms using signalling.

Single Sign-On: The ability to use an authentication assertion from one network operator/service provider to another operator/provider for a user either accessing a service or roaming into a visited network.

Spam: Unsolicited bulk commercial messages or calls.

Subscriber: The person or organization responsible for concluding contracts for the services subscribed to and for paying for these services.

Terminal Equipment Identity: A unique identifier of a terminal equipment.

User: The user is the actual user of the products or services offered by the Enterprise. The user consumes the product or service.

User Attribute: A characteristic that describes the user(e.g., user identity's life time, user status as being "available", "don't disturb", etc.).

User Identity: A type of password, image, or pseudonym associated with a user, assigned by and exchanged between operators and service providers to identify a user, to authenticate her/his identity and/or authorize the use of service. Examples are biometric identifiers such as a user eye image, a finger print, a SIP URI, etc.

3.2 Abbreviations

This document uses the following abbreviations and acronyms:

AMR Advanced Multi Rate CODEC

ANI Application Network Interface

API Application Programming Interface

ATM Asynchronous Transfer Mode

ASN	Application Service Networking
ASR	Application Service Resiliency
CC	Content of Communication
CDR	Call Detail Record
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
COLP	Connected Line Identification Presentation
COLR	Connected Line Identification Restriction
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
DTMF	Dial Tone Multi Frequency
ETS	Emergency Telecommunications Services
EVRC	Enhanced Variable Rate Codec
FCAPS	Fault, Configuration, Accounting, Performance and Security Management
GPS	Global Positioning System
IMS	IP Multimedia Sub-system
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
LAN	Local Area Network
LEA	Law Enforcement Agencies
MMS	Multimedia Messaging Service
MPLS	Multi-Protocol Label Switching
NAT	Network Address Translation
NGN	Next Generation Networks
NNI	Network Node Interface
NUI	NGN User Identity
NUIM	NUI Module
OAM	Operations, Administration and Maintenance
OMA	Open Mobile Alliance
OSS	Operations Support System
QoS	Quality of Service
PCM	Pulse Code Modulation

PDA	Personal Digital Assistant
PLMN	Public Land Mobile Network
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
TDM	Time Division Multiplexing
TDR	Telecommunications for Disaster Relief
UMTS	Universal Mobile Telecommunications System
UNI	User to Network Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VPN	Virtual Private Network
WB-AMR	Wideband-Advanced Multi Rate CODEC

4 Requirements for basic capabilities

4.1 Requirements for transport stratum capabilities

The following provides some requirements of the NGN transport stratum capabilities :

– Real time and non real time communications should be supported

– Various communicating patterns, such as one-to-one, one-to-many, many-to-many and many-to-one, should be supported

– Adequate performance, reliability, availability, scalability levels should be ensured.

4.2 Media resource management

The NGN should support various media resources and media resource management capabilities to enable a wide range of mediaapplications. The following provides a non-exhaustive list of applications which may require media resource management capabilities:

– Recorded and composed announcements;

– Interactive voice response;

– Audio recording;

– Voice mail;

– Advanced speech recognition;

– Text to speech conversion;

– Audio conference bridge;

– Video/text/audio/data bridges;

– Applications with usage of media forking (e.g. Lawful Interception scenarios);
– Media insertion (e.g. image, text , video) in multimedia streams;
– Content caching, hosting and serving;
– Facsimile receiving and sending; and
– Streaming media playing

4.2.1 Codecs

Requirements for codecs include:

– The NGN should support different types of codecs (e.g. audio, video and text codecs). It is recognized that some codecs play an important role in existing and emerging networks for audio and video services: For example - G.711 in circuit switched oriented networks, G.729 in packet-based networks, AMR (and WB-AMR for Wideband telephony) in 3G UMTS networks, EVRC in 3GPP2 networks.
– It is the responsibility of entities at the rim of the NGN (e.g. NGN terminals and user equipments) and network equipment originating and terminating the NGN IP media flows, to negotiate and select a common codec for each "end-to-end" media session. Therefore the NGN shall allow end-to-end negotiation of any codec between NGN entities (terminals, network elements).
– If needed, audio transcoding is performed to ensure end-to-end service interoperability. This may be performed for example by residential or home gateways located in the customer premises, or by access, media or network interconnect gateways depending on the communication configuration.
– Transcoding should be avoided wherever possible.

In order to enable interworking between the NGN and other networks (including the PSTN/ISDN, mobile networks and other NGNs) the NGN must be capable of receiving and presenting G.711 coded speech when interconnected with another network.

When a packetisation size is not selected by codec negotiation between terminals and/or network elements or agreed by bilateral arrangement, a speech packetisation size of 10ms samples should be used for G.711 coded speech; this is recommended as an optimum value balancing end-to-end delay with network utilisation. It is recognised that there may be network constraints which require that a higher value is agreed by bilateral arrangement; in such cases a value of 20ms is recommended.

NOTE – Where a packetisation size is selected by codec negotiation between terminals and/or network elements the present document places no requirements on the value to be selected.

NOTE – The above doesn't mandate that any audio codec be supported by terminals as well as it does not impose any requirement that NGN networks support audio transcoding between any arbritary codec and G.711.

In addition, the following list of audio codecs is recommended:

– Advanced Multi Rate Codec (AMR): in order to support 3GPP terminals and to facilitate interworking with 3GPP network
– Enhanced Variable Rate Codec (EVRC): in order to support 3GPP2 terminals and to facilitate interworking with 3GPP2 network
– G.729A [G.729A]: in order to facilitate interworking with existing VoIP networks and support existing VoIP terminals

A Wide-band codec: in order to provide voice service with a superior quality experience by the end-user.

Audio transcoding may be performed to provide end-to-end service interoperability when needed, but should be avoided wherever possible.

In order to enable the interworking for video communication services between NGN and other networks, the support of the H.263 profile 0 [H.263] and H.264 baseline profile [H.264] codecs is recommended.

In order to provide video services with a superior quality experience by the end-user, a high-quality video codec is recommended.

NOTE – The above doesn't put any requirement about the codecs to be supported by terminals nor does it mandate that NGN shall support video transcoding between any arbitrary codec and [H.263] or [H.264].

4.3 Access network

NGN is expected to support a wide variety of application service types, especially broadband multimedia services including video conference, streaming, and advanced telephony services. Since these services must be accessed through access networks, access networks must satisfy a number of requirements to enable use of such applications. In particular:

- NGNs shall support access transport functions of diverse technologies and capabilities [FGNGN-R1-SCOPE]
- NGNs shall accommodate various end-to-end network configurations including mixed technology access transport function configurations.
- All NGN access transport functions shall be capable of providing IP connectivity at the transport stratum level between the end-user functions and the core transport functions [FGNGN-R1-SCOPE].
- An NGN access network should support broadband capabilities.
- Services and applications, including session control, shall be independent of the access network type used.
- Parameters related to the access network should be manageable and controllable, (in order to realize functionalities such as QoS, security and accounting) and to enable the selection of the optimal data transmission mode, e.g. optimal speed and type of compression or conversion.
- NGNs should support connectivity of customer networks independently of their level of configuration complexity, such as home networks.
- NGN should have access registration features at the access network level, in order to access NGN services from the user equipment. Access networks should provide network level identification and authentication, manage the IP address space of the access networks and authenticate access sessions.

4.4 Interoperability and Interworking

Interoperability and interworking are two distinct functions and are defined respectively in Recommendations [Y.101] and [Y.1411]. Interoperability and interworking are key NGN concepts and it is required that all NGNs (and components of an NGN) be interoperable and that NGNs should be able to interoperate and interwork with other networks.

4.4.1 Interoperability

Interoperability among multiple NGNs is essential. The NGN shall support interoperability between different NGN domains to enable end-to-end services when users are located in different NGN domains.

4.4.1.1 Interoperability requirements between NGN components within a single NGN administrative domain

The NGN components within a single administrative domain should interoperate.

4.4.1.2 Interoperability requirements between different NGN administrative domains

Domain of an NGN is a management concept, that is, one domain is managed or controlled by one management entity. Since one operator may separate management of its NGN into multiple levels or using various policies, one operator may have multiple NGN domains.

In order to realize interoperability between NGN administrative domains, a set of network capabilities should be supported. Such network capabilities include:

– Creating, mapping, converting and transcoding the media traffic
– Static and dynamic routing configuration
– Signalling interworking
– Conversion of name, number or address
– Exchanging charging and billing information
– Security policy
– Exchanging user and terminal profile

Interfaces between networks may partition the network into separate administrative domains. These interfaces may need to support various functionalities for security and control. The interface between a trusted domain and a non-trusted domain may need to remove some of the trusted domain's internal information and hide the user's information. The interface between the trusted domains also may need to hide some information about each trusted domain to provide inter-domain safeguards. The NGN structure should be designed with these interface characteristics in mind.

4.4.2 Interworking

The NGN shall support interworking with existing fixed and mobile voice, multimedia and data networks.

In general, the interworking function should support the following:

– Control and signalling interworking;
– Media interworking;
– Application services protocol interworking

NGNs should support capabilities for determining where transcoding should be performed in the most efficient way. This is because transcoding is a processing resource intensive task for NGNs. The term "efficiency" used herein should be interpreted in the most general sense and thus efficiency considerations should include considerations related to resource consumption, e.g. extra media paths, and QoS aspects, e.g. delay impact.

4.4.2.1 Interworking with PSTN/ISDNs

NGN that interconnect with PSTN/ISDNs should support the following interworking requirements:

– Transcoding to allow interworking of different types of codecs (e.g. PCM G.711 codecs with [G.723.1] or [G.729] codecs)
– Conversion between PSTN text telephony and packetized real time text (e.g. [T.140]).
– Termination of different types of physical/logical links (e.g. TDM 64 kbit/s, 1544 kbit/s or 2 Mbit/s links and IP packet-based technology links.
– Support of echo cancellation and echo canceller control functions.
– Signalling protocol conversion.
– Translation, screening and filtering of signalling messages and message parameters.
– mapping between numbers and NGN resource identifiers (e.g. SIP URIs).

4.4.2.2 Interworking with other networks

NGN shall be capable of interworking with:

– Public Land Mobile Networks (PLMN)

– Internet

– Broadcast networks

– Packet cable networks

– Enterprise networks

4.5 Routing

NGN should support routing schemes most suitable for the NGN providers. In particular NGN should support:

– Both static and dynamic routing schemes;

– Routing schemes which can effectively operate across NGN network domain boundaries, thereby allowing interoperability of NGNs

4.6 QoS-based resource and traffic management

Quality of Service required by an application varies greatly depending on its context. It is imperative that the service level requested by an application is received. Further, it is desirable that processes exist to allow for verification of provided service levels.

Applications using the NGN to provide services should be able to place a service request which is explicitly or implicitly linked to QoS related parameters, such as throughput, delay, jitter and loss.

4.6.1 General QoS requirements

General QoS requirements:

– NGN should support a wide range of QoS-enabled services

– NGN shall provide end-to-end QoS within an NGN administrative domain

– QoS should be supported within NGN administrative domains and through the use of SLA's for links between NGN administrative domains.

NOTE – The definition of QoS apportionment agreements between domains of different network operators is for further study.

– Appropriate QoS levels should be maintained even when multicast functionality is used.

4.6.2 QoS service level support, classes and priority management

Key QoS parameters of the NGN should be negotiable between the customer and the provider. The provider response to a customer request, which includes explicit QoS needs, will be in the context of a SLA (Service Level Agreement). The SLA shall be managed by call control (signalling) protocols that support such QoS parameter exchanges.

NGN should support:

– User originated SLA negotiations with NGN service and network providers.

– User oriented QoS requirements, consistent with the general framework of quality of communication services as defined in [G.1000] and with the end-user multimedia QoS categories identified in [G.1010].

- Access technology independent QoS classes [Y.1541] (e.g. QoS classes should be applicable from a UNI in one access technology environment to a UNI in a different access technology environment).
- A flexible QoS architecture capable of supporting different QoS control mechanisms.
- QoS control mechanisms for traffic and congestion control.
  - which enable QoS negotiation at both the transport and the service strata and which allow dynamic modification of QoS parameters
  - which allow operators' implementation of transport independent and transport dependent QoS policy controls
  - which provide the capability to extend policy-based management across multiple domains in order to assure QoS across domains
  - corresponding to different technologies and business models
  - which allow negotiation between users and applications for multimedia sessions and for individual media components in a multimedia session, both at the time of a session establishment as well as during the session
- QoS policy control via QoS signalling.
- Priority Classification, Priority Signalling and Priority Enabling Mechanisms.

4.6.3 Quality measurement and prediction

Perceptual quality metrics for NGN services and performance metrics associated with NGN functions will be required, particularly when they are invoked in response to human-triggered actions.

Service quality should be measured pro-actively for each service. The frequency of measurement should depend on the service level specifications.

Mechanisms to predict the quality of the experience of the NGN services perceived by the customer should be provided.

4.6.4 Processing/traffic overload management

The NGN shall have mechanisms available to control overload that: [ETSI-TISPAN-R1-REQ]

- strive to automatically maximise effective throughput (i.e. admitted service requests/sec) at an overloaded resource.
- achieve this throughout the duration of an overload event, irrespective of the overloaded resource's capacity or of the number of sources of overload;
- are configurable by the service provider so that, under processing overload, a high proportion of response times at overloaded resources are low enough so as not to cause customers to prematurely abandon service requests;
- should be possible to be applied within a service provider's NGN, and between different service providers' NGNs;

4.7 Accounting, charging and billing

NGN requirements for accounting, charging and billing are summarised below:

- Accounting functions, off-line (i.e. post processing) and on-line charging (i.e. charging during the session), shall be available.
- Open mechanisms should be available for charging and billing management.
- Various charging and billing policies should be supported (e.g. fixed rate charging and usage based per-session charging and billing).

– Accounting functions should support services with multicast functionality. The accounting functions should be able to report which user received which information as well as session start and stop times.

– The NGN should enable all possible types of accounting arrangements, including transfer of billing information between providers. This requirement also includes e-commerce arrangements.

NOTE – In Content Delivery Services scenarios with multicast functionality, services may be provided by joint activities of multiple companies (e.g. several content service providers and a network service provider): charging/billing functionality between companies is necessary in addition to charging/billing functionality to end users.

Specific accounting, charging and billing detailed requirements are addressed in [Y.NGN-account].

4.8 Numbering, naming and addressing

The following requirements are necessary to support numbering, addressing, naming and directory services, except where noted, they apply to both the transport and service strata.

General requirements for Numbering, Naming and Addressing

– Both dynamic and fixed address assignment modes should be supported.

– Addressing system, naming system and directory service may be implemented by using an individual mapping scheme for each service, or via a mapping scheme that is common across different services.

– Dynamic update of the naming service database should be supported. For example, in the case of a mobile terminal, addresses at one or more layers may dynamically change depending on the terminal's location and databases must be capable of reflecting this.

Addressing schemes

– As a minimum, the NGN shall support Internet IP addressing schemes. [transport stratum].

– The NGN shall support IP multimedia communication establishment (in both the originating and terminating case) using at least E.164 Telephone uniform resource identifiers (TEL URIs), e.g. tel:+4412345678 and/or SIP Uniform Resource Identifiers (SIP URIs), e.g. sip:my.name@company.org, as a minimum.

– In some service scenarios, e.g. interworking with PSTN/ISDN, the NGN shall support IP multimedia communication establishment (in both the originating and terminating case) using E.164 numbering with ENUM-like support.

– Addressing schemes should support various service types, such as unicast, multicast and broadcast.

– A group addressing scheme, which enables multicasting for such services as remote conferencing, must be supported.

– Other naming and addressing schemes such as private numbering should be supported.

Address resolution

Recommendation [Y.2001] provides fundamental principles and requirements for name and/or numbering resolution. In line with those, the following are required:

– High resolution speed: Resolution of a name to a transport stratum address should be fast enough to not negatively impact real-time applications.

– High capacity: The databases storing addresses should have enough capacity to handle the numerous concurrent resolution requests which are generated throughout the entire network.

– Scalable: An NGN database should be scalable so that it can expand in order to handle increased demand for the address resolution.

– Reliability: The address resolution system is directly related to the running of an NGN, so it should have carrier class reliability. Address resolution systems shall be designed so that they are not a single-point of failure, for example, with distributed address resolution mechanism.

– Security: Security measures shall be in place for the address resolution system. This system may use databases that are internal or external to the NGN, e.g. an Internet DNS database. Security is mainly maintained by means of user access authentication, data security, network data synchronization and fault recovery.

NOTE – The criteria used to estimate whether the above address resolution requirements have been satisfied depend on the service under consideration.

Addressing and naming interworking

An address or name in one network needs to be translated to an address or name in another. This is done as one of the interworking functions performed when the networks interconnect. Databases and registries may be required to perform this interworking function.

– An NGN should support multiple transport stratum address interworking scenarios without affecting the service provided to end-users (i.e. interworking scenarios among different address domains, such as IPv4 and IPv6 address domains, public and private address domains).Address format conversion functionality shall be used to address format differences, in both the transport and service strata.

– An NGN should support transport stratum address translation without affecting the service provided to end-users.

When the address format differs or address ranges used overlap between two networks, address translation functions are necessary. The Network Address Translation (NAT) function may be used to resolve address range overlaps that occur for IP addresses.

4.9 Identification, authentication and authorization

The requirements in this section cover NGN User Identity (NUI). The NUI is used for addressing, identification, authentication and authorization, and as such is not tied to any specific set of NGN services or service modules. Furthermore, the concept of ubiquitous identification plans currently being defined and developed by SG2 should be applicable to NGN services as well.

4.9.1 General requirements

There are requirements for identification, authentication and authorization in both the transport stratum and the service stratum. In the transport stratum there are requirements on how the NGN transport resources can be used. In the service stratum requirements are on the association between a user and a service or between a user and another user, perhaps outside of the particular NGN under consideration. Sometimes the phrase “service provider” has been used to refer to the provider of transport stratum services. In this sub-clause, the network provider is usually shorted to “the NGN,” and the "service provider" is the exactly that, the "provider of the service" – it could be anywhere, and is not necessarily the same entity as the network provider.

– The NGN shall support authentication and authorization functions for both the transport and the service strata. Transport stratum authentication requires a user to be identified by the network in order to obtain access to the network and to privileged uses. An authentication function can be a significant factor in protection from unauthorized use of networks, such as SPAM mail prevention. By the authorization function, the access authority to network resources can be set up and access violation can be prevented.

– At any time the NGN shall be able to verify the identity of users and, if desired, their association to the terminal equipment they are using and to check the authorization of the users to use resources of the NGN.

A service provider may provide authentication and authorization functions. However, definition of authentication and authorization mechanisms is beyond the scope of the NGN.

An NUI is a means for a user to access telecommunication services at any terminal on the basis of a personal identifier and for a network operator or service provider to identify and authenticate the user. It also enables network operators and service providers to provide those services delineated in the user's service profile, e.g., addressing, routing and charging of the NGN user's calls. Furthermore, it provides a means for others to refer to an NGN user as a target for terminating services (e.g., voice calls), information queries, and other NGN services.

– User Identity types

  Every NGN end-user shall be uniquely identifiable by one or more of each of the following two types of NGN User Identities (NUIs)

  1.1. Public User Identity: An NGN number or address that is normally used by one NGN user to contact or communicate with another NGN user.

  1.2. Private User Identity: A private NGN user identity can be used to identify the NGN user to her/his NGN network or service provider. The private NUI is one component used for authentication.

– The NGN shall allow separate identification, authentication and authorization of both users and terminal equipment as well as verification of the association between the user and his/her terminal equipment.

– Authentication, Authorization and Accounting (AAA), performed by the NGN provider and the service provider should be processed securely.

– A service provider shall provide mechanisms that allow presentation of the public identity of the session initiator.

– A service provider shall provide mechanisms to withhold the public identity of the session initiator, if the presentation of this information is restricted by the session initiator or the network.

– A service provider who performs authentication shall support mechanisms to guarantee the authenticity of a public user identity presented for an incoming call (e.g. CLIP).

– A service provider who performs authentication shall provide mechanisms that allow the presentation of the public user identity of the connected party to the session originator, if this is not restricted by the connected party or the network (e.g. COLP).

– The NGN provider shall be able to verify the private identity of users and terminals. Additionally it shall be able at any time to check the authentication and authorization of users and terminals to use resources of the NGN.

– A service provider shall be able to verify at any time the private identity of users of the services it provides. Additionally the service provider shall be able at any time to check the authentication and authorization of users to use resources it manages.

– Both private and public identities of NGN users of the transport stratum resources, (identities used for authentication and authorization) shall be administered by the network operator.

– Both private and public identities of service users of the service stratum resources, (identities used for authentication, authorization and routing), shall be administered by the service provider and shall not be changeable by the user.

– Private NGN user identities provided for authentication/authorization shall not be visible to other users.

– Public NGN user identities of service users shall be visible to other users if no service intermediaries are involved.

– A service provider may allow a user to access a service from multiple terminals in parallel using the same public and private user identity.

– It may be possible for a single user authentication and authorization to be used for multiple services and using multiple private user identities via a single subscription procedure ("single sign-on"). Note: Even when only a single authentication event is required, multiple authorization events may still be needed. Also single-sign-on can be implemented on the client side, such that even though multiple authentications are required, the human user only needs to establish an authentication relationship once.

NGN Release 1 does not require support of single sign-on capabilities. However, where such support exists with current technologies, it is expected to be also used for NGN Release 1.

4.9.2 Requirements for User Identity

– Multiple User Identities

It shall be possible for an NGN end-user to have multiple public and private identities, and it shall be possible to segregate one identity from another (e.g. for personal use and business use). Examples of multiple private user identities are multiple registrations, call forking on multi-line phone systems or single sign-on procedures.

– Identity Portability

Public identities of users of service stratum resources should be portable, giving the NGN users/subscribers the ability to retain their assigned NUIs and change their service providers.

– Identity Independency

The public NUI should be assigned to users independent of its repository module, the user terminal and the underlying network technologies. However, backward compatibility (e.g. for POTS handset) may be achieved via proper inter-working functions

– Support of Multiple User Identities

As the repository for NGN user identities, an NUI module (NUIM) may contain multiple unique public and private identities each stemming from either –multiple profiles, e.g. Corporate, Enterprise, or multiple uses, e.g. personal use and business use.

– Support for Identity Attributes

An NUIM may contain different private identity attribute information such as the lifetime of that identity for the end-user, the subscriber, the network in use, etc.

– Support for Attribute Conditions

An NUIM may support specifying conditions (e.g. setting timer as validity conditions) for a user attribute/data stored in the NUIM by an attribute provider (e.g. network, principal user, end user).

– Selective Attribute Authorization

An NUIM shall support selective authorization of user's private identity attribute information by an attribute provider (e.g., identity lifetime).

– Support for subscriber programming

An NUIM should support subscriber's programming of different permissions for different attribute information, e.g. access to and usage of private identity attribute information, on a per attribute basis.

– User and Terminal Binding

  An NUIM shall support a dynamic binding of the public user identity and the terminal equipment identity.

– Multiple Terminal Association

  An NUIM shall allow association of an end user public or private identity to multiple (mobile or fixed) terminal equipment identities. The end user may be allowed to use multiple terminals at any given time.

– Identity Information Transfer

  An NUIM shall support the transfer of the NUI information by the NGN end users providing input either on their own terminal or on the receiving terminal (e.g. point of sale terminal).

4.9.3 Requirements for authentication

Authentication is the process of establishing confidence in user and terminal equipment identities. From the point of view of providers, the NGN may distinguish between network authentication and service authentication. From the perspective of consumers, the NGN may distinguish between user authentication and terminal equipment authentication. Network authentication is the process of verifying users/terminal equipments for network access only by network providers. Service authentication is responsible for verifying user/device identities for service usage purpose.

These distinct authentication concepts may be unified into a single concept or be applied separately, depending on the transport technology or business model. For example, a single authentication flow will be processed if a network provider is also a service provider.

Specific requirements for authentication include:

– NGN should provide the capability to authenticate users or terminal equipments for using resources in both transport stratum and service stratum.

– Depending on the underlying access networks, a variety of network authentication mechanisms may be applied and user profiles may be located separately.

– Service authentication should be independent of the underlying access network technique and maintain a consistent service authentication mechanism.

– The NGN may require a user/terminal equipment to either explicitly or implicitly input authentication information.

– Private identification should be used for network authentication. This may be associated in the scope of a single network provider (with multiple access networks) or in the scope of a single access network.

– The NGN should support both S/W-based and H/W-based authentication mechanisms.

– Some mechanisms for device authentication may use the device profile.

– NGN should provide capabilities for authentication of the user to the service provider, and authentication of the service provider to the user.

4.9.4 Requirements for authorization

General requirements for authorization for Release 1 NGN include:

– NGN should provide capabilities to allow service access by authenticated users or devices according to their access rights, subscriber profiles and network policy.

– Service authorization mechanisms should be independent of underlying network technologies.

– NGN should provide and maintain consistent service authorization mechanisms across the network.

– Authorization capability of NGN should support mobility.

4.10 Security and privacy

The NGN should provide:

– Protection against unauthorized use of network resources and unauthorized access to information flows and applications.

– Authentication of the identity of the communicating entities;

– Data confidentiality and avoidance of unauthorized disclosure of information;

– Integrity of data to ensure that data will not be altered or destroyed by unauthorized means;

– A means to allow for accountability, whereby individuals are held responsible for the effect of any of their actions;

– Availability and accessibility of the network, upon demand by an authorized entity

– Mechanisms to prevent non-repudiation, to prevent one of the entities or parties in a communication from falsely denying having participated in the whole or part of the communication

– Privacy of the end-user's data by only releasing information when authorization is obtained to do so, e.g. preferences, profiles, presence & availability and location information.

For detailed requirements of NGN security and privacy, refer to [FGNGN-SEC] and [FGNGN-SECREQ].

4.11 Mobility management

Mobility management involves the ability of mobile objects, such as users and terminals, to be able to roam between different networks (NGN or non-NGN).

For both wire-line and wireless terminals, the network has to keep track of the location of the terminal. This feature is similar to the roaming functionality associated with cellular phones. In NGN Release 1, nomadicity for personal mobility and terminal mobility shall be supported. This sub-clause provides the general requirements for mobility management focused on support of customer needs. For detailed requirements of NGN mobility management, refer to [FGNGN-FRMOB].

General requirements include:

– Support of location management for user registration, location update and address translation to enable mobility across providers' network boundaries.

– Support of subscription management of mobile objects (independent subscription of various objects)

– Support of device profile management which enables looking up device profiles from anywhere, such as address, geographical location, radio condition, etc.

– Support of user profile management thereby enabling access to the user profile data or parts of it within user's home network, from user's visited network's or 3rd party networks in a standardized and secure manner. This would allow performing management functions such as authentication, authorization, service subscription (based on geographic location), charging, etc.

– Support for mobility related management, assuring usage efficiency, support for existing systems, independent of access network technologies, QoS and security support.

– Provision of mechanisms for service continuity for mobile users, which enable receiving calls or data at any time and keeping data connection while terminals are moving within the same access network of the NGN.

– Support of security for handover to prevent unauthorised access and ensure user privacy.

– Support of location confidentiality to conceal location information of users from non-trusted entities.
– Support of paging capability for setup of incoming calls to save power in mobile terminals and reduce signalling in the network.

4.12 OAM Requirements for NGN

It is recognized that OAM functionality is important in public networks for ease of network operation, for verifying network performance, and to reduce operational costs by minimizing service interruptions, service degradation and operational downtimes. OAM functionality is especially important for networks that are required to deliver (and hence be measurable against) network performance and availability objectives [Y.1710] [Y.1730]

4.12.1 General OAM requirements for NGN

The following OAM requirements should be satisfied by NGNs;

– The ability for a network operator to choose the desired OAM functions.
– The applicability of OAM functions to point-to-point and multipoint-to-multipoint applications.
– The support of OAM functions to allow efficient scaling to large network sizes.
– The ability to support detection of faults, defects and failures.
– The ability to diagnose, localize and notify the network management entities and take appropriate corrective actions.
– The ability to prevent the customer from triggering any service or network provider OAM function.
– The ability to prevent the customer from detecting or localizing failures since this is part of service provider or network provider's responsibility.
– OAM functions should follow the same route/ path as the user plane traffic.
– The following anomalies should be automatically detected and corresponding defect states, with well defined entry/exit criteria and appropriate consequent actions, should be defined:
  • simple loss of connectivity
  • unintended self-replication
  • lost frames
  • errored frames
  • misinserted fames as per [Y.1730]
– OAM functions should be backward compatible. OAM function should be defined such that a network equipment that do not support such functions will be able to either silently discard the OAM function or let OAM function pass through transparently without disturbing the user traffic or causing unnecessary actions.
– OAM functions should perform reliably even under degraded link conditions, e.g., error events.
– Connectivity status assessment should not be dependent on the dynamic behaviour of customer traffic according to [Y.1710], [Y.1730]
– NGN should support server-client layer OAM relationships between lower layer and upper layers (e.g., signal fail/signal degrade) in case of a multi-layer network.
– A defect event in a given layer network should not cause multiple alarm events to be raised, nor cause unnecessary corrective actions to be taken, in any higher layer level client layer networks. The client layer network should support alarm suppression for server layer sourced defects whose

presence have been communicated by forward defect indication means. Client layer network should support forward defect indication capability. [Y.1710],[Y.1730]

- The functionality of an OAM flow should not be dependent on any specific lower or upper layer network. This is architecturally critical to ensure that layer networks can evolve, be added and removed without impacting other layer networks.
- The functionality of an OAM flow should be sufficiently independent of any specific control-plane such that any changes in the control plane do not impose changes in user plane OAM (including the case of no control-plane). Like the previous requirement, this is also architecturally critical to ensure that user plane and control plane protocols can evolve (or control plane protocols added/removed) without impacting each other.
- Support of multiple network operator environments.
- NGN services may be provided by multiple network providers. In such cases, it is necessary to detect and notify which network provider is responsible for the defect so that quick action can be taken.
- NGN should have mechanisms that make sure that service provider/network operator's OAM flows, which are meant for their internal use, are confined within their networks and do not leak out to customers or other service providers/ network operators.
- If NGN service is carried over networks belonging to different operators, the operator that offers the service to the customer should be aware of a service fault as minimal information even if the fault and detection point is located in the network of another operator.
- In order to realize end-to-end OAM functions in heterogeneous networks so that services can be managed, OAM functions need to be supported in interworked networks.
- In order to allow managing a portion of a network which is under the responsibility of a operator, and to allow defining maintenance entities flexibly, it is necessary to support "segment" OAM functions as well as end-to-end OAM functions. Segment means a part of an end-to-end connection which is defined for operation and maintenance purposes.
- NGN should support recording of service downtime for performance and availability measurements.
- The information produced by OAM functions should be managed so as to provide the appropriate indications to the maintenance staff for maintaining the Quality of Service level offered to customers [I.610].
- OAM for NGN should support capabilities for performance monitoring

4.12.2 Protection switching requirements

Survivability functions are necessary to realize highly reliable networks. Among the survivability techniques, protection switching is appropriate to realize fast and deterministic survivability.

The following are general requirements for NGN protection switching:

- Support of G.805 identified trail, connectionless trail and sub-networks.
- Ability to prevent network layering violations (e.g. a higher layer defect should not trigger lower layer protection switching).
- In case that there are more than one layer involved in protection switching, the lower layer shall have priority over the higher layer (this is known as Inter-layer escalation strategy).
- Support for fast triggering of protection switching mechanisms after a failure event occurred. A completion time of 50 ms is proposed as objective for protection switching.
- Both 1+1 and 1: n protection switching should be provided.
- Extra traffic should be supported where possible.

– Impacts on the performance of the network (e.g., additional delay, delay variation, bit errors, packet losses, etc.) due to protection switching should be minimized.
– Operator control such as lockout of protection, forced switch and manual switch commands should be supported.

Detailed requirements for specific technologies are given in various Recommendations such as [G.808.1].

4.12.3 Rerouting requirements

When serious accidents and special events occur, networks degrade or failure at the worst case may occur because of congestion triggered by network access and systems failure. Functionalities as rerouting (automatic switching to alternate route and dynamic routing), downgrading of performance or quality, traffic control mechanisms are therefore required.

These functionalities can also be regarded as part of network integrity functions.

In order to enable a dynamic routing function for maintaining communication at failure time in the network, it may be necessary to exchange failure information and composition information (routing information etc.) between the management functions of the network. For this reason, network status information such as failure type, emergency level and cause may be shared.

The following are general requirements for NGN rerouting:

– It should be possible to apply rerouting on a trail, connectionless trail or on a subnetwork.
– In case that there are more than one layer involved in rerouting activity, the lower layer shall have priority over the higher layer (this is known as Inter-layer escalation strategy).
– Rerouting mechanism should be capable of finding an alternative route within an acceptable time.
– Impacts on the performance of the network (e.g. additional delay, delay variation, bit errors, packet losses, etc.) due to the rerouting function should be minimized.
– Operator control should not be precluded.
– Network re-optimization should be possible where necessary after the restoration of the impaired traffic.
– When recovered from the fault and degraded state, it is required to restore performance and quality.

4.12.4 Requirements for application service resiliency

In NGN, required resiliency of application services in the case of occurrence of network's failure should be described clearly. Required conditions for resiliency should be described for each application service, since these vary greatly for each application service.

The following are general requirements for Application Service Resiliency (ASR):

– It should be possible for the network transport and control planes to together ensure a state of total availability of 99.999% for the application service in the face of anticipated failure conditions.
– It should be possible to independently assign different ASR classifications to different application services.
– It should be possible to independently assign different ASR classifications to different application services on a per flow basis
– Depending on the ASR level in question, it should be possible for the application services covered by ASR to experience the same level of service quality experienced prior to the failure event.
– ASR classifications should not necessarily have to be signalled to the network element by the end user terminal

– It should be possible for ASR to be supported from the point of ingress to the point of egress of the service provider network.
– It should be possible to differentiate between media and control plane message flows.
– It should be possible for the user to be informed if the required ASR level cannot be met by the network

4.13 Management aspects

Management of Next Generation Networks is intended to support a wide variety of management areas which cover the planning, installation, operations, administration, maintenance and provisioning of networks and services. The high-level goal will be to provide survivable and cost-effective networks.

Detailed requirements for the management of NGN networks are beyond scope of this document and are provided in the management-specific recommendations, such as [M.3060]

5 Requirements for service support capabilities

5.1 Open service environment

Implementing new functionalities in current networks may be limited or impossible due to the capabilities of the installed equipment. Software provisioning to implement new functionalities is essentially restricted to the equipment vendors, since the application programming interfaces (APIs) are typically proprietary (i.e. not open).

NGN enables new capabilities and could support a wide range of emerging services, including those with advanced and complex functionalities. Due to a drive from the 3rd party applications and service providers to develop new service functions and capabilities accessible via open and standard interfaces, there is an increasing need for network and service providers to cooperate in the development of standard APIs. Furthermore, software reusability, portability, and use of commercial software should be supported to facilitate cost effective development.

Some general benefits of an open service environment (i.e. an environment where public standards define the interfaces) are:

– Network services can be easily developed by network operators as well as by 3rd parties.
– Network services can be made portable and/or reusable across networks.
– Open and standard application network interface (ANI) will accommodate interactions between the NGN entities and the 3rd Party application and service providers. The ANI may also be used by network services and applications for service creation.

Within the open service environments, each enabler shall be able to function either independently or in conjunction with other enablers for realization of a service. Each enabler performs all corresponding service functions for the requesting entity (e.g. third party). The services may be realized in different networks, hence the enablers must be able to function independently from underlying network technologies.

5.1.1 Service independence

The open service environment should support the following service independence requirements.

– Independence from network providers: functionality, operations and management of third party service provider applications and value added services should be all independent from underlying network providers' technologies and infrastructure.

– Independence from manufacturers: a multi-vendor open service environment should be supported, providing users with a wide range of value added services and applications in a competitive environment.

5.1.2 Transparency

The open service environment should support the following transparency requirements.

– Location transparency: In a distributed environment, third party service providers should be able to access services from anywhere through a variety of access networks and the relevant service capability servers, regardless of the actual physical location of such servers.

– Network transparency: The open service environment should allow services to be technology and terminal agnostic.

– Protocol transparency: Protocol transparency should be achieved by providing standardized protocol programming interface tools for realizing independent service control process and shielding complex network technical details to the open service environment.

5.1.3 Services coordination

The NGN open service environment should provide capabilities for coordinating identities, sessions and services. In addition, it should offer coordination between network user device resources and applications, either in a centralized way or with support functions distributed across user devices, edge devices, etc. Service coordination should be supported where mechanisms already exist, e.g in open service environments such as OSA/Parlay, Parlay X and Open Mobile Alliance (OMA) service environments.

5.1.4 Application service interworking

The NGN open service environment capability should allow interworking between application services and network entities for creation and provisioning of value added services.

5.1.5 Service discovery

The NGN should support a wide range of services and applications which may also change over time.

– NGN should support service discovery capabilities to allow users and their devices to discover the services, applications, and other network information and resources of their interest.

– Service discovery capabilities should allow users and their devices to discover services over any specific underlying networking technology (*e.g.,* cellular systems, wireless local area networks, DSL).

– Service discovery mechanisms should be independent of the underlying networking technologies so that they can support heterogeneous and changing network technologies

– The service discovery capabilities should allow users to discover user-interest and device-interest services and network information.

  • User-interest services can be directly used by users. Examples of user-interest services include directory services, translation services and shared facilities (e.g., IT support information).

  • Device-interest services can be directly accessed by, for example, mobile handsets or portable PCs. Examples include printers, backup devices, and CD/DVD-writers.

  • Network information allows users or devices to detect and select networks.

– The service discovery capabilities should support multimedia user-interest content search (e.g., searching by text, image, and video). Device-interest services and information may not be directly usable to human users, but may instead be used by user terminal devices to support networking functions and/or the applications running on the user terminal devices. Examples of device-interest services and information include the addresses of key networking elements that user devices need to

know, such as authentication servers, IP address allocation servers (e.g., DHCP servers), and SIP servers.

– The service discovery capabilities should not be limited to only the traditional client-server based systems. Instead, service discovery may be realized using peer-to-peer technologies or a combination of client-server and peer-to-peer technologies. The service discovery capabilities should support a variety of scoping criteria (e.g. location and cost) to provide appropriate scaling, with appropriate mechanisms to ensure security and privacy.
– The service discovery capabilities developed for the NGN should be independent of lower layer protocols and should take into account scalability and bandwidth consumption (e.g. broadcast methods should be avoided).

5.1.6 Service registration

The Open Service Environment shall provide the means to manage the registration of services. General requirements are as follows.

– A means of configuring, installing, activating, publishing and removing services should also be provided.
– Enablers or components of multiple third parties, and the relationship between these enablers or components should be tracked.
– Information on changes of state should be made available, for example, due to upgrades.
– Mechanisms for discovery of service enablers or components should be provided.

5.1.7 Developer support

Developer support is a key issue of the service delivery chain, both within the incumbent service provider and within third parties who can extend service capabilities and broaden the overall service offering.

Hence, lower service life cycle costs can be achieved by automating the process, reducing administration and reducing integration costs in areas such as service and subscription provisioning and OAM. In addition, service level diagnostics can be implemented in order to improve the manageability of the development process, in order to isolate faults before service deployment.

The NGN should offer an efficient development support environment which should support:

– construction of new applications
– trialing of applications
– deployment of applications
– removal of applications

The support offered to developers should include:

– component re-use and interchangeability
– mixing-and-matching of components by management of interfaces and having consistent
– semantics of shared data/schema across these components
– support for the full life cycle of components, ranging from installation, configuration, administration, publishing, versioning, maintenance and removal
– support of a consistent multi-vendor environment and application space
– support for delivery-agnostic application design to allow applications to be implemented without requiring re-design for each path over which they are served.
– Tracking of dependencies between service components

5.2 Profile management

5.2.1 User profile management

A user profile is a set of stored information related to a user (or a subscriber). In an NGN environment, the management of the user profile attributes is especially important since the user information is required to implement a number of capabilities, including authentication, authorization, service subscription, mobility, location, charging, etc. user profiles include transport-related information, media-related information and service-related information. User profiles can be stored in separate databases in the service stratum and in the transport stratum or in collocated databases. User profiles typically include the following information (the management of this information is a basic function of this capability):

– User identity, attribute information of individual user, e.g., uniquely assigned number or name

– User location information

– User presence information (including aggregation, which allows a user to subscribe to a single presence entity to watch the presence information of users, which are subscribed to presence services residing in different networks and being owned by different service providers)

– User' subscription information of services and applications, such as name of service or application, the address of the application server, information of detect point or trigger type

– User preference information, such as privacy policy, security policy and media preferences.

– User personal information, such as contact information and address book.

– User-specific or device-specific service profiles

– Billing information, such as the address where the invoice is to be delivered

General requirements for user profile management are as follows:

– The NGN shall allow multiple user identities to be assigned to and supported by a single subscription.

– The NGN shall allow multiple service subscriptions to be assigned to and supported by a single user identity.

– User profile management shall include information about resources associated with the user and user-specific rules (e.g. types of owned terminals, terminal capabilities, user preferences, etc.)

– It shall be possible to notify the NGN control entities about changes in the user profile data.

– It shall be possible for user profile information to be independent of any physical objects, such as terminal and access link.

– It shall be possible to identify and authenticate users independently of terminals/devices recognized by the network.

– User location is necessary to get geographical information as a network function in case of an emergency call, etc. The NGN shall provide means to identify the location of the user from any recognized network device. [Note: it is not expected that device location will always be known; however, the capability should be defined within NGN.] Using a fixed phone, user location can be identified because telephone carriers have the terminal addresses in the databases. As for mobile phones, geographical information by Global Positioning System (GPS) may be used. For wireless LANs, User location can be assumed based on the location of the access point.

– In order to support the user's preferences for multimedia applications, the negotiation capability may take into account the information in the user profile whenever applicable. This includes the capability to route a multimedia session to a specific terminal/device, when multiple terminals/devices share the same NGN service subscription. This also includes the capability to route a multimedia session through a media translation service to match media preferences and capabilities, i.e. relay services and interactive voice response.

- Portions of identities of NGN users such as those used for authentication, authorization and routing, shall be administered and secured by the operator and shall not be changeable by the user.
- User profile management capability shall be consistent throughout all NGNs. That is, moving from one NGN to another should not cause alteration of how a user profile is managed.
- User profile management capability of NGN should be backward compatible with user profile management capability of the existing networks, to the extent practical.
- User profiles shall allow uniform network interfaces (regardless of location) and service ubiquity (*i.e.*, the users' subscribed services are also available on a "host" network). Thus users may need to identify the entity they wish to call and the profile will interact with the network to initiate the call.
- The management and application of these profiles should reflect the interaction characteristics of a user at a specific time (*i.e.* they should respect and reflect the user profile's characteristics that are time related). The system should recognize and modify its presented interface to properly reflect the time nature of the user profile. Note that user profiles are independent and may be dynamic.
- User profile shall maintain real-time and up to date information.
- User profile management should respond to queries regarding the user profile. Services and other network functions require adequate user data in order to be appropriately customized. These can either be "user subscription data" or "network data".
- User profile should include service profiles that are specific for the subscribed service, user preference or user terminal.
- User profiles may include billing information and shall identify information that may affect personal security.

5.2.2 Device profile management

The NGN should manage the profiles of user equipments. The information for user device profiles may include:

- Terminal/device identification, address or name
- General terminal information such as serial number, model, terminal type (for telecommunications, for multimedia use, etc.)
- Supported media, e.g. video, text, audio
- Applicable service type such as multimedia, Internet access, communication, etc.
- Static attributes such as supported protocols, transmission speed, bandwidth, and processing power
- Dynamically changing attributes such as the user terminal, geographical location, applications running on the terminal
- Configuration information such as configuring communication quality, configuring the codec, configuring the network / port
- Software versions of the Operating System (OS), application manager, application client
- Status information, such as network status, terminal software status, resource status, and on/off status

User device profile information is also required in conjunction with "user profile" by a number of capabilities, including authentication, authorization, service subscription, mobility, location, charging etc.

In order to establish the required quality for a connection between terminals in the same network or in different networks, the terminal has to know the other party's terminal information and has to negotiate connection quality. For example, in the case of services like content distribution throughout networks, the terminal characteristic information is necessary to determine the optimal speed, codec and protocol. Or, in

the case of services which require to be aware of a user's location, it is necessary to acquire the geographical location information.

General requirements for device profile management are as follows:

– The NGN should allow the simultaneous use of multiple access transport functions by a single device.

– Appropriate authentication should be processed whenever an individual tries to use a device based on user profiles.

– The NGN should allow alternative user interface devices that may have specific features of value for people with disabilities.

– The NGN should allow use of various kinds of device types, such as different mobile and fixed terminal types, NGN and non-NGN terminals. Device types may include personal type (e.g. cellular phone, SIP phone, smart phone, soft phone), family type (e.g. fixed phone, multimedia terminal, PC, home appliance), and gateway type (e.g. home gateway, set-top box).

– The NGN shall allow multiple terminals/devices to be assigned to and supported by a single subscription.

– Device profile management capability shall be consistent throughout NGN networks, and should be backwards compatible with device profile management capability of existing non-NGN.

– As part of device authentication, suitability of the device for services demanded and for the network type should be ensured.

– The device profile should provide applicable service types such as communication service, multimedia service, and others.

– The device profile shall include the IP address, MAC address and access point address assigned by fixed or dynamic methods.

– If the device supports self-provisioning, the device profile should manage the applicable configuration files.

– The device profile management should be responsible for responding to queries regarding the device profile

– The device profile management shall have the ability to notify the NGN control entities about changes in the device profile data.

– Applications should have "read" access to device profile data, irrespective of the connection status of the device.

– Device profiles should maintain the latest device information.

– Device profile management shall include data on capabilities (e.g. ownership, access rights, terminal capabilities, user preferences, etc.)

– A mechanism shall be provided to allow users, or agents of users, to modify their device profile data.

5.3 Policy management

The NGN communication services identified in this document require a capability to ensure consistency across a range of network types and access technologies. These services must also be applied consistently across various service provider networks. The mechanisms to provide this capability in NGN are policy mechanisms.

Policy management may be applied to:

– Service provisioning systems

– Service set-up
– Authorization (ie. Entitlements)
– Service delivery
– Billing/metering

Policy functions should refuse or not respond to unauthorized requests, and respond to authorized requests.

5.4 Service enablers

5.4.1 Group management

This capability manages groups of users. A typical case which requires group management is a VPN service provided by network operators. In the VPN case, a closed user group has to be defined with a member list of users, and communications within this group should be securely protected from other users. NGN should manage such user groups and provide secure group communications.

In addition to the VPN case, there are many applications of group communication, which require group information. For example, simultaneous distribution of video contents by multicast requires destinations which represent groups of users. For such application, group management is also essential.

– NGN should provide a capability which enable user groups' definition.
– NGN should manage such user groups and provide secure group communications.

5.4.2 Personal information support

Personal information is typically stored in a user preference profile, which contains application-specific information representative of the user's service preferences across various mobile devices and access network types [ATIS-NGN-FMWK]. Today, most users locally store contact information on individual devices (mobile phones, handhelds, PCs, POTS line phones, and so forth). Managing these devices to maintain synchronization can be complicated and time-consuming. The NGN is envisioned to enable users to manage contact information and provide access to this content in a much simpler way. Personal information types which should be supported include aspects of personal identity information, names and phone numbers, service membership (passwords, etc.), default application parameters, bandwidth/QoS preferences (e.g. according to available access networks), media preferences and capabilities and provision for user-specified data. Personal information should be protected within the network and between the network and the user to ensure privacy and prevention of stolen identity information. Support for different user contexts and use cases should also be provided to support mobility across home, work and vehicle environments.

Key requirements include:

– Access mode optimized for the input capabilities of the terminal device (speech recognition, keyboard/terminal, pointer device, and so on).
– Multiple ways to manage the information to allow for different user capabilities and preferences.
– Integration of the Contact Information Base with call management and control functionality.
– Use of standard protocols for synchronizing information into local devices (e.g., LDAP)
– Privacy/security mechanisms for protecting user data
– Replication and resilient mechanisms should be provided to allow access to this information from any one of a group of devices, and when parts of the NGN are not available.

5.4.3 Message handling

Commonly used messaging mechanisms for different device types should be supported across both fixed and mobile networks. Examples of messaging services include

– Instant Messaging
– Chat
– Email
– SMS
– MMS

In today's networks, some services are supported in both wired and wireless, others are only found in one. For example, SMS has been designed for a wireless environment, although it can now be found in some fixed networks, whereas Instant Messaging has been designed for a wired environment, although some mobile networks have implemented Instant Messaging type services. The expectations of these services also differ in that some services are designed to be used in what is perceived as 'real time' and others are designed as a 'mailbox' service where the message is stored ready for collection or delivery at a later date.

General requirements for supporting messaging services are as follows.

– NGN should support messaging service for both fixed and mobile terminals.
– NGN should support both real time and non-real time messaging services.

Instant messaging should also be supported across fixed and mobile networks, key requirements include:

– Low latency (i.e. the user perceives the message exchange as quasi-real time)
– Efficient use of available network resources (especially wireless)
– Security
– Mobility
– Support for multiple content types, for example according to device type
– Group management and message filtering should also be supported. In addition the user should be able to configure aspects of the messaging service, such as selection, filtering, formatting, group management and processing (e.g. SPAM isolation).

5.4.4 Broadcast/Multicast support

Services which involve transmission of data to many users simultaneously can benefit from broadcast and multicast techniques, allowing efficient use of bandwidth. Mechanisms are needed to deploy and operate scalable multicast services supported by a single NGN provider and which span multiple transport service providers. Such services should be transport-agnostic as far as possible, however content reformatting or transcoding from an application perspective may be required to optimize transmitted data according to access network and terminal device capabilities. This is particularly important for multimedia information, and in particular video which generally places high requirements on QoS and data-carrying capability.

General requirements for supporting broadcast/multicast services include.

– NGN should support multicast capabilities in order to realize efficient and scalable data delivery.
– NGN should provide capabilities to realize broadcast/multicast service across multiple NGN providers.

5.4.5 Presence service

The presence service provides access to presence information and its availability to other users or services. Presence is a set of attributes characterising the current properties (e.g., status, location, etc.) of an entity.

An entity in this respect is any device, service, application, etc., that is capable of providing presence information. Availability, on the other hand, denotes the ability and willingness of an entity to communicate based on various properties and policies associated with that entity -- e.g., time of day, device capabilities,

media preferences and capabilities etc. The terms presence and availability are almost always used together to provide a complete set of presence information.

NGN customers shall be able to be both the suppliers of presence information (sometimes called presentities), as well as the requesters of presence information (watchers).

The Presence Service is enabled by three capability groupings. Requirements for each capability grouping are described below.

Presence Collection

– The NGN should provide a capability to collect information describing the connectivity state of the device used by the user. This capability could be used, for example, to describe the subscriber's state of connectivity or availability to the network.

– The NGN should provide a capability to collect information concerning location of the device used by the user.

Presence Distribution

– The NGN should provide a capability to enable another user to be informed of current presence status of a particular user. The capability can also be used for another service to access the users' presence information.

Presence Management

– The NGN shall provide presence management, a set of capabilities to manage the presence information collected.

– Access control to the presence information (using the presence distribution capabilities) shall be managed in compliance with user privacy and access rules requirements.

– The presence management should enable the distribution capability to supply only part of the presence information.

– The presence management should enable collection of requests from users to receive presence information for another user. The presence management also provides the user with the ability to determine the distribution of their presence information, e.g. to accept or reject a request for presence information on a per watcher basis.

5.4.6 Location management

Some NGN applications may require location information for devices or people. So, NGN shall support a mechanism that offers network asserted location information to applications. Mechanisms to determine and report locations information will generally vary by access technology. This means that support for location services should be implemented within each access technology. The NGN should provide additional services to ensure the correctness and authenticity of location information used for its services to mitigate any adversary effects due to fraudulent or false location information. The following are requirements for location management.

– Privacy issues must be taken into account when defining location services.

– Personal profiles provide a means for the user to control the release of location information.

5.4.7 Push-based support

'Push' operations refer to service initiated data transmissions to a client device. Whereas the user typically has the ability to configure push services from a range of services provided by the service providers, the client device does not have to issue a specific request for the data to be sent. Data can be sent either as a result of a single invocation application-dependent trigger or periodically over some time period (location

management and device management are other service enablers that can be used in order that users can be reached appropriately). Support should be given for using push mechanisms to give notice that other services are available, eg. notification that a MMS message is available, or that a new application is available for download to a terminal.

5.4.8 Device management

Device management should handle events and alarms generated by devices, servicing through software installation or upgrading, and configuration of terminals by setting of parameters. Over the air device management of wireless devices should be possible taking into consideration available bandwidth and latency in the network.

Device management is the capability of service providers, service providers and device manufacturers to manage and control the device.

– Hardware/software configuration management such as device hardware information, media capabilities, software version
– Remote software upgrades such as bug-fix, capability enhancing, upgrade OS, firmware, application client
– Remote fault diagnosis and correctness

General requirements for device management are as follows:

– Service providers, network providers and service manufacturers can automatically upgrade the operating system, firmware and software.
– In case of auto-configuration, a user purchasing a device can install the software and register a device for service by himself/herself.
– A network operator can gather device connection information such as IP and location and use it to remotely manage and control a device.
– Device management provides a function for registering, managing and updating device information.
– Device management remotely checks the status of devices at home, status changes and upgrades, and can generate diagnostic reports.
– Device management capability should be performed automatically or manually upon the client's request.
– Device management shall be secure and always carried out by a trusted entity
– Device management should allow installation of user preferences and applications

5.4.9 Session handling

The goal of session handling in NGN is to provide capabilities to setup, manage, and terminate an end-to-end service session that involves a membership of multiple parties, a group of endpoints associated with the membership parties, and a description of multimedia connection among the endpoints. Session handling is a basic capability which may be used by multiple services.

The specific session handling functions are listed below:

– Session establishment;
– Presentation of identity of originating-party and connected-to party of a session;
– Suppression of identity of originating-party and connected-to party of a session;
– Delivery of additional information (e.g. Picture, Video, text) during session establishment;
– Handling of an incoming session (by the terminating entity)
– Capability negotiation of an incoming session

– Accepting, ignoring, re-directing or rejecting an incoming session
– Negotiation of media and media components during session establishment;
– Handling of an ongoing session
– Modification of media and media components in an ongoing session;
– Suspending and resuming of an ongoing session
– Ending a session
– Network Controlled Session Termination

General requirements for session handling are as follows:

– The user should be able to invoke one or more sessions, and to activate concurrent multimedia applications within each session.
– Sessions in NGN should be able to support a variety of different media types.
– NGN should provide session handling to accommodate different service application requirements as well as to route session signaling to appropriate application servers.
– The NGN shall provide support for session admission control. Session admission control only admits the sessions that can achieve some defined level of QoS and security control.
– The following mechanisms for QoS-related session admission control should be supported in the NGN.
  • Maintaining session counts which admit session requests according to the knowledge of how many sessions (or how much bandwidth) has been allocated
  • Out-of-band measurement which admits session requests based on measured network resource availability through periodic polling of routers or switches
  • In-band measurement which admits session requests based on the measured network performance through active probes or other in-band performance metrics
  • Reservation based mechanisms which admit calls/sessions or flows only if an explicit request for bandwidth reservation for that session/flow is successful
– The admission control mechanisms must span multiple service types (e.g., voice, text and video).

5.4.10 Web-based application support and content processing

Web-based applications can provide users a consistent web environment which spans multiple environments (home, office, vehicle, etc) and multiple devices (PC, laptop, PDA, cell phone, etc.).

Web-based applications should support the following interactions:

– Server-to-server
– Server-to-terminal
– Terminal-to-server
– Terminal-to-terminal (or peer-to-peer)

Also, Web-based applications should follow commonly used standards, such as W3C and OMA.

Web-based applications should support:

– re-use of existing technologies and system components (e.g., authentication)
– re-use of authoring and integration tools
– interoperability across a wired and wireless internet
– trusted third party applications across the value chain
– a consistent user experience across networks

– scalable applications, which allows efficient provision of web services
– roaming and mobility across networks, devices and applications
– low time delays and efficient bandwidth use
– efficient access to email and configurations of the email server
– service choreography and service composition

The use of web-based applications shall not degrade the reliability of the NGN.

Content processing should be supported to tailor content transmission according to network and terminal characteristics. Support shall be offered, for example, for:

– spam protection
– virus protection
– content filtering/translation
– content screening
– content transcoding

5.4.11 Data synchronization

Data synchronization is defined as the act of establishing equivalence between two data sets and their data sets are maintained as equivalent. The data synchronization mechanism should synchronize networked data with many different terminal types, including handheld computers, mobile phones, laptop PCs and desktop PCs. The data types supported for synchronization will be digital contents, e-mail and other enterprise data.

In particular, the data synchronization mechanism should:

– Synchronize networked data with any terminal
– Synchronize a terminal with any networked data
– Synchronize data between terminals

A user should be able to access and manipulate the same set of data from different devices. For example, a user could read e-mail from either a handheld or a mobile phone, and still maintain a consistent. In addition to email, other commonly used applications include calendar, contact management information, enterprise data stored in databases, and documents on the web.

To accomplish these overall goals, the data synchronization mechanism should support a variety of features including:

– Operate effectively over wireless and wire line networks
– Support a variety of transport protocols
– Support arbitrary networked data
– Enable data access from a variety of applications
– Address the resource limitations of the mobile device
– Build upon existing Internet and Web technologies
– The protocol's minimal function needs to deliver the most commonly required synchronization capability across the entire range of devices.

5.4.12 Commerce & Charging

The NGN should provide the means to collect call, application and service data from the network elements. Such collected data may be due to the use of services and applications provided by the service provider or

the network operator, or by a trusted third party service provider. Also the NGN should provide charging interfaces among service providers, content providers and network operators.

Data collected should support charging for services consumed. For example, according to:

– usage of the access network (wireless or wireline). The charging information should describe the amount of data transmitted categorised with QoS and user protocols
– usage duration
– destination and source of the communication event
– usage of the external services offered by third parties

5.5 Network evolution aspects

Evolution of networks to NGN is dependent on operator's choices and their needs. Network operators will choose an evolution path depending on their actual resources, business plans and strategies. Therefore, they may choose different technologies and time frames. The main objectives for evolving to NGN are to improvements of network performance and enhancements of service capabilities.

For evolution to NGN the followings are required:

– The ability to gracefully evolve both existing fixed and mobile networks
– The ability to provide the same or better quality of service as currently provided by existing network
– Services evolution must remain independent from the underlying transport infrastructure.

The following sub-clauses provide requirements for evolution of PSTN/ISDN to NGN.

5.5.1 PSTN/ISDN emulation requirements

5.5.1.1 General requirement for PSTN/ISDN emulation

The NGN shall support PSTN /ISDN emulation providing the end-user with an identical experience to that of the existing PSTN/ISDN.

5.5.1.2 Terminal requirement for PSTN/ISDN emulation

The NGN shall support legacy terminals (e.g. black phones, text phones, facsimile machines, and other types of existing PSTN/ISDN terminals).

Note: Emulation of the full PSTN/ISDN service set may not be possible and service support may be restricted to certain terminal types, i.e. legacy terminals or user equipment that behaves like legacy terminals.

5.5.1.3 Service requirement for PSTN/ISDN emulation

For emulation of PSTN/ISDN services the following aspects should be considered.

– The user shall be unaware of a change from legacy PSTN/ISDN to PSTN/ISDN emulation for those services that are emulated.
– The NGN shall support the ability for a service operator to emulate one or more of their PSTN/ISDN services.
– The NGN shall support service capability definitions inherited from existing PSTN/ISDN specification.
– The NGN may not support all service capabilities and interfaces which are present to provide an emulation of a particular PSTN/ISDN network.

5.5.2 PSTN/ISDN simulation requirements

5.5.2.1 General requirement for PSTN/ISDN simulation

The NGN shall support PSTN/ISDN simulation services that provide the end-user with an experience that may or may not differ to an existing PSTN/ISDN experience.

5.5.2.2 Terminal requirement for PSTN/ISDN simulation

The NGN shall support advanced NGN terminals. It may also support adaptation devices to allow existing terminals to connect to the NGN (e.g. black phones, text phones and facsimile machines).

5.5.2.3 Service requirement for PSTN/ISDN simulation

For PSTN/ISDN simulation services the following aspects should be considered.

– The NGN shall support PSTN/ISDN-like service capabilities using session control over IP interfaces and infrastructure.

– The NGN should provide the ability for a service operator to simulate PSTN/ISDN services.

– The NGN may not support services identical to those currently provisioned in the PSTN/ISDN, and these services need not utilize PSTN/ISDN call models or signalling protocols.

5.6 Public interest service aspects

National, regional and international regulatory aspects are beyond the scope of this document.

5.6.1 Lawful interception

Where required by regulation or law, an NGN transport provider and/or NGN service provider shall comply with Lawful Interception requirements. Therefore, an NGN shall provide mechanisms that make Lawful Interception possible. These mechanisms shall provide Content of Communication (CC) and Intercept Related Information (IRI) to Law Enforcement Agencies (LEA), as per the requirements of Administrations and International treaties.

Because the nature of lawful interception is dependent upon national/regional customs and laws, requirements are dependent upon the regulatory environment of each country. As such, lawful interception requirements are not explicitly specified in this document.

5.6.2 Malicious communication trace

The NGN should include functionality that can be used to identify the source of a malicious communication, by tracing and obtaining the identity of the individual, the terminal involved and the location of the originator of the communication.

5.6.3 Emergency communications

Recommendations [Y.1271] and [E.106] respectively provide “Framework(s) on network requirements and capabilities to support emergency telecommunications” and “International Emergency Preference Scheme (IEPS) for disaster relief operations”. The NGN shall provide continuity of existing emergency communications and, in addition, NGN capabilities may be used to provide new services.

The NGN shall:

– Support routing of calls to appropriate authorities or individuals in charge or being affected

- Support continuation of communication between the authority and individuals until the authority terminates the session, even though the individual may have hung up (e.g. 911 call in North America)
- Provide, to the authority, information regarding the individual's geographical location as well as his/her identity according to national or regional regulation requirements. When required by regulation or law, this information can be acquired by the authority even though the individual requested to prevent the indication of these information.
- Provide the ability for both authenticated/authorized and unauthenticated access to emergency communication services according to national or regional regulation requirements
- Support preferential and priority traffic mechanisms for emergency communications consistency across the NGN
- Support exemption of emergency communications from certain restrictive network management functions
- Support emergency calls with alternative and multiple media, when required by regulation or law. Video, text and voice and any combination thereof as well as various forms of messaging are essential for communication with the emergency services for people with disabilities.

Further details on ETS/TDR scenarios and requirements are provided, in ITU-T Recommendations Y.1271 and E.106, respectively.

5.6.4 User identity presentation and privacy

The NGN should support mechanisms to provide and present identities of the calling user (or session initiator) and the connected user (or connected party to the session initiator) when all parties are located within a single NGN. This is equivalent to the network having the ability to offer calling line identification presentation (CLIP) and connected line identification presentation (COLP) services, which are currently offered in current telephony networks.

The NGN shall support mechanisms to restrict the presentation of the identity of the calling user (or session initiator) and/or the connected user (or connected party to the session initiator) when all parties are located within a single NGN. This is equivalent the network having the ability to offer calling line identification restriction (CLIR) and connected line identification restriction (COLR) services, which are currently offered in telephony networks. However, while the network shall have the capability to offer these services, it must also comply with other requirements when these services are invoked.

5.6.5 Network or Service provider selection

NGN shall support the capability for provider selection, where required by regulation or law.

5.6.6 Users with disabilities

Users with disabilities have a general need to be provided with means to control and use terminals and services in alternative ways and modes, suiting varied capabilities and preferences. Such requirements are best met by inclusive design of the general provision of terminals and services.

NGN shall provide the means needed for invocation of relay services in a call. Relay services translate between various modes of communication that are of interest for people with disabilities. (e.g. sign language, lip reading, text, voice)

Invocation of relay services may be based on user preferences, address resolution or user commands.

NGN shall have capability to invoke relay services by either party in an emergency call.

Other needs for users with disabilities to communicate with emergency services are handled in section 5.6.3.

5.7 Other Basic Capabilities of Interest to Network and Service Providers

5.7.1 Critical Infrastructure Protection

Service providers should have capabilities to protect their NGN infrastructure from malicious attacks, such as denial of service, eavesdropping, spoofing, tampering with messages (modification, delay, deletion, insertion, replay, re-routing, misrouting, or re-ordering of messages), repudiation or forgery. Protection may include prevention, detection and recovery from attacks, measures to prevent service outages due to natural events (weather, etc.), as well as management of confidential information.

5.7.2 Non disclosure of information across NNI interfaces

Where required by regulation or law, NGN shall provide capabilities to not disclose service provider's internal network information across NNI interface and it shall enable restriction of the network topology view to authorised entities.

5.7.3 Inter-provider and universal service compensation

According to regulation or law, NGN may be required to support mechanisms, at least for accounting and management, for inter-provider and universal service compensation. These compensation mechanisms are based on criteria related to usage of resources made available to other providers.

5.7.4 Service unbundling

Where required by regulation or law, NGN should support mechanisms to realize the service unbundling. These mechanisms allow customers' flexible choice of services and providers, and also allow providers' competitive offering of their services to customers.

5.7.5 Exchange of user information among providers

Where required by regulation or law, NGN should support mechanisms to exchange user information for the sake of realizing the services provided across providers. The user information may be location information, device profile information, information of services supported by providers etc.

5.8 Other Service Support Capabilities of Interest to Network and Service Providers

5.8.1 Digital Rights Management

NGNs may be required to support the digital right management (DRM) capabilities to protect intellectual property of digital contents.

5.8.2 Fraud Detection and Management

NGN may be required to support the detection and minimization of activities such as 'identity theft' and suspicious transactions. NGN should support mechanisms which enable the network or service provider to detect fraud and initiate mitigation actions.

5.8.3 Number portability

Number portability is a network capability that allows users to use the same number, e.g. same telephone number, even when the users move from one physical location to another physical location. This includes portability within one operator's network, portability among different operators' networks, as well as portability between different access technologies, e.g. fixed and mobile. Where required by regulation or law, the NGN should support number portability.

6 Other general requirements

6.1 NGN user equipment general requirements

NGN user equipment are connected via the customer network to the NGN access network and provide services to end users. NGN user equipment general requirements include:

– A variety of user equipment should be supported.

– These include residential gateway, black phones, text phones, SIP phones, soft-phones (program on PC), set-top box, multimedia terminals, cellular phones, PCs, PDAs, etc. These include user equipment with intrinsic capability to support a simple service set, and user equipment that can support a programmable service set [ETSI-TISPAN-R1-DEF].

– Legacy terminals should be supported

– User equipment should be capable of making an emergency call.

– Easy/automatic configuration setup should be supported

For example, remote downloading of setup information or software updates from network to user equipment (e.g., home gateway) allows network operators to undertake user equipment setup or software update on behalf of users. Then, users have only to connect their equipment to the network to access NGN services.

NOTE – Specification or mandate of a particular user equipment type or capability is out of scope of standardisation.

6.2 End user general requirements

End user general requirements include:

– End users should be able to use multiple terminals and services in parallel whether inside or outside of the customer network.

– Services should be provisioned without requiring user technical knowledge or complex setup procedures.

WORKING GROUP 2
DELIVERABLES

FUNCTIONAL ARCHITECTURE AND MOBILITY

2.3 Functional requirements and architecture of the NGN (*Status A*)

2.4 Mobility management capability requirements for NGN (*Status A*)

2.5 IMS for Next Generation Networks (*Status A*)

2.6 PSTN/ISDN emulation architecture (*Status A*)

2.3 – Functional requirements and architecture of the NGN*

Table of Contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

2.3 – Functional requirements and architecture of the NGN

1 Scope

The objective of this Document is to describe the functional requirements and architecture of the Next Generation Network (NGN) [1] for Release 1, as described in the TR-Release 1 scope [2] and TR-Release 1 requirements [3].

The functional architecture provided in this Document allows a clear distinction between the definition/specification aspects of services provided by the NGN and the actual specification of the network technologies used to support those services. In line with Y.2011 [4] principles, an implementation-independent approach is adopted. This Document describes the functional architecture of the NGN by using the generic definitions, symbols, and abbreviations that are defined in related ITU-T Recommendations.

The names of various NGN functional entities and reference points used in this Document may be the same or similar to functional entities and reference points identified in other documents, but the specific functionalities and reference points may be different as identified in this document. The specific protocols used for NGN systems are defined in other signalling-related or management-related documents that are part of the set of NGN system documents.

The scope of release 1 specifies that nomadism shall be supported between different network termination points. While no major new interfaces for mobility are proposed for development as part of release 1, other mobility-related functionalities beyond nomadism, such as handover, are not precluded and may be supported through the use of existing technologies. Thus, any mobility-related functions or functional entities described here that support capabilities beyond nomadism are only included because they represent functionalities that already exist in the mobile environment. They should be applied in the areas related to mobility within the architecture.

2 References

The following ITU-T Recommendations and other references contain provisions that, through references in this text, constitute provisions of this Document. At the time of publication, all the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Document are therefore encouraged to investigate the possibility of consulting the most recent editions of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ITU-T Recommendation Y.2001 (2004), General overview of NGN

[2] ITU-T FGNGN Document TR-Release 1 scope

[3] ITU-T FGNGN Document TR-Release 1 requirements

[4] ITU-T Recommendation Y. 2011 (2004), General principles and general reference model for next generation networks

[5] ITU-T FGNGN Document TR-RACF

[6] ITU-T Recommendation M.3060

[7] ITU-T FGNGN Document TR-IFN

[8] ITU-T FGNGN Document TR-PIEA

[9] ITU-T FGNGN Document on NGN Security Requirements for Release 1

[10] ITU-T FGNGN Document on Guidelines for NGN Security

3 Definitions

This Document defines the following terms.

3.1 Functional Entity: An entity that comprises a specific set of functions at a given location. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.2 Functional architecture: A set of functional entities used to describe the structure of an NGN. These functional entities are separated by reference points, and thus, they define the distribution of functions. The functional entities can be used to describe a set of reference configurations. These reference configurations identify which reference points are visible at the boundaries of equipment implementations and between administrative domains.

3.3 Media: One or more of audio, video, or data.

3.4 Media stream: A media stream can consist of audio, video, or data, or a combination of any of them. Media stream data conveys user or application data (i.e., a payload) but not control data.

3.5 Reference point: A conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing between these functional entities. A reference point may or may not correspond to one or more physical interfaces between pieces of equipment.

3.6 Stream: A flow of real-time information of a specific media type (e.g., audio) and format (e.g., G.722) from a single source to one or more destinations.

3.7 Topology: Information that indicates the structure of a network. It contains the network address and routing information.

4 Abbreviations

This Document uses the following abbreviations.

ABG-GE	Access Border Gateway Functional Entity
AGC-FE	Access Gateway Control Functional Entity
ALG	Application Level Gateway
AMF	Account Management Function
AMG-FE	Access Media Gateway Functional Entity
AN-FE	Access Node Functional Entity
ANI	Application-to-Network Interface
APL	Application
APL-SCM-FE	Application Service Coordination Manager Functional Entity
APL-GW-FE	Application Gateway Functional Entity
AR-FE	Access Relay Functional Entity
AS-FE	Application Server Functional Entity
ATM	Asynchronous Transfer Mode

A-TRC-FE	Access Transport Resource Control Functional Entity
BGC-FE	Breakout Gateway Control Functional Entity
B2BUA	Back-to-Back User Agent
CBF	Charging and Billing Function
CCF	Charging Collection Function
CDR	Call Detail Record
CS	Capability Set
CTF	Charging Trigger Function
C-TRC-FE	Core Transport Resource Control Functional Entity
DNS	Domain Name System
DTMF	Dial Tone Multi Frequency
E-NNI	External Network-to-Network Interface
EN-FE	Edge Node Functional Entity
FE	Functional Entity
FW	Firewall
GGSN	Gateway GPRS Support Node
GIS	Geographical Information Systems
GPRS	General Packet Radio Service
IBC-FE	Interconnection Border Gateway Control Functional Entity
IBG-FE	Interconnection Border Gateway Functional Entity
I-CSC-FE	Interrogating Call Session Control Functional Entity
ICMP	Internet Control Message Protocol
IMS	IP Multimedia Subsystem
IN	Intelligent Network
INAP	Intelligent Network Application Protocol
IN-AS-FE	Intelligent Network Application Server Functional Entity
I-NNI	Internal Network-to-Network Interface
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
ISDN	Integrated Services Digital Network
LAN	Local Area Network
L2TP	Layer2 Tunneling Protocol
MGC-FE	Media Gateway Control Functional Entity

MLT-FE	Multimedia Services Functional Entity
MPLS	Multi Protocol Label Switching
MRB-FE	Media Resource Broker Functional Entity
MRC-FE	Media Resource Control Functional Entity
MRP-FE	Media Resource Processing Functional Entity
NACF	Network Attachment Control Functions
NAC-FE	Network Access Control Functional Entity
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NE	Network Element
NGN	Next Generation Network
NNI	Network-to-Network Interface
NSIW-FE	Network Signalling Interworking Functional Entity
OCF	Online Charging Function
OMA	Open Mobile Alliance
OSA	Open Service Architecture
OSE	OMA Service Environment
P-CSC-FE	Proxy Call Session Control Functional Entity
PD-FE	Policy Decision Functional Function
POTS	Plain Old Telephone Service
PPP	Point to Point Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RACF	Resource and Admission Control Functions
RAN	Radio Access Network
RF	Rating Function
SAA-FE	Service Authentication and Authorization Functional Entity
SCP	Service Control Point
S-CSC-FE	Serving Call Session Control Functional Entity
SDH	Synchronous Digital Hierarchy
SG-FE	Signalling Gateway Functional Entity
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol

SIP UA	SIP User Agent
SLA	Service Level Agreement
SL-FE	Subscription Locator Functional Entity
SS-FE	Service Switching Functional Entity
SS7	Signalling System No.7
STP	Spanning Tree Protocol
SUP-FE	Service User Profile Functional Entity
TAA-FE	Transport Authentication and Authorization Functional Entity
TDM	Time Division Multiplex
TLM-FE	Transport Location Management Functional Entity
TMG-FE	Trunk Media Gateway Functional Entity
TUP-FE	Transport User Profile Functional Entity
UNI	User-to-Network Interface
URI	Uniform Resource Identifier
USIW-FE	User Signalling Interworking Functional Entity
VAS	Value-Added Services
VLAN	Virtual LAN
W-CDMA	Wideband-Code Division Multiple Access
WLAN	Wireless LAN
xDSL	x Digital Subscriber Line
3G	3rd Generation

5 General principles of the NGN functional architecture

The NGN functional architecture shall incorporate the following principles.

Support for multiple access technologies: The NGN functional architecture shall offer the configuration flexibility needed to support multiple access technologies.

Distributed control: This will enable adaptation to the distributed processing nature of IP networks and support location transparency for distributed computing.

Open control: The network control interface should be open to support service creation, service updating, and incorporation of service logic provision by third parties.

Independent service provisioning: The service provision process should be separated from network operation by using the above-mentioned distributed, open control mechanism. This is intended to promote a competitive environment for NGN development in order to speed up the provision of diversified value-added services.

Support for services in a converged network: This is needed to generate flexible, easy-to-use multimedia services, by tapping the technical potential of the converged, fixed-mobile functional architecture of the NGN.

Enhanced security and protection: This is the basic principle of an open architecture. It is imperative to protect the network infrastructure by providing mechanisms for security and survivability in the relevant layers.

Functional entity characteristics: Functional entities should incorporate the following principles:

- Functional entities may not be distributed over multiple physical units but may have multiple instances.
- Functional entities have no direct relationship with the layered architecture. However, similar entities may be located in different logical layers.

6 Overview of the NGN architecture

Along with a new architecture, the Next Generation Network will bring an additional level of complexity beyond that of existing networks. In particular, support for multiple access technologies and mobility results in the need to support a wide variety of network configurations. The specific configurations used in the NGN are not the subject of this Document. Some examples of configurations, however, are provided in Appendices I II, and III and serve to provide a context for the functional architecture described in this section.

The NGN architecture provided in this Document supports the delivery of services identified in the TR-NGN-Release 1 scope [2], as well as the requirements identified in the TR-NGN-Release 1 requirements [3]. NGN services include multimedia services, such as conversational services (SIP based), and content delivery services, such as video streaming and broadcasting. The NGN provides support for PSTN/ISDN replacement (i.e., PSTN/ISDN emulation), as well as PSTN/ISDN simulation. In addition, it provides capabilities and resources to support third-party applications for value-added services.

Figure 1 shows an overview of the NGN functional architecture that allows the support of the Release 1 services. The NGN functions are divided into service stratum functions and transport stratum functions according to Y.2011 [4].

To provide these services, several functions in both the service stratum and the transport stratum are needed, as illustrated in Figure 1.

The delivery of services/applications to the end-user is provided by utilizing the Application/Service Support functions and Service control functions.

The NGN supports a reference point to the “Third-Party Applications” functional group called Application-to-Network Interface (ANI), enabling application of NGN capabilities to create and provision enhanced services for NGN users.

The Transport stratum provides IP connectivity services to NGN users under the control of Transport control functions, including the Network Attachment Control Functions (NACF) and Resource and Admission Control Functions (RACF).

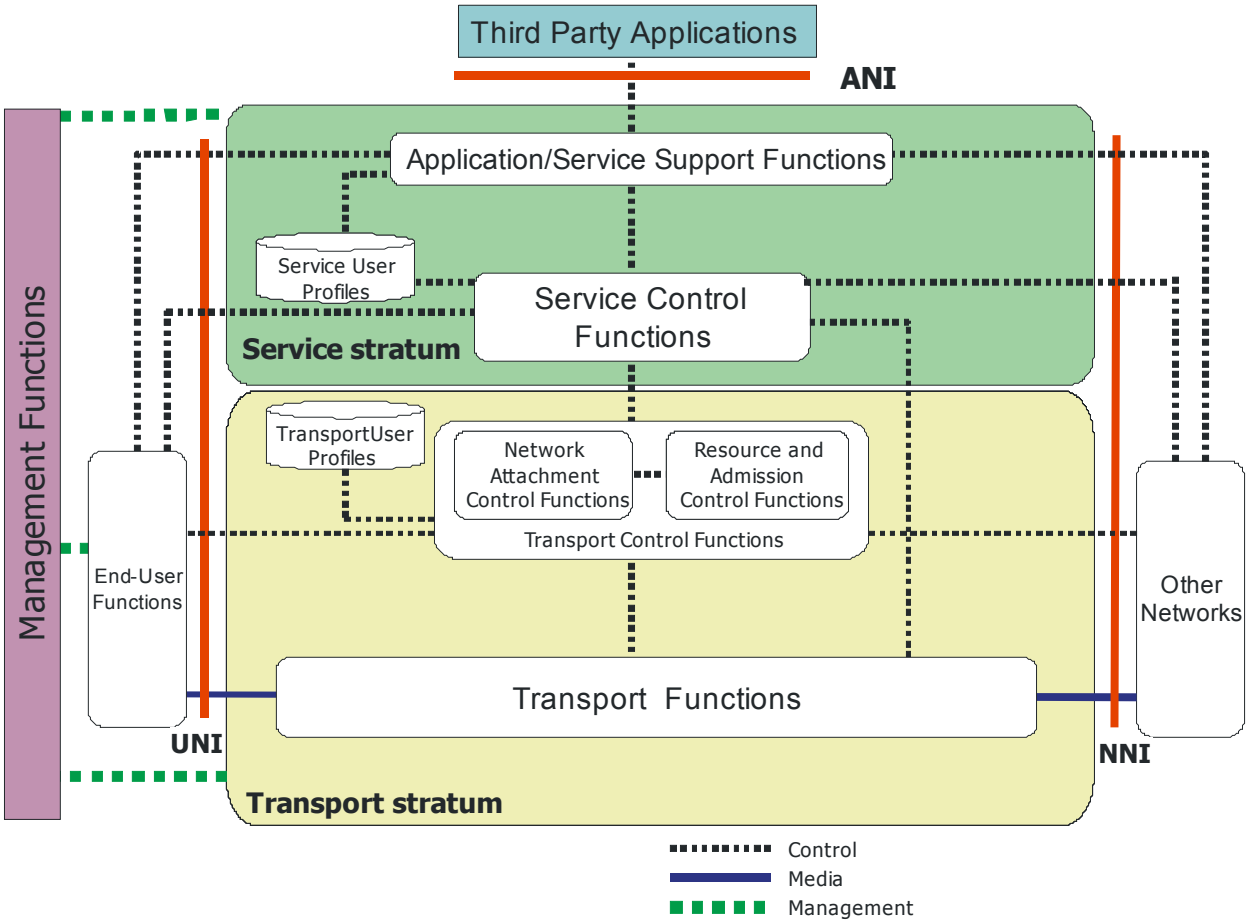


Figure 1 – NGN architecture overview

Note 1 – The UNI/NNI/ANI should be understood as general NGN reference points that can be mapped to specific physical interfaces depending on the particular physical implementations.

Note 2 – Boxes in Figure 1 identify high level functional groups, for which overall descriptions are given later in this section.

Note 3 – The control links between the functional groups represent high-level logical interactions.

Note 4 – Some functional groups, such as RACF, NACF, and Service Control functions, may be distributed and instantiated over different NGN provider domains. The functional groups in the Service stratum and the Transport stratum may be distributed between a visited network and a home network. Refer to Appendix I for the details.

Note 5 – User profiles in both the service stratum and the transport stratum are shown as separate functional databases. Depending on the business model in place, these two functional databases can be co-located. Note that other functional databases required for the support of NGN release 1 services (such as DNS) are not illustrated in Figure 1.

6.1 Transport stratum functions

The transport stratum functions include transport functions and transport control functions, per Y.2011 [4].

6.1.1 Transport functions

The transport functions provide the connectivity for all components and physically separated functions within the NGN. These functions provide support for the transfer of media information, as well as the transfer of control and management information.

Transport functions include access network functions, edge functions, core transport functions, and gateway functions.

NOTE – No assumptions are made about either the technologies to be used or the internal structure, e.g., the core transport network and the access transport network.

6.1.1.1 Access network functions

The access network functions take care of end-users' access to the network as well as collecting and aggregating the traffic coming from these accesses towards the core network. These functions also perform QoS control mechanisms dealing directly with user traffic, including buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing, and shaping.

The access network includes access-technology dependent functions, e.g., for W-CDMA technology and xDSL access. Depending on the technology used for accessing NGN services, the access network includes functions related to:

1) Cable access
2) xDSL access
3) Wireless access (e.g. IEEE 802.11 and 802.16 technologies, and 3G RAN access)
4) Optical access

6.1.1.2 Edge functions

The edge functions are used for media and traffic processing when aggregated traffic coming from different access networks is merged into the core transport network; they include functions related to support for QoS and traffic control.

The edge functions are also used between core transport networks.

6.1.1.3 Core transport functions

The Core transport functions are responsible for ensuring information transport throughout the core network. They provide the means to differentiate the quality of transport in the core network.

These functions provide QoS mechanisms dealing directly with user traffic, including buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing, shaping, gate control, and firewall capability.

6.1.1.4 Gateway functions

The gateway functions provide capabilities to interwork with end-user functions and other networks, including other types of NGN and many existing networks, such as the PSTN/ISDN, the public Internet, and so forth.

Gateway functions can be controlled either directly from the Service Control functions (see Section 6.2.1) or through the Transport control functions (see Section 6.1.2).

6.1.1.5 Media handling functions

This series of functions provides media resource processing for service provision, such as generation of tone signals and trans-coding. These functions are specific to media resource handling in the transport stratum.

6.1.2 Transport control functions

The Transport control functions include Resource and Admission Control Functions and Network Attachment Control Functions.

6.1.2.1 Resource and Admission Control Functions (RACF)

In the NGN Architecture, the Resource and Admission Control Functions (RACF) provide QoS control (including resource reservation, admission control and gate control), NAPT and/or FW traversal control Functions over access and core transport networks. Admission control involves checking authorisation based

on user profiles, SLAs, operator specific policy rules, service priority, and resource availability within access and core transport.

Within the NGN architecture, the RACF act as the arbitrator for resource negotiation and allocation between Service Control Functions and Transport Functions.

The RACF interacts with Service Control Functions and Transport Functions for Session-based applications (e.g. SIP call) and non-session based applications (e.g. Video Streaming) that require the control of NGN transport resource, including QoS control and NAPT/FW control and NAT Traversal.

The RACF interact with Transport Functions for the purpose of controlling one or more the following functions in the transport layer: Packet filtering; Traffic classification, marking, policing, and priority handling; Bandwidth reservation and allocation; Network address and port translation; Firewall.

The RACF interact with Network Attachment Control Functions (NACF, including network access registration, authentication and authorization, parameters configuration) for checking user profiles and SLAs held by them.

For those services across multiple providers or operators, Service Control Functions, RACF and Transport Functions may interact with the corresponding functions in other packet networks.

NOTE: The details and other aspects of the RACF are specified in TR-RACF [5].

6.1.2.2 Network Attachment Control Functions (NACF)

The NACF provide registration at the access level and initialization of end-user functions for accessing NGN services. These functions provide network-level identification/authentication, manage the IP address space of the access network, and authenticate access sessions. They also announce the contact point of NGN Service/Application support functions to the end user.

The NACF provide the following functionalities:

- Dynamic provision of IP addresses and other user equipment configuration parameters.
- Authentication at the IP layer (and possibly other layers).
- Authorization of network access, based on user profiles.
- Access network configuration, based on user profiles.
- Location management at the IP layer.

6.1.3 Transport user profile functions

These functions take the form of a functional database representing the combination of a user's information and other control data into a single "user profile" function in the transport stratum. This functional database may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.

6.2 Service stratum functions

This abstract representation of the functional grouping in the service stratum includes the Service control functions and the Application/Service support functions, as well as service user profiles.

6.2.1 Service control functions

The Service control functions include both session and non-session control, registration, and authentication and authorization functions at the service level. They can also include functions for controlling media resources, i.e., specialized resources and gateways at the service-signalling level.

6.2.2 Application/Service support functions

The Application/Service support functions include functions such as the gateway, registration, authentication and authorization functions at the application level. These functions are available to the "Third-Party Applications" and "End-User" functional groups. The Application/Service support functions work in conjunction with the Service control functions to provide end-users and third party application providers with the value added services they request.

Through the UNI, the Application/Service support functions provide a reference point to the end-user functions (e.g., in the case of third-party call control for Click to Call service). The Third-party applications' interactions with the Application/Service support functions are handled through the ANI reference point.

6.2.3 Service user profile functions

The service user profile functions represent the combination of user information and other control data into a single user profile function in the service stratum, in the form of a functional database. This functional database may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.

6.3 End-user functions

No assumptions are made about the diverse end-user interfaces and end-user networks that may be connected to the NGN access network. Different categories of end-user equipment are supported in the NGN, from single-line legacy telephones to complex corporate networks. End-user equipment may be either mobile or fixed.

6.4 Management functions

Support for management is fundamental to the operation of the NGN. These functions provide the ability to manage the NGN in order to provide NGN services with the expected quality, security, and reliability.

These functions are allocated in a distributed manner to each functional entity (FE), and they interact with network element (NE) management, network management, and service management FEs. Further details of the management functions, including their division into administrative domains, can be found in M.3060 [6].

Management functions apply to the NGN service and transport strata. For each of these strata, they cover the following areas:

a) Fault management

b) Configuration management

c) Accounting management

d) Performance management

e) Security management

The accounting management functions also include charging and billing functions (CBF). These interact with each other in the NGN to collect accounting information, in order to provide the NGN service provider with appropriate resource utilization data, enabling the service provider to properly bill the users of the system.

A detailed description of the CBF functions can be found in clause 7.5.

7 NGN concepts

7.1 Mobility aspects

7.1.1 Mobility levels in the NGN architecture

The NGN architecture supports the capability to provide mobility within and between its various access network types and mobility technologies. This mobility may be supported at various levels in the NGN architecture, starting with service-level mobility at the top and ending with radio-level mobility at the bottom.

7.1.1.1 Service-level mobility

Service level mobility is the mobility of users across service domains in the NGN. This might be within a single NGN implementation or across multiple implementations. Service level mobility might, for example, exploit the "E.164 to SIP-URI" address resolution capability. In this way, service-level mobility can be provided when a user is roaming between different administrative domains, which would necessitate inter-domain mobility at the session control level.

7.1.1.2 Inter-access-network-level mobility

Inter-access-network mobility is related to the possibility for a user to roam within domains, across different access technologies, by using various network mobility technologies, such as Mobile IP or MAP.

7.1.1.3 Intra-access-level mobility (wide area)

Wide-area intra-access-level mobility refers to mobility within an access network or between access networks using common technology in the NGN. User mobility at this level is provided by the access network technology. For example, it might be provided by GPRS roaming technology for movement between SGSNs within a GGSN.

7.1.1.4 Intra-access-network-level mobility (local area)

Local-area intra-access-network-level mobility refers to the mobility of users within a particular access technology, and generally within a limited geographic area. This might be handled at or above the radio resource control layer.

7.2 NGN Value-Added Service architecture

7.2.1 Introduction

The application environment of the traditional intelligent network for value-added services (VASs) was built upon circuit-switched network technology. Hence, it has characteristic limitations, such as centralized SCP-based control, an SS7-based signalling protocol, an operator network's embedded closed system, a long, complicated standards update process, and so forth. The packet-switched technology (especially the IP network) used in the NGN for end-to-end data transmission does not require a centralized standard Intelligent Network (IN) capability set (CS) for offering value-added services. The advantage of the NGN architecture is that only the service provider needs to be aware of its service, thus enabling the creation and provision of a variety of new, innovative services that do not have to be standardized.

7.2.2 Model of NGN VAS architecture

The value added service (VAS) aspect of the NGN architecture, as shown in Figure 1, consists of three distinct domains: i) "Third-Party Applications"; ii) "Application/Service support functions" in the service stratum of the NGN; and iii) certain NGN resources and capabilities, including those in the transport stratum, capabilities such as presence, location information, charging function, security schemes, etc. The third-party applications domain may break into two categories: those trusted by network/server providers, and those that

are not. The former may consist of network/server providers themselves and subordinate organizations or partners, while the latter may consist of independent service providers, whose access to southbound resources must be authenticated, controlled, and filtered by the functions in the VAS enablers and servers.

As shown in Figure 1, through the ANI, the NGN block of "Application/Service Support Functions" interacts with the VAS environment and offers a wealth of service-enabling resources to the "Third-Party Applications" block, independently of the underlying network technologies. Also through the ANI, the "Third-Party Applications" block benefits from the capabilities and resources of the "NGN Infrastructure" block.

Specifically, the NGN VAS architecture has the following three main functional characteristics:

a. Agnosticism: The Third-party Application Providers functional group NGN VAS architecture shall consist of functions that are agnostic with respect to their underlying NGN infrastructure.

b. Support for legacy capabilities and features: There shall not be any limiting impacts on the NGN core as a result of this VAS architecture. On the contrary, the use of NGN capabilities such as session management, authentication, location information, charging, and so forth shall be supported. Furthermore, the legacy-IN-influenced features of IMS, such as triggers, filter criteria, and the service capability interaction manager, will be available through the abstraction of the IMS AS (Application Server) in the "Application/Service Support Functions" block.

c. Support for open service interface: The NGN VAS platform should provide an open service interface, which provides an abstract of the network capabilities (i.e., the interface is network agnostic). This interface should include such functions as authentication, authorization, and security to ensure that third-party service providers can make use of the network capabilities.

7.3 Network topology hiding functions and NAT traversal functions

7.3.1 Service stratum topology hiding

Service stratum topology hiding is achieved by removing any topological information carried in application signalling packets to the peering network. For example, in SIP-based applications, topology information is present in SIP headers, like the via and Record Route headers.

7.3.2 Transport stratum topology hiding

Transport stratum topology hiding is achieved by modifying any topological information in media packets, or by blocking network control packets including any topological information.

Examples of transport stratum topology hiding are as follows:

- Change the IP addresses and/or port numbers of media packets that pass through the border of access-to-core network and/or of core networks.
- Block the network control packet at the border of access/core networks, such as STP, ICMP and routing protocol.

7.3.3 Remote NAT traversal

NAT traversal copes with the traversal of far-end (remote) NAT in access networks. The owner of the far-end NAT is different from the owner of the service control functional entities (e.g., P-CSC-FE), i.e., the far-end NAT cannot be controlled by NAT ALG or other service control functional entities affiliated with the service provider domain.

7.4 Overload Control

To defend session control functional entities such as S-CSC-FE, against the concentration of malicious or unexpected requests, the following functions are necessary at each boundary between access and/or core networks.

– Detection of the concentration of requests to an S-CSC-FE at each FE.
– Detection of the concentration of requests to an S-CSC-FE by gathering information from two or more FEs.
– Transmission of the detected information on the concentration of requests to other FEs.
– Traffic control according to the information on the concentration of requests.

7.5 Charging and Billing Functions (CBF)

The CBF described in this section are meant to represent a generalized architecture to support an NGN provider operator's need to collect and process information, such that customers can be charged for the services provided.

The CBF provide accounting data to the network operator regarding the utilization of resources in the network. They support the collection of data for later processing (offline charging), as well as near-real-time interactions with applications, such as for pre-paid services (online charging).

The CBF include a Charging Trigger Function (CTF), an Online Charging Function (OCF), a Charging Collection Function (CCF), a Rating Function (RF), and an Account Management Function (AMF).

Figure 2 shows the functions that comprise the CBF.

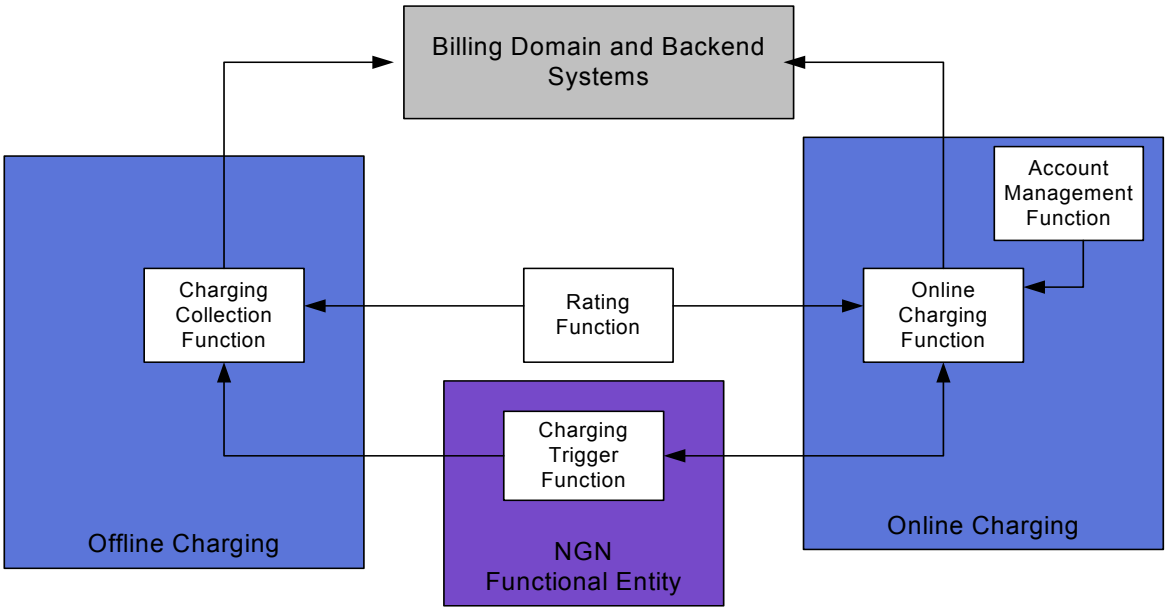


Figure 2 – Charging and Billing Functions

7.5.1 Charging Trigger Function (CTF)

The CTF generates charging events based on the observation of network resource usage. In every network and service element that provides charging information, the CTF is the focal point for collecting information pertaining to chargeable events within the network element, assembling this information into matching charging events, and sending these charging events to the Charging Collection Function. The CTF is therefore a necessary component in all network elements that provide offline-charging functionality.

The CTF also creates the charging events used for online charging. The charging events are forwarded to the Online Charging Function (OCF) in order to obtain authorization for the chargeable event or network resource usage requested by the user. It must be possible to delay the actual resource usage until permission

has been granted by the OCF. The CTF must be able to track the availability of resource usage permissions (i.e., quota supervision) during the network resource usage. It must also be able to enforce termination of the end user's network resource usage when permission by the OCF is not granted or expires.

NOTE – The specific entities that contain charging trigger functionality are not defined in this document.

7.5.2 Charging Collection Function (CCF)

The CCF receives charging events from the CTF. It then uses the information contained in the charging events to construct Charging Data Records (CDRs). The results of the CCF tasks are CDRs with well-defined content and format. The CDRs are later transferred to the billing domain.

7.5.3 Online Charging Function (OCF)

The OCF receives charging events from the CTF and executes in near real time to provide authorization for the chargeable event or network resource usage requested by the user. The CTF must be able to delay the actual resource usage until permission has been granted by the OCF. The OCF provides a quota for resource usage, which must be tracked by the CTF. Subsequent interactions may result in an additional quota being provided according to the subscriber's account balance, or they may result in no additional quota being provided, in which case the CTF must enforce termination of the end user's network resource usage.

The OCF allows more than one user to share the same subscriber's account simultaneously. The OCF responds to the charging requests from various users at the same time and provides a certain quota to each user. The quota is determined by default or by certain policies. Users can resend requests for larger quotas during the same session. The maximum available quota, however, will not exceed the subscriber's account balance.

7.5.4 Rating Function (RF)

The RF determines the value of the network resource usage (described in the charging event received by the OCF from the network) on behalf of the OCF. To this end, the OCF furnishes the necessary information to the RF and receives the rating output.

The RF also works with the offline charging module, and it determines the value of the network resource usage (described in the charging event received by the CCF from the network).

7.5.5 Account Management Function (AMF)

The AMF stores the subscriber's account balance within the online charging system.

The subscriber's account balance could be represented by the remaining available traffic volume (e.g., bytes), time (e.g., minutes for calling), or content (e.g., a movie), as well as money.

Security and robustness should be emphasized by encrypting key data, providing backup and failure alarm capabilities, keeping detailed logs, and so forth.

8 Generalized NGN functional architecture

This section describes the generalized functional architecture for the NGN, including the definitions of the generalized functional entities. This architecture is a general service- and technology-independent architecture that can be later instantiated in customized architectures that can respond to specific contexts in terms of the services offered and the technologies used.

8.1 NGN functional entities (FEs)

In general, an FE is characterized by functions identified as sufficiently unique with respect to other FEs. In the case of the generalized NGN architecture, the functional entities, called NGN FEs, are to be understood as generic FEs to allow for their possible instantiation in more specific technology-oriented contexts. It is

therefore possible that when NGN FEs are instantiated, they can be used and can behave in a slightly different manner depending on the context. For example, this may lead to the case where at a given reference point (between the same NGN FEs), the interface and the associated protocols are different depending on the instantiation. This means that interfaces, as well as protocol descriptions, can only be provided on the basis of a specific instantiation of the generalized functional architecture.

8.2 Generalized functional architecture

The generalized NGN functional architecture shown in Figure 3 is based on the NGN architecture overview provided in section 6. In particular, the functional groups identified in Figure 1 are used to structure the general layout of Figure 3.

As already mentioned in section 6, the NGN architecture, and as a consequence, the generalized functional architecture described in this section, are expected to provide functionality for all envisaged services over packet-based networks as is specified in TR-Release 1 scope [2] and TR-Release 1 requirements [3].

In this sense, it is expected that, in line with Y.2011 [4] principles, most of the NGN transport stratum functions (such as RACF or NACF) will be able to support these different types of NGN services in a common way. NGN implementations do not, however, have to implement certain transport stratum FEs, such as gateway FEs with respect to PSTN/ISDN, if they do not require support for such capabilities.

Note – The T-10 T.Network Access Control FE may reside in a visited network or a home network. It depends on the administrative domain and the business scenario.

Note – T-4 and T-9 are neither subject to the measurement nor policy enforcement.

Note – Lines terminating on the dotted box around S-4 and S-5 indicate connection to both internal FEs. Inclusion of these two FEs in the dotted does not imply that they are collocated.

Note – Allocation of some functions to the IBG-FE needs further study: IBG-FE may/may not perform media conversion under the control of IBC-FE. A direct link between IBG-FE and IBC-FE is under study. (Refer to Section 8.3.1.6 on T-6 IBG-FE!!)

In this functional architecture, some FEs include functions relating to the NGN service stratum and the NGN transport stratum. On the one hand, the transport stratum covers transport functions and associated control functions up to the IP layer. On the other hand, the service stratum includes functions that handle the layers above the IP layer. Attention needs to be paid to which layer is addressed by each relationship between FEs. For instance, there are several relationships between end-user functions and the transport stratum. For example, there are IP-based relationships and analogue POTS/ISDN relationships related to media transport, and there are also some signalling relationships. The relationships between the end-user functions and service functions represent service protocol layer relationships. The relationships to the application functions represent application layer protocol relationships.

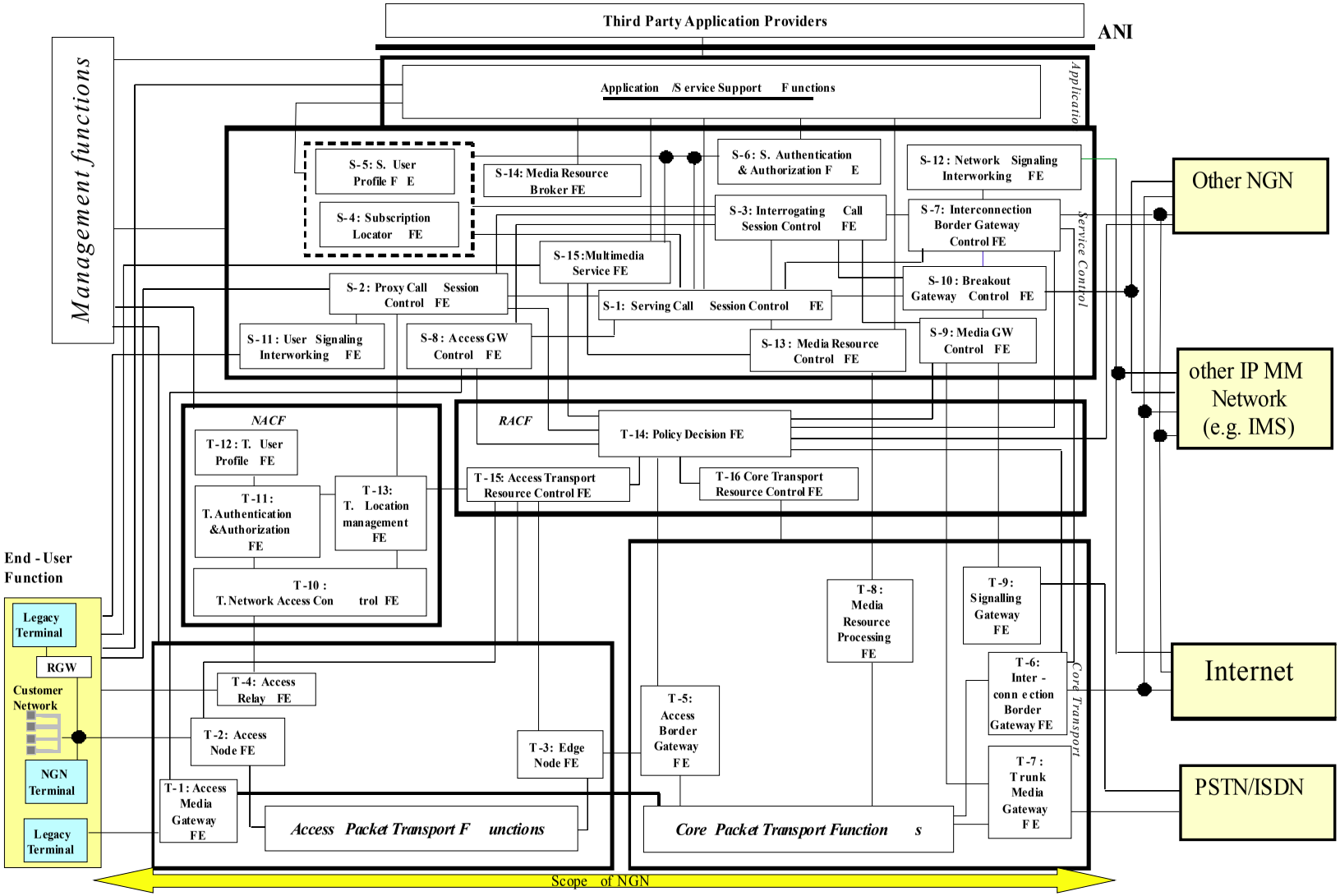


Figure 3 – NGN generalized functional architecture

8.3 Functional entity descriptions

This section describes each FE with figures.

This document uses the following conventions. These conventions are specific to this document and are used to facilitate referencing different items.

A-S$_n$, This term is used to indicate the relationship between functional entities in Application/Service Support Functions and functional entities in Service Control Functions.

S-ON$_n$, This term is used to indicate the relationship between Service stratum functional entities and other networks, including other NGNs

S-T$_n$, This term is used o indicate the relationship between Service stratum functional entities and Transport processing functional entities

S-TC$_n$, This term is used to indicate the relationship between Service stratum functional entities and Transport control functional entities

S-U$_n$, This term is used to indicate the relationship between Service stratum functional entities and end-user function

T-ON$_n$, This term is used to indicate the relationship between Transport processing functional entities and other networks, including other NGNs

T-U$_n$, This term is used to indicate the relationship between Transport processing functional entities and end-user function

TC-T$_n$, This term is used to indicate the relationship between Transport control functional entities and Transport processing functional entities

TC-TC$_n$, This term is used to indicate the relationship between the entities of Network Attachment Control Function (NACF) and Resource and Admission Control Functions (RACF). NACF and RACF constitute Transport control function.

8.3.1 Transport processing FEs

Figure 4 shows the transport processing FEs

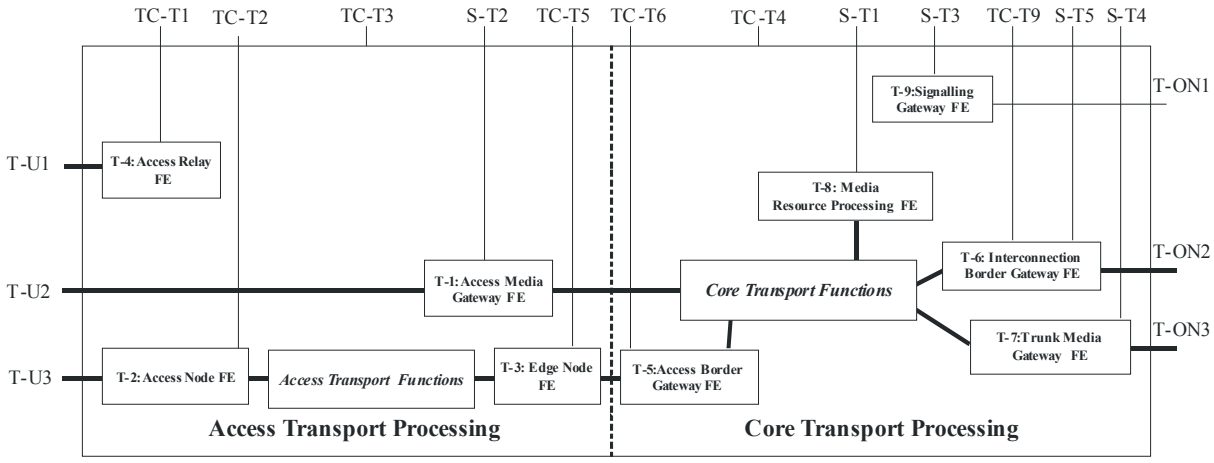


Figure 4 – Transport processing FEs

8.3.1.1 T-1 Access Media Gateway Functional Entity (AMG-FE)

The AMG-FE provides interworking between the packet-based transport used in the NGN and analogue lines or ISDN access.

a) It provides bi-directional media processing functions for user plane traffic between PSTN/ISDN and the NGN under the control of the AGC-FE (see section 8.3.3.8).

b) It provides adequate transfer functions for PSTN/ISDN user call control signalling to the AGC-FE for processing.

c) It optionally supports payload processing functions (e.g., codecs and echo cancellers).

8.3.1.2 T-2 Access Node Functional Entity (AN-FE)

The Access Node Functional Entity (AN-FE) in IP access network directly connects to CPN and terminates the first/last mile link signals at the network side. Generally, it is a Layer 2 device that may be IP capable.

As one key injection node for support of dynamic QoS control, the AN-FF may perform packet filtering, traffic classification, marking, policing and shaping at flow level or user level under the control of the A-TRC-FE.

8.3.1.3 T-3 Edge Node Functional Entity (EN-FE)

The Edge Node Functional Entity (EN-FE) in IP access network acts as the upstream traffic egress that connects IP access network to the external networks and terminates the Layer 2 access session with the CPE. It shall be a Layer 3 device with IP routing capabilities.

The EN-FE performs QoS mechanisms dealing with the user traffic directly, including buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing, shaping, and forwarding.

As one key injection node for support of dynamic QoS control, the EN-FE performs packet filtering, traffic classification, marking, policing and shaping at flow level or user level under the control of the A-TRC-FE.

8.3.1.4 T-4 Access Relay Functional Entity (AR-FE)

The AR-FE is a relay between end-user equipment and the NAC-FE that inserts local pre-configuration information when necessary.

8.3.1.5 T-5 Access Border Gateway Functional Entity (ABG-FE)

The Access Border Gateway Functional Entity (ABG-FF) is a packet gateway between an access network and a core network used to mask a service provider's network from access networks, through which CPE accessing packet-based services (e.g. IMS, Internet).

The functions of the ABG-FE may include Opening and closing gate, Packet filtering based firewall, Traffic classification and marking, Traffic policing and shaping, Network address and port translation, Media Relay (i.e. media latching) for NAT traversal, and Collecting and reporting resource Usage information (e.g. start-time, end-time, octets of sent data).

As one key injection node for support of dynamic QoS control, NAPT/FW control and NAT traversal, the ABG-FE performs the above functions on an IP flow under the control of the RACF.

8.3.1.6 T-6 Interconnection Border Gateway Functional Entity (IBG-FE)

The Interconnection Border Gateway Functional Entity (IBG-FE) is a packet gateway used to interconnect an operator's core network with another operator's core network supporting the packet-based services. There may be one or multiple IBG-FE in a core network.

The functions of the IBG-FE may be the same as that of the ABG-FE.

As one key injection node for support of dynamic QoS control, NAPT/FW control and NAT traversal, the IBG-FE performs the above functions on an IP flow under the control of the RACF.

Alternative means of control such as direct control by IBC-FE need further study.

In addition, the IBG-FE may support the following:

1) Media conversion (e.g., G.711 and AMR, T.38 and G.711)

2) Inter-domain IPv4/IPv6 conversion

3) Media encryption

4) Fax/modem processing

Note – Allocation of the above functions to the IBG-FE needs further study: IBG-FE may/may not perform media conversion under the control of IBC-FE. A direct link between IBG-FE and IBC-FE is under study.

8.3.1.7 T-7 Trunk Media Gateway Functional Entity (TMG-FE)

a) The TMG-FE provides interworking between the packet-based transport used in the NGN and trunk lines from the circuit-switched network. It is under the control of the MGC-FE.

b) It may support payload processing (e.g., codecs, echo cancellers, and conference bridges).

8.3.1.8 T-8 Media Resource Processing Functional Entity (MRP-FE)

The MRP-FE provides payload processing of packets used in the NGN.

a) It allocates specialized resources (such as announcement server, notification tone, and voice recognition resources, and voice menu and conference resources).

b) It provides media mixing functions under the control of the MRC-FE.

c) It receives and generates DTMF signals.

d) It generates tone signals (e.g., ring back).

e) It generates announcements.

f) It provides trans-coding, text-to-speech, video mixing, conference bridge, data conference, fax, voice and video recording, and voice recognition capabilities.

8.3.1.9 T-9 Signalling Gateway Functional Entity (SG-FE)

The SG-FE is responsible for signalling transport interworking between the NGN and existing networks such as PSTN, ISDN, IN networks, and Signalling System No.7.

8.3.2 Transport control functional entities

Figure 5 shows the functional entities related to transport control.

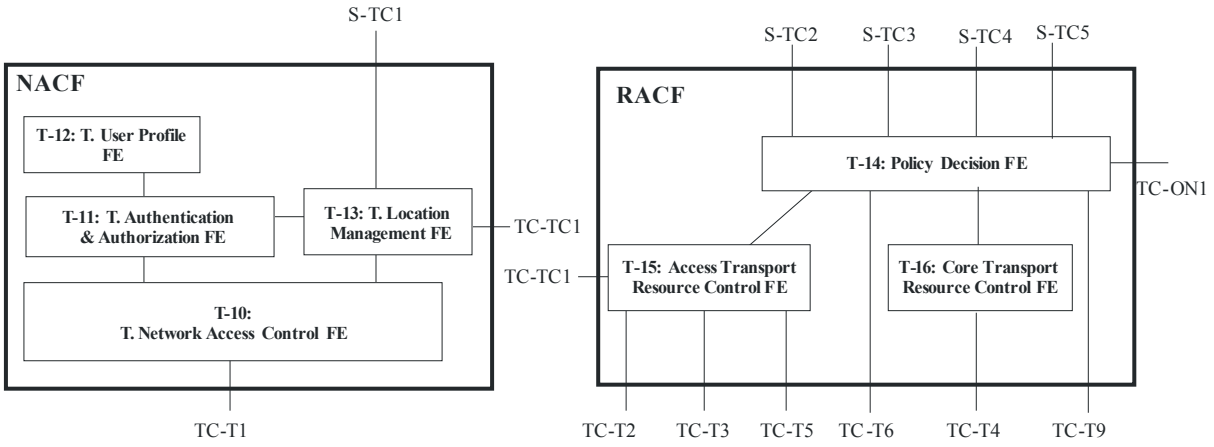


Figure 5 – Transport-control-related functional entities

8.3.2.1 T-10 Network Access Control Functional Entity (NAC-FE)

The NAC-FE is responsible for IP address allocation to terminals. It may also distribute other network configuration parameters, such as the addresses of DNS servers and signalling proxies (e.g., the address of the P-CSC-FE in order to have access to service stratum functions).

The NAC-FE should be able to provide an access network identifier to a terminal. This information uniquely identifies the access network to which the terminal is attached.

The NAC-FE should be able to support location information functions and register the association between the IP address allocated to a terminal and related network location information, i.e., a line identifier (Line ID), and so forth.

The NAC-FE controls the following:

a) Firewall policy

b) Network Address and Port Translation (NAPT) policy

c) Security policy

8.3.2.2 T-11 Transport Authentication and Authorization Functional Entity (TAA-FE)

The TAA-FE provides authentication and authorization functions in the transport stratum.

a) Protocols such as Mobility Management protocols shall specify how users or terminals are identified in networks. The identification function is the first step and is used for authentication, authorization, and accounting (AAA) of users/terminals.

b) Support for commonly used AAA and security schemes is provided.

These protocols are thus required to cooperate with commonly used AAA and security schemes to support authentication, authorization, accounting, and security for services.

8.3.2.3 T-12 Transport User Profile Functional Entity (TUP-FE)

The TUP-FE is responsible for storing user profiles, subscriber-related location data, and presence status data at transport stratum.

1) The TUP-FE performs basic data management and maintenance functions.

- User profile management functions

  These functions are based on some data, either "user subscription data" or "network data" (e.g., the current network access point and network location). The storage and update of this data are handled by the user profile management functions.

A user profile shall be provided in support of:

- authentication
- authorization
- service subscription information
- subscriber mobility
- location
- online/offline status management
- charging

The user profile may be stored in one database or separated into several databases.

2) The TUP-FE is responsible for responses to queries for user profiles.

   a) It provides access to user data.

      Other network functions require some user data in order to be appropriately customized. This can be either "user subscription data" or "network data". This function provides filtered access to the user data, which may be restricted to certain interrogating entities (i.e., restricted rights to access user data), in order to guarantee user data privacy.

   b) It may also be used for support of commonly AAA and security schemes.

NOTE – Transport User Profile may reside in the visited or home networks

8.3.2.4 T-13 Transport Location Management Functional Entity (TLM-FE)

It is for further study.

8.3.2.5 T-14 Policy Decision Functional Entity (PD-FE)

The PD-FE manages and controls the policies and resources of the transport stratum.

- It provides a single point of contact to the service request functional entities in the service stratum (e.g., P-CSC-FE, IBC-FE, and AGC-FE), and it receives and responds to resource requests from these FEs.
- It maps the service request parameters and classes received from the service request functional entities in the service stratum (e.g., P-CSC-FE, IBC-FE, and AGC-FE) to network parameters and classes according to service-dependent policy rules.
- It locates the involved access networks and core networks in order to offer the requested resource.
- It interacts with the A-TRC-FE and C-TRC-FE in the involved access/core networks to check whether the requested resource is available.
- It performs mediation based on the resource availability information from the A-TRC-FE and C-TRC-FE; then, it responds to the service request functional entities in the service stratum (e.g., P-CSC-FE, IBC-FE, and AGC-FE).

In addition, the following mobility features are supported.

- Route optimization function
  - It should be possible to select proper routing paths between the traffic-originating node and the traffic-receiving node according to the traffic contract and the overall network traffic conditions after movement.

- The selected routing paths should be able to maintain specific QoS levels, or better, after movement, where possible.
- It should be possible to use both static and dynamic routing schemes.
- The route optimization should be able to include alternate paths to cope with routing path failures (e.g., by using a pre-assigned routing table or a dynamic algorithm for path calculation).
- The exchanged routing information should include QoS and other parameters for internetworking situations.

• Switching function
- This function performs routing or path management.
- It may be used when a change in a route or path for transmitting packets is needed.
- It may support routing optimization.
- It may include a local switching function.
- The local switching function performs routing or path management within a region.
- The region is covered by a system that is responsible for mobility.
- This function may support regional mobility.

8.3.2.6 T-15 Access Transport Resource Control Functional Entity (A-TRC-FE)

Refer to TR-RACF [5].

8.3.2.7 T-16 Core Transport Resource Control Functional Entity (C-TRC-FE)

Refer to TR-RACF [5].

8.3.3 Service control functional entities

Figure 6 shows the service stratum FEs.

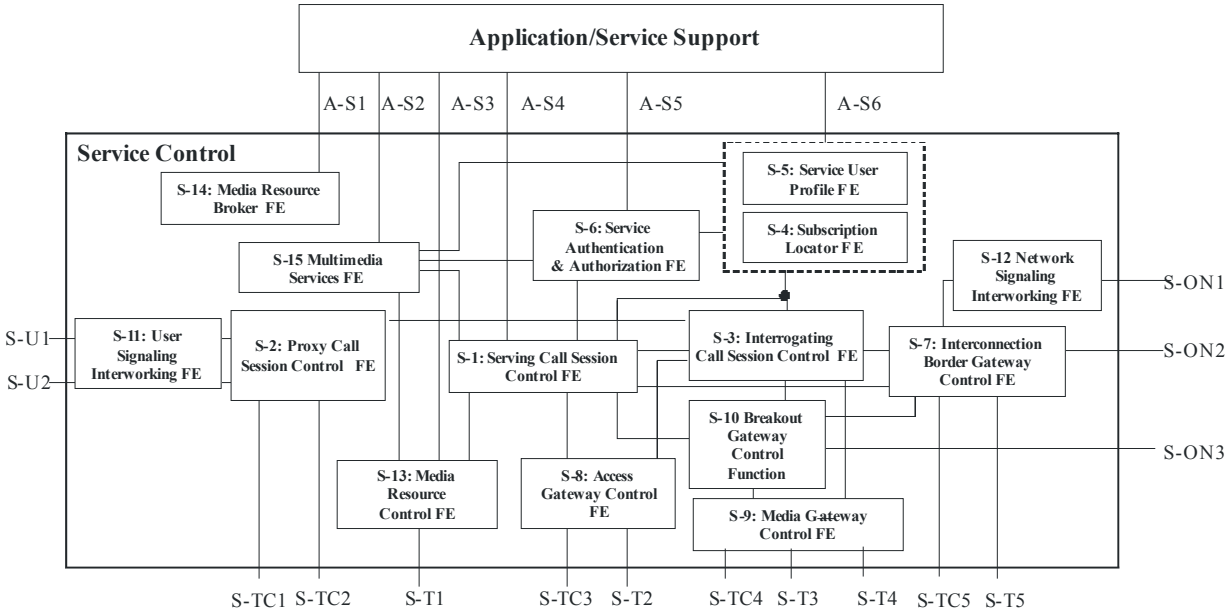


Figure 6 – Service stratum functional entities

8.3.3.1 S-1 Serving Call Session Control Functional Entity (S-CSC-FE)

The S-CSC-FE handles functionality related to session control, e.g., registration, origination of sessions (session setup, modification, and teardown), and routing of session messages.

a) It interacts with the Application/Service Support functions to trigger requested services.

b) It processes requests from users (and terminals) for registration;

c) It can route messages to terminals based on the routing (location) information obtained at registration.

d) It interacts with the AGC-FE to communicate with PSTN or ISDN users.

The S-CSC-FE maintains a session state as needed by the network operator for support of services. Within an operator's network, different S-CSC-FEs may have different functionalities.

For session-related and session-unrelated flows, the S-CSC-FE:

1. May behave as a proxy server as defined in RFC 3261, i.e., it can accept requests and service them internally or forward them on, possibly after translation.
2. May behave as a user agent as defined in RFC 3261, i.e., it may terminate and independently generate SIP transactions.
3. Interacts with the AS-FE to support services and third-party applications.
4. Performs as follows for an originating endpoint (i.e., the originating user/UE or originating AS-FE):
    a. It obtains from a database the address of the contact point for the network operator serving the destination user from the destination name (e.g., a dialled phone number or SIP URI), when the destination user is a customer of a different network operator, and it forwards the request or response to that contact point.
    b. When the destination name of the destination user (e.g., a dialled phone number or SIP URI) and the originating user belong to the same network operator, it forwards the SIP request or response to an I-CSC-FE within the operator's network.
    c. It forwards the SIP request or response to a BGC-FE for call routing to the PSTN.
    d. In case the request is an originating request from an AS-FE:
        – It verifies that the request coming from the AS-FE is an originating request and applies procedures accordingly (e.g., it invokes interaction with the service platforms for the originating services, etc.).
        – It processes and proceeds with the request even if the user on whose behalf the AS-FE had generated the request is unregistered.
        – It processes and proceeds with other requests to and from the user on whose behalf the AS-FE had generated the request.
        – It reflects in the charging information that an AS-FE had initiated the session on behalf of the user.
5. Performs as follows for a destination endpoint (i.e., the terminating user/UE)
    a. It forwards the SIP request or response to an P-CSC-FE for a terminating session procedure for a home user within the home network, or for a user roaming within a visited network where the home network operator has chosen not to have an I-CSC-FE in the path.
    b. It forwards the SIP request or response to an I-CSC-FE for a terminating session procedure for a roaming user within a visited network where the home network operator has chosen to have an I-CSC-FE in the path.
    c. It forwards the SIP request or response to a BGC-FE for call routing to the PSTN.

d. If the SIP request contains preferences for the characteristics of the destination endpoint, it performs preference and capability matching as specified in RFC 3312.

8.3.3.2 S-2 Proxy Call Session Control Functional Entity (P-CSC-FE)

The P-CSC-FE acts as the contact point to the user terminal for session services. Its address is discovered by terminals using mechanisms such as static provisioning, an NACF, or other access-specific techniques. The P-CSC-FE behaves like a proxy (as defined in RFC 3261), i.e., it accepts requests and services them internally or forwards them on. The P-CSC-FE shall not modify the Request URI in a SIP INVITE message. It may behave as a user agent (as defined in the RFC 3261), i.e., under abnormal conditions it may terminate and independently generate SIP transactions. The functions performed by the P-CSC-FE include the following:

a) It forwards a register request received from a terminal to an I-CSC-FE determined using the home domain name, as provided by the terminal. (Figure needs to be fixed.)

b) It forwards SIP messages received from the terminal to the SIP server (e.g., an S-CSC-FE) whose name the P-CSC-FE has received as a result of the registration procedure.

c) It forwards SIP requests or responses to the terminal.

d) It detects and handles emergency session establishment requests.

e) It maintains a security association between itself and each terminal.

f) It may perform message compression/decompression, if needed.

g) It may participate in the authorisation of media resources and QoS management, e.g., by interacting with resource control when no explicit signalling (i.e., QoS signalling) is available and application-specific intelligence is required to derive resource control commands from the application signalling.

h) It supports an NAPT Proxy Function (NPF) for network address hiding and remote NAT traversal. It requests address mapping information and modifies the addresses and/or ports contained in the message bodies of application signalling messages according to the address binding information provided by the RACF at the border of the access and core networks.

8.3.3.3 S-3 Interrogating Call Session Control Functional Entity (I-CSC-FE)

The I-CSC-FE is the contact point within an operator's network for all connections destined to a user of that network operator. There may be multiple I-CSC-FEs within an operator's network. The functions performed by the I-CSC-FE are as follows:

Registration

– Assigning an S-CSC-FE to a user performing SIP registration.

Session-related and session-unrelated flows

– Obtaining from the SUP-FE the address of the currently assigned S-CSC-FE.

– Forwarding a SIP request or response to the S-CSC-FE determined by the above step for incoming sessions.

In performing the above functions the operator may use the optional topology hiding function in the I-CSC-FE or other techniques to hide the configuration, capacity, and topology of the network from the outside. When an I-CSC-FE is chosen to meet the hiding requirement, for sessions traversing different operators' domains, the I-CSC-FE may restrict the following information from being passed outside an operator's network: the exact number of S-CSC-FEs, the capabilities of the S-CSC-FEs, and the capacity of the network.

8.3.3.4 S-4 Subscription Locator Functional Entity (SL-FE)

The SL-FE may be queried by the S-CSC-FE, I-CSC-FE, or AS-FE to obtain the address of the SUP-FE for the required subscriber. The SL-FE is used to find the address of the physical entity that holds the subscriber data for a given user identity when multiple, separately addressable SUP-FEs have been deployed by the network operator. This resolution mechanism is not required in networks that utilise a single logical SUP-FE element (e.g., a single server farm architecture).

8.3.3.5 S-5 Service User Profile Functional Entity (SUP-FE)m

The SUP-FE is responsible for storing user profiles, subscriber-related location data, and presence status data in the Service stratum.

1) The SUP-FE performs basic data management and maintenance functions.

   • User profile management functions

   These functions require access to certain data, either "user subscription data" or "network data" (e.g., the current network access point and network location). The storage and update of this data are handled by the user profile management functions.

   A user profile shall be provided in support of:

   • authentication
   • authorization
   • service subscription information
   • subscriber mobility
   • location
   • presence (e.g., online/offline status)
   • charging

   The user profile may be stored in one database or separated into several databases.

2) The SUP-FE is responsible for responses to queries for user profiles.

   a) It provides access to user data.

   Other network functions require some user data in order to be appropriately customized. This data can be either "user subscription data" or "network data". This function provides filtered access to the user data, which may be restricted to certain interrogating entities (i.e., restricted rights to access user data), in order to guarantee user data privacy.

b) It may also be used for support of commonly AAA and security schemes.

8.3.3.6 S-6 Service Authentication and Authorization Functional Entity (SAA-FE)

The SAA-FE provides authentication and authorization in the service stratum.

1) It ensures that the end-user has valid utilization rights for the requested service.
2) It performs policy control at the service level by using policy rules contained in a user profile database.
3) It works as the first step in the mobility management process and is used for authentication, authorization, and accounting of users/terminals.
4) The result of the authorization function is a yes/no response to a user connection request.

8.3.3.7 S-7 Interconnection Border Gateway Control Functional Entity (IBC-FE)

The IBC-FE controls Interconnection Border Gateway Functional Entities (IBG-FEs) to interwork with other packet-based networks.

1) Inter-domain network topology hiding

2) Control of IBG-FEs to implement session-based processing (E.g. media conversion and NA(P)T). (To be studied)

3) Inter-domain protocol repair (To be studied)

4) Interaction with PD-FE for resource reservation, resource allocation and/or other resource related information (e.g., the available resource parameters if the required resources are not available, Qos label etc.)

8.3.3.8 S-8 Access Gateway Control Functional Entity (AGC-FE)

The AGC-FE controls one or more AMG-FEs to access PSTN or ISDN users and handles registration, authentication, and security for the user. The AGC-FE performs registration, authentication, and security for AMG-FE.

a) It provides signalling translation and conversion between up-links and down-links or between SIP and H.248-based control (i.e., it appears as a SIP UA to the network).

b) It may initiate and terminate UNI protocols in order to provide ISDN supplementary services.

c) It forwards the session control flow to the S-CSC-FE.

d) It processes and forwards requests from the AMG-FE to the S-CSC-FE.

e) It may process and forward value-added service requests from the AMG-FE to the AS-FE through the S-CSC-FE. For example, a POTS user can request and use a multimedia 800 service provided by the AS-FE with media restrictions.

f) It may participate in the authorisation of media resources and QoS management, e.g., by interacting with resource control when no explicit signalling (i.e., QoS Signalling) is available and application-specific intelligence is required to derive resource control commands from the application signalling.

g) It supports an NAPT Proxy Function (NPF) for network address hiding and remote NAT traversal. This is done by requesting address mapping information and modifying the addresses and/or ports contained in the message bodies of application signalling messages, according to the address binding information provided by the RACF at the border of the access and core networks.

8.3.3.9 S-9 Media Gateway Control Functional Entity (MGC-FE)

The MGC-FE controls the TMG-FE to interwork with PSTN/ISDN.

a) It processes and forwards requests from the SG-FE to the S-CSC-FE through the I-CSC-FE;

b) It may include an IN mediation function (i.e., an SSF: Service Switching Function) in order to provide services for legacy IN SCPs. To do so, it interworks with the SG-FE and BGCF.

c) It may process and forward value-added service requests from PSTN/ISDN to the AS-FE through the BG-FE and S-CSC-FE. For example, a PSTN user can request and use a multimedia 800 service provided by the NGN AS-FE with media restrictions.

8.3.3.10 S-10 Breakout Gateway Control Functional Entity (BGC-FE)

The BGC-FE selects the network in which PSTN breakout is to occur and selects the MGC-FE.

8.3.3.11 S-11 User Signalling Interworking Functional Entity (USIW-FE)

The USIW-FE has the responsibility for the interworking and information screening functions for different types of application signalling at the subscriber side (access-to-core), which can be located at the border of the access and core networks for subscriber-side signalling interworking.

8.3.3.12 S-12 Network Signalling Interworking Functional Entity (NSIW-FE)

The NSIW-FE has the responsibility for the interworking and information screening functions for different types of application signalling at the trunk side (inter-operator), which can be located at the border of the core networks for trunk-side signalling interworking.

8.3.3.13 S-13 Media Resource Control Functional Entity (MRC-FE)

The MRC-FE controls the Media Resource Processing Functional Entity (MRP-FE) by operating as a media resource control function.

The MRC-FE allocates/assigns MRP-FE resources that are needed for services such as streaming, announcements, and Interactive Voice Response (IVR) support.

8.3.3.14 S-14 Media Resource Broker Functional Entity (MRB-FE)

The MRB-FE does the following:

- It assigns specific media server resources to incoming calls at the request of service applications (i.e., an AS); this happens in real time as calls come into the network.
- It acquires knowledge of media server resource utilization that it can use to help decide which media server resources to assign to resource requests from applications.
- It employs methods/algorithms to determine media server resource assignment.
- It acquires knowledge of media server resources status related to in-service and out-of-service status and reservations via an operational type of reference point.

8.3.3.15 S-15 Multimedia Services Functional Entity (MLT-FE)

The generic NGN functional architecture also provides support for non-session-based services, since it is expected to provide a platform for all envisaged services over packet-based networks.

Some functions may be common to both categories of services, such as Media Resource Control Functional Entity (MRC-FE) or RACF.

In the transport layer, it is anticipated that most of the functions will be common to both non-session and session-based services, although it is assumed that some NGN implementations may not utilize all the transport functions. For example, some gateway functions may not be involved in support of such services.

NOTE – Specific use of the MLT-FE is beyond Release 1 and needs further study.

8.3.4 Application/Service Support Functions

The Application/Service Support Functions provides control for services accessed by interacting with the S-CSC-FE, MLT-FE, or end-user directly. Application/Service Support Functions may reside either in the End-user's home network or in a Third Party location. The Application/Service Support Functions may comprise the following Functional Entities:

- A-1: Application Server FE (AS-FE) – Support generic application server functions including:
  - SIP application server,
  - Open Service Architecture (OSA) application server,
  - OMA Service Environment (OSE) service enabler and
- A-2: Intelligent Network Application Server FE (IN-AS-FE) - Contains service logic programs for providing intelligent network-based value added services.
- A-3: Application Gateway FE (APL-GW-FE) – Serves as an interworking entity between the Third Party Application Providers block and the S-CSC-FE of the Service stratum. Appearing to the S-CSC-FE as if it were an AS-FE, the APL-GW-FE provides a secure open interface for the Third-Party Application Providers block to use the capabilities and resources of the NGN. Specifically,

the APL-GW-FE is the interworking entity between various functions of NGN and all external application servers and value added service enablers.

- A-4: Application Service Coordination Manager FE (APL-SCM-FE) - Manages interactions between multiple application services (or servers).
- A-5: Service Switching Functional Entity (SS-FE) – Provides access and interworking to a legacy IN SCP. For the IN SCP, the session controller is connected through SS-FE supporting INAP to interact with legacy SCP.

The Application/Service Support Functions can influence and impact the SIP session on behalf of services through its interface with the S-CSC-FE.

It shall be possible for Application/Service Support Functions to generate SIP requests and dialogs on behalf of users. Such requests are forwarded to the S-CSC-FE serving the user, and the S-CSC-FE shall perform regular originating procedures for these requests. Residing either as a trusted entity in the user's home network or as an un-trusted entity in a third-party location (requiring certain level of authentication), the Application/Service Support Functions interacts with other entities in the network as shown in Figure 7.

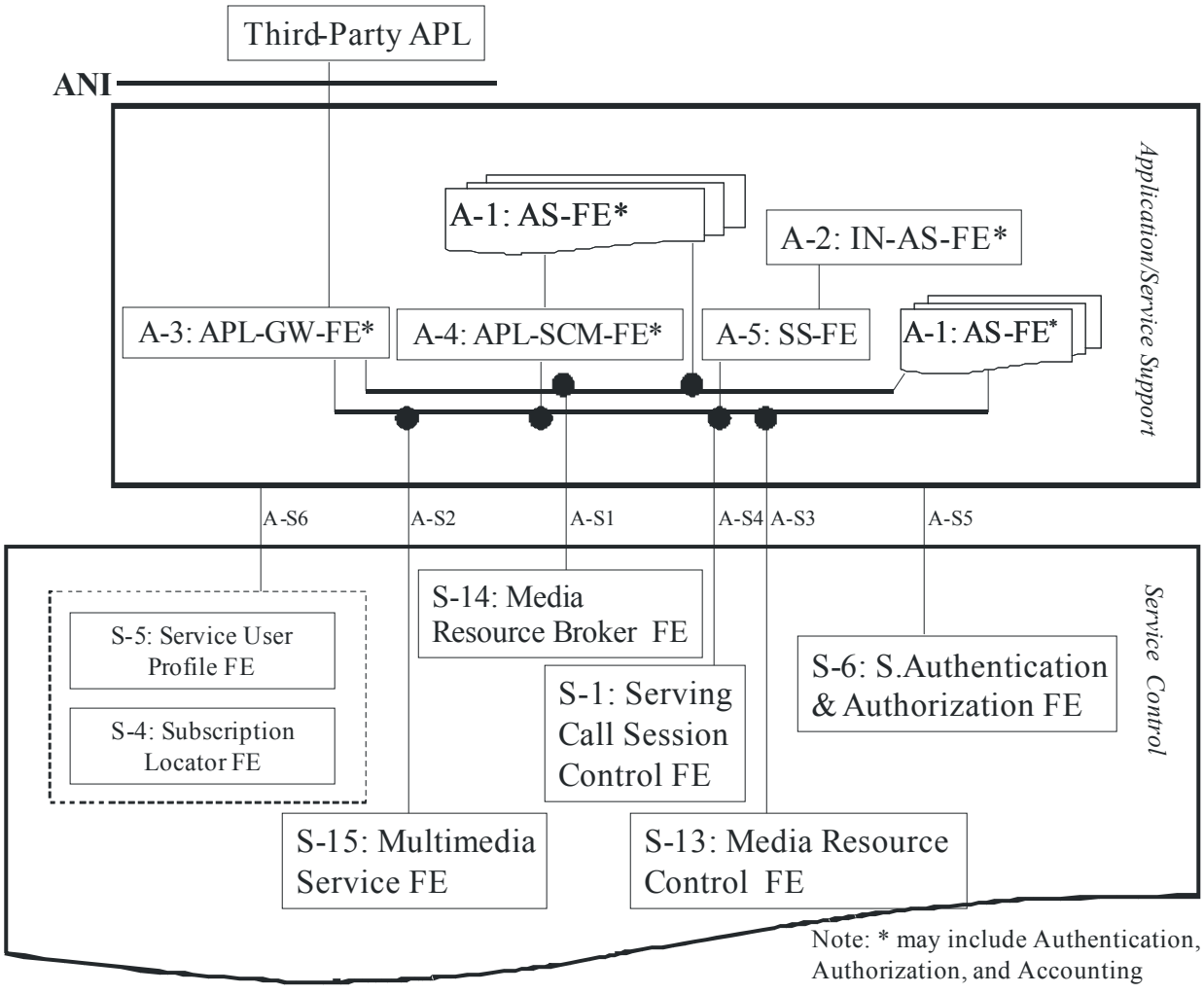


Figure 7 – Application/Service support functions

The Application/Service Support Functions does the following:

a) It executes service logic based on the subscriber's service profile and/or on the terminal capability (device profile).

b) It interworks with other application servers, such as a presence server, geographical information systems (GIS) server, or another AS, to provide convergent services to the end user.

c) It acts via four session interaction models with respect to the S-CSC-FE:
   – as a terminating user agent
   – as an originating user agent
   – as a SIP proxy
   – as a Third-Party Call Control (Back-to-Back User Agent)

d) It interacts with the AGC-FE directly or through the S-CSC-FE to communicate with PSTN or ISDN users.
   –

Application/Service Support Function examples include call feature application servers, presence servers, various messaging servers, conference servers, home application servers, etc.

9 Transport and service configuration of the NGN

This section introduces multiple configurations of the NGN functional architecture, derived from the generic functional model specified in Section 8. Since one of the aims of the NGN is to provide a wide variety of services, the functional architecture makes use of existing technologies. Thus, some NGN FEs may be represented by FEs used in existing technologies, which may support only some of the functions of the NGN FE. It is therefore possible for these FEs to be used in a different manner depending on the context. In this section, an NGN configuration refers to such a context. Multiple configurations are described in terms of the service control functions in the service stratum and access transport functions in the transport stratum. The exact functionality and interface associated with each FE and the reference points in these configurations are described in other documents specifically covering each configuration.

The representation shown in Figure 8 makes extensive use of colour to group related aspects of service delivery. Service delivery and control are represented by components and intended to collate related control functions. A wide variety of services is supported in the NGN by application functions.

The service components are related to each other and may contain common or shared functionality. No assumptions should be made concerning their representation as separate components in the figure.

Figure 8 shows several NGN service and transport configurations. In release 1, three configurations are identified in the service stratum: IP multimedia service, PSTN/ISDN emulation service, and streaming service configurations. Regarding the transport stratum, multiple configurations are represented in the access transport area. Other NGN components, such as the Network Attachment Control Functions (NACF), Resource and Admission Control Functions (RACF), and user profile functions are common to all configurations.

A particular link between boxes and clouds shows a possible linkage there.

The IP multimedia service component (orange) makes use of IMS specifications with adaptation to fixed-network access (green). PSTN/ISDN simulation service is also provided by this component.

The PSTN/ISDN emulation service component (fluorescent green) provides all of the network functionality associated with supporting existing services for legacy end-user interfaces and equipment.

Physical transport networks provide the connectivity for all components and physically separated functions within the NGN. Transport is divided into access networks and the core network, with a border gateway linking the two transport network categories. IP connectivity is provided to the NGN end-user equipment by

the transport functions, under the control of the network attachment control functions and the resource and admission control functionality.

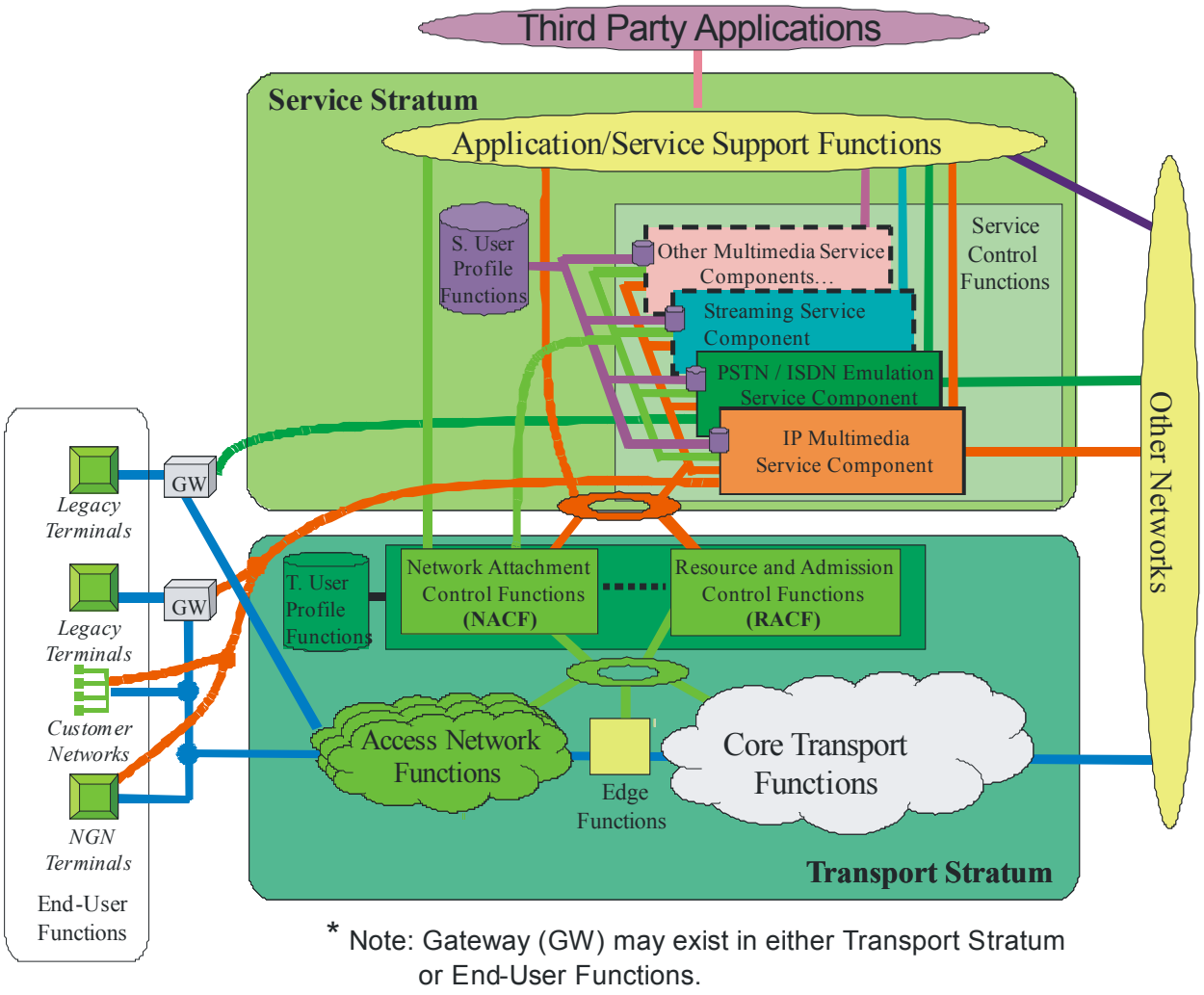


Figure 8 – Transport and service configuration of the NGN

In the transport stratum, multiple configurations are possible with the access transport functions.

The figure represents the compilation of user information and other service control related data into user profile functions. These functions may be specified and implemented as a set of cooperating databases with functionality residing in any part of the NGN.

End-user interfaces are supported by both physical and functional (control) interfaces, and both are shown in the figure. No assumptions are made about the diverse end-user interfaces and end-user networks that may be connected to the NGN access network. All categories of end-user equipment are supported in the NGN, from single-line legacy telephones to complex corporate networks. End-user equipment may be either mobile or fixed.

The NGN interface(s) to other networks includes many existing networks, such as PSTN/ISDN and the public Internet. The NGN interfaces other networks both at the control level and at the transport level, by using border gateways. The border gateways may involve media transcoding and bearer adaptation. Interactions between the control and transport levels may take place, either directly or through the RACF.

9.1 Service-specific configurations

9.1.1 IP Multimedia Service component

An IP Multimedia Service component utilises SIP-based control. These services may include multimedia session services, such as voice or video telephony or PSTN/ISDN simulation, and some non-session services, such as subscribe/notify for presence information and the message method for message exchange. In contrast to the emulation service described in section 9.1.2 below, PSTN/ISDN simulation service refers to the provision of PSTN- / ISDN-like services to advanced terminals such as IP phones. In addition, the IP Multimedia Service Component supports the mobility requirements of release 1.

The IP Multimedia Service Component is specified further in TR-IFN [7].

9.1.2 PSTN/ISDN Emulation Service Component

PSTN/ISDN emulation refers to mimicking a PSTN/ISDN network in order to support a legacy terminal connected through a gateway to an IP network. All PSTN/ISDN services remain available and identical (i.e., with the same ergonomics), such that end users are unaware that they are not connected to a TDM-based PSTN/ISDN.

By contrast, PSTN/ISDN simulation refers to the provision of PSTN- / ISDN-like services to advanced terminals such as IP phones. The IP Multimedia Service Component described in section 9.1.1 may provide such simulation services. The PSTN/ISDN Emulation Component is specified further in TR-PIEA [8].

9.1.3 Streaming Service Component

The NGN may provide streaming services as defined in the NGN release 1 scope document [2]. These may include, for example, content delivery services, multimedia multicast or broadcast services, and push services.

The streaming service Component will be specified further in a separate document.

9.1.4 Other service components for providing NGN services

Other NGN services are defined in the NGN release 1 scope document [2]. These may include, for example, data retrieval applications, data communication services, online applications, sensor network services, remote control services, and over-the-network device management.

The NGN service components used to provide such other NGN services will be specified further in a separate document.

9.2 Access-network-specific configuration

Because the NGN supports several types of access networks, specific components for access transport functions exist in the transport stratum. These include fixed access with a wire line, fixed access with a wireless LAN, and cellular access.

The access network components are specified in a separate document.

10 Security considerations

The security requirements within the functional requirements and architecture of the NGN are addressed by the NGN Security Requirements for Release 1 [9] and the Guidelines for NGN Security [10].

When deploying the architecture, these requirements should be met.

Appendix I

Examples of NGN network configurations

I.1 Configurations and topology of the NGN

Along with new architecture and services, the NGN brings an additional level of complexity over existing fixed networks. The addition of support for multiple access technologies and for mobility results in the need to support a wide variety of network configurations. Figure I-1 shows an NGN core network with a set of example access networks. In this figure, the core network is that part of the NGN that provides the telecommunications and/or multimedia services of the NGN to the user. It is distinguished from the access network(s) in that it provides common functions shared across one or more access networks. The NGN core network may be distinguished from other NGN core networks based on administrative needs or ownership. The access networks are distinguished from the core in that they do not provide end-user services directly (other than transport). The access networks may be distinguished from each other based on aspects such as technology, ownership, or administrative needs.

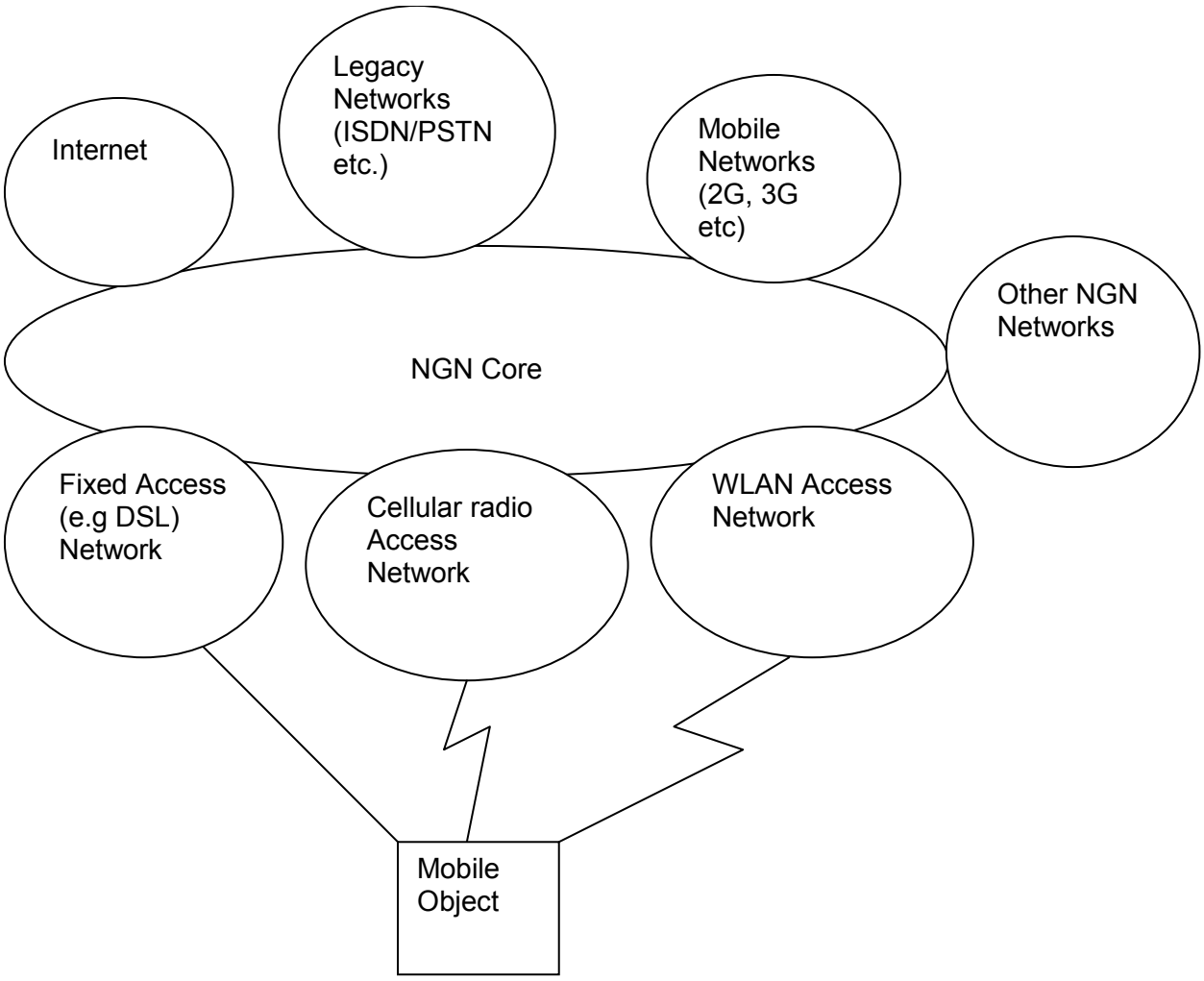


Figure I-1 – NGN core and access networks [Insert a comma before each instance of "etc.", and add a period to the instance under "Mobile Networks". Capitalize “radio”.]

In addition to the need to distinguish between the NGN core and access networks, the NGN support for roaming introduces another configuration aspect, that of a home network reached from a visited (sometimes called serving) network. Figure I-2 shows a configuration involving an end-to-end NGN session. In this example, User 1 is roaming outside his home network domain, and thus there is a need to distinguish between the home network and the visited network. User 2 in this case is in his home network.

It should be noted that the concept of a home network is not necessarily tied to the geographic location of a user's residence or workplace. Rather, it is based on the principle that an operator holds a subscription for the service being offered to the user. This operator is responsible for authorizing the user's access to the service and billing the user for this access. It is possible for an entire service to be provided by the visited network, for example, while still having a separate home network operator that authorizes the service through an appropriate business arrangement with the visited operator. More typically in the NGN, the home operator will provide the service control for the user while the visited operator will provide only access-related capabilities, such as support for authentication, support for authorization, data integrity services, and QoS support.

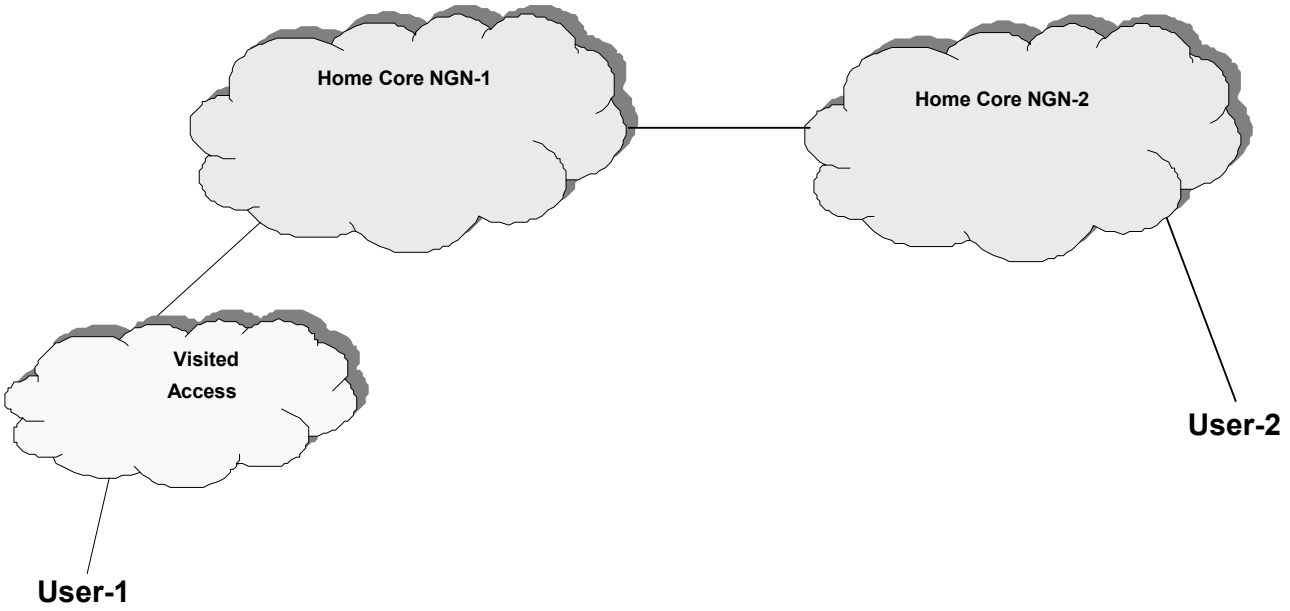


Figure I-2 – NGN example of home and visited networks

Figure I-2 also introduces the notion that multiple NGN core networks may interoperate to provide an end-to-end service to the user. In a simple case, an end-to-end session will have originating and terminating core networks. Depending on the operator's particular configuration and whether or not roaming is involved, one or more separate access networks might be involved. In a more complex case, some visited core network capabilities may be used in a roaming situation. Figure I-3 shows such an example, where User 1 is roaming outside his home network and support for services such as location information or media transcoding, for example, is provided by the visited operator's NGN core network.

Since, in many cases, the specific division of functionality between the core and access networks, between the home and visited networks, and between the originating and terminating networks is based on the operators' business decisions, it is difficult to precisely define the attributes that make up each of these configuration elements. Rather than hard points of separation in the architecture, these aspects should be thought of as configurable topology elements that may be mixed and matched in many different ways. The specification of the NGN architecture should not place any limitations on the operator's freedom to deploy capabilities or to use the capabilities of other business partners.

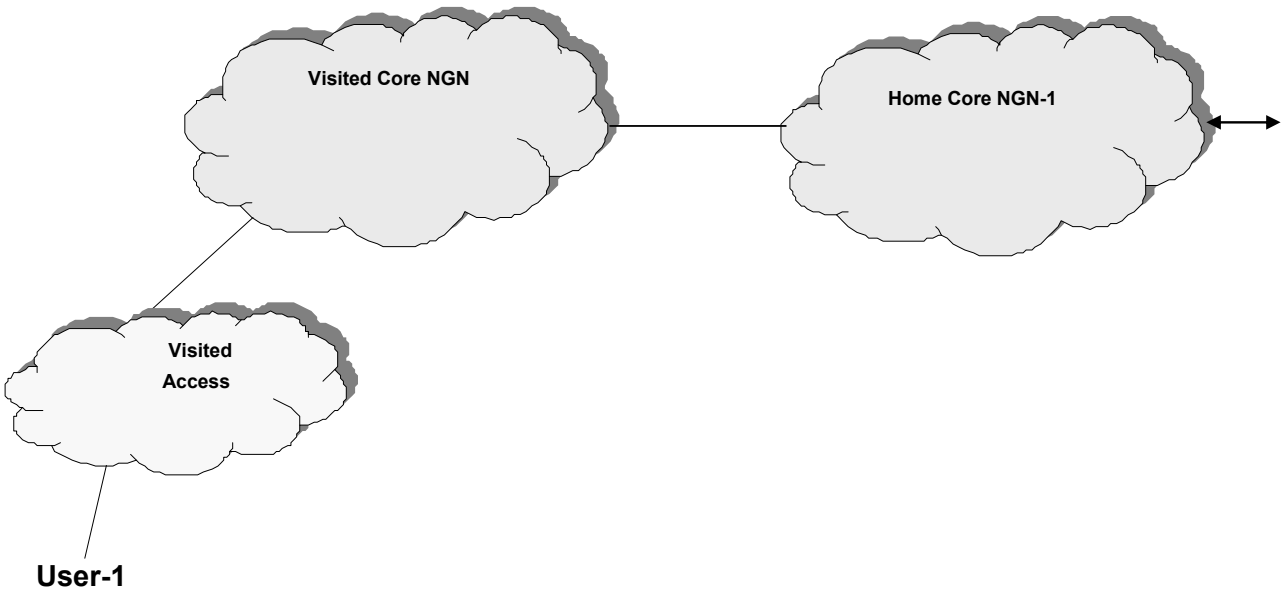


Figure I-3 – NGN example of visited NGN core network support

I.2 Relationship between the NGN and administrative domains

The NGN network can be logically decomposed into different subnetworks, as shown in Figure I-4. The emphasis on logical decomposition instead of physical decomposition is based on the fact that, in the future, physical equipment may have features of both the access network and the core network. A pure physical decomposition will encounter difficulties when such features are combined into a single network element.

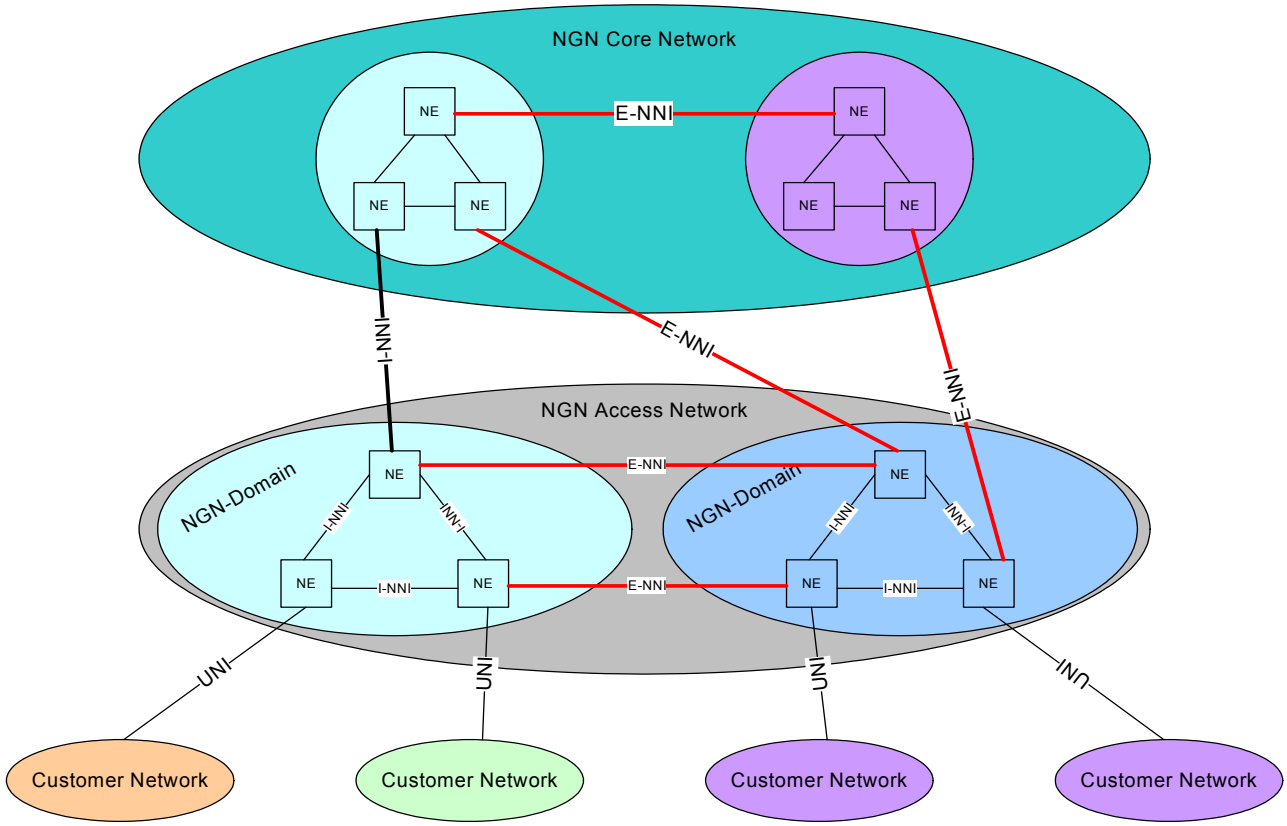


Figure I-4 – Major components of the NGN at the network level

The major components of an NGN network are as follows:

- End-user Network: An end-user network can be a home network or an enterprise network. It is connected to the service provider's network via a UNI (User-to-Network Interface). The UNI is also the demarcation point between the service provider and the user. An end-user network may obtain its content service from
  - the core network,
  - another instance of the end-user network providing public services, or
  - another instance of the end-user network providing private services, possibly with a private addressing scheme.
- Access Network: An access network collects end-user traffic from the end-user network to the core network. The access network service provider is responsible for the access network. The access network can be further partitioned into different domains, with the intra-domain interface being termed an I-NNI (Internal Network-to-Network Interface) and the inter-domain interface being termed an E-NNI (External Network-to-Network Interface). The access network belongs to the transport stratum.
- Core Network: The core network belongs to both the transport stratum and the service stratum. The core network service provider is responsible for the core network. The interface between the core network and the access network or between core networks can be an I-NNI (in the case of partitioning as a single domain) or an E-NNI.

The concept of an NGN domain is introduced to outline the administrative boundaries. Detailed topology information may or may not be shared across the E-NNI, but may be shared if available for I-NNI links. As depicted in the diagram above, the access network and the core network may or may not belong to the same NGN domain.

I.3 Relationship between the NGN and service domains

The NGN provides access to a wide variety of services. The specific services offered by any service provider are determined by business needs and customer needs. Figure I-5 shows an example of an NGN configuration to illustrate multiple domains within which services may be accessed.

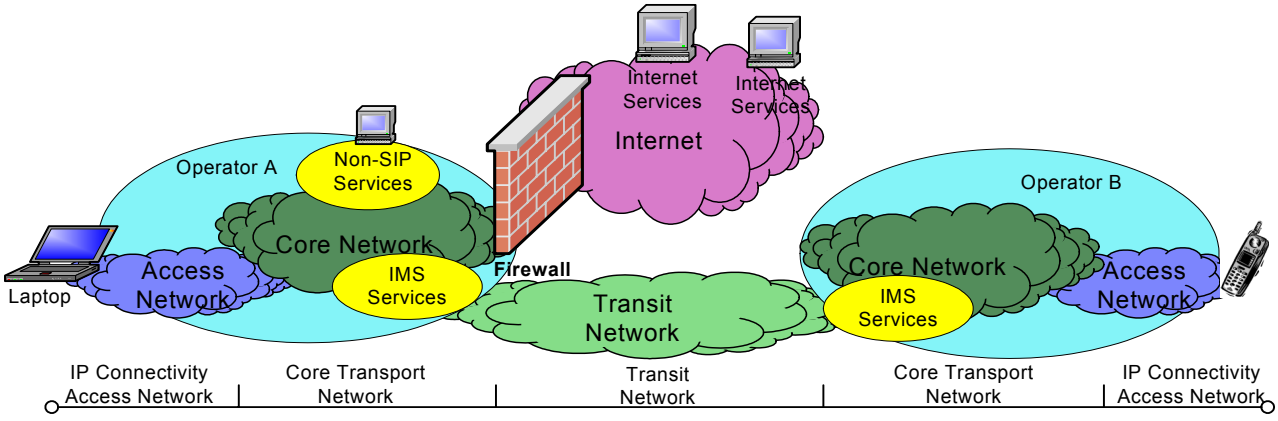


Figure I-5 – NGN example of service domains

In this example, Operator A supports a single access network technology that provides access to three service domains via its core network.

One service domain is that provided by the IMS services bubble. These services may be completely within Operator A's domain or may support end-to-end services to other operators. In this example, Operator A supports end-to-end IMS services along with Operator B's IMS. They are interconnected through a trusted transit network. Other transit network configurations are of course allowed, and the transit network may be null in the case where Operator A is directly connected to the other endpoint network. In some cases firewalls or other gateway elements might be used to protect the operator from the transit network. It should also be noted that the network on the other side of the transit network might be another type of external network, such as PSTN.

A second service domain in this example is the non-SIP services bubble of Operator A. This would provide services such as streaming video. These service entities may be attached directly to Operator A's core network or may be provided by third parties through trusted security arrangements.

A third service domain shown here is access to Internet-based services. These services are not part of Operator A's domain, nor are they provided by business arrangements with Operator A. These services are accessed by Operator A providing a transport connection to the Internet. Such a connection by Operator A may only be allowed via firewall techniques.

As mentioned earlier, this example shows only a small set of the possible configurations that might be supported by NGN operators. It illustrates the three basic domains of service access that are provided by the NGN.

I.4 Enterprise role model

The primary purpose of an enterprise model is to identify interfaces that are likely to be of general commercial importance. To do this, a number of roles are identified, which describe reasonably well-defined business activities that are unlikely to be subdivided between a number of players [1/Appendix I]. The players may aggregate roles as they see fit. Therefore an enterprise model does not limit players in anyway, but it does identify the roles that the architecture should enable.

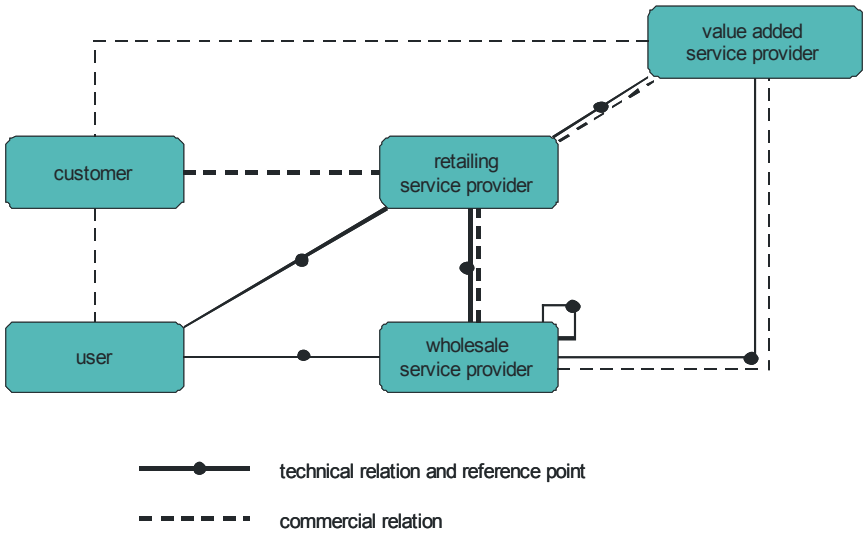


Figure I-6 – Basic NGN roles

A basic role model for NGN is shown in Figure I-6. The model itself is taken from [2/Appendix I], but we have modified the names to better align with the current NGN terminology. It identifies the following roles:

- *Customer:* The role denoting a person or other entity that has a contractual relationship with a service provider on behalf of one or more users.

- *User:* The role in which a person or other entity authorised by a customer uses services subscribed to by the customer.
- *Retailing Service Provider:* The role that has overall responsibility for the provision of a service or set of services to users associated with a subscription as a result of commercial agreements established with the users (i.e., subscription relationships). The user profile is maintained by the retailing service provider. Service provision is the result of combining wholesale network services and service provider service capabilities.
- *Wholesale Service Provider:* The role that combines a retailing service provider's service capabilities with its own network service capabilities to enable users to obtain services.
- *Value-Added Service Provider:* The role that provides services other than basic telecommunications service (e.g., content provision or information services) for which additional charges may be incurred. These may be billed via the customer's service provider or directly to the customer.

This basic model provides a kind of superclass for roles and their relations. Wholesale service provider players may need to combine their services to provision an end-to-end service. This is illustrated by the looped line and reference point in the figure. The figure further illustrates whether a relationship between roles is technical or commercial. In the latter case the relationship may or may not be supported by a technical reference point. Such a reference point would be in the management plane, which is not detailed in the FRA. We have therefore limited further elaboration of the model to the technical relationships and the roles that have at least one technical relationship. Hence, the customer role is not shown in the following figures.

The basic model can be extended to reflect the types of specialization that are already visible in the marketplace. To date, we mainly see specialization for the wholesale service provider role, and this is the only one we will consider in the following description. Specialization of the retailing and value-added service provider roles may be considered at a later stage.

The first specialization step is based on the domains as they have been defined by 3GPP in [3/Appendix I]. Unfortunately, it is not possible to reuse the terminology, as the distinction between serving and home network domains is functional, rather than an enterprise role distinction. The same player will support both functions, depending on the subscription of the user. For lack of a better term, we have used the term core for the server/home network role. The access and transit service provider roles map directly to the respective domains in [3/Appendix I]. Note that 3GPP uses the term "core network domain" for the combination of server, home, and transit network domains.

At this point it is also worth noting that [4/Appendix I] defines an IP Connectivity Access Network (IP-CAN) as the non-IMS part of a complete network solution, excluding terminals. It is not an access network domain as defined in [3/Appendix I], nor does it map to the access service provider role.

The first step in wholesale provider specialization (subclassing) is shown is Figure I-7.

A basic tenet of the NGN architecture is the separation of transport and service stratum functions. The main motivation for this is the requirement for the transport stratum to support different types of service control systems, not just IMS. This will be a functional requirement from any player, including cases where the transport and service stratum functions are combined in the core service provider role. We can take this one step further by specializing the core service provider into a core transport provider and a "service control and integration" provider role. The implication is that the reference points between functions in the transport stratum and the service stratum become trust boundaries and will have to support inter-operator security requirements.

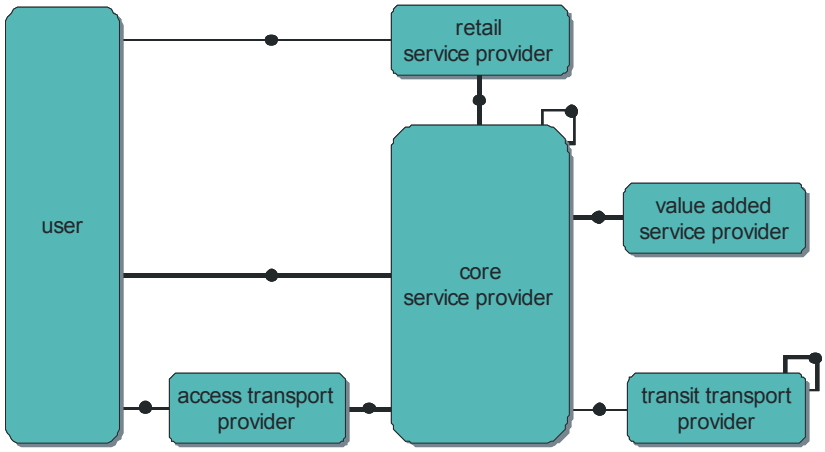


Figure I-7 – NGN roles: first level of specialization

For completeness, we have split the service control and integration provider role into separate service control provider and integration service provider roles. Virtual network operators are players who perform this role, and these are so well established that it is deemed appropriate to reflect this in the second level of specialization. The resulting role model is depicted in Figure I-8.

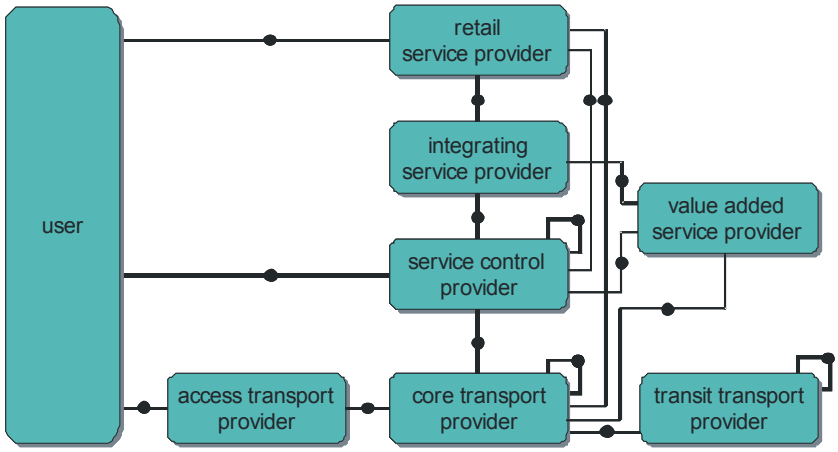


Figure I-8 – NGN roles: second level of specialization

Each of the new roles has a relationship with the retailing service provider role that holds the user profile database. A retailing role player may hold the user information for all three roles, or a user may have a relationship with multiple retailing role players. This cannot be derived from the figure, because it does not show the cardinality of these relationships.

In summary, the second level of specialization of the NGN enterprise model defines the following roles:

- *User:* The role in which a person or other entity authorised by a customer uses services subscribed to by the customer.
- *Retailing Service Provider:* The role that has overall responsibility for the provision of a service or set of services to users. The user profile is maintained by the retailing service provider. Service provision is the result of combining retailing service provider services with wholesale services from at least the access and core transport provider roles and at most from all other provider roles.

- *Integrating Service Provider:* The role that creates unique new service offerings from the wholesale services provided by other roles.
- *Service Control Provider:* The role that provides session and call control and related services, such as registration, presence, and location, wholesale to retailing and integrating service providers.
- *Value-Added Service Provider:* The role that provides value-added services (e.g., content provision or information services) on top of the basic telecommunications service provided by the service control provider role. It does not provide a complete service on its own.
- *Core Transport Provider:* The role that provides connectivity either end-to-end or in part, and related services such as registration for connectivity service, by combining its own services with those of the access transport provider and transit provider roles as necessary.
- *Access Transport Provider:* The role that provides a wholesale connectivity service between the user and a core transport provider.
- *Transit Transport Provider:* The role that provides a wholesale connectivity service between core transport providers, in conjunction with other transit transport providers as necessary. It also provides related DNS services.

Functional roles

In the previous section, we alluded to the fact that the core service provider role shown in Figure I-7 will, in general, support both home network as well as serving network functionality. If we apply a strict separation between the transport and service stratum functions as represented in the FRA and implied by the NGN enterprise model shown in Figure 8/Appendix I, both the service control provider and the core transport provider have to independently support home and serving network functions.

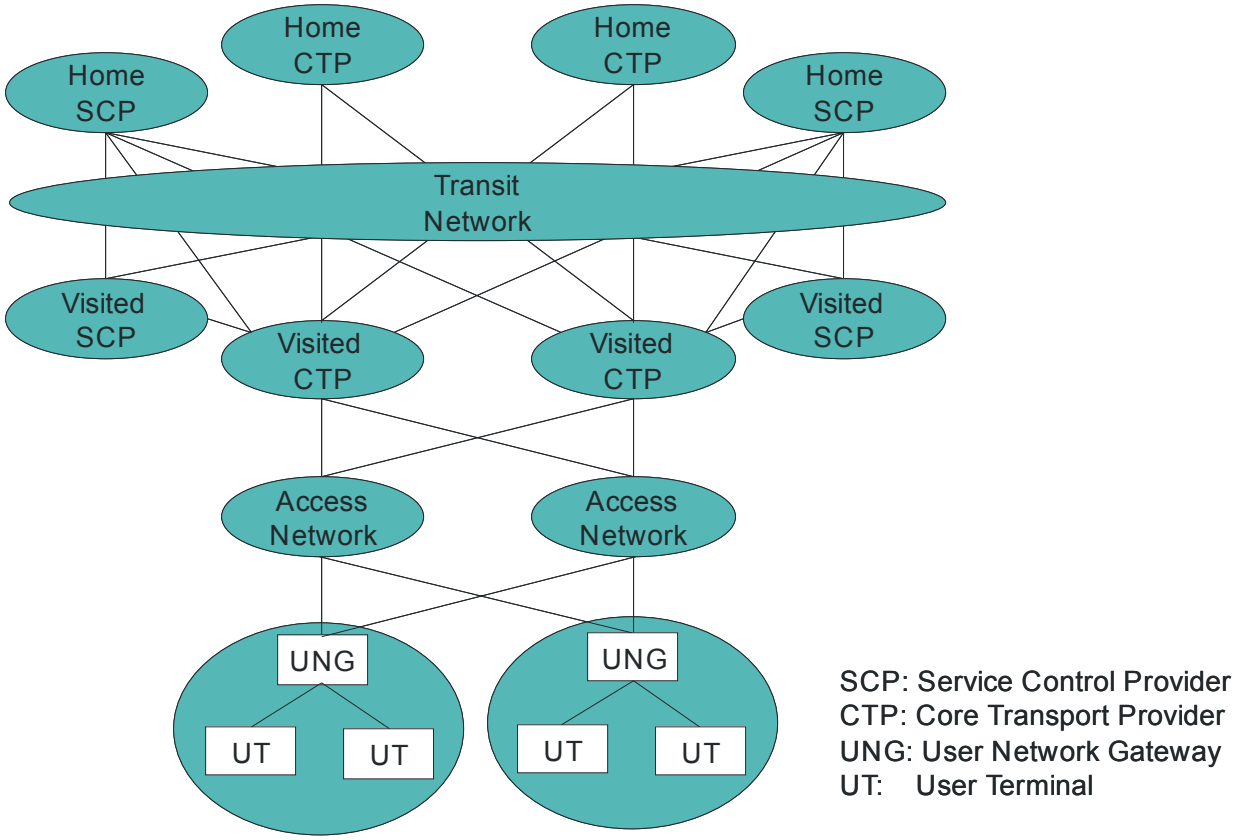


Figure 9/Appendix I – Home and visited network functional roles

The requirement to support user networks with nomadic terminals is another reason why the home network function of the user terminal in the service stratum may need to be supported by a different player than the one that supports the home network function for the User Network Gateway (UNG) in the transport stratum. In release 1, the UNG will be connected to a fixed network, which means that the access network will connect it directly to the core transport provider that provides the home network functionality. For moving networks this is no longer the case, and the UNG may roam as well.

The wide range of possibilities this creates is illustrated in Figure I-9. The UNG may be at a location where it has potential access to more than one access transport provider. Each access network may in turn be connected to multiple core transport providers. This scenario is already recognised and supported for WLAN interworking [5/Appendix I]. The additional complexity that is introduced by transport and service stratum independence significantly increases the number of routing possibilities, and it still needs to be verified whether this is fully supported by the current architecture.

We do not question the need to provide this flexibility since it will be required to support moving networks anyway. It will, however, undoubtedly increase the complexity, and release 1 will take longer to complete if it has to support the business model shown in Figure I-8, as opposed to the simpler one shown in Figure I-7.

1] ITU-T Recommendation Y.110 (1998), Global Information Infrastructure principles and framework architecture

[2] UMTS 22.01: Universal Mobile Telecommunication System (UMTS); Service aspects, Service principles

[3] ETS 123.101 v6.0.0: Universal Mobile Telecommunication System (UMTS); General UMTS Architecture

[4] ETS 123 228 v6.9.0: Universal Mobile Telecommunication System (UMTS); IP Multimedia Subsystem (IMS); stage 2

[5] 3GPP TS 24.234 v6.4.0: Universal Mobile Telecommunication System (UMTS); 3GPP system to WLAN Interworking; System description

Appendix II

Transport-stratum access network scenarios

II.1 Introduction

This section describes some transport-layer access network deployment scenarios that show user equipment accessing the NGN. The figures used to illustrate these scenarios show physical devices and indicate high-level functionality but do not indicate business models, enterprise roles, or operator domain boundaries. In general, many different business models may be used with each functional scenario. Some of the text used to describe the figures contains examples of such business model considerations.

Also, note that the term “policy enforcement” as used here covers generalized transport-layer user-plane policy enforcement actions, such as QoS traffic conditioning, packet filtering, NAT binding manipulation, usage metering, flow-based charging, and policy-based forwarding, which may in some cases be broader in scope than NGN Release 1. In this discussion, the terms “link layer” and “layer 2” are used synonymously. In the diagrams, some link-layer segments are shown with a specific type (e.g., VLAN), but in general any type of link layer can be used (e.g., SDH, ATM, MPLS, etc.).

II.2 Scenario 1: Multi-layered transport stratum

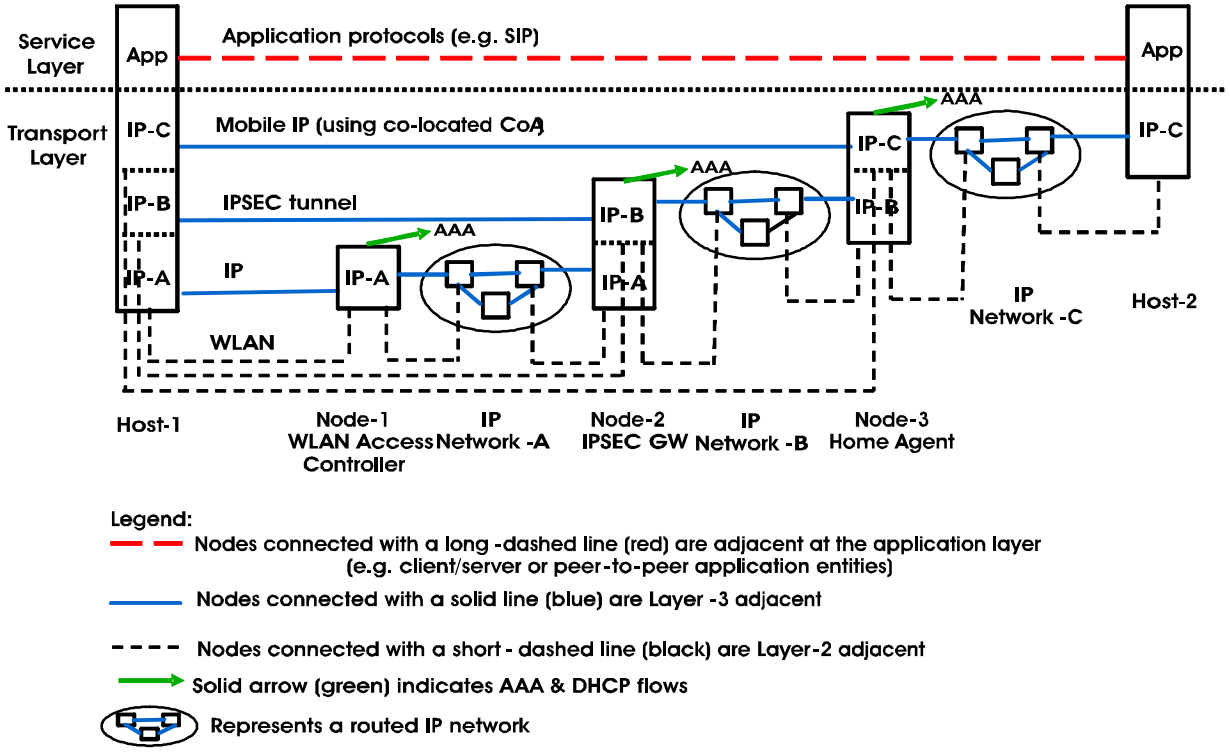


Figure II-1 – Multi-layered transport stratum

The transport stratum may be multi-layered, with a number of different access technologies layered on top of each other. For example, IP can run over a stack of link-layer technologies, such as IP/Ethernet /ATM/SDH/WDM. IP itself can also be used as a link-layer technology via IP tunnelling, and these IP tunnels can form part of a stack of link layers.

Figure II-1 shows a host running a stack of Mobile IP/IPsec/WLAN. For example, a terminal could connect to a public WLAN hotspot, establish an IPsec tunnel to an IPsec gateway located in a service provider domain, and then perform Mobile IP registration with a home agent also in the service provider domain. In this example, a co-located care-of address is used, so there is no foreign agent. Here, the terminal has three IP addresses, one for each layer. The first IP address is assigned when the terminal connects to the WLAN network; the second, when the terminal connects to the IPsec gateway; and the third, when Mobile IP registration is performed. Also, an AAA request may be issued independently at each layer for the purposes of user authentication and authorisation.

The terminal may send all application traffic over Mobile IP, or it can bypass one or more layers in the stack and send application traffic via a lower layer. For example, split IPsec tunneling could be used, whereby only traffic destined to the service provider domain is sent via IPsec, with general Internet traffic bypassing IPsec.

Transport-layer user-plane policy enforcement may be performed at each layer. For example, when a user connects to the WLAN, a packet filter for that user may be installed in the WLAN access controller that restricts traffic to a set of IPsec gateways. In turn, the IPsec gateways may have a packet filter for that user that restricts traffic to a set of Mobile IP home agents, such that the user is required to run Mobile IP. In turn, the home agents may have packet filters that allow the user to access some service platforms but not others.

When this scenario is mapped to a 3GPP WLAN IP access environment, the WLAN Access Gateway (WAG) functionality is located in node 1, and the Packet Data Gateway (PDG) functionality is located in node 2.

Mappings onto NGN Functional Architecture

In this scenario Node-1 acts as an EN-FE (e.g. handling QoS enforcement for the WLAN network). Node-1 may also act as an ABG-FE (e.g. performing NAT). Node-2 and Node-3 act as ABG-FEs, handling policy enforcement for their respective IP layers. This scenario illustrates that ABG-FE and EN-FE functionality may be performed independently at each IP layer in a transport stratum which contains multiple IP layers. Node-2 and Node-3 may also act as EN-FEs, handling QoS enforcement for the IP tunnels for which they are performing a layer-2 termination function. This scenario illustrates that ABG-FE and EN-FE functionality may be performed independently at each IP layer in a transport stratum which contains multiple IP layers.

II.3 Scenario 2: Access aggregation using layer 2

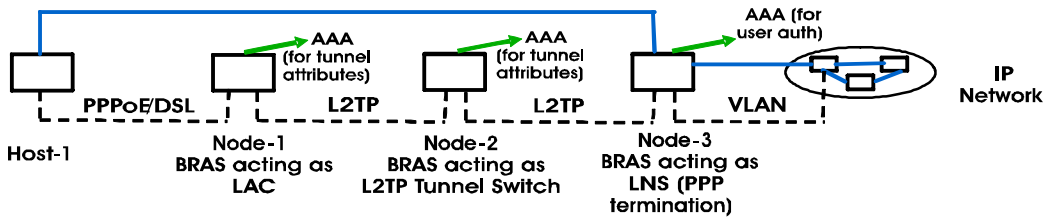


Figure II-2 – Access Aggregation using Layer-2

Within a single layer of the transport stratum, there may be multiple points where access traffic is aggregated. Traffic forwarding between different aggregation segments may be done at layer 2 or layer 3.

Figure II-2 shows a host running PPPoE connected over DSL to a BRAS. This BRAS acts as a LAC and forwards the traffic by using L2TP to a second BRAS acting as an LNS. Node 1 may issue a Radius request to obtain attributes for the tunnel to be established (e.g., RFC 2868). The second BRAS performs L2TP tunnel switching and in turn acts as a LAC and forwards the traffic to a third BRAS acting as an LNS. Node 2 may also issue a Radius request to obtain attributes for the tunnel to be established. The third BRAS terminates the PPP state machine and may issue a Radius request to perform user authentication. Forwarding at nodes 1 and 2 is done at layer 2, with traffic being switched between two link-layer segments: IP header information is not examined in making forwarding decisions. Policy enforcement (e.g., traffic conditioning, packet filtering, NAT, etc.) is generally only done in node 3, though there are cases where some policy enforcement may be done at nodes 1 or 2. For example, a similar scenario can be used in a mobile environment with a mobile operator providing a network-based VPN service and backhauling traffic to a corporate LNS. If a pre-paid charging model is used, service termination upon reaching a zero-balance condition may be enforced at nodes 1 or 2.

The scenario shown here may be used in a wholesale business model, where one party owns the physical DSL lines and aggregates traffic to a second party acting as a wholesaler, who in turn aggregates traffic to a third party acting as a service provider (e.g., an ISP). By introducing a wholesale intermediary, the party dealing with the physical lines (or more generally, the party operating the access-technology-specific equipment) does not need to maintain a business relationship with all the service providers, and a party acting as a service provider does not need to maintain a business relationship with multiple operators each handling some specific access technology, such as DSL, 2G/3G, or WiMax.

Mappings onto NGN Functional Architecture

In this scenario Node-1 acts as an EN-FE (e.g. handling QoS enforcement for the DSL aggregation network). Node-3 acts an ABG-FE (e.g. performing traffic conditioning, packet filtering, NAT etc. Node-3 may also act as an EN-FE, handling QoS enforcement for the L2TP tunnels it terminates. Typically Node-2 is acting as a pure layer-2 relay and is not playing either an EN-FE or an ABG-FE role. Node-2 acts as an ABG-FE if it is performing IP-level policy enforcement (e.g. accounting).

II.4 Scenario 3: Access aggregation using layer 3

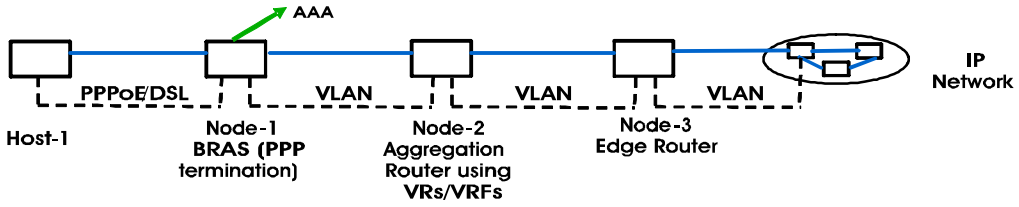


Figure II-3 – Access Aggregation using Layer-3

This is similar to scenario 2, except that forwarding between different aggregation segments is done at layer 3. Node 1 terminates PPP and associates the traffic for a PPP session with a particular domain (e.g., using the realm part of the PPP username to identify the domain). In the upstream direction, policy-based forwarding is used, so that traffic for different domains is segregated and the correct IP next-hop for each domain is chosen. In the downstream direction, node 1 performs regular IP forwarding based on the longest match prefix. Node 2 implements multiple virtual routers, one for each domain. Again, policy-based forwarding is done in the upstream direction, such that all traffic for a given user is sent upstream to node 3, and regular IP forwarding is done in the downstream direction. In this example, nodes 1, 2, and 3 see all the traffic for a given subscriber. Node 1 may issue a Radius request to perform user authentication. This request may be sent via a Radius proxy, or directly over the virtual routed network itself, thus avoiding the need for a Radius proxy.

Aggregation at layer 3 may simplify node 3, since it does not need to terminate large numbers of L2TP tunnels and associated PPP state machines, but it instead receives an aggregated traffic stream delivered over a single VLAN. Note that node 3 can still identify individual subscriber traffic flows for the purposes of performing subscriber-specific policy enforcement actions, but on the user plane this is done using layer-3 information (e.g., the source IP address) rather than by maintaining an individual link-layer connection for each subscriber. Policy enforcement actions (e.g., traffic conditioning, packet filtering, NAT, etc.) may be carried out in all nodes, and this may be done at the subscriber-flow level or at coarser granularities such as at the virtual router level (e.g., some VRs may have a higher level of QoS than others).

Mappings onto NGN Functional Architecture

In this scenario Node-1 acts as an EN-FE (e.g. handling QoS enforcement for the DSL aggregation network). Node-3 acts an ABG-FE (e.g. performing traffic conditioning, packet filtering, NAT etc). Node-1 and Node-2 act as ABG-FEs if they are performing IP-level policy enforcement (e.g. NAT or support of different QoS classes). Node-2 and Node-3 may also act as EN-FEs, handling QoS enforcement for the VLANs they terminate.

II.5 Scenario 4: Multi-stage policy enforcement

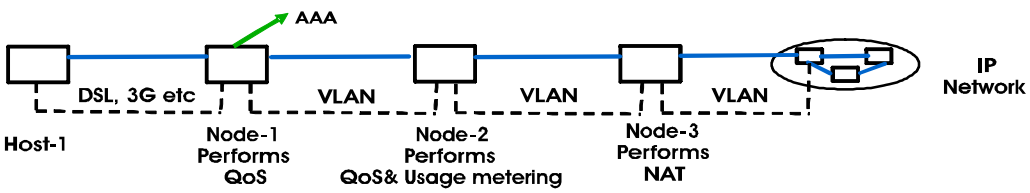


Figure II-4 – Multi-Stage Policy Enforcement

Within a single layer of the transport stratum, the set of policy enforcement actions carried out for traffic for a given subscriber may be distributed across a sequence of devices, with each device doing a subset of the total work. This may reflect a network deployment strategy where there is a set of access-technology-specific

edge devices (e.g., GGSNs or BRASs) and one or more devices behind these that perform policy enforcement in an access-technology-independent manner. Different devices may have different capabilities or be optimized for a certain type of policy enforcement action.

Figure II-4 shows an example where policy enforcement is distributed across a sequence of devices. Here, node 1 terminates some access technologies and performs QoS functions that require visibility of link-layer technology -specific parameters, such as the mapping of DiffServ codepoints to 802.1p priorities or GPRS traffic classes. Node 2 performs QoS functions that operate at layer 3 and above and also performs usage metering. Node 3 is used as a NAT traversal gateway. Node 3 could either be layer-3 adjacent to node 2, or it could be used as a user-plane/media relay and located anywhere in the IP network. In the relay case, packets from host 1 are explicitly addressed to node 3, and when node 3 forwards the traffic onwards, it re-originates the traffic with an IP address belonging to node 3. Similarly in the reverse direction, packets are explicitly addressed to node 3 and re-originated with a node-3 IP address.

Mappings onto NGN Functional Architecture

In this scenario Node-1 acts as an EN-FE (e.g. handling QoS enforcement for the access network). Node-2 and Node-3 are acting as ABG-FEs, handling IP-level policy enforcement. Node-2 and Node-3 may also act as EN-FEs, handling QoS enforcement for the VLANs they terminate.

II.6 Scenario 5: Partitioning into transport-layer traffic subdomains

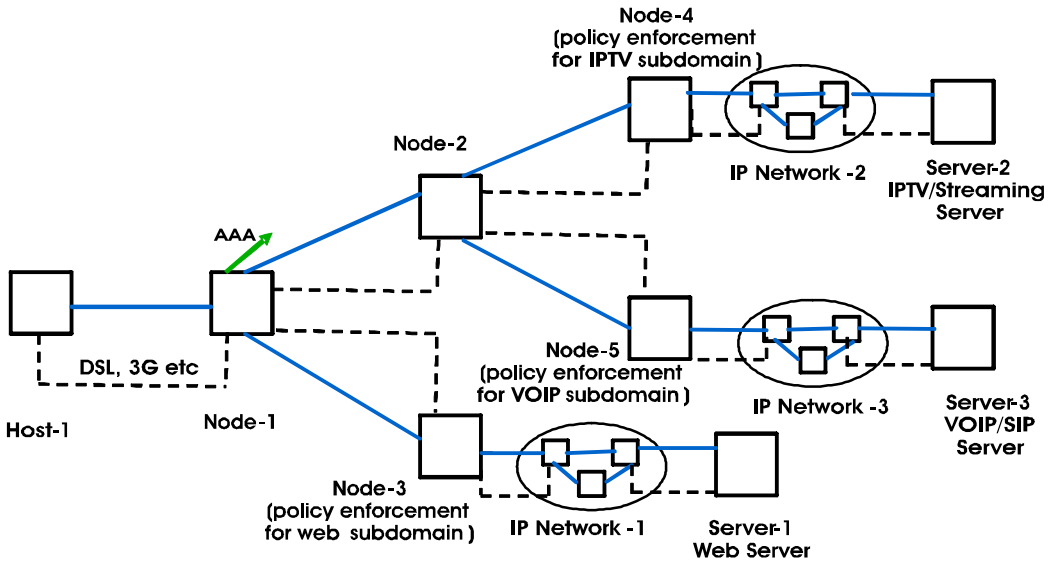


Figure II-5 – Partitioning into Transport-Layer traffic subdomains

Within a single layer of the transport stratum, traffic may be partitioned into multiple subdomains, such that policy enforcement may be carried out separately in each subdomain. Certain nodes act as branch points, whereby traffic for a given subdomain is identified and then subjected to a certain traffic treatment, such as being forwarded to a next-hop node through policy-based forwarding. A transport-layer-traffic subdomain may be associated with a specific set of service-layer services and applications (e.g., IPTV, VOIP, or Internet traffic). A transport-layer-traffic subdomain could also be associated with peer-to-peer traffic, with the NGN providers only supplying transport-layer services, such as a QoS-enabled path between two customer hosts.

Figure II-5 shows such an example where traffic for a given user is split at node 1 into two subdomains: one for Web or non-real-time traffic, and the other for real-time traffic. The real-time traffic in turn is split at node 2 into an IPTV/streaming subdomain and a communications subdomain used for VOIP, video telephony, and so forth. This could map to a business model where one service provider is used for Internet traffic, another for IPTV, and another for communications services, and each independently performs policy

enforcement on its respective traffic subdomain. Note that many variants of this scenario are possible; for example, nodes 1 and 2 could be collapsed so that there is a 3-way split at node 1. Also, nodes 2 and 5 could be collapsed so that both the branching of traffic between domains (IPTV and VOIP) and the policy enforcement for a specific domain (VOIP) occur at the same node.

Mappings onto NGN Functional Architecture

In this scenario Node-1 acts as an EN-FE (e.g. handling QoS enforcement for the access network). Node-1 also acts an ABG-FE, steering upstream traffic to the right subdomain. Node-2, Node-3, Node-4 and Node-5 are acting as ABG-FEs, handling traffic steering and/or IP-level policy enforcement. Node-2, Node-3, Node-4 and Node-5 may also act as EN-FEs, handling QoS enforcement for the link layers they terminate.

Appendix III

Session/Border Control functions

III.1 Introduction

In existing VoIP networks, S/BC (Session/Border Control) functions have already been introduced for network interconnection of NGN/IP networks. S/BC's can play a role in VoIP services by controlling borders to resolve VoIP-related problems such as NAT or firewall traversal. S/BC is already being used in existing VoIP services and is thought to be essential in the NGN architecture.

III.2 Definition of S/BC

Session Border Control is a set of functions that enables interactive communication across the borders or boundaries of disparate IP networks. It provides sessions of real time IP voice, video and other data across borders between IP networks and provides control over security, Quality of Service, Service Level Agreements, legal intercept and other functions using IP signalling protocols.

III.3 Functions of S/BC

The media path and call control signalling path functions are list below.

- Functions related to media path:
  - VPN bridging or mediation
    - This function allows the connection or bridging of different types of VPNs to enable media packets to pass through. Signalling packets may be interrupted in order to control media packets. Specific mechanisms for this function depend on VPN types and interconnection patterns.
  - Opening and closing of a pinhole (Firewall)
    - Triggered by signalling packets, a target IP flow is identified by "5-tuples," i.e., source/destination IP addresses, source/destination port number and protocol identifier, and the corresponding pinhole is opened to pass through the IP flow.
  - Policing and marking
    - Conformance checking of the IP flow against the traffic contract
    - Policing or rate limiting of the IP flow up to the limits defined in the traffic contract
    - Packet marking for overflow traffic of the IP flow

    - Traffic shaping to reduce burstiness
    - Packet marking by overriding the allocated traffic class regardless of the incoming class
  - Detection of inactivity
    - Metering the target IP flow traffic and detecting an inactive period which may be notified by signalling-related functions to terminate the session.
  - NAT and NAPT
    - Rewriting source/destination IP addresses as well as source/destination port number in case of NAPT.
  - Assisting remote NAT/NAPT traversal
    - Performing an agent function to make the target IP flow pass through a remote NAT/NAPT
  - Resource and admission control
    - For links directly connected to the element, and optionally networks behind the element, resource availability is managed and admission control is performed for the target session.
  - IP payload processing
    - Transcoding (e.g., between G.711 and G.729) and DTMF interworking
  - Performance measurement
    - Quality monitoring for the target IP flow in terms of determined performance parameters, such as delay, jitter, and packet loss. Performance results may need to be collected for aggregated IP flows.
  - Denial of service (DOS) detection and protection
    - Detection of unusual incoming IP packets which may then be blocked to protect the receiving user.
    - To prevent distributed denial of service (DDOS) attack, destination specific monitoring, regardless of the source address, may be necessary.
  - Media encryption
    - Encryption of media stream (e.g., IPsec)
  - Support for lawful interception
    - Capturing characteristics of IP flows including contents of the target IP flow.
- Functions Related to call control signalling path:
  - Traffic control for signalling messages
    - Restriction of session establishment in case of signalling-level congestion
    - Load balancing among receiving or target servers
  - Authentication, Authorization, and Accounting (AAA)
    - User/endpoint authentication
    - Session admission control
    - Detail record generation for a session
  - Signalling protocol translation
    - Translation of signalling protocol including protocol normalization, compensation, and repair
  - Signalling protocol interworking
    - SIP and H.323 protocol interworking

- Termination and generation of different signalling transport protocols such as TCP and UDP
- Interworking at IP layer such as between IPv4 and IPv6.

– Session-based routing
- Session-based routing - ability to assign sessions to servers in the case of point-to-multipoint transmission
- User/endpoint registration - ability to assign user/endpoint registration request to a server
- Session routing - ability to assign session to route in the case that it crosses multiple operators

– DSP service control
- Codec negotiation and control of lower layer service

– End-user information hiding
- Hiding identity and address

– Topology and infrastructure hiding
- Hiding information included in "Route" header of SIP message

– DOS protection
- Protecting the C-plane from DDOS attacks

– Signalling encryption
- Encryption of session control signalling (e.g., IPsec)

– Support for lawful intercept
- Capturing session control signalling

III.4 Deployment Area

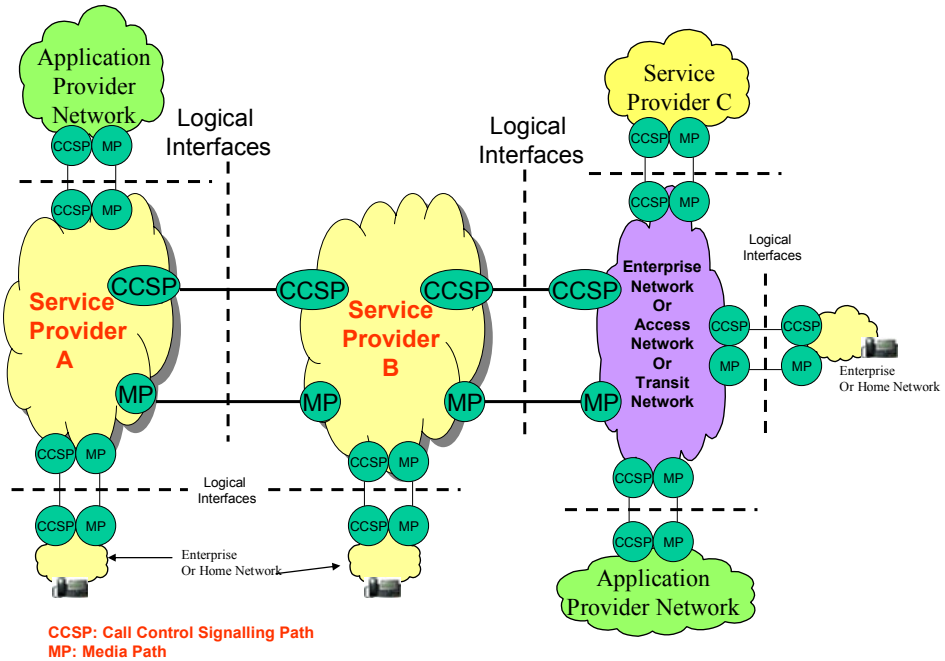


Figure III-1 – Locations of S/BC functions

Figure III-1/ illustrates the location of the S/BC Call Control Signalling Path (CCSP) and Media Path (MP) functions. There are different functions at the customer edge, access network, transit network, and service provider core network. At the customer edge, either at the customer side or at the network entrance, the S/BC provides functionality on behalf of the customer, such as protecting the customer, hiding the customer's IP address, and enforcing QoS. This is applicable for enterprise customers. At the access network, the S/BC provides functionality on behalf of each network segment such as the access network and the service provider core network. At the service provider core network, it provides functionality on behalf of each service provider core network.

III.5 Composition of S/BC

The separation of S/BC functionality as currently shown in Section 8, Figure 3, is appropriate and necessary for several reasons:

– In the NGN architecture, there is a need for multiple functions (instantiated in multiple devices) to control the media portion of the S/BC function. In particular, the Interconnection Border Gateway Control FE (IBC-FE) and the Policy Decision FE (PD-FE) will both need to interface with the Interconnection Border Gateway FE (IBG-GE). In addition, there may be a need for Media Resource Control FE (MRC-FE), Proxy Call Session Control FE (P-CSC-FE), and Access Gateway Control FE (AGC-FE) to interface with the Interconnection Border Gateway FE (IBG-GE) FE for S/BC functions. Similar considerations govern the Access Border Gateway FE (ABG-FE) and its relationship to the Proxy Call Session Control FE (P-CSC-FE). A fully integrated S/BC would complicate this interworking.

– Signalling interworking may be separate from the S/BC because it will not be required in many network scenarios. When it is required, there will be a need for the network to determine, before call completion, the type of signalling interworking that is required. In addition, as networks evolve, it is likely that the need for signalling interworking will decrease over time. Because of this, it must be possible to flexibly insert signalling interworking functionality into the session, perhaps initiated by the Interrogating Call Session Control FE (I-CSC-FE).

– Initial deployments of NGN networks may find an integrated approach to S/BC a useful mechanism to satisfy all initial architectural requirements. As NGN networks expand, separation of the various functional entities related to S/BC will allow networks to scale more efficiently, especially when the requirements for signalling/control functions and media functions evolve independently.

S/BC functions can be logically split into two types: signalling-related functions and media-related functions. According to whether these functions are co-located or not, it can be considered that there are two different models: the unified model and the distributed model. Figure III-2 illustrates two different models.

1. Unified model : This model is both signalling-related functions and media-related functions are co-reside within the same physical component. Hence the relationship between signalling-related functions and media-related functions is 1:1.

2. Distributed model : Two functions are separated with a protocol as the interface between them. Relationships between two functions are 1:N, N:1, N:M.

   - The 1-to-N configuration should be considered in cases of redundant configuration for media-related functionality that assumes synchronization of a pair or set of media-related functions.
   - In case of the N-to-1 configuration, a single media-related function is controlled by multiple signalling functions. This allows multiple accesses to a single media resource from different types of signalling or application-specific functions.
   - The N-to-M configuration allows multiple media-related functions are controlled by multiple signalling functions; A signalling-related function is selected depending on status of multiple signalling-related functions. Once one signalling-related function is selected, it will determine which media-related function is served for that signalling-related function. This configuration is the most reliable configuration among three distributed models. However it requires more

considerable technology to determine which signalling-related function and media-related function will be served.

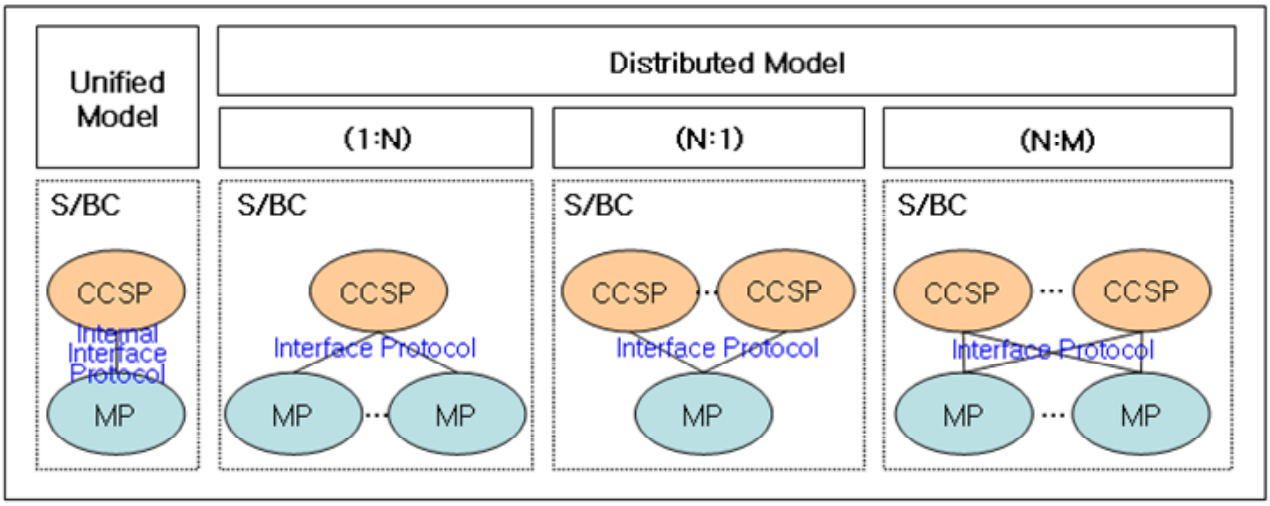


Figure III-2 – Two models of S/BC

III.6 Mapping to NGN Architecture

Figure III-3 illustrates three types of S/BC depending on its location:

1. S/BC-CA (Customer to Access S/BC): S/BC-CA is located at the customer edge, either at customer side or at the access network entrance. It provides functionality on behalf of the customer, such as protecting the customer, hiding the customer's IP address, and enforcing QoS. And it is applicable for enterprise customers and residential customers.
2. S/BC-AC (Access to Core S/BC): S/BC-AC is located at the network edge, either at enterprise access network or residential access network to service provider network.
3. S/BC-CC (Core to Core S/BC): S/BC-CC is located at the service provider core network and provides functionality on behalf of each service provider core network.

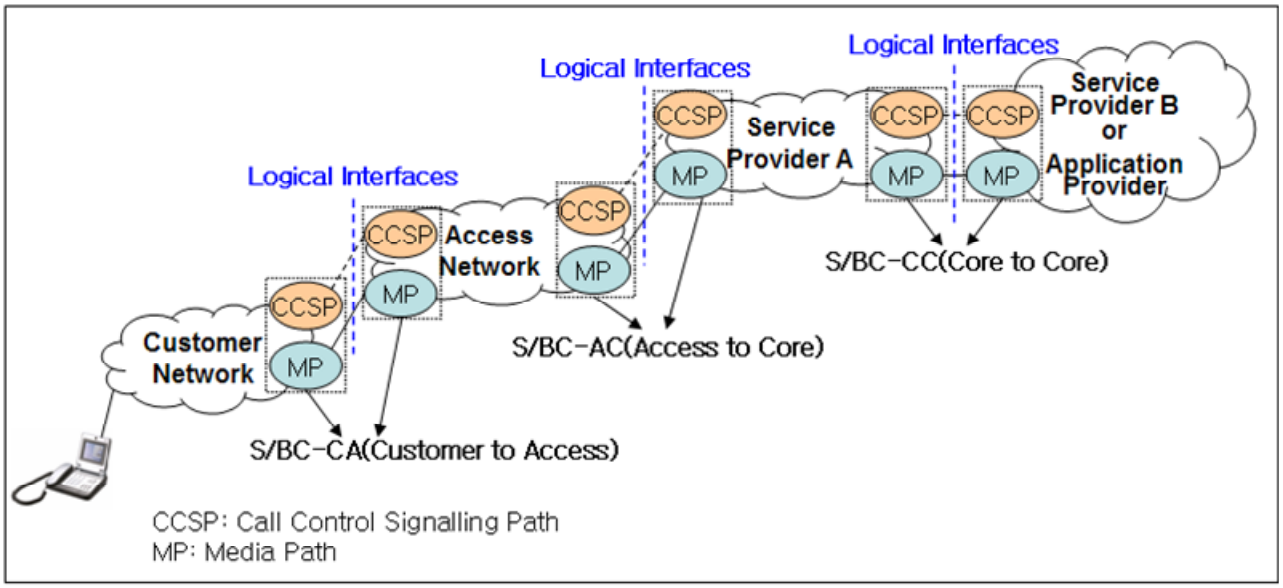


Figure III-3 – Location of S/BC Functions

Table III-1 identifies the Architecture Functional Entities that perform S/BC Functions for the media and signalling paths.

Table III-1 – Architecture Functional Entities with S/BC Functions

	Customer to Access	**Access to Core**	**Core to Core**
Functions Relating to Media Path			
Transport Stratum	Access Node FE (T-2) Access Media GW FE (T-8) A-TRC-FE (T-16) Policy Decisions FE (T-14)	Edge Node FE (T-3) Access Border Gateway FE (T-5) Policy Decisions FE (T-14) A-TRC-FE (T-15)	Interconnection Border Gateway FE (T-6) Policy Decisions FE (T-14)
Service Stratum			Interconnection Border Packet GW Control FE (S-7)
Functions Relating to Signalling Path			
Transport Stratum	Access Node FE (T-2) Access Media GW FE (T-8) A-TRC-FE (T-15) Policy Decisions FE (T-14)	Edge Node FE (T-3) Access Border Gateway FE (T-5) Policy Decisions FE (T-14) A-TRC-FE (T-15)	Interconnection Border Gateway FE (T-6) Signalling Interworking FE (S-11) Policy Decisions FE (T-14)
Service Stratum	Proxy Call Session Control FE (S-2) Access GW Control FE (S-8)	Proxy Call Session Control FE (S-2)	Interconnection Border Packet GW Control FE (S-7) Interrogating Call Session Control FE (S-3)

Figure III-4 shows the NGN architecture contained in [REF], highlighting the FEs that support S/BC functions.

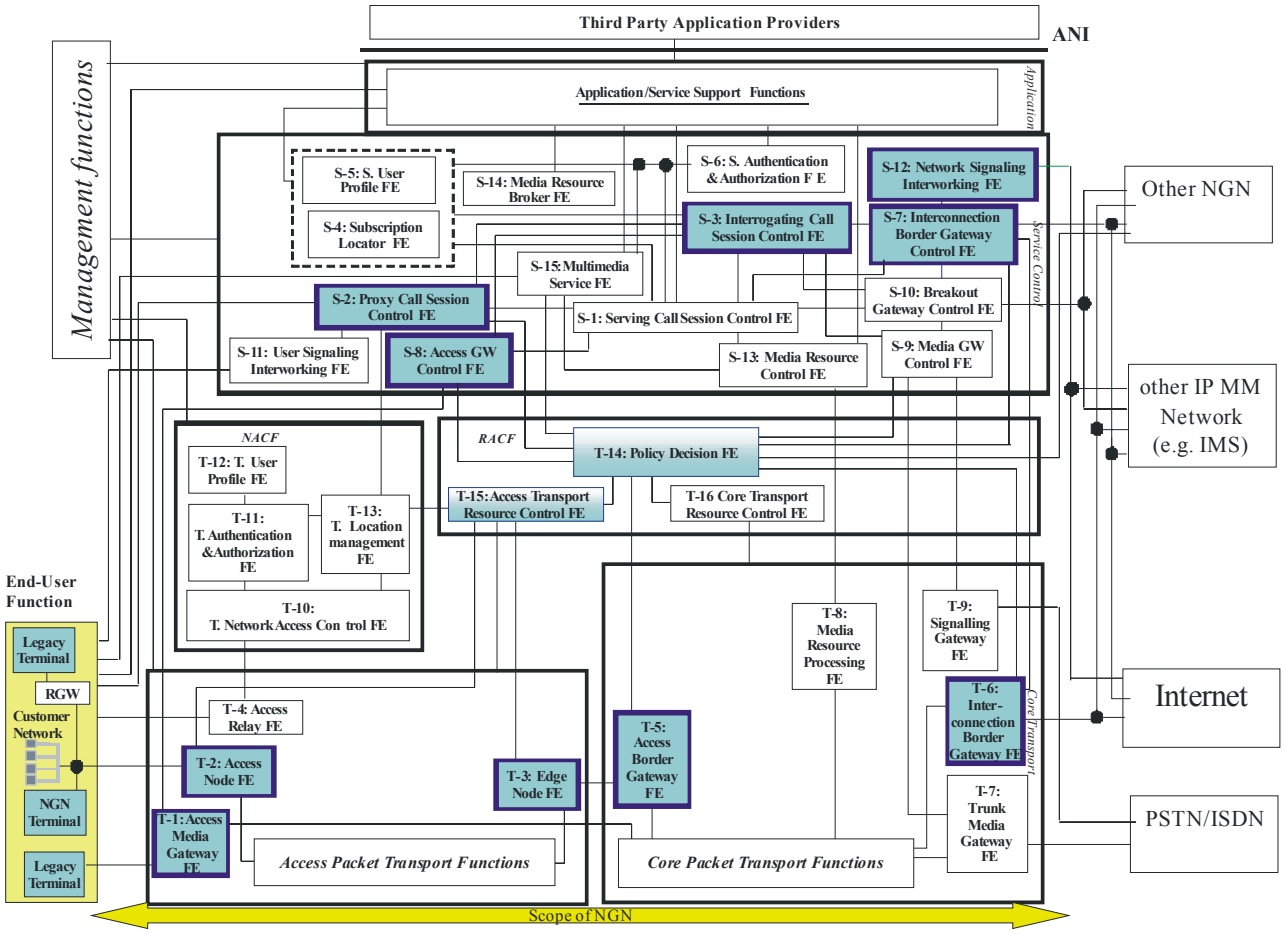


Figure III-4 – Functional entities corresponding to S/BC (highlighted)

Table III-2 describes the mapping of S/BC functions within the NGN architecture FEs.

Table III-2 – S/BC Functions to FE Mapping

	Deployment area in NGN	**Customer to Access Network boundary**		**Access-to-core network boundary**		**Core-to-core network boundary**	
	NGN stratum	**Transport**	**Service**	**Transport**	**Service**	**Transport**	**Service**
S/BC functions related to media path	Opening and closing of a pinhole	M (T-2 & T-1)	(T-15 & T-14)	M (T-3 / T-5)	(T-15 & T-14)	M T-6	T-61 & T-14
	Policing and Marking	O (T-2 & T-1)	(T-15 & T-14)	M (T-3 / T-5)	(T-15 & T-14)	M (T-6)	(T-61 & T-14)
	Detection of inactivity	-	-	O (T-3 / T-5)	(T-15 & T-14)	O (T-6)	(T-61 & T-14)
	NAT and NAPT	-	-	M (T-3 / T-5)	(T-15 & T-14)	O T-6	T-61 & T-14
	Assisting remote NAT/NAPT traversal	-	-	M (T-3 / T-5)	(T-15 & T-14)	O (T-6)	(T-61 & T-14)
	Resource and admission control	-	-	M (T-3 / T-5)	(T-15 & T-14)	M (T-6)	(T-61 & T-14)
	IP payload processing	-	-	O (T-3 / T-5)	(T-15 & T-14)	O T-6	T-61 & T-14
	Performance measurement	-	-	M (T-3 / T-5)	(T-15 & T-14)	M (T-6)	(T-61 & T-14)
	Denial of service (DOS) detection and protection	M (T-2 & T-1)	(T-15 & T-14)	M (T-3 / T-5)	(T-15 & T-14)	M (T-6)	(T-61 & T-14)
	Media encryption	O (T-2 & T-1)	(T-15 & T-14)	O (T-3 / T-5)	(T-15 & T-14)	O T-6	T-61 & T-14
	Support for lawful interception	-	-	O (T-3 / T-5)	(T-15 & T-14)	O (T-6)	(T-61 & T-14)

Table III-2 – S/BC Functions to FE Mapping

	Deployment area in NGN	Customer to Access Network boundary		Access-to-core network boundary		Core-to-core network boundary	
	NGN stratum	Transport	Service	Transport	Service	Transport	Service
S/BC functions related to signalling path	Traffic control for signalling messages	-	-	-	M (S-2,T-15 & T-14)	-	M (S-7, S-3, T-61 & T-14)
	Authentication, Authorization, and Accounting (AAA)	-	-	-	M (S-2,T-15 & T-14)	-	M (S-7, S-3, T-61 & T-14)
	Signalling protocol translation	-	O (T-15 & T-14)	-	M (S-2,T-15 & T-14)	-	O (S-7, S-3, S-11)
	Signalling protocol interworking	-	O (T-15 & T-14)	-	M (S-2,T-15 & T-14)	-	O (S-7, S-3, S-11)
	Session-based routing	-	O (T-15 & T-14)	-	M (S-2,T-15 & T-14)	-	M (S-7, S-3)
	DSP service control	-	-	-	O (S-2,T-15 & T-14)	-	O (S-7, S-3)
	End-user information hiding	-	-	-	M (S-2,T-15 & T-14)	-	M (S-7, S-3)
	Topology and infrastructure hiding	-	-	-	M (S-2,T-15 & T-14)	-	M (S-7, S-3)
	DOS protection	-	M (T-15 & T-14)	-	M (S-2,T-15 & T-14)	-	M (S-7 & S-3, T-61 & T-14)
	Signalling encryption	-	-	-	O (S-2)	-	O (S-7 & S-3)
	Support for lawful intercept	-	-	-	O (S-2)	-	O (S-7 & S-3)

2.4 – Mobility Management Capability Requirements for NGN*

Summary

This document specifies the Mobility Management requirements for Next Generation Networks.

Key words

NGN, Mobility, TBD

Table of Contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

2.4 – Mobility Management Capability Requirements for NGN

1 Scope

The scope of this Document is to specify the Mobility Management Capability Requirements for Next Generation Networks in support of NGN service requirements [1] and the NGN Scope document [2]. This document addresses capability requirements and high-level architecture concepts for the support of mobility capabilities. Stage 1 service descriptions, detailed Stage-2 and Stage-3 material is beyond the scope of this document.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Document. At the time of publication, the editions indicated are valid. All Recommendations and other references are subject to revision; all users of this Document are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this document does not give it, as a stand-alone document, the status of a Recommendation.

[1] NGN Focus Group draft deliverable, NGN Release 1 requirements

[2] NGN Focus Group draft deliverable, NGN Release 1 Scope

[3] ITU-T Supplement Q.Sup52, NNI Mobility Management Requirements for Systems beyond IMT-2000

[4] NGN Focus Group draft deliverable, Security Requirements for NGN Release 1

[5] NGN Focus Group draft deliverable, Guidelines for NGN-Security for Release 1

3 Terms and definitions

3.1 Handover: The ability to provide mobility with service continuity with some possible interruption to the service as seen by the user during and/or after movement.

3.2 Home Network: The network associated with the operator/service provider that owns the subscription of the user.

3.3 Mobility: The ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment.

3.4 Mobility management: The set of functions used to provide mobility. These functions include authentication, authorization, location updating, paging, download of user information and more.

3.5 Network mobility: The ability of a network, where a set of fixed or mobile nodes are networked to each other, to change, as a unit, its point of attachment to the corresponding network upon the network's movement itself.

3.6 **Nomadism**: The ability of the user to change his network access point on moving. When changing the network access point, the user's service session is completely stopped and then started again, i.e., there is no service continuity or hand-over used. It is assumed that normal usage pattern is that users shutdown their service session before moving to another access point.

3.7 **Personal mobility:** This is the mobility for those scenarios where the user changes the terminal used for network access at different locations. This is the ability of a user to access telecommunication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile.

3.8 **Roaming:** The ability of the users to access services according their user profile while moving outside of their subscribed home network, i.e. by using an access point of a visited network.

3.9 **Roaming agreement:** A business arrangement between a pair of operators in which it is agreed that the one operator will provide service to the customers of the other operator. Among other issues, a roaming agreement may address the level or type of service to be provided to the roaming customers as well as arrangements for compensation for the use of the roamed-to operators resources.

3.10 **Seamless handover**: This is one special case of mobility with service continuity, when it's preserved the ability to provide services without any impact on their service level agreements to a mobile object during and after movement.

3.11 **Service continuity**: The ability for a mobile object to maintain ongoing service including current states, such as user's network environment and session for a service.

3.12 **Service discontinuity**: The inability for a mobile object to maintain ongoing service including current states, such as user's network environment and session for a service.

3.13 **Service Mobility**: This is mobility, applied for a specific Service, i.e. the ability of a mobile object to use the particular (subscribed) service irrespective of the location of the user and the terminal that is used for that purpose.

3.14 **Terminal Mobility:** This is the mobility for those scenarios where the same terminal equipment is moving or is used at different locations. This is the ability of a terminal to access telecommunication services from different locations or while in motion, and the capability of the network to identify and locate that terminal.

3.15 **Visited Network:** The network that is local to the user in a roaming configuration.

4 Abbreviations

AAA Authentication, Authorization and Accounting

AN Access Network

BS Base Station

BSC Base Station Controller

BTS Base Transceiver Station

CDMA Code Division Multiple Access

CN Core Network

CS Circuit-Switched

FA Foreign Agent

GGSN	Gateway GPRS Support Node
GMSC	Gateway MSC
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HA	Home Agent
IMS	IP Multimedia Subsystem
IP	Internet Protocol
MIP	Mobile IP
MM	Mobility Management
MSC	Mobile Switching Center
MT	Mobile Terminal
NAP	Network Attachment Point
NGN	Next Generation Network
NT	Network Termination
PS	Packet-Switched
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RNC	Radio Network
RR	Radio Resource
RRC	Radio Resource Control
SDOs	Standards Development Organizations
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SP	Service Platform
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
VHE	Virtual Home Environment
WLAN	Wireless LAN
xDSL	Digital Subscriber Line technology of type x
2G	2nd Generation
3G	3rd Generation

5 Introduction to mobility in NGN Release 1

One of the crucial requirements for NGN is to provide the mobility management (MM) for users and terminals so as to ensure the mobility within the home network and across different networks.

Over the years, some MM techniques have been proposed and/or deployed in the networks to effectively manage the movement of mobile users and all related functionalities, such as identification, registration, authentication etc.. Some of these techniques have been unique to the respective system and hence manage only the movement of users within a specific homogeneous mobile system. The provisioning of seamless services with mobility across different heterogeneous systems is currently not possible in many cases due to several factors, such as:

- Differences in the (wired/wireless) access network technologies used
- Differences in the services available in the various systems and the non-portability of these services
- Differences in the MM techniques deployed in the various systems

This restriction of mobility within a single network, and dependence on access network type is to be overcome in NGN.

In the NGN, it is expected that a variety of the existing and new wired/wireless access network technologies are supported, such as WLAN, xDSL and 2G/3G mobile networks etc as shown in Figure 1. Each of the access networks is connected to the NGN core network, to provide the same set of services for users (more generally, for mobile objects), preferably independently of the access network type.

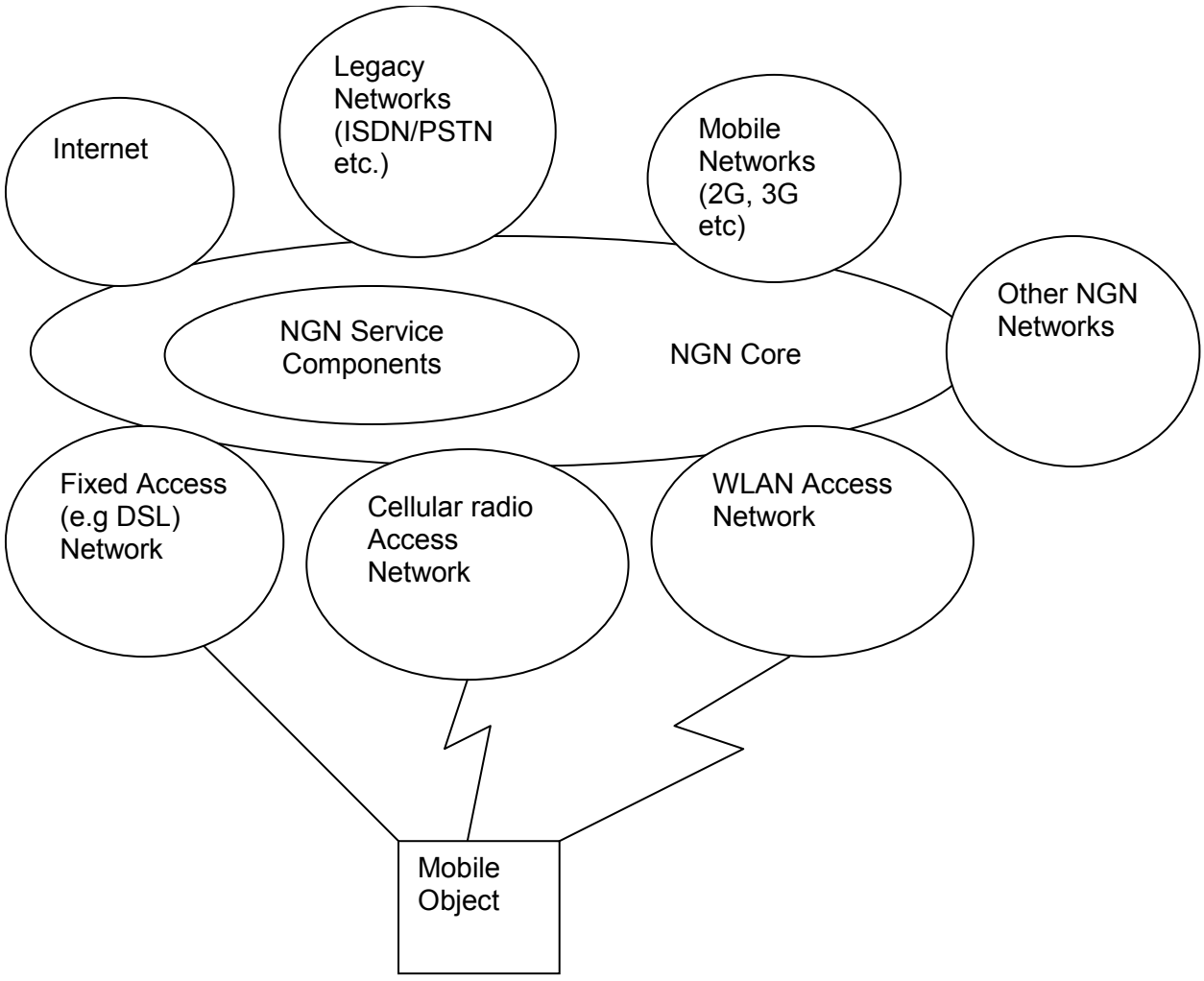


Figure 1 – NGN core with heterogeneous Access Networks and interconnection with other Networks

6 Architectural concepts on mobility

6.1 Mobility and identifiers

From an architectural perspective mobility is about changing the point of attachment of a mobile endpoint to the NGN. Mobility management is maintaining and updating state information about the binding between mobile endpoints and points of attachment somewhere in a network in order to provide continued reach ability and connectivity. The reason that mobility terminology is complicated in the NGN environment is that there are different types of mobile endpoints to be considered. SIP for instance stores state information related to an application instance, so the application is the mobility endpoint. Mobile IP on the other hand stores state information related to an interface, so the interface is the mobile endpoint. In case of moving networks, the moving network itself becomes a mobile endpoint. In order to develop mobility requirements first the entities should be identified that may act as either fixed or mobile endpoints and to which other entities may be bound.

6.2 Customer network

NGN Release 1 needs to consider the general case of a customer network as depicted in Figure 2 below. It shows a customer network with multiple Service Platforms and each Service Platform may run multiple Service Applications. In such a customer network multiple users may associates themselves with one or more service applications, by providing one of their user identifiers to the application. In NGN Release 1 this will typically be a SIP URL. The service application is bound to a TCP/IP socket of the Service Platform Interface. Via the customer's connectivity network the SPI binds itself to an access network specific Network Termination. Finally the network termination is bound to the Network Attachment Point of the access network.

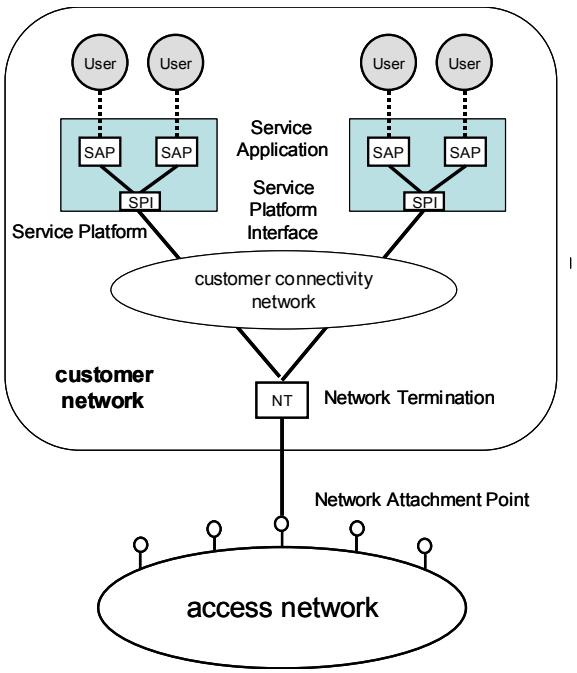


Figure 2 – Customer network configuration

Only one Network Termination is shown in the customer network, because multi-homing is not supported in release 1. Multi-homing may be considered for later releases.

In this customer network scenario there is a many to one relation between the different types of endpoints. A mobile terminal may represent a limit case where there is a one to one relation between the user and his service application, the service application and the service platform interface and between the service platform interface and the network termination.

6.3 Mobility scenarios

What is meant by a terminal in the 3G context is clear thanks to the one-to-one relationships. If NGN customer networks are included, this becomes ambiguous, and therefore it is also ambiguous what terminal mobility implies.

In Figure 3 below is shown a - non-exhaustive - number of mobility scenarios.

Figure 3 shows a number of mobility scenarios including some that involve mobility within the end user equipment area. It is not agreed that NGN systems will handle these scenarios behind the UNI on the user network, especially scenarios for handing over from one user network to another. The behaviour of the user network is outside the scope of this document.

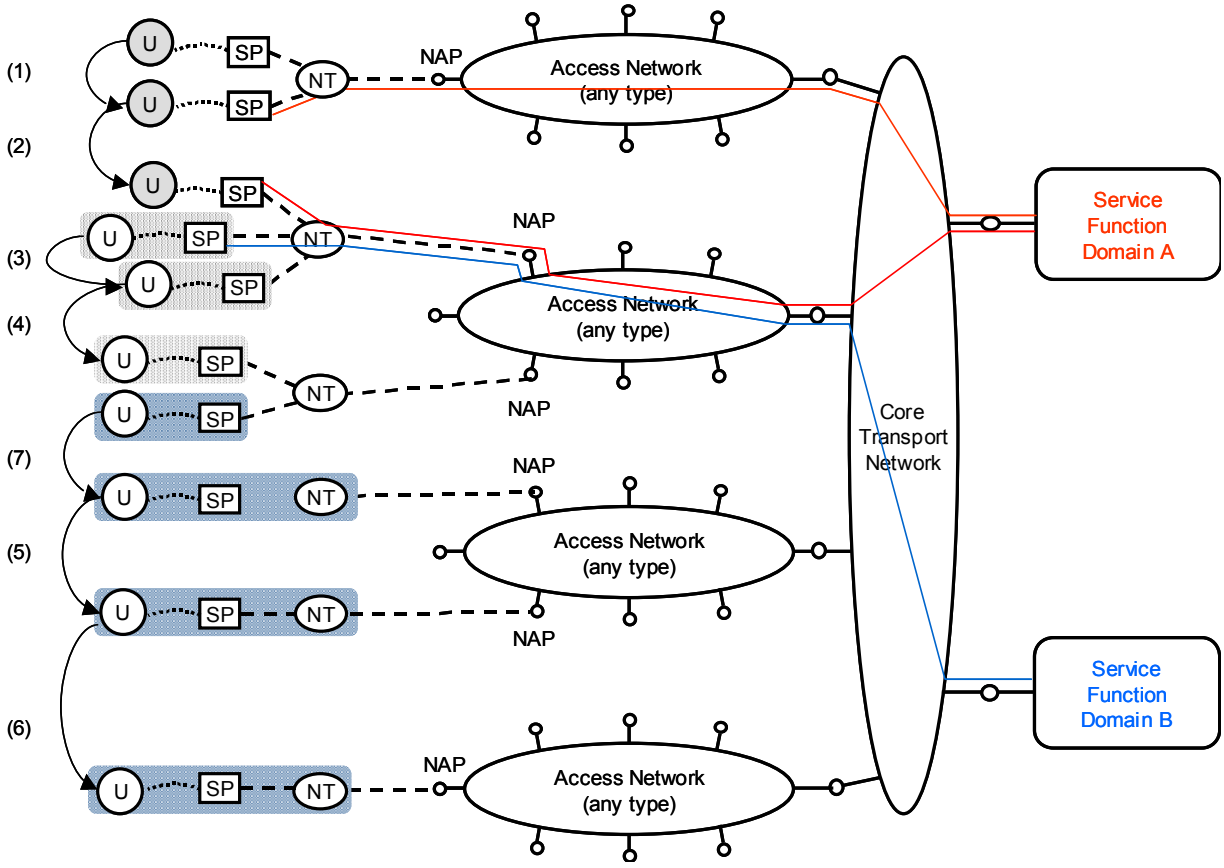


Figure 3 – Mobility Scenarios

The arrows show mobility taking place as described in the following paragraphs. Each mobility scenario is numbered to the left of the figure.

A user may only change his association with a Service Application when he moves from one Service Platform to another, either within a customer network (1) or when he moves from one customer network to another (2). All other bindings remain fixed in this case.

The user may also move his Service Platform, thereby changing the binding between the Service Platform Interface and his Network Termination. Again this may be done within a customer network (3) or when moving from one customer network to another (4). The binding between the Network Termination and the Network Attachment Point doesn't change in these two scenarios.

If the Network Termination supports mobility, the user may change the binding between the Network Termination and its Network Attachment Point. The change may be to another NAP on the same access network (5) or on another access network (6). The other bindings do not change in these scenarios.

Finally a more complex scenario is shown in (7) where the SPI supports mobility. Such an SPI could be used to bind to either a NT in a customer network or act as an NT to bind to a NAP.

Figure 4 further illustrates the option to gain access to different Service Providers from different Service Platforms (or different Service Applications on the same Service Platform) in the same customer network.

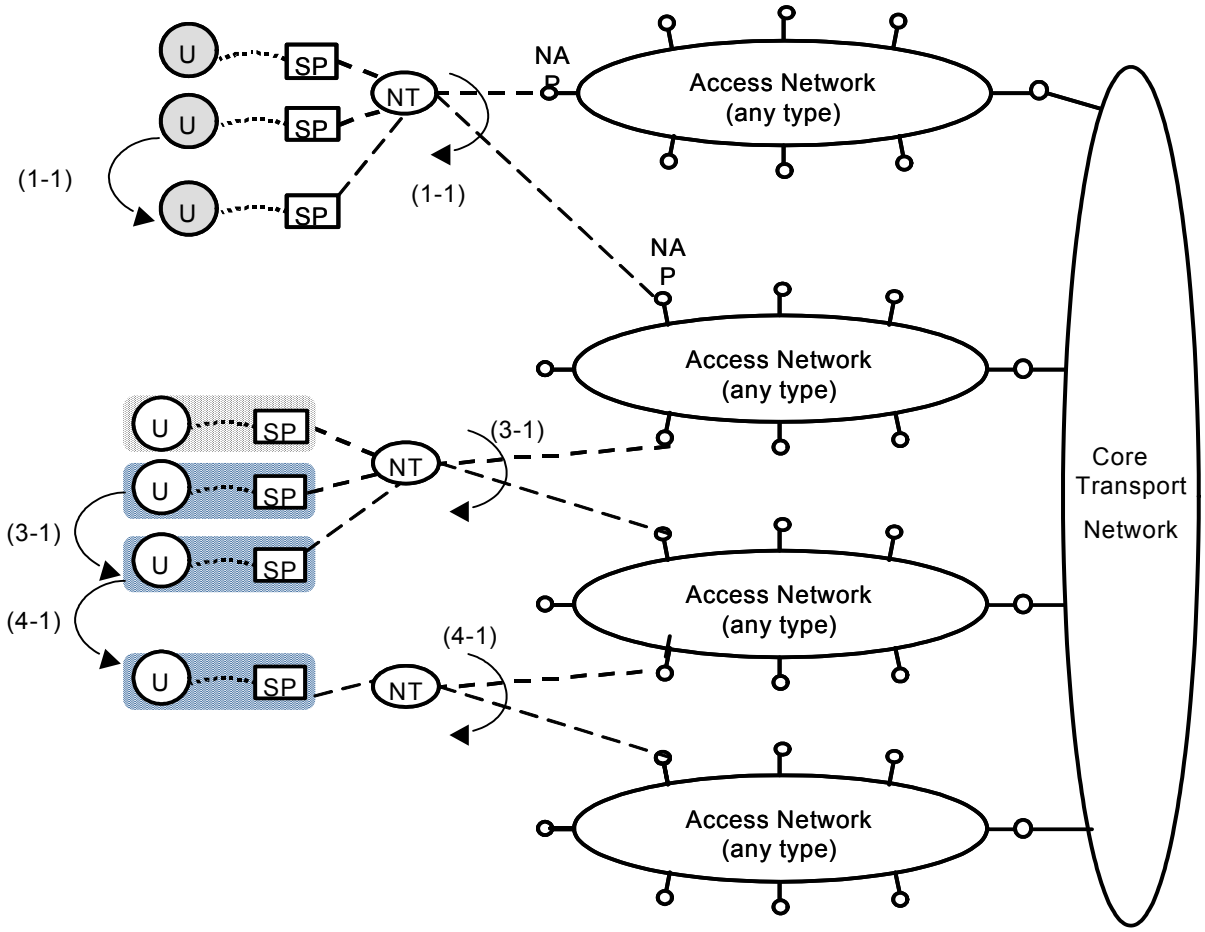


Figure 4 – Single NT with multiple ANs

A user uses the same service application and the same network termination but changes his network interface card within the same terminal, which has two or more network interface cards of Service Platform (1-1). In this case, the user uses the same Network Termination (NT) but can change its access network, which is matched with the network interface card.

A user can move his service platform, thereby changing the binding between the Service Platform Interface and his Network Termination. Changing the binding between the Service Platform Interface and his Network Termination is done within a customer network and between two access networks (3-1) as well as between two customer network and between two access networks (4-1). These scenarios can occur for improving network performance, and so on.

7 MM requirements

7.1 Network requirements

7.1.1 General

IP based transfer in the core network will enable the bridging of diverse fixed and wireless access technologies. However, IP-based interoperability at the transport stratum is not sufficient to achieve the mobility goals of NGN. The following requirements need to be addressed to support mobility in the NGN.

1. The NGN MM architecture shall support user mobility across heterogeneous access networks preserving service quality.
2. The NGN MM architecture shall avoid to implement as many authentication mechanisms as access network technologies.
3. Access to user data:
   - Services and other network functions require some user data in order to be appropriately customized. These can be either "user subscription data" or "network data".
4. Support of commonly used Authentication, Authorization and Accounting (AAA), and security functions (AAAF):
   - The MM functions are required to cooperate with commonly used AAA and security schemes to be authenticated, authorized, accounted and secured for the services.
   - These functions need to be performed for each mobile object because NGN should support mobility for each mobile object, such as a user, a mobile terminal, and a mobile network.
5. Interworking of MM functions used in the various network topology-based mobility scenarios is required.
7. Support of several kinds of mobile endpoints:
   - In the NGN environment there are different types of mobile endpoints to be considered. The mobile endpoint can be an application in SIP, interface in the Mobile IP, and so on as well as it can be in a core network, an access network, a customer premise network or a service platform. So, each network related to the mobile endpoints should be able to support the mobility of every mobile endpoint.
9. Maintenance of binding information:

   There are many types of bindings for services as follows:
   - between a user and a service application
   - between an application and a network interface card
   - between a Service Platform and a Network Termination
   - between a Network Termination and a network access point
   - between two different access networks

   In NGN environment, all above bindings should be maintained for supporting mobility. Because of this, binding information needs to be maintained in a relevant place.

7.1.2 Independence to Network Access Technologies

It is expected that NGN will consist of an IP based core network with several access networks that use different radio technologies. In this architecture, Inter-Network MM should provide the mobility between either homogeneous or heterogeneous type of access networks that belong to the same or different operators each other. Accordingly, it is required that the Inter-Network MM should be independent of the underlying access network technologies such as 2/3G Cellular, WLAN, etc.

7.1.3 Harmonization with the IP-based Core Networks

The future converged CNs in NGN are envisaged to be IP-based. Accordingly, the MM protocols for NGN should be IP-based or, at least, well harmonized with IP technology for its efficient and integrated operation in such future CNs. It is also recommended to re-use to the extent as further as possible the existing MM techniques/technologies for the design of the MM protocols for NGN, potentially through co-operation with external forums and SDOs.

7.1.4 Separation of Control and Transport

It is required that the bearer plane be separated from the control plane for efficient mobility management and scalability. Such separated planes could provide the architectural flexibility that facilitate the introduction of new technologies and service. The open interface between control and transport functions is also necessary to implement their separation.

7.1.5 Provision of Location Management

For supporting the mobility of user/terminal, the locations of users/terminals are tracked and maintained by location management function whenever they move. Location management will be performed based on an IP-specific location database such as the Mobile IP Home Agent, or the SIP registrar.

7.1.6 Provision of Mechanisms for Users/Terminal Identification

The MM protocols in NGN should specify how the users/terminals are to be identified in the networks or systems for mobility management. This identification functionality will be the first step to be taken in the mobility management process and thus used for authentication, authorization and accounting of user/terminal.

7.1.7 Interworking with the Established AAA and Other Security schemes

The MM protocols for NGN should specify how the users/terminals are to be authenticated, authorized, accounted and secured for the services, as done in the typical AAA and security mechanisms. For this purpose, the use of the existing AAA schemes will be preferred.

The result of the AAA functionality will be a yes/no decision on the connection request made by a user. As a next step, the access network configuration will be adapted to the mobile/nomadic user such that it satisfies the particular QoS level and security association for the requested user connection. These mechanisms will be done based on the user subscription profile and the technical resource constraints of the respective access networks.

7.1.8 Provision of Mechanisms for Context Transfer

When an MT moves across different networks, transferring the context information of current session, such as QoS level, security method, AAA mechanism, compression type in use, might be helpful in minimizing the handover latency to re-setup the session. The proper use of context transfer mechanism would be able to reduce at the comprehensive amount the overhead in the servers that are, respectively or in combined manner, used to support QoS, security, AAA and so on.

7.1.9 Effective Interworking with Intra-Network MM Protocols

For overall seamless mobility, the Inter-Network MM should effectively interwork with the Intra-AN and Inter-AN MM protocols.

7.1.10 Location Privacy Provisioning

The location information of particular users should be protected from non-trusted entities. This will entail mutual authentication, security association, and other IP security requirements between the mobile terminal and the location management function.

7.1.11 Paging Support with Location Management

The paging capability is essential in large-scale cellular networks because it provides the power saving in mobile terminals as well as the signalling reduction in the networks, which will improve the scalability of NGN. In particular, paging support needs to be provided in such networks together with location management.

7.1.12 IP version independence

The MM protocols should be able to support IPv6 as well as IPv4.

7.2 Requirements for mobile terminals

In order to achieve the goals of seamless service, the following functions are required on mobile terminal.

1. Automatically detect the presence of wireless networks

   There may exist more than one wireless network in particular circumstance, e.g., WLAN, GPRS etc. For a multi-mode mobile terminal, it shall have the capability to quickly detect the presence of all the wireless networks that it can connect to.

2. Support of policy-based and dynamic network selection

   After detecting the presence of a wireless network, it shall be possible for the user to choose to connect to one of the networks to obtain service, based on the following policies:

   i) Quality of service level needed for a particular service, e.g., bandwidth availability, time delay, packet loss ratio, etc.

   ii) Cost for the particular service in each network.

   iii) Security level that the network can provide.

Once connected the terminal shall be able to track information of the current network based on the above-mentioned aspects. For example, when a user detects that the QOS level has gone down, it can handover the service to a new network instantly. From the user's point of view, the network switchover is not visible.

8 Security Considerations

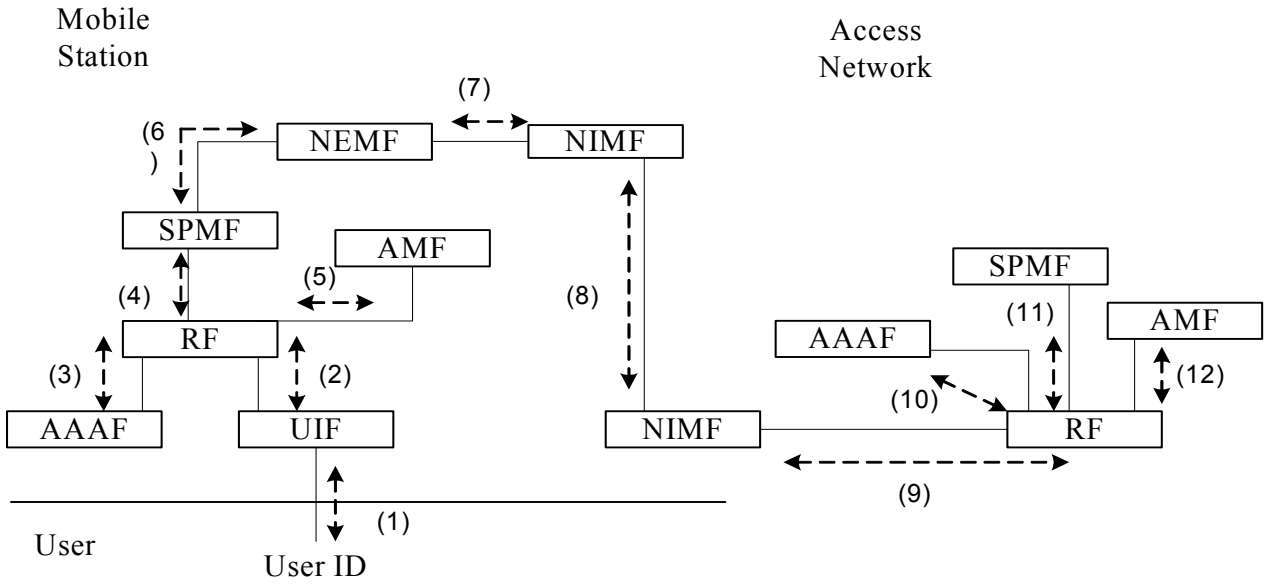
The security requirements within the functional requirements and architecture of the NGN are addressed in the NGN Security Requirements for Release 1 [4] and the Guidelines for NGN Security [5].

When deploying the architecture, these requirements should be met.

Appendix A

Scenarios for MM

A.1 Registration



(1) User access with identification (for example, password or fingerprint)

(2) User registration

(3) AAA for User

(4) Service profile (for example, for adult or for child)setup for the user

(5) Address allocation of the service for the user

(6) Network environment (for example, QoS) setup for the service

(7) Network information (for example, bandwidth, wireless technology, etc)

(8) Network to network negotiation according the network information

(9) Mobile station (MS) and the user registration

(10) AAA for the MS and the user

(11) Service profile setup for the MS and the user

(12) Address allocation of the service for the MS

Appendix B

Classification of Mobility based on network topology

B.1 General

Figure B.1 shows an example of multiple levels of mobility for certain access network types and mobility technologies. Other examples for other access network types and mobility technologies are, of course, possible. The figure depicts that mobility supported at lower levels in the architecture may not be visible to higher levels. It also shows that mobility may be handled at levels all the way up to the application.

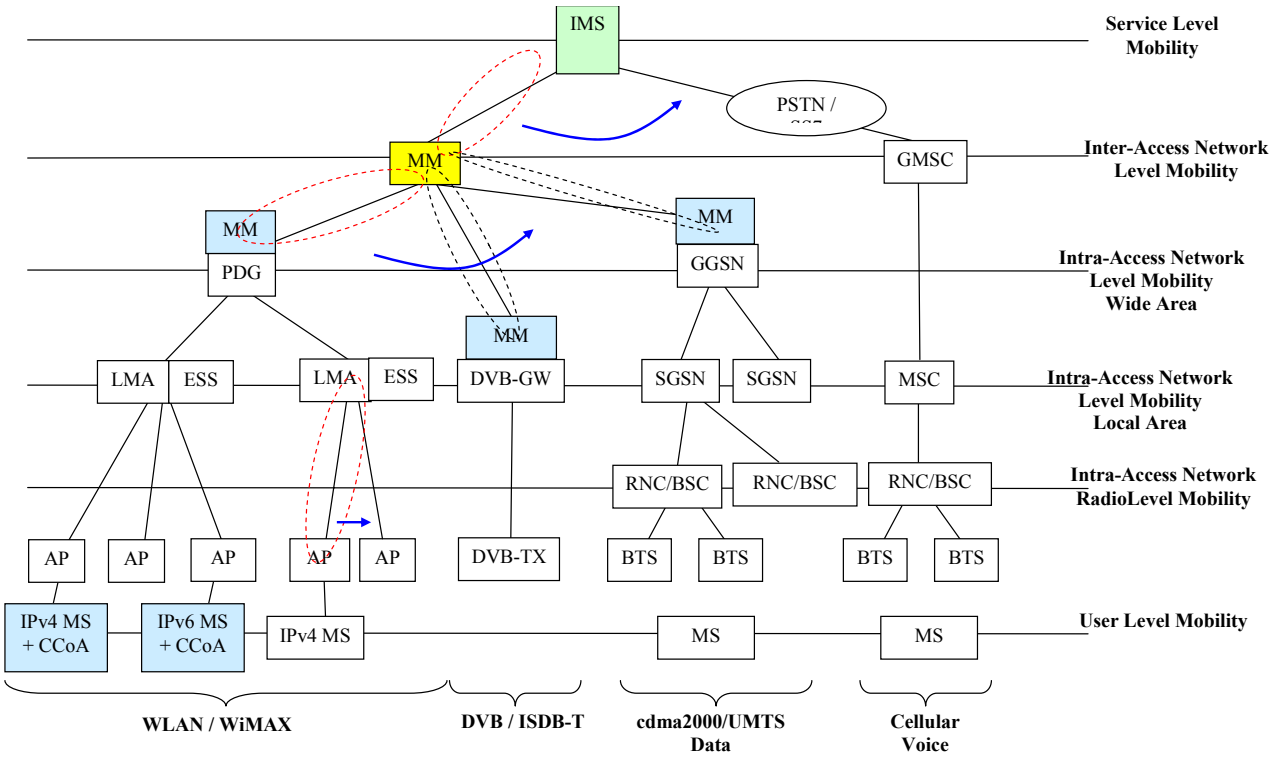


Figure B.1 – Example of levels of mobility

B.1.1 Mobility at the Service Level

Service level mobility is mobility across CS or PS domains in NGN. This might be within a single NGN or across NGNs. Service level mobility might for example exploit E.164 address to SIP-URI resolution capability. This way, service level mobility can be provided when a user is roaming between different administrative domains, which would necessitate inter-domain mobility at session control level. Service level mobility between different combinations of CS and PS session is possible for NGN.

B.1.2 Mobility at the Inter-Access Network Level

Inter-access network mobility is related to the possibility for a user to roam across access networks using various network mobility technologies such as Mobile IP or MAP.

B.1.3 Mobility at the Intra-Access Level (Wide Area)

Intra-access level mobility (wide area) refers to either the PS domain or CS domain in NGN. Mobility is provided by the access network technology. For example, mobility at this level might be provided by GPRS roaming technology for movement between SGSNs within a GGSN.

B.1.4 Mobility at the Intra-Access Network Level (Local Area)

Intra-access network level mobility (local area) refers to mobility within a particular access technology, generally within a limited geographic area, but handled above the radio resource control layer.

B.1.5 Mobility at the Intra-Access Network Radio Level

Intra-access network radio level mobility refers to the mobility at radio level (e.g. RRC layer in UMTS or cdma2000, RR layer in GPRS).

B.1.6 Mobility at the Personal Level

Personal level mobility refers to the mobility at user level. For example, a user can perform mobility between terminals, such as an IPv4 MS (Mobile Station) and an IPv6 MS.

B.2 Mobility Layering in NGN for beyond release 1

Handover support for mobility within or between different types of access networks is not explicitly provided in Release 1 although systems supporting handover may utilize these capabilities in Release 1. Beyond Release 1, handover may need to be supported in all levels defined in section B.1. To support this, existing functions in the NGN may need to be modified.

2.5 – IMS for Next Generation Networks*

Table of Contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

2.5 – IMS for Next Generation Networks

1 Scope

The IP Multimedia Subsystem (IMS) as specified by the 3rd Generation Partnership Project (3GPP) and the 3rd Generation Partnership Project 2 (3GPP2) has been adopted for use to support session and other Session Initiation Protocol (SIP) [1] based services in the Next Generation Networks (NGN) as described in Y.2001 [2] and Y.2011 [3]. This document identifies the IMS for use in NGN. It provides an introduction to the IMS functional architecture and operation and identifies those IMS architecture documents that are relevant in the context of NGN.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Document are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this document does not give it, as a stand-alone document, the status of a Recommendation.

[1] IETF RFC 3261, SIP: Session Initiation Protocol

[2] ITU-T Recommendation Y.2001, NGN overview

[3] ITU-T Recommendation Y.2011, General principles and general reference model for next generation networks

[4] ETSI TS 123 228 V6.11.0, IP multimedia Subsystem (IMS), stage 2

[5] TIA-873.002-A, IP multimedia Subsystem, Stage 2

[6] ITU-T Recommendation Q.1741.4, IMT-2000 references to release 6 of GSM evolved UMTS core network

[7] ITU-T Recommendation Q.1742.4, IMT-2000 references (approved as June 30, 2004) to ANSI-41 evolved core network with cdma2000 access network

3 Definitions

This Document defines the following terms:

3.1 **Home Network:** The network associated with the operator/service provider that owns the subscription of the user.

3.2 **Visited Network:** The network that is local to the user in a roaming configuration.

4 Abbreviations

This Document uses the following abbreviations.

3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AS	Application Server
CS	Circuit Switched
CSCF	Call Session Control Function
DB	Database
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
I-CSCF	Interrogating CSCF
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
ISC	IMS Service Control
I-SIM	IMS Subscriber Identity Module
MGW	Media Gateway
MGCF	Media Gateway Control Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
NAPT	Network Address and Port Translation
NGN	Next Generation Network
PDF	Policy Decision Function
P-CSCF	Proxy CSCF
PSTN	Public Switching Telephone Network
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SLF	Subscription Locator Function
xDSL	x-Digital Subscriber Loop
WLAN	Wireless Local Area Network

5 Introduction to IMS

IMS is a collection of core network functional entities for the support of SIP based services [4], [5]. IMS supports the registration of the user and terminal device at a particular location in the network. As part of registration, IMS supports authentication and other security arrangements. IMS utilises SIP based control.

The services supported by IMS may include multi-media session services and some non-session services such as Presence services or message exchange services.

In addition to services for the user, IMS defines a number of network reference points to support operator provided services. IMS supports various application services via the services support architecture. IMS supports operation and interworking with a variety of external networks via defined reference points. IMS supports defined reference points for the collection of accounting data in support of charging and billing operations.

IMS also supports defined reference points to the underlying transport infrastructure for the enforcement of QoS negotiated by session signalling and for flow gating. These reference points also support the exchange of information in support of correlation of charging between IMS and the underlying transport.

The list of documents defining IMS and that are relevant in the context of NGN are listed in Section 7.

6 Use of IMS in NGN

6.1 General

This section provides details about the IP Multimedia Subsystem and the adaptation and extension of the IMS specifications to support additional access network types, such as those based on xDSL and WLAN. IMS and its extensions support:

- The control of IP Connectivity Access Networks (QoS, admission control, authentication, etc.);
- The co-ordination of multiple control components to a single core transport for resource control;
- The interworking and interoperability with legacy and other networks;
- Mutual de-coupling of the applications from the session/call control and the transport;
- Access technology independence of session/call control and applications.

The references contained in Section 7 of this document define the base for IMS considered to be relevant in NGN. The access networks able to be supported by the current versions of these documents are limited. Some extensions to this base are necessary to fully support the NGN access networks identified as part of NGN [3]. Some areas where extensions to IMS for use with NGN will be needed are identified in this document. The type of modifications required varies from one functional entity/reference point to another.

6.2 Relationship between IMS and NGN

IMS is comprised of a number of functional entities that together can provide support for some of the capabilities of the service stratum of NGN [3]. The following functional entities are defined in IMS as specified by the documents in section 7 of this document. The IMS functional entities and their environment are illustrated in Figure 1.

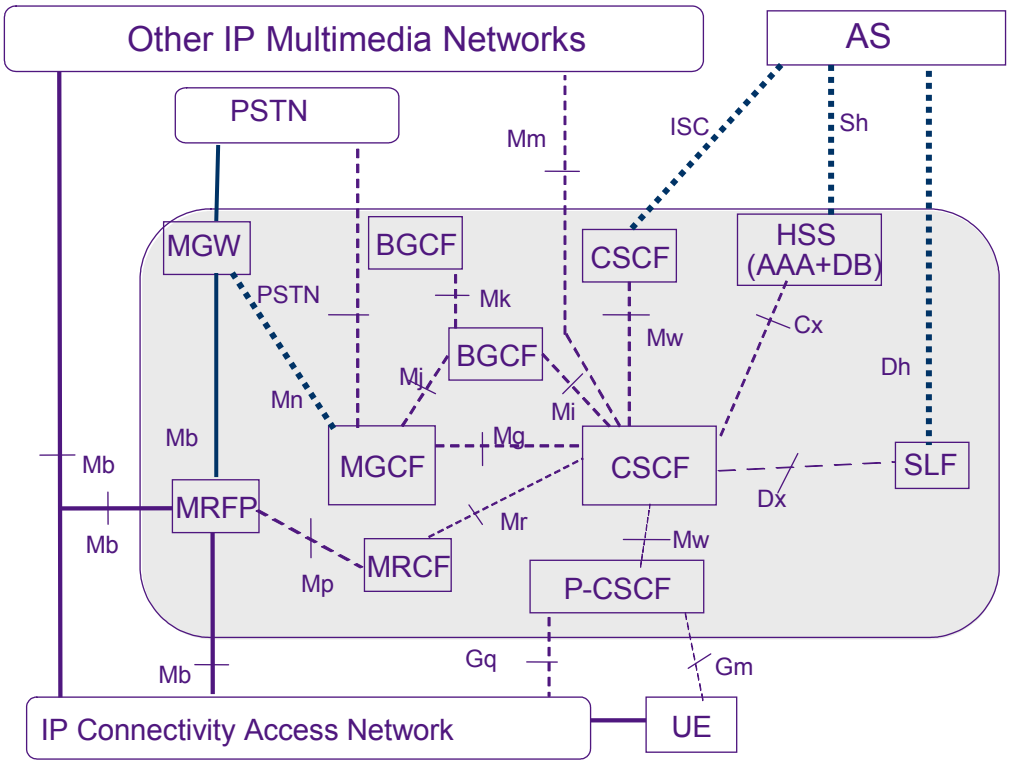


Figure 1 – IMS and its environment

Figure 1 shows the set of functional entities that comprise IMS. IMS, as a collection of core network functional entities may be utilized by both home networks and by visited networks in roaming situations. Figure 1 shows these functional entities but it doesn't represent the possible distribution of these entities among home and visited NGN core networks. Figure 2 shows the IMS session control entities along with an indication of the core networks within which they may reside.

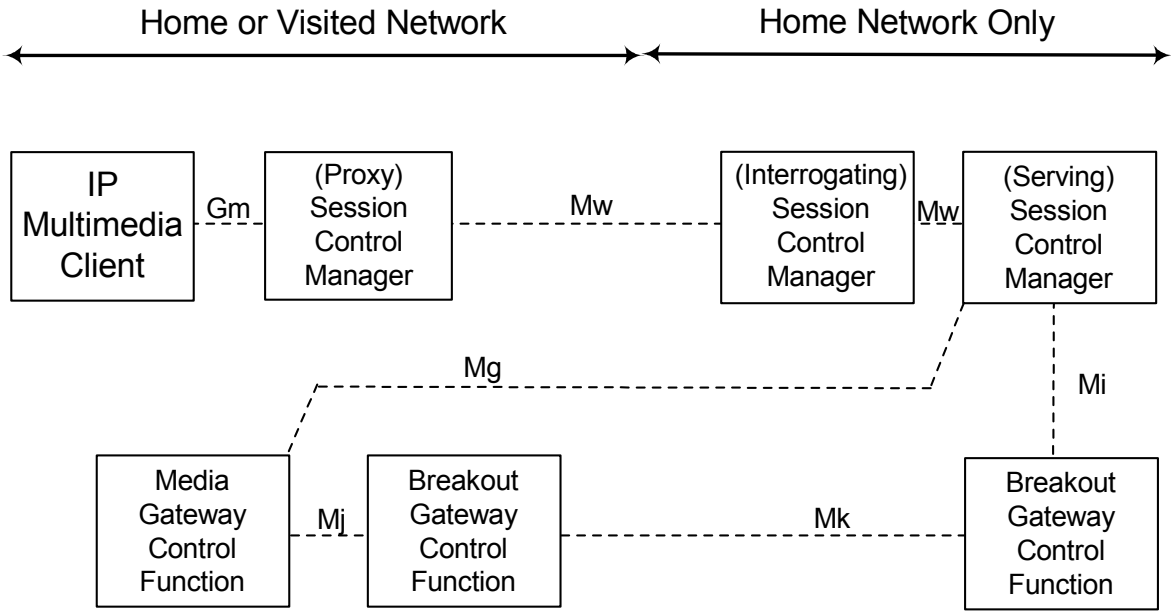


Figure 2 – Relationship of session control entities to NGN core networks

As can be seen from Figure 2, the first SIP session control entity (P-CSCF) and the reference point to the PSTN can be supported in the visited network as well as in the home network assuming that the operators have the appropriate business relationship. However the S-CSCF, which controls the access to IMS services, is always located in the home network.

6.3 IMS External Reference points

6.3.1 Reference points to the IP Connectivity Access Network

IMS interfaces to the IP-Connectivity Access Network (IP-CAN), at an identified reference point. Ideally, this reference point should be fully access independent. However, this is only valid for IP-Connectivity Access Networks that conform to a set of requirements with regards to resource management. The xDSL based access networks may not fulfil some of these requirements. In particular, the reference point for cellular access networks assume that end user equipments have the ability to issue explicit resource reservation requests, which may not be available in xDSL based access networks. Moreover, there might be a need to exchange NAPT bindings over this reference point (as well as over lower level reference points) to enable the modification of SDP descriptions accordingly.

The IMS specifications were developed for use with cellular access networks and were based on certain assumptions regarding the access network such as bandwidth available. Inherent differences between the different types of access networks will have concrete consequences on the IMS specifications. Examples of such consequences are:

1. To Support xDSL based access networks the IMS may also need to interface to specific NGN functions for the purpose of accessing location information. No equivalent reference point exists in the IMS architecture. It should be further noted that, unlike the wireless IMS access, there may be more than one IMS users behind the xDSL line and each users may have different IMS subscription.
2. Support of IPv4 has to be taken into account and this leads to a requirement to support NAPT functionalities. There are at least two reasons leading to this:
    - Some operators have (or will have) to face IPv4 addresses shortage.
    - Privacy of IP addresses for media streams cannot rely on RFC 3041 (Privacy Extensions for Stateless Address Auto-configuration in IPv6), as would have been the case for IPv6. NAPT provides an alternative for hiding terminal addresses.

Extensions to IMS for working with configurations containing NAPT are provided in the IMS specifications.

3. Relaxing the constraint on the support of I-SIM by end-user equipments would imply the need to develop alternative authentication procedures that provide equal security.
4. Relaxing the constraints on bandwidth scarcity may lead to consider optional the support of some features that are currently considered mandatory (e.g.; SIP compression).
5. Differences in location management will impact various signalling flows that convey this information, both on signalling reference points and charging reference points.
6. Differences in resource reservation procedures in the access network will require changes to the IMS resource authorisation and reservation procedures, as the resource reservation procedures for xDSL based access networks will have to be initiated by a network entity (i.e.; the P-CSCF in case of SIP-based services), on behalf of end-user terminals.
7. The differences between the fixed line and cellular access environments may mandate different security requirements. For example, in the cellular environment, the register message is transported without encryption. It may be of minimum security and privacy risk for a cellular environment but it may be an issue in the fixed environment. Further study on the security issue in the fixed environment may identify modifications to the IMS infrastructure.

6.3.2 Reference points to Application Servers

IMS supports various reference points between the IMS and application servers. These reference points support the interactions between the S-CSCF and various types of application servers, possibly through mediation devices. They also support the interaction between Application Servers and the HSS, which is the subscriber information database. This supports the downloading of subscriber data from the HSS to the AS (as well as subscriber data updating by the AS) and enables the HSS to notify an AS of changes occurring on subscriber data. No specific extensions to these reference points are identified for IMS use in NGN.

6.3.3 Reference points to the charging environment

The IMS specifications define the signalling flows and procedures for transferring (off-line) charging information between the IMS components and charging collection functions. Procedures and signalling flows between IMS components and the Online Charging System for online charging are also defined. No specific extensions to these reference points are identified for IMS use in NGN.

6.3.4 Reference points to external networks

The IMS specifications identify interworking with other IMS networks, other IP networks that are not IMS, and also interworking with the PSTN. The same interworking capabilities should be available for NGN applications of IMS. No specific extensions to these reference points are identified for IMS use in NGN.

6.4 Security considerations

Security within the IMS architecture is addressed by the IMS specifications found in Table 1.

7 Relevant IMS Specifications in the context of the NGN functional architecture

Table 1 provides a list of documents that define IMS and are considered relevant in the context of the NGN functional architecture. This list identifies the documents developed by 3GPP and 3GPP2, and published by their various partner regional standards bodies, for the access independent portion of the IMS. These document identifiers are associated with documents published by Standards Development Organizations as identified in the appropriate version of Q.1741 [6] and Q.1742 [7].

Table 1 – Specifications for IMS

ETSI Release 6 Specifications	TIA Revision A Specifications
ETSI TS 123 002: "Network architecture"	TIA-873.000-A: "All IP Network Multimedia Domain - Overview"
ETSI TS 123 218: "IP Multimedia (IM) session handling; IM call model; Stage-2"	TIA-873.003-A: "IP Multimedia (IM) Session Handling; IM call model; Stage 2"
ETSI TS 123 228: "IP Multimedia Subsystem (IMS); Stage 2"	TIA-873.002-A: "IP Multimedia Subsystem; Stage 2"
ETSI TS 124 229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3"	TIA-873.004-A: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3"
ETSI TS 129 228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents"	TIA-873.005-A: "IP Multimedia (IM) Subsystem Cx Interface; Signalling flows and message contents"
ETSI TS 129 229: "Cx and Dx Interfaces based on the Diameter protocol; Protocol details"	TIA-873.006-A: "Cx Interface based on the Diameter protocol, Protocol details"
ETSI TS 129 328: "IP Multimedia Subsystem (IMS) Sh Interface; signalling flows and message contents"	TIA-873.010-A: "IP Multimedia (IM) Subsystem Sh interface; signalling flows and message contents; Stage 2"
ETSI TS 129 329: "Sh interface based on the Diameter protocol "	TIA-873.011-A: "Sh interface based on the Diameter protocol; Protocol details"
ETSI TS 132 260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging"	TIA-873.008-A: "IP Multimedia Subsystem - Accounting Information Flows and Protocol"
ETSI TS 132 296: "Telecommunication management; Charging management; On line Charging System (OCS): Applications and interfaces"	TIA-873.015-A: "IP Multimedia Subsystem - On line Charging System (OCS): Applications and interfaces "
ETSI TS 133 203: "3G security; Access security for IP-based services"	TTAT.3G-S.R0086-A v1.0: "IMS Security Framework"
ETSI TS 123 141: "Presence service; Architecture and functional description; Stage 2"	TIA-1032.001: "Presence service; Architecture and functional description"
ETSI TS 124 141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3"	TIA-1032.002: "Presence Service; Functional Models, Information flows, and Protocol Details"
ETSI TS 133 141: "Presence service; Security"	TIA-1032.003: "Presence Security"
ETSI TS 124 147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3"	TIA-1069: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3"

2.6 – PSTN/ISDN emulation architecture*

Table of contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

2.6 – PSTN/ISDN emulation architecture

1 Scope

This document describes the functional architecture, interworking with other components, and interface requirement of the PSTN/ISDN emulation component including impacts of Call server -based and other implementations.

2 Reference

The following ITU-T Recommendations and other references contain provisions, which, through references in this text, constitute provisions of this document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this document are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this document does not give it, as a stand-alone document, the status of a Recommendation.

[1] ITU-T NGN FG NGN Release1 scope

[2] ITU-T NGN FG Release 1 requirements for services and capabilities

[3] ITU-T NGN FG FGNGN-FRA

[4] ITU-T NGN FG PSTN Evolution to NGN

[5] ITU-T NGN FG Evolution of networks to NGN

[6] ITU-T NGN FG PSTN Evolution to NGN

[7] ITU-T NGN FG PSTN/ISDN emulation and simulation

[8] ITU-T SG13 draft recommendation Y.csem

3 Definitions

This document uses or defines the following terms:

Call Server: The element which is responsible for call control, gateway control (Access GW, Media GW), media resource control, routing and subscriber authentication, authorization and accounting. The Call Server shall provide PSTN/ISDN basic services and supplementary services, and may provide value added services through service interaction with an external SCP (Service Control Point) equipment and/or AS (Application Server) in the Service/Application layer.

Functional Entity: An entity that comprises a specific set of functions at a given location. Functional entities are logical concepts. Grouping of functional entities is used to describe practical physical realizations.

Functional architecture: A set of functional entities which are used to describe the structure of a NGN. These functional entities are separated by reference points and thus they define the distribution of functions.

These functional entities can be used to describe a set of reference configurations. These reference configurations identify which of the reference points are visible at boundaries of equipment implementations and between administrative domains.

Reference point: A conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing between these functional entities. A reference point may or may not correspond to one or more physical interfaces between pieces of equipment.

4 Abbreviations

This document uses the following abbreviations.

AS	Application Server
ABGF	Access Border Gateway Function
AGCF	Access Gateway Control Function
APL GW	Application Gateway
AMG	Access Media Gateway
AMGF	Access Media Gateway Function
ASF	Application Server Function
CCF	Call Control Function
CS	Call Server
CS-PES	Call Server based PSTN/ISDN Emulation Service component
FE	Function Entity
IMS-PES	IMS base PSTN/ISDN Emulation Service component
MGCF	Media Gateway Control Function
MRCF	Media Resource Control Function
MRPF	Media Resource Process Function
NAPF	Network Access Processing Function
NACF	Network Access Control Function
PES	PSTN/ISDN Emulation Service component
PGCF	Packet Gateway Control Function
PGF	Packet Gateway Function
RF	Routing Function
SG	Signalling Gateway
SGF	Siginalling Gateway Function
SIF	Siginalling Interworking Function
SPF	Service Provide Function

SSF	Service Switching Function
TMG	Trunk Media Gateway
TMGF	Trunk Media Gateway Function
UPF	User Profile Function

5 PSTN/ISDN Emulation in NGN

As shown in Figure 5.1, PSTN/ISDN emulation, as one of the service components of NGN, provides PSTN/ISDN basic and supplementary services, and co-exists with Multimedia service component, Streaming service component, and other service components.

PSTN/ISDN emulation, as one of the service components of NGN, interworks with the existing network and other service components.

It provides the emulation of PSTN/ISDN services for legacy terminal connected via residential gateways and access gateways to the NGN.

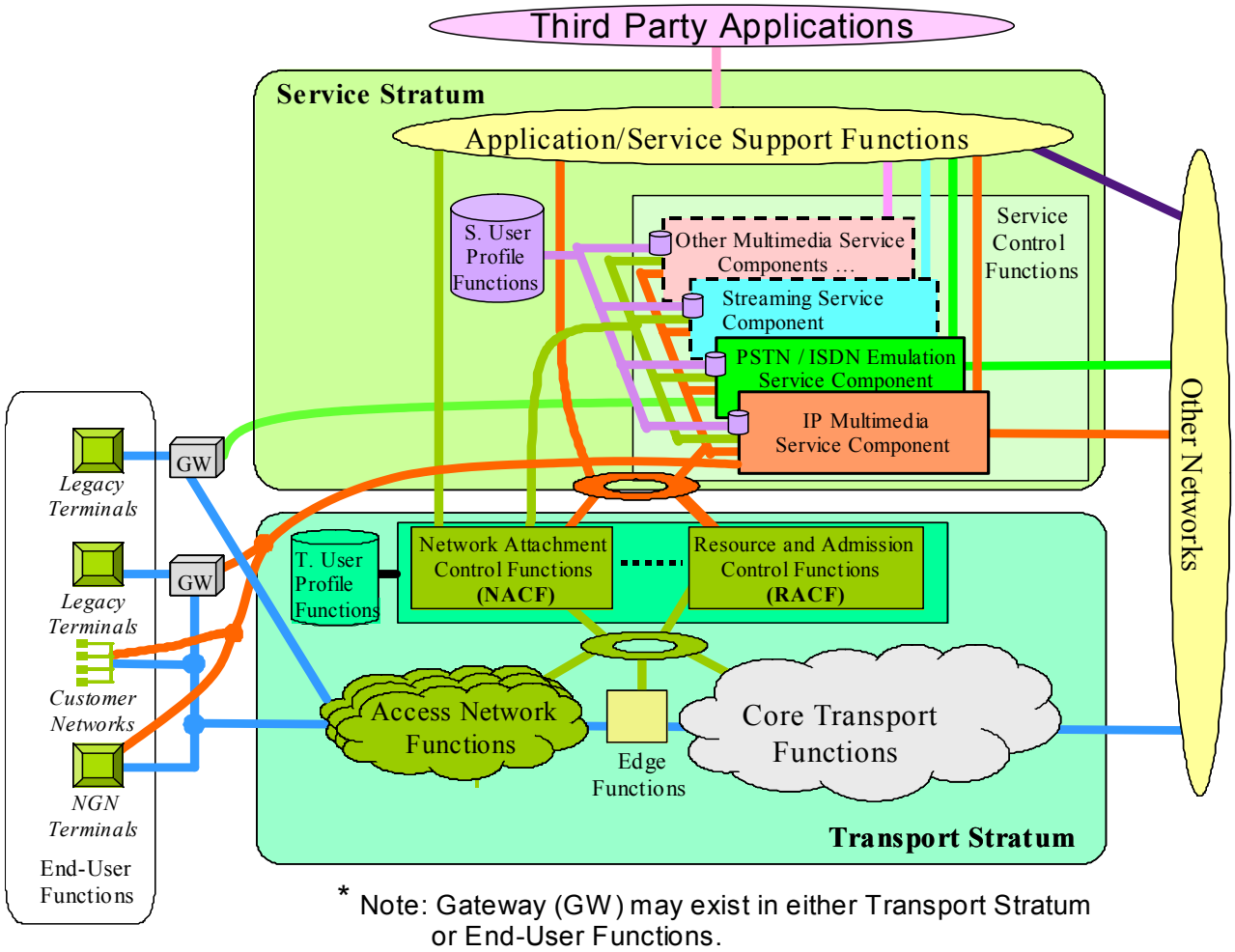


Figure 5.1 – PSTN/ISDN Emulation in NGN

6 Generic PSTN/ISDN Emulation Architecture

There are two solutions for PSTN/ISDN Emulation Service component, which are known as Call Server-based emulation and IMS-based emulation. The two solutions suit for difference network situations, but can provide equal emulation services both.

7 Call Server based PSTN/ISDN Emulation functional architecture

7.1 Functional architecture

This sub-clause describes a functional architecture for CS-based PSTN/ISDN emulation. The various functional entities and reference points that comprise this service component are shown in Figure 7.1.

The following subsection describes the logical functions of CS. The behaviours of other functional entities are identical in the CS based PSTN/ISDN Emulation service component and in the Functional Requirements and Architecture of the NGN(FRA).

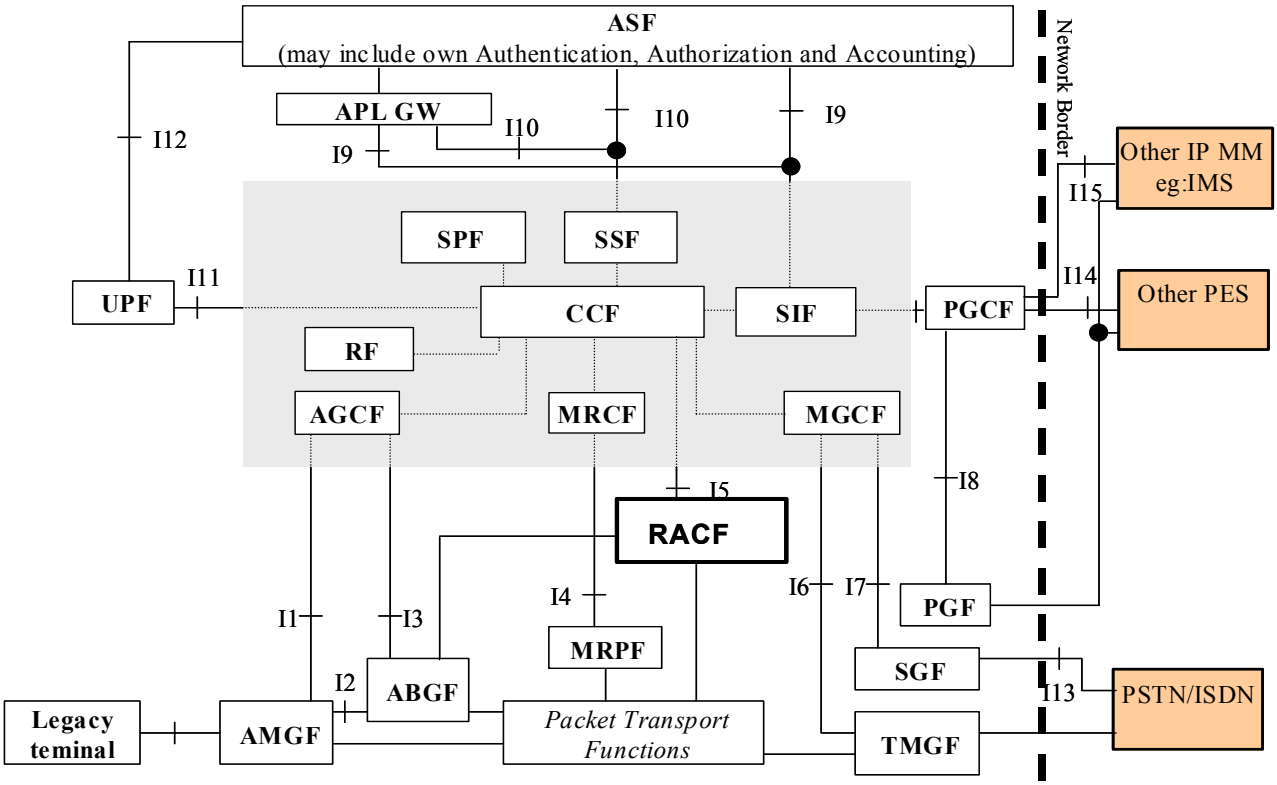


Figure 7.1 – Functional architecture of CS-based PSTN/ISDN emulation

Editor note: the reference point between SIF and PGCF needs further study, and also reference points I4 and I7 need further confirmation.

7.2 Functional entities description

This section provides a high level and not exhaustive description of CS based functional entities which may not be fully same with the functional entities in FRA.

7.2.1 Call Control Function(CCF)

Call control function(CCF) performs the following functions:

a) Providing call control capabilities :call control function, providing two party call control function and multi-party call control function;

b) Providing trigger mechanisms to access IN functionality (e.g. passes events to the SSF).

7.2.2 Access Gateway Control Function(AGCF)

The Access Gateway Control Functional (AGCF) controls one or more AMGFs to access PSTN or ISDN users, and security of the AMGF to the AGCF. It:

a) is in charge of the registration, authentication to AMGF;

b) shall recognize the main events such asoff-hook, dialing of digits, end of dialing and on-hook event from AMGF, and can control AMGF to send all sorts of signalling indications for voice services to users, e.g. dial-up tone, ringing tone and ringing back tone, busy tone, etc.

c) allocates AMGF resource .

7.2.3 Media Resource Control Function (MRCF)

The Media Resource Control Function (MRCF) controls MRPF and allocates resources which are needed for services such as streaming, announcements, and IVR (Interactive Voice Response) support.

The MRCF together with MRPF may also provide multi-party conference bridges and media transcoding.

7.2.4 Media Gateway Control Function (MGCF)

The Media Gateway Control Function (MGCF) controls the TMGF to interwork with PSTN/ISDN. The MGCF allocates and releases resources of the TMGF, as well as modifies of the usage of the resources.

7.2.5 Packet Gateway Control Function (PGCF)

The Packet Gateway Control Function (PGCF) controls PGF to interwork with other packet-based network.

7.2.6 Routing Function(RF)

The RF may be located within the CS or may be outside the CS. If the RF is outside the CS, it may be shared between and accessed by different CS.

Routing Function is specified as the function of analysing of uer characteistics(such as called number,service profile) and choosing the route to destination user. It may include routing policy function(such as routing depends on average load sharing, routing depends on time, etc.-),and routing database.

Note: In FRA, the routing function is included in the SC-FE. In this document, routing function is regarded as a separate entity. In this case, the routing function may implement in a separate physical box.

Note: This needs further study.

7.2.7 Service provide function(SPF)

It may provide the PSTN/ISDN supplementary services to user. And SPF provides the services logic about PSTN/ISDN supplementary services.

Note: In FRA, the supplementary services and value added services are provided in AS-FE in the application layer. In CS based PSTN/ISDN emulation architecture, SPF is specified to provide the PSTN/ISDN supplementary services in the control layer, while value added services are still provided in ASF in the application layer. SPF only provides service logical, and doesn’t provide the function about Application specific authorization and authentication.

Note: This needs further study.

7.2.8 Service Switching Function（SSF）

The SSF is enable to access to IN service logic programs hosted in legacy SCPs. The SSF is associated with the CCF, the function required for SSF is interaction between the CCF and SCF .

The detailed behaviors of the SSF can be found in Q.1214.

7.2.9 Signalling Interworking Function (SIF)

The SIF is associated with CCF and performs the function of Protocol adapter. The following functions are provided in the SIF:

a) May provide SIP User Agent function and send/receive SIP messages to/from the SIP Application Server,

b) Provides protocol adaptation function and connection with other NGN through PGCF. If it interworks with IMS network , SIF sends/receives SIP message. If it interworks with other Call Server based PES network, SIF may send/receive SIP-I or BICC message.

7.3 Reference point

As shown in figure7.1,reference points are described as follows:

I1: reference point between AMGF and AGCF;

I2: reference point between AMGF and ABGF;

I3: reference point between AGCF and ABGF;

I4: reference point between MRCF and MRPF;

I5: reference point between CCF and RACF;

I6: reference point between MGCF and TMGF;

I7: reference point between MGCF and SGF;

I8: reference point between PGCF and PGF;

I9: reference point between SIF and APL GW/ASF;

I10: reference point between SSF and APL GW/ASF;

I11: reference point between CCFand UPF;

I12: reference point between ASF and UPF;

I13: reference point between SGF and PSTN/ISDN;

I14: reference point between PGCF and other PSTN/ISDN Emulation service component;

I15: reference point between PGCF and other Multimedia service component(eg:IMS).

7.3.1 I1

Reference point I1 is between AMGF and AGCF. The information flows at this reference point are used to send the register message and event message such as telephone hook, off-hook, and dial-up, etc. It is expected to carry the message for controlling the resource of AMGF. This is usually thought of as being H.248 interfaces but that is not the only interface that can be used.

7.3.2 I2

Reference point I2 is between AMGF and ABGF. ABGF acts as a signaling proxy between AMGF and AGCF. So at this reference point, the information flows from AMGF to ABGF are used to transfer the register message and event message such as telephone hook, off-hook, and dial-up etc. The information flows from ABGF to AMGF are used to transfer the control message from AGCF.

7.3.3 I3

Reference point I3 is between ABGF and AGCF. The information flows at this reference point are used to transfer the message from AMGF such as register message, event message and the message for controlling the resource of AMGF.

7.3.4 I4

Reference point I4 is between MRCF and MRPF. The information flows at this reference point are used to carry the message for controlling the media resource in MRCF. The message from MRPF to MRCF is used to notify its resource information and state.

7.3.5 I5

Reference point I5 is between CCF and RACF. The information flows at this reference point are used to request the capacity to create, modify and release resources for the media flow. When the call is set up, CCF will request the RACF to create resources for the medial flow of the call. When the call is released, CCF will be requested to withdraw the arranged resource.

7.3.6 I6

Reference point I6 is between MGCF and TMGF. The information flows at this reference point are used to carry the register message and state notify message from TMGF and control message from MGCF which are used to allocate the resource such as trunk circuits, and codec resource etc.

7.3.7 I7

Reference point I7 is between MGCF and SGF. The information flows at this reference point are related to call control and supplementary services, which are used for CS based PES interworking with PSTN. The connection is based on IP.

7.3.8 I8

Reference point I8 is between PGCF and PGF. The information flows across this reference point are related to control message, which is used to control the PGF to implement the media codec conversion function.

7.3.9 I9

Reference point I9 is between SIF and APL GW/ASF. This reference point is used to provide services to user which implement in AS. The information flows at this reference point are related to service request and response.

7.3.10 I10

Reference point I10 is between SSF and APL GW/ASF. This reference point is used to provide services which implement in AS or SCP to user. The information flows at this reference point are used to send call related information to ASF. And ASF will send call control information to SSF.

7.3.11 I11

Reference point I11 is between UPF and CCF. This reference point is used to download the user subscription information, such as user service characters.

7.3.12 I12

Reference point I12 is between UPF and ASF. This reference point is used to carry the user information or service information to ASF.

7.3.13 I13

Reference point I13 is between SGF and PSTN. This reference point is used to carry the call control information to interwork with PSTN.

7.3.14 I14

Reference point I14 is between PGCF and other PES. This interface is NNI with other PES, and the information flows are used to carry the call control information between PESs. This point is required to convey signalling which is equivalent to ISUP (e.g. SIP-I).

7.3.15 I15

Reference point I15 is between PGCF and other multimedia service component. This is NNI. This reference point is used to interwork between CS based PES and other multimedia network. When the Other NGN is a PSTN/ISDN Simulation network or connection, a possible example of this interface is IMS based SIP.

7.4 Relationship between functional entities in Call Server architecture and NGN architecture

7.4.1 Correspondence between Call Server functional entities and NGN functional entities

Table 7.1 shows the relationship of the Call Server-based architecture functional entities to the functional entities identified in the NGN functional architecture.

Table 7.1 – Correspondence between Call Server functional entities and NGN functional entities

CS based PES functional entities	NGN functional entities
CCF	S-CSC-FE
RF	
SIF	NSIW-FE
SSF	SS-FE
SPF	AS-FE
AGCF	AGC-FE
MRCF	MRC-FE
MGCF	MGC-FE
PGCF	PGC-FE
UPF	SUP-FE
AMGF	AMG-FE

Table 7.1 – Correspondence between Call Server functional entities and NGN functional entities

CS based PES functional entities	NGN functional entities
ABGF	ABG-FE
MRPF	MRP-FE
PGF	IBG-FE
SGF	SG-FE
TMGF	TMG-FE
ASF	SIP AS-FE, IN-AS-FE
APL GW	APL-GW-FE
Legacy Terminal	Terminal Functions

7.4.2 The unique characteristics of the Call Server architecture

1) In Call Server architecture, BICC protocol may be used as signalling protocol besides SIP protocol.

2) Supplementary services can be provided by SPF in the service control layer in Call Server architecture.

3) ABGF in Call Server architecture may have the following additional functions:

- Acting as proxy node. All packets including signalling packets and media packets sent to and obtained from untrusted AMGF should go through ABGF.
- Address conversion function. ABGF needs to modify the address information related to AMGF and AGCF in the IP packets with its address information assigned for the session.
- Security functions .Such as firewall function and preventing DDOS attacks functions.

4) The SSF should be include in Call Server architecture.

7.5 Interworking with other subsystems

7.5.1 Interworking with other call server based PSTN/ISDN emulation service component

Call server based PSTN/ISDN emulation service component interworks with other Call server based PSTN/ISDN emulation service component through CCF, SIF, PGCF and PGF functional entities. CCF performs call control function. SIF performs siginalling adaptation function, when call server based PSTN/ISDN emulation interworks with other Call Server based PES network, SIF may map the interworking protocol to SIP-I or BICC message. PGCF interconnects with other call server based PSTN/ISDN emulation service component at I14 reference point, which controls the PGF entity behaviour and performs topology hiding function in control layer. PGF interconnects with other call server based PSTN/ISDN emulation service component at transport level, which performs the media conversion and QoS marking function under control of PGCF.

The following figure shows the architecture of call server based PSTN/ISDN emulation service component interworking with each other.

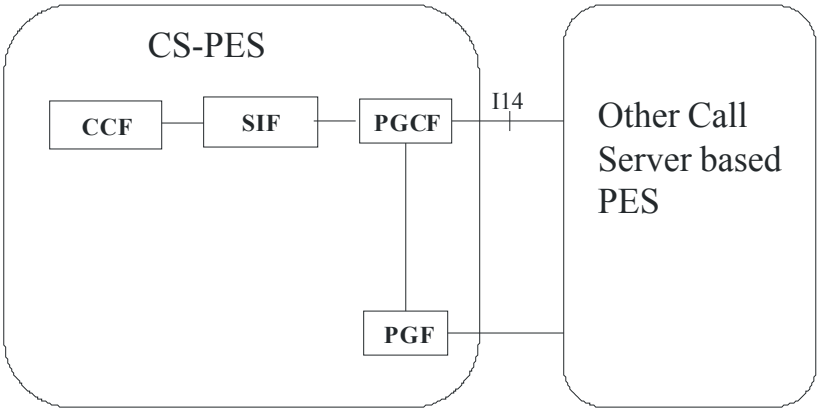


Figure 7.2 – Architecture of Call Server based PSTN/ISDN emulation service component interworking with each other

7.5.2 Interworking with IP multimedia service components

Call server based PSTN/ISDN emulation service component interworks with other IP multimedia service components(IMS) through CCF, SIF, PGCF and PGF functional entities. The CCF,PGCF and PGF perform the same functions as them used in interworking with other call server based PSTN/ISDN emulation service component. The only difference is that SIF will map the interworking protocol to SIP when interworking with IMS.

The following figure shows the architecture of call server based PSTN/ISDN emulation service component interworking with IMS.

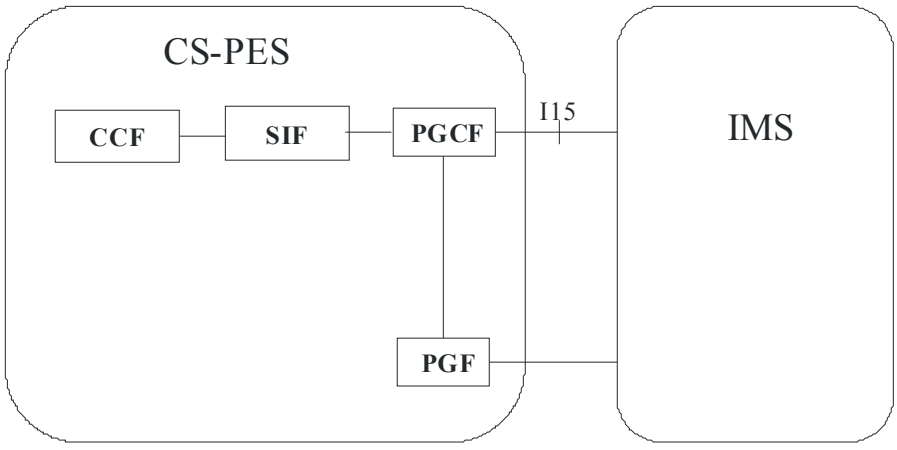


Figure 7.3 – Architecture of Call Server based PSTN/ISDN emulation service component interworking with IMS

7.6 Interworking with other networks

7.6.1 Interworking with PSTN/ISDN

Call server based PSTN/ISDN emulation service component interworks with PSTN/ISDN through CCF, MGCF, TMGF and SGF functional entities. CCF performs call control function. MGCF controls TMGF behavior and maps the interworking protocol to SIGTRAN, SGF interconnect with PSTN/ISDN at reference point I13 in signalling level which transfer the protocol to SS.7. TMGF interconnect with PSTN in media level which converts the IP packet voice to TDM trunk under the control of MGCF.

The following figure shows the architecture of call server based PSTN/ISDN emulation service component interworking with PSTN/ISDN.

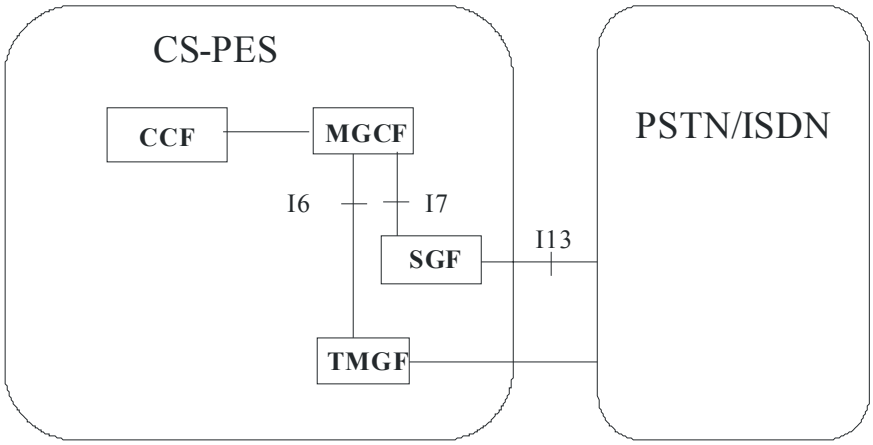


Figure 7.4 – Architecture of Call Server based PSTN/ISDN emulation service component interworking with PSTN/ISDN

8 IMS based PSTN/ISDN Emulation functional architecture

8.1 Overview

Figure 8.1 illustrates the legacy configurations supported by the PSTN/ISDN Emulation component described in this specification.

Figure 8.1 – Legacy configurations

Legacy terminals and/or legacy access nodes are connected to residential gateways or access gateways using standard interfaces. The protocol running on interfaces between these gateways and the PES is either H.248 (P1 reference point)or SIP (Gm reference point), depending on the type of gateway: media gateway (MG) or call control aware SIP-based voice over IP gateway (VGW). PSTN/ISDN islands may also be connected via trunking media gateway, controlled using the H.248 protocol.

NOTE: The Z interface is defined in clause 6.1 of Q.512 Digital exchange interfaces for subscriber access.

The functional architecture of the IMS based PSTN/ISDN Emulation service component (IMS-PES) described in this Technical Specification is based on the same architecture as the IMS. Figure 8.2 provides an overview of the functional entities that make up this architecture and shows their relationships to the other components of the NGN architecture.

NOTE: This document from IMS-PES point of view specifies modifications to the 'IMS for Next Generation Networks (IFN)'. Wherever in this documents modifications to IMS are proposed they should be read as modifications to IFN.

NOTE: In section 8.10 a mapping is provided between the IMS-PES and the NGN functional entities.

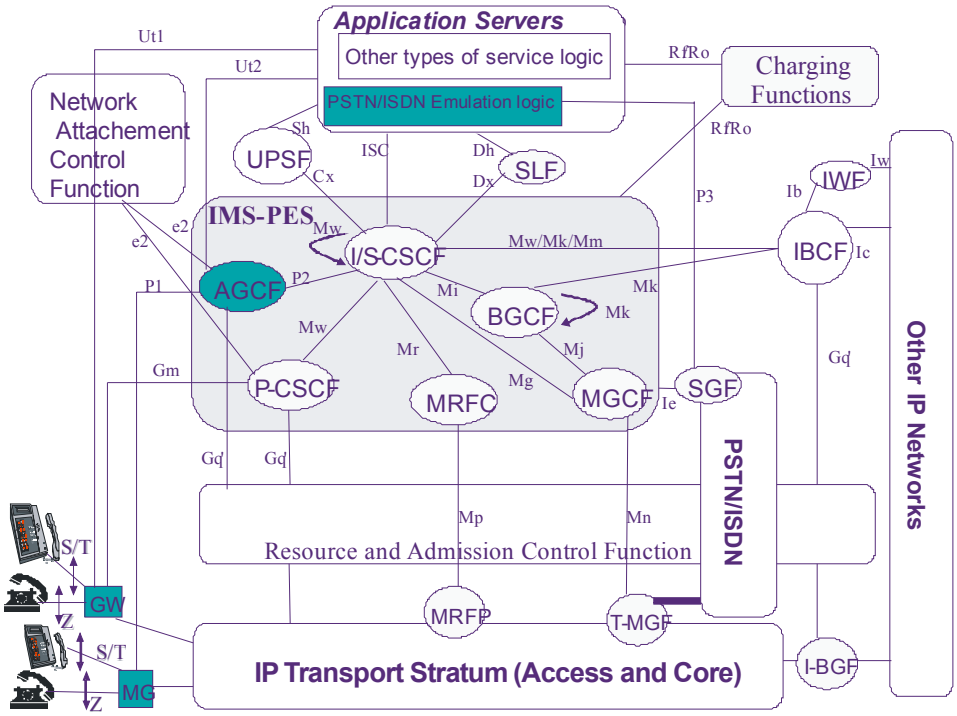


Figure 8.2 – IMS based PSTN/ISDN Emulation service component Functional Architecture

NOTE: The FE's and RP's as shown in the IMS-PES may require enhancements as indicated in sections 8.2 and 8.3.

Most of the functional entities inside the IMS based PSTN/ISDN Emulation service component are identical or derived from their IMS counterpart, with the noticeable exception of an Access Gateway Control Function (AGCF) that has the responsibility of controlling residential and access media gateways, using the H.248 protocol. For the other functional entities, any differences are noted in the following section.

NOTE: SIP-based Voice over IP gateways may also be connected to the IMS component.

8.2 Overview of Functional entities of the IMS-PES

8.2.1 Access Gateway Control Function (AGCF)

This functional entity is the first point of contact for residential and access media gateways. This entity is specific to the IMS based PSTN/ISDN emulation component. It performs the following functions:

- Act as an MGC for controlling media gateways functions located in residential and access gateways.
- Interact with the resource and admission control function (RACF).
- Interact with the network attachment Control Function (NACF) to retrieve line profile information.
- Perform signalling inter-working between SIP (including any ISUP information that may be encapsulated) and analog signalling (through H.248 signals and events).
- Manage SIP registration procedures on behalf of legacy terminals connected behind the media gateways.

Moreover, the AGCF shall provide basic feature logic for

- placing, holding and transferring of calls;
- determining end of dialling;
- reporting the state of a terminal (e.g. parking, out of order, on service, off-hook, on-session, etc.) via SIP.
- supporting the collection and reporting of events to AS via SIP for example basic call events, service activation, service deactivation, service interrogation and mid-call events. From the service point's of view they are transparent to AGCF.
- delivering several dial tone patterns selected by the application server;

The AGCF does not hold any user profile but shall be made aware if user equipment can handle several simultaneous calls.

NOTE 1: A solution based on AGCF shall be able to provide similar response time (e.g. dial tone, ring tone) as today in the PSTN networks.

NOTE 2: If desired, a network operator could choose to deploy an H.248 MGC that controls a set of media gateways following most of the AGCF call processing rules defined in this document, and supports the Gm interface into an IMS or PES network via a P-CSCF, but this entity would fill the role of "Gateway (GW)" depicted in Figure 8.2 and would not be part of the trusted IMS core.

8.2.2 Multimedia Resource Function Controller (MRFC)

The behavior of the MRFC is identical in the IMS based PSTN/ISDN Emulation service component and in the IMS.

8.2.3 Media Gateway Control Function (MGCF)

The role of the MGCF is identical in the IMS based PSTN/ISDN Emulation service component and in the IMS. Signaling procedures for inter-working with ISUP signaling are slightly different due to the presence of encapsulated ISUP information inside the IMS-PES and the need to ensure full ISDN transparency in case of ISDN calls transiting through the IMS-PES.

8.2.4 Proxy Call Session Control Function (P-CSCF)

The behavior of the P-CSCF is identical in the IMS based PSTN/ISDN Emulation service component and in the IMS. However, the P-CSCF is not used in configurations where an AGCF is required to control residential or access media gateways, using H.248.

8.2.5 Service Call Session Control Function (S-CSCF)

The behavior of the S-CSCF is identical in the IMS based PSTN/ISDN Emulation service component and in the IMS, except that, as an option, the presence of encapsulated ISUP information may be used as a potential Service Point Trigger (SPT) in SIP signaling.

8.2.6 Interrogating Call Session Control Function (I-CSCF)

The behavior of the I-CSCF is identical in the IMS based PSTN/ISDN Emulation service component and in the IMS.

8.2.7 Breakout Gateway Control Function (BGCF)

The behavior of the BGCF is identical in the IMS based PSTN/ISDN Emulation service component and in the IMS.

8.3 Internal Reference Points

8.3.1 Reference Point MGCF – CSCF (Mg Reference Point)

The Mg reference point allows the MGCF to forward incoming session signaling (from the PSTN) to the CSCF for the purpose of inter-working with PSTN networks, and vice-versa.

The protocol used for the Mg reference point is SIP. In case of the S-CSCF and I-CSCF, SIP messages may contain encapsulated ISUP information.

The role of this reference point is identical in the IMS-PES and IMS.

8.3.2 Reference Point CSCF – MRFC (Mr Reference Point)

The Mr reference point allows the S-CSCF to relay signaling messages between an application server function and an MRFC.

The protocol used for the Mr reference point is SIP.

The role of this reference point is identical in the IMS-PES and IMS.

8.3.3 Reference Point CSCF – CSCF (Mw Reference Point)

The Mw reference point allows the communication and forwarding of signaling messaging between CSCFs, e.g. during registration and session control.

The protocol used for the Mg reference point is SIP. In case of the S-CSCF and I-CSCF, SIP messages may contain encapsulated ISUP information.

The role of this reference point is identical in the IMS-PES and IMS.

When two CSCF are located in different networks, signaling information for the Mw reference point crosses the IBCF.

8.3.4 Reference Point CSCF – BGCF (Mi reference point)

This reference point allows the Serving CSCF to forward the session signaling to the Breakout Gateway Control Function for the purpose of inter-working to the PSTN networks.

The Mi reference point is based on external specifications is SIP, possibly with encapsulated ISUP.

The role of this reference point is identical in the IMS-PES and IMS.

8.3.5 Reference Point BGCF – MGCF (Mj reference point)

This reference point allows the Breakout Gateway Control Function to forward the session signaling to the Media Gateway Control Function for the purpose of inter-working to the PSTN networks.

The Mj reference point is SIP, possibly with encapsulated ISUP.

The role of this reference point is identical in the IMS-PES and IMS.

8.3.6 Reference Point BGCF – BGCF (Mk reference point)

This reference point allows the Breakout Gateway Control Function to forward the session signaling to another Breakout Gateway Control Function.

The Mk reference point is SIP, possibly with encapsulated ISUP.

The role of this reference point is identical in the IMS-PES and IMS.

When two BGCF are located in different networks, signaling information for the Mw reference point crosses the IBCF and may also cross an I-CSCF.

8.3.7 Reference Point AGCF – CSCF (P2 reference point)

This reference point is between the AGCF and a CSCF playing the I-CSCF or S-CSCF role. The AGCF acts as a P-CCSF from the point of view of the S-CSCF and I-CSCF.

8.4 Value Added Service Architecture

8.4.1 Overview

The value added service architecture for the IMS based PES component is based on the VAS Architecture of the IMS component. The generic behavior of application server functions is identical with respect to the PSTN/ISDN Emulation Service component and the IMS component. However, depending on the type of services to be emulated, application servers may need to understand and terminate the ISUP protocol encapsulated in SIP.

Three types of Application Server Functions (ASF) can be accessed by the S-CSCF, through the ISC reference point (See Figure 8.3).

- SIP Application Servers (SIP AS)
- The IM-SSF Application Server
- The OSA SCS Application Server

A SIP Application Server may contain “service capability interaction manager” (SCIM) functionality and other application servers. The SCIM functionality is an application which performs the role of interaction management. The internal structure of the application server is outside the standards.

The purpose of the IM SSF is to enable access to IN service logic programs hosted in legacy SCFs. The IM-SSF functionality encompasses the emulation of the IN Call Model (BCSM) on top of SIP signaling, IN triggering and feature management mechanisms, emulation of the IN Service Switching Finite State Machine and inter-working with INAP.

NOTE 1: The role of the IM-SSF is identical in the IMS based PSTN/ISDN Emulation component and in the IMS component. Basic behavior is also identical. However, in the IMS based PES case, mapping procedures may take into account ISUP information encapsulated in SIP messages.

NOTE 2: The IM SSF is intended to enable access from the IMS based PES to IN service logic programs hosted in legacy SCFs. Access to IMS based PES services (i.e. hosted in SIP-based Application Servers) from legacy SSFs in the PSTN/ISDN is outside the scope of this document. Appropriate gateway functions (e.g. SPIRITS gateway as defined in

RFC 3136) have to be implemented in the PSTN/ISDN network for supporting such scenarios. The purpose of the OSA Service Capability Server is to provide access to OSA applications, according to the OSA/Parlay framework.

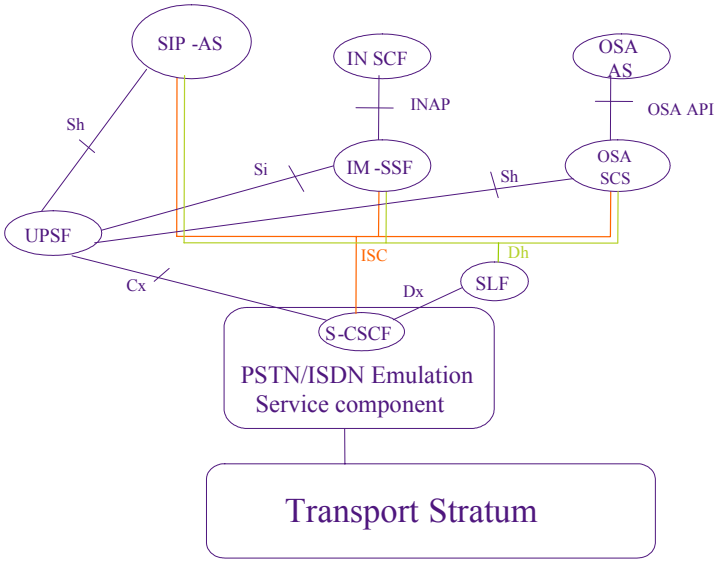


Figure 8.3 – Value Added Services architecture

8.4.2 Reference points

8.4.2.1 Reference Point CSCF – ASF (ISC Reference Point)

The information flows across this reference point are identical for the IMS based PSTN/ISDN Emulation Service component and the IMS component.

8.4.2.2 Reference Point UPSF – SIP AS or OSA SCS (Sh Reference Point)

The information flows across this reference point with respect to the IMS bases PSTN/ISDN Emulation Service component and the IMS component are identical.

8.4.2.3 Reference Point UPSF – IM SSF (Si Reference Point)

The information flows across this reference point with respect to the PSTN/ISDN Emulation Service component and the IMS component are identical.

8.4.2.4 Reference Point ASF- SLF (Dh Reference Point)

The information flows across this reference point with respect to the PSTN/ISDN Emulation Service component and the IMS component are identical.

8.4.2.5 Reference Point ASF – UE (Ut1 Reference Point)

This reference point enables a SIP-based gateway to manage information related to the services provided to the legacy equipment it connects.

8.4.2.6 Reference Point ASF – AGCF (Ut2 Reference Point)

This interface enables the AGCF to manage information related to the services provided to the legacy equipment connected to the media gateways it controls.

8.5 External Reference Points

8.5.1 Reference Points with entities in the transport stratum

8.5.1.1 Reference Point MGCF – T-MGF (Mn Reference Point)

The role of this reference point with respect to the IMS based PSTN/ISDN Emulation Component and the IMS is identical.

8.5.1.2 Reference Point MGCF – SGF (Ie Reference Point)

The Ie reference point enables the MGCF to exchange SS7 signaling information over IP with the SGF, according to the SIGTRAN architecture.

8.5.1.3 Reference Point AS – SGF (P3 Reference Point)

The IMS-PES uses the SGF primarily in support of the MGCF signaling to the PSTN, as does the IMS. In addition, some Application Servers involved in supporting IMS-PES users may use the SGF to support non-call related signaling interactions with the PSTN (e.g. TCAP-based messages for CCBS).

8.5.1.4 Reference Point MRFC – MRFP (Mp Reference Point)

The role of this reference point with respect to the IMS based PSTN/ISDN Emulation Component and the IMS is identical.

8.5.2 Reference Point with the UE

Legacy terminals connected to call control aware VoIP gateways interact with the IMS-PES via the Gm reference point. The protocol used for the Gm reference point is SIP.

The role of this reference point is identical in the IMS-PES and IMS.

Legacy terminals connected to H.248-based media gateways interact with the IMS-PES via the P1 reference point.

8.5.3 Reference Point with the user profile

The behavior of the UPSF and SLF in relation to the IMS based PSTN/ISDN Emulation Component is identical to its behavior in relation to the IMS.

8.5.3.1 Reference Point with the SLF (Dx reference point)

The role of this reference point with respect to the IMS based PSTN/ISDN Emulation Component and the IMS are identical.

8.5.3.2 Reference Point with the UPSF (Cx reference point)

The role of this reference point with respect to the IMS based PSTN/ISDN Emulation Component and the IMS are identical.

8.5.4 Reference Points with Charging Functions

The following functional entities in the IMS-PES may act as charging trigger points

– AS;

– BGCF;

– (I-/P-/S-) CSCF;

– MGCF;

– MRFC.

For off-line charging the Rf reference point is used. For on-line charging the Ro reference point is used.

NOTE: The IBCF to which the Core IMS is connected may also act as a charging trigger point.

8.6 Interconnection with other networks

8.6.1 Interconnection with the PSTN/ISDN

Interconnection at the signaling level is provided via the SGF.

Interconnection at the media level is provided by the trunk interfaces at the T-MGF.

8.6.2 Interconnection with other external IP-based Service components

Interconnection with other IP-based service components (including other PSTN/ISDN Emulation service components) is performed via the IBCF at the signaling level.

The interface between the IMS-PES and the IBCF coincides with either of the P2, Mw, Mk or Mm reference points. The Mm reference point is used for interconnecting with non-IMS based systems.

Interconnection between PSTN/ISDN emulation components occurs either between two home domains (e.g. session originating and terminating domain) or between a visited domain and a home domain (i.e. support of roaming capabilities).

8.7 Reference Points with the Network Attachment Function (NACF)

The e2 reference point supports information transfer between the P-CSCF or the AGCF and the Network Attachment Component.

The role of this reference point with respect to the PSTN/ISDN Emulation Component and the IMS component is identical.

NOTE: Interaction with the NACF is not be required in case the AGCF controls access gateways only.

8.8 Reference Point with the Resource and Admission Control Function (RACF)

The Gq' reference point enables the P-CSCF or the AGCF to interact with the resource control component for the following purposes:

– authorization of QoS resources

– resource reservation

– gate control (including NAPT binding information relay).

With regard to the RACF architecture; the P-CSCF and the AGCF play the role of an Application/Service Support Function.

The role of this reference point with respect to the PSTN/ISDN Emulation Component and the IMS component is identical.

NOTE: Interaction with the RACF may not be required in case the AGCF controls access gateways only and dedicated transport resources are used to support PES traffic. In case of network interconnection, interactions with the resource control component may also take place at the edge of the PES, at the IBCF level for the following purposes:

– gate control (including NAPT binding information relay).

With regard to the RACF architecture; the IBCF plays the role of an Application/Service Support Function.

8.9 Mode of operation

8.9.1 General Principles

Emulating PSTN/ISDN services using the IMS-based PES architecture described in this document assumes that the logic of the service to be emulated resides in one or more application servers rather than in the AGCF or in gateways.

For certain call configurations, this requires that encapsulated ISUP information be sent/received by some of these application servers.

NOTE: Although SIP with encapsulated ISUP is usually known as SIP-I, the procedures assumed in this document rely on the IMS SIP profile with encapsulated ISUP messages, which should not be confused with Q.1912.5 SIP Profile C.

The logic embedded in the AGCF is either inter-working logic (e.g. the AGCF has to know how to convert the information contained in an incoming SIP INVITE into a presentation message of the protocol for display services over analog lines or service independent feature logic (e.g.; on receipt of an off-hook or flash-hook event from a media gateway, the AGCF shall autonomously request the media gateway to play a dial tone).

Although some application servers may be dedicated to the provision of PES-specific services, the PES architecture does not restrict the type of applications that a PES-user can access. (See Figure 8.4)

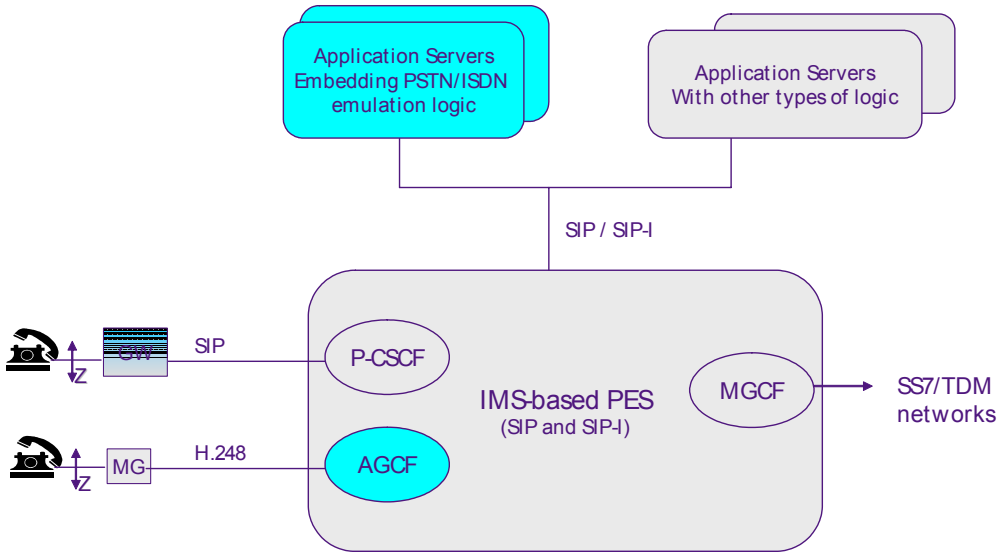


Figure 8.4 – Service Access via the PES

8.9.2 Service Provisioning

The service profile of PES users is stored in the UPSF as for any other type of user. Appropriate filter criteria are set to ensure that PES-enabled Application Servers are involved in the processing of calls from/to PES-users. Setting these criteria does not require any specific service point trigger beyond those used in relation to the IMS component.

8.9.3 Registration

Registration and deregistration procedures are initiated by SIP-based gateways on behalf of each line it serves. The rest of the procedures are identical in the PES and IMS components.

Registration and deregistration procedures are initiated by the AGCF on behalf of each line connected to the media gateways it controls, based on the information contained in service change messages received from those media gateways. The rest of the procedures are identical in the PES and IMS components.

8.10 Mapping between IMS-PES functional entities and NGN functional entities

Table 8.1 – Correspondence between IMS-PES functional entities and NGN functional entities

IMS_PES Functional Entities	NGN Functional Entities
1. S-CSCF	S-CSC-FE
2. P-CSCF	P-CSC-FE
3. I-CSCF	I-CSC-FE
4. MGCF	MGC-FE
5. TMGF	TMG-FE
6. MRFC	MRC-FE
7. MRFP	MRPFE
8. BGCF	BGC-FE
9. UPSF	SUP-FE, SAA-FE
10. SLF	SL-FE
11. AS	AS-FE
12. UE	Terminal Functions
13. IM-SSF	SSF
14. IN-SCF	IN-AS-FE
15. SCIM	APL-SCM-FE
16. SIP-AS	SIP AS-FE
17. OSA AS	OSA AS-FE
18. OSA SCS	OSA APL-GW-FE
19. AGCF	AGC-FE
20. IBCF	IBC-FE
21. IW	NSIW-FE
22. SGF	SG-FE
23. MG	AMG-FE
24. IBGF	IBG-FE

WORKING GROUP 3
DELIVERABLES

QUALITY OF SERVICE

2.7 A QoS Control architecture for Ethernet-based IP access network (*Status P*)

2.8 Multi service provider NNI for IP QoS (*Status S*)

2.9 Requirements and framework for end-to-end QoS in NGN (*Status D*)

2.10 The QoS Architecture for the Ethernet Network (*Status D*)

2.11 Functional requirements and architecture for resource and admission control in NGN (*Status D*)

2.12 A QoS framework for IP-based access networks (*Status D*)

2.13 Performance measurement and management for NGN (*Status A*)

2.14 Algorithms for achieving end to end performance objectives (*Status P*)

2.7 – A QoS Control architecture for Ethernet-based IP access network*

Table of Contents

* Status P: This deliverable has already been passed to ITU-T Study Group 13.

2.7 – A QoS Control architecture for ethernet-based IP access network

1 Scope

This document provides a QoS control architecture for support of dynamic and per-session QoS control over Ethernet-based IP access network. It refers to the definitions provided in Y.1231 regarding IP access network and IP core network.

Based on the existing QoS mechanisms in the data plane, this document specifies:

1) a QoS control architecture for support of dynamic and per-session QoS control over Ethernet-based IP access network;
2) QoS-related control interfaces and their requirements;
3) Mapping of the QoS parameters between the service layer and the transport layer;
4) Mapping of the different QoS mechanisms between the adjacent segments.

The QoS mechanisms for the last mile user access segment are MAC technology-specific and as such are out of the scope of this document.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[Y.1231] ITU-T Recommendation Y.1231 (2000), *IP access network architecture*

[Y.1241] ITU-T Recommendation Y.1241 (2001), *Support of IP-based services using IP transfer capabilities*

[Y.1221] ITU-T Recommendation Y.1221 (2002), *Traffic control and congestion control in IP-based networks*

[Y.1540] ITU-T Recommendation Y.1540 (1999), *Internet protocol data communication service – IP packet transfer and availability performance parameters*

[Y.1541] ITU-T Recommendation Y.1541 (2002), *Network Performance Objectives for IP-based services*

[Y.1291] ITU-T Recommendation Y.1291 (2004), *An architectural framework for support of Quality of Service (QoS) in packet networks*

[802.1p] IEEE 802.1p (1998), *Traffic Class Expediting and Dynamic Multicast Filtering*

[802.1q] IEEE 802.1q (1998), *Virtual Bridged Local Area Networks (Virtual LANs)*

[IP DSCP] IETF RFC2474, *Definition of the Differentiated Services Operation Over DiffServ Networks*

[DiffServ] IETF RFC2475, *An Architecture for Differentiated Services (DiffServ)*

[Policy Control] IETF RFC2753, *A Framework for Policy-based Admission Control*

[MPLS EXP] IETF RFC3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*

3 Definitions

This Recommendation defines the following terms:

3.1 IP access network: An implementation comprising network entities to provide the required access capabilities between an "IP user" and an "IP service provider" for the provision of IP services. "IP user" and "IP service provider" are logical entities which terminate the IP layer and/or IP related functions, and may also include lower layer functions, and may also include lower layer functions [refers to Y.1231].

3.2 IP core network: IP service provider's network, including one or more IP service providers. [refers to Y.1231]

3.3 Ethernet-based IP access network: An IP access network comprises the Ethernet aggregation network, access nodes (such as DSLAM), and edge nodes (such as BRAS) and may also include the IP aggregation network. Edge nodes are typically IP capable. Access nodes may be IP capable.

3.4 Connection-oriented network service: A network service that establishes logical connections among service users before transferring information.

3.5 Connectionless network service: A network service that allows the transfer of information among service users without the need for logical connection establishment procedures.

3.6 Flow [IP flow]: A sequence of packets sent from a particular source to a particular destination to which the common routing is applied. If using IPv4, a flow is identified by IPv4 5-tuple including source/destination IP addresses, protocol ID, source/destination port numbers. If using IPv6, a flow is identified by IPv6 3-tuple including source/destination IP addresses, flow label.

3.7 Session: A period of communication between two (or more) terminals which may be conversational or non-conversational (for example retrieval from a database).

3.8 Relative QoS: This term refers to a traffic delivery service without absolute bounds on the achieved bandwidth, packet delay or packet loss rates. It describes the circumstances where certain classes of traffic are handled differently from other classes of traffic, and the classes achieve different levels of QoS.

3.9 Absolute QoS: This term refers to a traffic delivery service with numerical bounds on some or all of the QoS parameters. These bounds may be physical limits, or enforced limits such as those encountered through mechanisms like rate policing. The bounds may result from designating a class of network performance objectives for packet transfer.

4 Abbreviations

IETF Internet Engineering Task Force

ITU-T International Telecommunication Union – Telecommunication Standardization Sector

QoS Quality of Service

DSCP DiffServ Code Point

MPLS	Multi-Protocol Label Switching
SLA	Service Level Agreement
BRAS	Broadband Remote Access Server
CPN	Customer Premises Network
CPE	Customer Premises Equipment
NTRD	Network Topology and Resource Database
IP	Internet Protocol
MAC	Media Access Control
DSLAM	Digital Subscriber Line Access Multiplexer
VoIP	Voice over IP

5 Definition of Ethernet-based IP access network

According to the type of access aggregation technologies, IP access networks can be classified into two main categories: Ethernet-based IP access network and ATM-based IP access network. (Note that in some cases people use IP-based in comparison with ATM-based, which actually implies Ethernet-based.)

An Ethernet-based IP access network comprises the Ethernet aggregation network, access nodes (e.g. DSLAM), and edge nodes (e.g. BRAS) and may also include the IP aggregation network. Edge nodes are typically IP capable.

An Ethernet-based IP access network may contemporarily support several different types of the last mile user access technologies. For example, an Ethernet-based IP DSLAM may be able to contemporarily support LAN/xDSL/WLAN user access. And different types of Access Nodes may be deployed and aggregated to the same BRAS in an Ethernet-based IP access network.

6 Reference model of Ethernet-based IP access network

6.1 Generic architectural and topological model

Most of the Ethernet-based IP access networks can be shown as the following architectural and topological model.

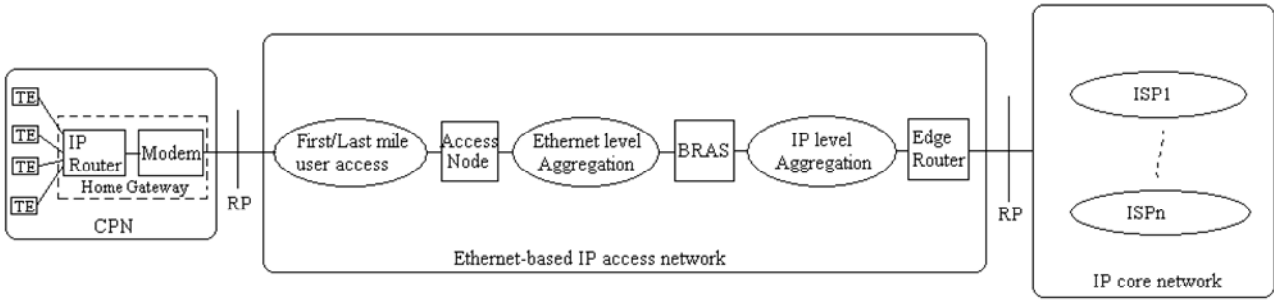


Figure 1 – Generic architectural and topological model of Ethernet-based IP access network

Depending on the size of an access network and the position of BRAS, the IP level aggregation segment may be optional. BRAS may be located close to Access Node or close to Edge Router, depending on the network scale and subscriber amount. In some cases, BRAS may serve as an Edge router which directly connected to IP core network.

Generally, L2 or L3 switches are used for Ethernet level traffic aggregation per subscriber, and L3 switches or IP routers for IP level aggregation per QoS class or service type.

TE: Terminal Equipment

CPN: Customer Premises Network

Home Gateway: consists of Modem and IP router. Either element can be optional, depending on the types of the last mile user access technologies.

Access Node: terminates the last mile link signals at the network side, and physically can be a single device or a chain of subtended devices. It may be located at a Central Office or a remote site or both if subtended. It must have one or more Ethernet uplink interface when residing in an Ethernet-based IP access network.

BRAS: (Broadband Remote Access Server) terminates the user access session (e.g. PPP, EAP (rfc2284), VLAN), performs network access control and aggregates the user traffic into VLAN, VPN, or tunnels as with native IP traffic. It must have one or more Ethernet downlink interface and be able to terminate its Ethernet layer when residing in an Ethernet-based IP access network. The BRAS also provides policy management interface, AAA interface and DHCP interface. Based on that, it makes user access control and assigns user IP addresses.

Edge Router: is an egress IP router which connects an IP access network to one or multiple IP service providers in IP core network. An Edge Router aggregates IP traffic from one or multiple BRAS. It may also contain NAT and/or firewall elements.

The last mile user access technologies are diverse which may be LAN, xDSL, WLAN, EPON, PLC and so on. Different types of the last mile user access systems have different types of Modems and Access Nodes. Examples are given below. This list is not exhaustive.

Last mile user access technology	Access Node	Modem/Adapter
LAN	L2 Switch	LAN adapter
Xdsl	DSLAM	xDSL modem
WLAN	WLAN AP	WLAN adapter
Cable	CMTS	Cable Modem
PLC	EPLC-SHE	EPLC-SCPE
EPON	OLT	ONU
UMTS	RNC+Node B	USIM card

6.2 Generic protocol layered model

Figure 2 illustrates a generic protocol layered model of Ethernet-based IP access network.

The physical layer makes use of various types of physical media. This layer is terminated at points where the connectivity is switched by equipment using Ethernet technologies, and as such has no end-to-end significance.

The Ethernet layer provides connection-oriented or connectionless transport to support the IP layer. This layer is terminated at points where IP packets are forwarded (i.e., "routers", "SRC", and "DST"), and as such has no end-to-end significance.

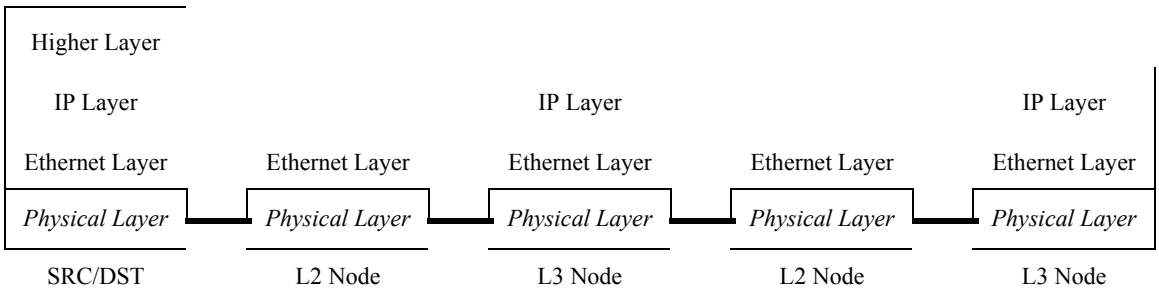


Figure 2 – Generic protocol layered model of Ethernet-based IP access network

The IP layer provides connection-oriented or connectionless transport of IP packets. This layer has end-to-end significance for a given pair of IP addresses.

Higher layers, supported by the IP layer, further enable end-to-end communications. The higher layers may include, for example, TCP, UDP, FTP, RTP, and HTTP.

7 QoS issues of Ethernet-based IP access network

With the predominating of IP in core networks and CPN, Ethernet is gradually gaining more and more share for access aggregation due to its cheapness and simplicity. Meanwhile, the requirement for supporting multi-services on broadband IP access is also increasing. Metro Ethernet networks are being constructed by carriers for access aggregation and other service goals, whilst QoS issues are being addressed so that Ethernet aggregation can provide QoS-assured data delivery performance close to what ATM can provide.

QoS issues and mechanisms of Ethernet-based IP access network differs greatly from that of ATM-based IP access network due to the native difference between ATM and Ethernet.

In nature, the bearer QoS (i.e. bearer network performance) control issues are the network resource control issues. Through optimizing resource allocation among traffic, the network performance objectives including the upper bound on packet delay, jitter, loss and error can be met well.

According to the difference of the resource attributes, an Ethernet-based IP access network could be partitioned into three segments, namely the last mile user access segment, the Ethernet level aggregation segment, and the IP level aggregation segment. For each segment, there are typical QoS mechanisms available in the data plane.

At the joint nodes such as Access Node, BRAS and Edge Router, the mapping between the different QoS mechanisms should be done for end-to-end QoS delivery.

In addition, these joint nodes are usually as the injection nodes for support of policy control and gate control.

7.1 QoS mechanisms in the last mile user access segment

Generally this segment is IP-unaware and the technologies vary greatly. Each kind of the last mile user access technology has its QoS mechanisms that are concomitant with its physical and link layer mechanisms.

The bandwidth resource contention among users in this segment should be solved to ensure for each user the subscribed line rate, especially if users must share the upstream/downstream link bandwidth. The QoS mechanisms for this segment are highly MAC technology-dependent , which are out of the scope of this document.

7.2 QoS mechanisms in the Ethernet level aggregation segment

IEEE 802.1p defines eight priority levels and the traffic class expediting mechanisms utilizing these priorities for support of different classes of service. IEEE 802.1q defines the tag format for adding VLAN ID, priority level and canonical format indicator fields into an Ethernet MAC frame header. They enable QoS information can be tagged onto any MAC frame, and thus effect Ethernet switches to handle the tagged frames with differentiation at the Ethernet layer. Queuing, scheduling, policing, shaping and filtering mechanisms can be applied based on classification and marking the 802.1q tag.

The inner VLAN could be configured per user from the Access Node to BRAS for user traffic separation, traceability and security, usually called the 'user VLAN'. Q-in-Q (i.e. VLAN stacking defined by IEEE 802.1ad) mechanism could be used for Ethernet level traffic aggregation in case 4096 VLAN IDs are not enough. The granularity of the user VLAN could be smaller so that BRAS could easily distinguish service types and aggregate service traffic according to the VLAN ID without IP level inspection, e.g. a user may have multiple VLANs, each respectively for voice, video and data services. MEF (Metro Ethernet Forum) also defines some reference traffic management mechanisms and parameters on the basis of IEEE 802.1q for the SLA enforcement of Ethernet services.

The Access node is the first point where the traffic from multiple user access lines are aggregated into a single network, and thus should shape and police the traffic on a user access line to the subscribed access rate. BRAS should shape and police the traffic on user VLANs to the subscribed access rate and do the mapping between IP DSCPs and 802.1p priorities.

7.3 QoS mechanisms in the IP level aggregation segment

IETF rfc2474 defines the DSCPs (maximum 64) in the DiffServ field of the IP headers for support of different classes of service. IETF rfc2475 defines the DiffServ architecture utilizing these IP DSCPs. Queuing, scheduling, policing, shaping and filtering mechanisms can be applied based on classification and marking the IP DSCPs. At each DiffServ router, the packets that belong to the same class of service are subjected to the same Per-Hop-Behaviour (PHB) (i.e. a group of forwarding behaviours). A number of PHBs and their related DSCPs have been standardized within IETF, including the Expedited Forwarding (EF) PHB, the Assured Forwarding (AF1~4) PHB group, and the default Best Effort (BE) PHB.

The tunnels (e.g. L2TP, GRE), VLANs, MPLS LSPs and VPNs could be configured per service type or QoS class for IP level traffic aggregation as additions to native IP and for traffic separation among different services. MPLS LSP can be established for resource reservation and explicit routing. BRAS and Edge router should do the mapping between 802.1p priories, IP DSCPs, and MPLS EXP bits.

8 Requirements for support of dynamic and per-session QoS control

In an IP access network, there are two broad categories of IP service flows: 1) the session-oriented service flows that are associated with some form of session control procedure using a protocol such as SIP or H.323, and 2) the non session-oriented service flows without any session control procedure.

Reserving a QoS path through path-decoupled signalling (e.g. RSVP, RSVP-TE or CR-LDP) for a flow or a traffic aggregate that may contain any kind of application data is viewed as a particular kind of connection-oriented network service. However, that's not the focus of this recommendation.

The flow is generally described by the IPv4 5-tuple or IPv6 3-tuple.

Different service types and user applications may have quite different QoS requirements. Some session-oriented services may need traffic delivery with absolute QoS. To enable various session-oriented services over IP (including voice, video, VPN and etc.), the IP access network should be able to support dynamic and per-session QoS control on demand.

Before a session-oriented service flow is classified and marked at the network edge node, the flow must be identified at first. Since a lot of IP service port numbers are determined through dynamic negotiation in the service layer, it is very difficult for the network edge nodes themselves to dynamically identify all of the happening flows. Static configuration at per-flow level is unpractical. Only after the service layer informs the transport layer of the flow description (IPv4 5-tuple or IPv6 3-tuple), can the problem be effectively solved. Meanwhile, the QoS requirements (including bandwidth and QoS classes) of the service flow could also be determined by the service layer according to the service type, Service Level Agreement, or user explicit QoS request. Hence, it is also necessary for the service layer to inform the transport layer of the QoS requirements of the service flow.

A dynamic and per-session QoS control architecture should be able to make efficient use of network resource and avoid the occurrence of bandwidth contention, especially to those real-time services and multimedia services that consume bandwidth greatly. For this purpose, it should support admission control for a service flow with QoS requirements based on user profiles, SLA, operator policy rules and network resource availability. Network topology and resource attributes collection function is required for checking network resource availability. Traditional policy control framework defined by IETF RFC2753 only makes admission control at per-user or per-network level based on SLA and policy rules.

9 Reference architecture for support of dynamic and per-session QoS control

Figure 3 illustrates a reference architecture for support of dynamic and per-session QoS control over Ethernet-based IP access network.

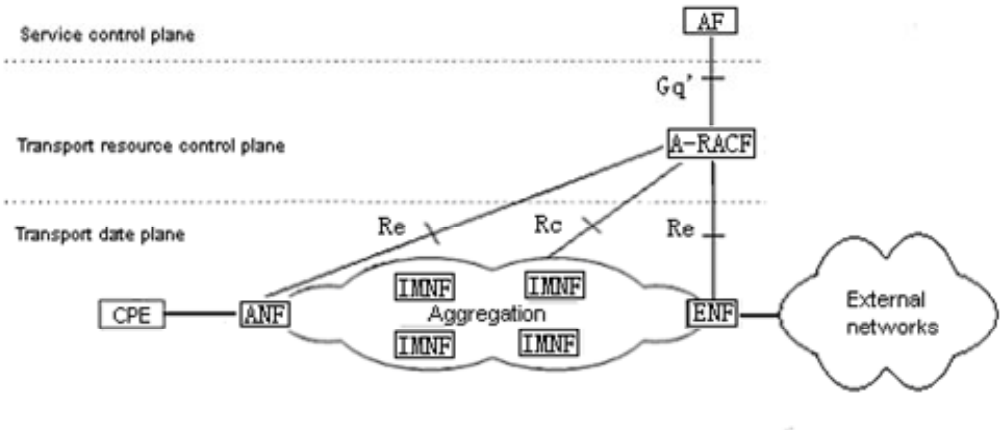


Figure 3 – Reference architecture for support of dynamic and per-session QoS control

The reference architecture consists of three planes: Service control plane, Transport resource control plane and Transport data plane. Such a clear separation between the planes allows different applications over a single access network being independent of different access technologies, and also allows new applications to be added quickly as long as the network resources are available.

Service control plane comprises the application functions (AF) dealing with service requests. AF determines the QoS requirements (including bandwidth and QoS classes) of each service flow by inspecting the service type or user explicit QoS request in application layer signalling (e.g. in SDP) or transport layer signalling (e.g. RSVP). It then sends the resource request to the Access Resource and Admission Control Functional entity (A-RACF) via the Gq' interface. AF is service specific and may be realized in any service subsystems offering services that require the control of IP bearer resources, e.g. IP multimedia subsystem. AF is a

logically independent function that may be implemented as a stand-alone box or as a function module embedded in other equipment.

Transport resource control plane comprises Access Resource Control Functional entities (A-RACF) dealing with resource requests containing specific QoS requirements for IP flows. A-RACF makes admission control, route determination and resource allocation for the resource request of a service flow based on user profile, SLA, operator policy rules and network resource availability. A-RACF is also a logically independent function that may be implemented as a stand-alone box or as a function module embedded in other equipment.

Transport data plane comprises an Ethernet-based IP access network infrastructure, which includes three types of entities: ENF, ANF and IMNF.

ENF (Edge Node Functional entity) is the functional entity in an IP access network acting as the upstream traffic egress that connects the IP access network to the external networks. It shall be a Layer 3 device with IP routing capabilities.

ANF (Access Node Functional entity) is the functional entity in an IP access network that directly connects to CPN and terminates the last mile link signals at the network side. Generally, it is a Layer 2 device that may be IP capable.

IMNF (Intermediate Node Functional entity) refers to all the functional entities between ENF and ANF in an Ethernet-based IP access network. Generally, it is an Ethernet switch.

CPE (Customer Premises Equipment) refers to all the devices in a CPN. It generally is a customer terminal, e.g. Ethernet phone or Media Gateway. If a CPN is composed of Layer 2 switches and customer terminals, the CPN should be able to forward customer packets without congestion, and ensure the QoS of the customer flows within the CPN.

For support of relative QoS, A-RACF configures L2/L3 QoS parameters and behaviours of ANF, IMNF and ENF at per-user or per-network level respectively via interfaces Re and Rc to enforce its admission control decision. ANF and ENF shall classify, mark, police, shape, queue and schedule the traffic entering and leaving the access network according to the QoS configuration. The interface requirements of Re and Rc for support of relative QoS should conform to the policy control framework defined by IETF RFC2753.

For non session-oriented services with relative QoS requirements, the same architecture is applicable. SLA between customer and provider is viewed as a static and manual service request for data delivery quality, and network administrators serve as AF. For automatic and dynamic SLA negotiation and management, web application or other means could be used.

For support of absolute QoS, bandwidth contention and traffic congestion within the network must be avoided, besides bandwidth policing and traffic shaping at the edge of the network. There are two ways for this purpose. One way is to use a certain resource reservation protocol (e.g. RSVP-TE) to setup logical network connections (e.g. LSP) and give A-RACF the full awareness of the topology, bandwidth and QoS attributes of these connections. A-RACF makes admission control based on this awareness to ensure that sufficient resources are available within these connections for the happening service flows with absolute QoS requirements. Since usually most nodes within an access network are non IP-capable and non MPLS-capable, the alternative way is to give A-RACF the full awareness of a logical tree-based network topology and link resource attributes of the whole access network. A-RACF makes admission control based on this awareness to ensure that sufficient resources are available within the network for the happening service flows with absolute QoS requirements. The logical tree-based network topology can be achieved by running STP (Spanning Tree Protocol) or configuring VLANs. To enforce its admission control decision for providing absolute QoS, A-RACF shall also make gate control at ANF and ENF at per-flow level via the interface Re, besides configuring L2/L3 QoS parameters and behaviours at per-user or per-network level at the access network nodes. In this context, gate means packet filtering at IP flow level.

10 Procedures for support of dynamic and per-session QoS control

This section defines the procedures that can be applied in the reference architecture for support of dynamic and per-session QoS control.

10.1 Network topology and resource attributes collection

Topology and resource attributes of an Ethernet-based IP access network can be obtained by means of static configuration or dynamic collection. In the case of dynamic collection, the information can be acquired from the MIBs of the network nodes via a certain protocol and then sorted together. The logical connection state is available in the VLAN MIB and MPLS MIB. The spanning tree state is available in the Bridge MIB. The link speed is available in the Interface MIB. The adjacent device connectivity is available in the LLDP MIB (Link Layer Discovery Protocol defined by IEEE 802.1ab). The acquired network topology and resource attributes, as well as the resource allocation status are stored in the network topology and resource database (NTRD), which is generally maintained on A-RACF. Flow admission control, route determination and resource allocation are done on the basis of user profiles, SLAs, operator policy rules and NTRD.

10.2 Resource allocation

This section introduces the procedure of resource allocation as illustrated in Figure 4.

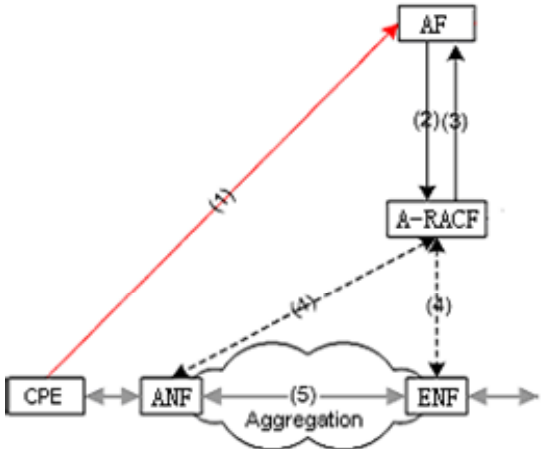


Figure 4 – The resource allocation procedure

(1) Service Request. A terminal or application gateway/server sends a service request to AF through a signalling protocol (e.g. SIP or H.323). A resource request is triggered by the service request. Service requests are various and application-specific.

(2) Resource Request with specific QoS requirements. AF sends a resource request containing the parameters such as the IP address of the customer terminal, flow description, bandwidth demand and priority to A-RACF.

(3) Admission Control and Resource Allocation. A-RACF finds the path of the flow according to the NTRD and IP address of the source terminal, and judges whether or not there is enough network resource for the flow to access. If there is, A-RACF sends an access admission response to AF and marks this part of the resource as occupied in the network topology and resource database; if there is not, the access is denied and the admission control procedure terminates.

(4) QoS Parameters Configuration. A-RACF sends the flow description, bandwidth and priority of 802.1p to ANF. If the service is bi-directional, A-RACF should also send flow description, bandwidth limitation and priority of the flow to ENF.

(5) Flow Identification, Classification, Marking and Forwarding. ANF identifies a service flow according to the flow description, classifies the flow packets, limits the bandwidth of the flow, marks and forwards the packets according to its priority. The intermediate devices forward packets according to priority too. Unidentified packets, which don't match any flow description configured at ANF, are not assured to be forwarded with their original priority if any value was set and may be treated as best-effort packets. If the service flow is bi-directional, ENF performs the same procedures with ANF.

10.3 Resource release

This section introduces the procedure of resource release as illustrated in Figure 5.

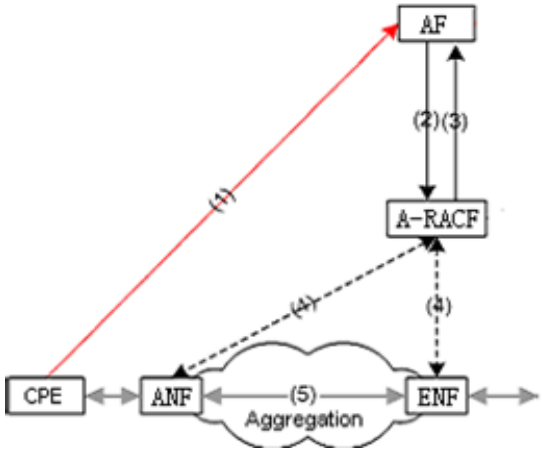


Figure 5 – The Resource Release procedure

(1) Service Release Request. A terminal or application gateway/server sends a service release request to AF. A resource release request is triggered by the service release.

(2) Resource Release Request. AF sends a resource release request containing the parameters of the IP address of the source terminal and the flow description to A-RACF.

(3) Resource Release. The resource occupied by the flow is marked as idle in network topology and resource database, and an acknowledgement is sent to AF.

(4) Removal of QoS Parameters Configuration. A message containing flow description is sent to ANF, and then the device removes the identification and classification of the flow. The flow is regarded as best-effort traffic. If the service flow is bi-directional, ENF performs the same procedures with ANF.

11 Interface requirements

This section defines the interface requirements for support of dynamic and per-session QoS control.

11.1 Interface between A-RACF and Access Network Nodes (Rc)

The A-RACF interacts with the access network nodes through the interface Rc. The main function of this interface is to gather information on resource attributes and network topology. Network topology and

resource attributes collection is the basis for making flow route determination, admission control and resource allocation for support of dynamic and per-session QoS control.

This interface should meet the following requirements.

(1) It should be able to timely and accurately gather the link layer topology and resource attributes.

(2) It should be able to timely and accurately track the changes of the link layer topology and resource attributes.

(3) It should be able to timely and accurately gather the topology and resource attributes of the logical network connections (e.g. LSP, VLAN).

(4) It should be able to timely and accurately track the changes of the topology and resource attributes of the logical network connections.

11.2 Interface between AF and A-RACF (Gq')

The interface between service control plane and transport resource control plane is very important. Since a lot of IP service port numbers are determined through dynamic negotiation in the service control plane, if without the information from AF, it is very difficult for layer 2 network devices by themselves to dynamically identify all of the happening flows. Static configuration at per-flow level is unpractical. Only after AF informs the transport layer of the flow description, can the problem be effectively solved. Meanwhile, it will be beneficial to service charging since the QoS parameters of the service flow are determined by the service control plane. Hence, it is necessary for the service layer to inform the transport layer of the QoS requirement parameters of an IP service flow.

This interface should support the following functions.

(1) Allow AF to initiate a resource allocation request to A-RACF for an IP service flow. This request may include flow identifier and QoS parameters (including bandwidth and QoS classes). The QoS classes may use those defined in Y.1541.

According to the resource allocation request with specific QoS requirements, A-RACF allocates the network resource for the IP service flow.

(2) Allow AF to send A-RACF a resource modification request for an IP service flow

For some kinds of services, it may be necessary to modify the QoS requirement during the running of a service flow. According to the resource modification request, A-RACF modifies the bandwidth and priority previously allocated. Modifications can happen multiple times.

(3) Allow A-RACF to send AF an acceptance response for a resource allocation request or a resource modification request

Upon success in resource allocation or modification, A-RACF shall send an acceptance response to AF.

(4) Allow A-RACF to send AF a rejection response for a resource allocation request or a bandwidth modification request

Upon failed to meet a resource request or a bandwidth modification request, A-RACF shall send a rejection response to AF.

(5) Allow AF to initiate a resource release request to A-RACF for an IP service flow

When a service flow is terminated, AF shall initiate a resource release request to A-RACF. According to the resource release request, A-RACF idles the allocated resource and sends back a resource release confirmation to AF.

(6) Allow AF to send A-RACF a resource allocation status query for an IP service flow

In case of any change of network resource attributes (e.g. a link or a virtual connection is no longer available due to failure), AF should be allowed to query A-RACF the resource allocation status for an IP service flow.

(7) Allow A-RACF to send AF a resource allocation status report for an IP service flow

In case of any change of network resource attributes (e.g. a link or a virtual connection is no longer available due to failure), A-RACF should be allowed to report the resource allocation status to AF for an IP service flow.

11.3 Interface between A-RACF and ENF/ANF (Re)

When a service flow is admitted, A-RACF informs ENF and/or ANF of the flow description, priority and bandwidth limitation parameters. When releasing service connection, A-RACF informs ENF and/or ANF to remove the flow identification and mark, and then the flow is regarded as best-effort.

This interface should support the following functions.

(1) Allow A-RACF to instruct ENF/ANF to perform the flow identification and the specified QoS treatment for an IP service flow.

According to the resource allocation request from AF, A-RACF makes resource admission control, routing control, forwarding priority control and media resource control for the service flow. To implement the above control, A-RACF must send a QoS installation instruction to ENF/ANF to install their QoS configuration and behaviours.

(2) Allow A-RACF to instruct ENF/ANF to modify the specified QoS treatment for an IP service flow.

According to a resource modification request from AF, A-RACF modifies the resource allocation for the service flow during its running. To implement the above modification, A-RACF must send a QoS modification instruction to ENF/ANF to modify their QoS configuration and behaviours.

(3) Allow A-RACF to instruct ENF/ANF to cancel the specified QoS treatment for an IP service flow

According to a resource release request from AF, A-RACF idles the resource allocated for the service flow. To implement the release, A-RACF shall send a QoS cancellation instruction to ENF/ANF to delete the QoS configuration and behaviours for the flow.

(4) Allow ENF/ANF to send A-RACF a QoS configuration response for a QoS installation/modification/cancellation instruction.

12 QoS parameters

As described above, AF determines the QoS requirements (including bandwidth and QoS classes) of each service flow based on service type or user explicit QoS request. It then sends the resource request to the access resource control function (A-RACF) via the Gq' interface. A resource request shall contain at least the following information for A-RACF to make resource and admission control.

(1) Flow identifier (to uniquely identify a flow within a session)

(2) Flow direction (uplink/downlink/bi-directional)

(3) Flow description (IPv4 5-tuple or IPv6 3/5-tuple)

(4) Maximum and mean bandwidth required

(5) QoS classes (to indicate the service type)

When a service flow is admitted, A-RACF sends the gate control instruction to ANF and/or ENF across the Re interface. A gate control instruction shall also contain at least the above information for ANF and/or ENF to enforce the gate function.

There are two options for the QoS classes exchanged across the Gq' and Re interfaces: Y.1541 and 3GPP TS29.207.

For end-to-end data delivery with QoS assured in the transport data plane, ANF and ENF should be able to support the mapping between service QoS classes (defined respectively in Y.1541 and 3GPP TS29.207), IP DSCPs, 802.1p priorities, and MPLS EXP bits.

Appendix I provide several QoS parameter mapping examples for reference.

13 Operation scenarios

For operational flexibility and gradual deployment, the mechanism is slightly restrictive in terms of admission control. There are some access network operation scenarios for which simplified admission control could work.

Assume that all IP flows are forwarded through one Edge Node. Then the access network looks like a star topology consisting of pipes between the ENF and each ANF.

Scenario 1: If assume that the bandwidth per pipe is reserved and guaranteed, we do not have to care about the topology of the access network, and admission control can be simplified. For example, A-RACF can perform admission control based on the reserved bandwidth for the user (i.e. the pipe), the total bandwidth of the existing connections over the pipe, and the bandwidth of the newly requested connection.

Scenario 2: If assume that the bottleneck of the bandwidth is limited, such as the link between the Edge Router and the first L2 switch, we do not have to care about the resources of other links in the access network, and again admission control can be simplified. For example, A-RACF can perform admission control based on the provisioned bandwidth for such bottleneck link, the total bandwidth of the existing connection over the link, and the bandwidth of the newly requested connection.

14 Security considerations

The QoS architecture described in this recommendation enhances the security of Ethernet-based IP access network and does not raise any new security issues.

VLAN may be configured to separate voice and video service flows from Internet data traffics, which makes it possible for the well-known multimedia application ports to be invisible to the Internet. It is helpful to protect voice and video services against viruses and simple attacks.

Network topology and resource attributes collection can help network administrators locate illegal access nodes and link failures. Moreover, private IP addresses may be assigned to access devices, which makes intermediate access devices invisible to the external networks and as such is helpful for protecting the access devices against attacks from the external network.

Resource requests are initiated by service control function instead of by hosts, which prevents the happening of the malicious resource requests and the resulting excessive resource reservation, exhaustion and even DoS (denial of service). All resource requests are triggered by the service requests that have been authenticated and authorized.

Admission control is helpful for protecting an access network against fabrication attacks, unauthorized traffic and the resulting congestion. Traffic marking is done by access nodes and edge routers. And the mark is trusted and reused by intermediate devices.

The signalling for IP QoS across the Gq', Re and Rc is out-of-band and path-decoupled, which can be delivered on the dedicated link with security encryption. Access nodes, edge routers and service control function should protect themselves from DoS attacks.

Still, the conventional network security mechanisms such as firewalls, intrusion detection software (IDS) and proxies are used against network attacks. If needed, authentication and integrity mechanisms can be used to protect signalling against interception, modification and fabrication attacks.

Appendix I

QoS class mapping examples

In this appendix, the mapping between 3GPP TS29.207 and Y.1541 QoS class refers to the relevant work progress on this matter within 3GPP and ITU-T.

Table I-1 provides an Y.1541 QoS class to IP DSCP mapping example extracted from Appendix VI of Y.1541.

Table I-1 – Y.1541 QoS class to IP DSCP mapping

IP DSCP	Y.1541 QoS class	Remarks
BE	Unspecified QoS class 5	A legacy IP service, when operated on a lightly loaded network may achieve a good level of IP QoS
AF	QoS classes 2, 3, 4	The IPLR objective only applies to the IP packets in the higher priority levels of each AF class. The IPTD applies to all packets
EF	QoS classes 0 and 1	

Table I-2 provides an 802.1p priority to IP DSCP mapping example.

Table I-2 – 802.1p priority to IP DSCP mapping example

802.1p priority	IP DSCP
7	CS6 (Class Selector 6)
6	EF
5	AF41
4	AF31
3	AF21
2	AF11
1	-
0	BE

Table I-3 provides an IP DSCP to MPLS EXP mapping example for E-LSP.

Table I-3 – IP DSCP to MPLS EXP mapping example for E-LSP

IP DSCP	MPLS EXP
CS6, CS7	111
EF	110
AF41	101
AF31	100
AF21	011
AF11	010
-	001
DF	000

2.8 – Multi Service Provider Interface for IP QOS – Architecture and Requirements*

Summary

This draft focuses on the required functions and procedures necessary for support of for Multi Service Provider Network to Network Interface for support of IP Quality of Service (QoS).

Multi Service Provider Network to Network (NNI) interfaces may support different higher layer services. To ensure that public networks will interwork with each other supporting a set of services, this draft specifies the Network to Network Interface (NNI) for IP QOS between Network Operators. This will enable next generation of IP based networks as global telecom infrastructure.

It specifies requirements for Inter-Service Provider (Network Operator) interoperability and service provisioning at the NNI.

Table of Contents

* Status S: The FGNGN considers that this deliverable has reached a mature state but would require further consideration in Study Group 13.

2.8 – Multi Service Provider Interface for IP QOS – Architecture and Requirements

1 Scope

This draft focuses on the required functions and procedures necessary for support of for Multi Service Pronnnvider interface for support of IP Quality of Service (QoS).

A standardized IP QOS across service provider boundaries will be needed to support different services. To ensure that IP QOS based networks will interwork with each other supporting a set of services, this draft specifies the network-to-network interfaces between network operators.

It supports the following objectives of the Next Generation Network:

- In a multi-service provider network, a specific objective is to define and facilitate Interoperability between networks
- End-to-end IP QOS

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this draft. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this draft are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this draft does not give it, as a stand-alone document, the status of a Recommendation.

[1] IETF, RFC 2474, *Definitions of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*

[2] IETF, RFC 3032. MPLS Label Stack Encoding

[3] IETF, RFC 3031. Multiprotocol Label Switching Architecture

[4] Rec. G.1000, Communications Quality of Service: A Framework and Definition

[5] Rec. E.800, Terms and Definitions Related to Quality of Service and Network Performance Including Dependability (08/94)

[6] Rec. Y.1291, An architectural framework for support of Quality of Service (QoS) in Packet networks (from Q.16/13)

[7] Rec. Y.1540, IP Packet Transfer and Availability Performance Parameters

[8] Rec. Y.1541: Network Performance Objectives for IP-based Services

[10] Rec. Y.1221: “traffic contract” complements QoS class by describing flow characteristics/limits (from SG 13)

[11] 3GPP 23.207. End-to-End Quality of Service (QoS) concept and architecture (Release 6)

[12] 3GPP2 S.R0035. Quality of Service. Stage 1 Requirements

[15] 3GPP TS 26.236 version 5.4.0 Release 5: Universal Mobile Telecommunications System (UMTS); Packet switched conversational multimedia applications; Transport protocols [16] Rec. G.1010 "End-user multimedia QoS categories": from Q.13/12

[16] Rec. H.360 (from Q.H/16), An Architecture for End-to-End QoS Control and Signalling

[17] PacketCable, Dynamic Quality-if-Service Specification, PKT-SP-DQOS1.45-I02-050812

3 Definitions

This draft defines or uses the following terms:

4 Abbreviations

This draft uses the following abbreviations.

AF assured forwarding

DS differentiated services

E1 Digital Hierarchy Transmission at 2.048 Mbit/s

EF expedited forwarding

IDQ Inter-domain QoS

IP Internet protocol

IPDV IP packet delay variation

IPER IP packet error ratio

IPLR IP packet loss ratio

IPTD IP packet transfer delay

NNI Network to Network interface

PDB per domain behavior

PHB per hop behavior

QoS quality of service

T1 Digital Hierarchy Transmission at 1.544 Mbit/s

ICI Inter Carrier Interface

5 Conventions

–

6 Multi Service Provider (Network Operator) Interfaces Architecture

Figure 6-1 provides a general network architecture and interface at which the functions are described in this draft. Multi service provider networks encompassing different transport technologies, services and applications will need to be interoperable.

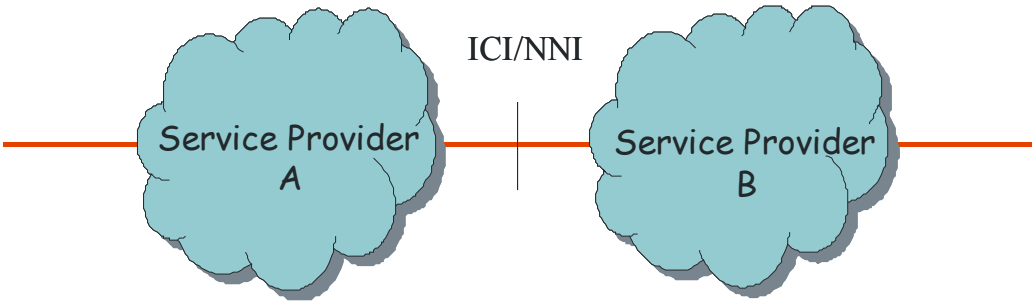


Figure 6-1 – Scope of Multi-Service Provider Interfaces

Editor's Note: The term ICI will be used rather than NNI.

The ICI consists of data, control and management plane aspects with the additional consideration of security.

7 Requirements

Solution requirements and constraints for Inter-Domain QoS (IDQ) must be understood prior to development and design, and kept in mind during development and design. This section lists the requirements gathered for Service Providers and their Customers. These needs include those required to design a working system and those that make it deployable.

Some of these needs are listed below, together with key recommendations. This list of needs may appear to be lengthy, but as made clear by the 7x11 QoS matrix given by ITU-T Rec. G.1000 (see Annex), capturing all of the elements that can affect QoS involves many items.

7.1 SPs needs

1) Agreement of consistent Service Specifications
2) Agreement of consistent minimum Service Class definitions
3) Defined impairment targets across each SP
4) Minimize impact to existing SP operations
5) Place as few restrictions on each SP as feasible – preserve flexibility
6) Clearly defined interfaces with other SPs and its customers
7) Flexible low overhead measurement system
8) Tools to support operation
9) A management system to support operation
10) Wide applicability
11) Clearly stated responsibilities of terminating and transit SPs

7.1.1 Agreement of consistent Service Specifications

A commonly defined and agreed upon set of service specifications are needed to enable concatenation of service from multiple providers to deliver an IDQ service. These specifications form the technical agreement

between Providers and their customers. In essence, if a customer's egress traffic conforms to the agreed bandwidth (measured using a "standard" method) for a Service Class, then the Provider will deliver that traffic meeting the performance of that Service Class to another subscriber.

7.1.2 Agreement of consistent minimum Service Class definitions

Rather than offer Services based upon a set of values for several network metrics, Service Classes such as "low latency" are typically being offered by SPs for services offered within their domain. Each Service Class is associated with a set of values for those metrics. However, many SPs have different definitions which complicate Inter-domain QoS. Furthermore, there are many possible Service Classes. An agreement of a minimum set of Service Classes to be supported together with their method of identification and performance is required. Additional Service Classes may be added over time or by SPs that wish to offer them for differentiation purposes.

Key Recommendation: An initial set of Service Classes should be selected using criteria of their known demand, well understood applications, and customer perceived value.

7.1.3 Impairment targets

Impairment targets for the selected metrics must be well specified for each SP along the delivery path. It is expected that certain metrics will not be concatenatable by simple addition, and that new methods will be required.

Key recommendation: Any Delay metric should be determined in part by the distance between an SP's ingress and egress routers.

7.1.4 Minimize impact to existing SP operations

- Maximize the use of existing infrastructure
- Minimize incremental traffic overhead – control, measurement, management, etc.
- Maintain privacy
- Maintain security levels.

A solution should not require hardware changes to network equipment (routers, switches, modems, etc.). New/changes to protocols and/or network equipment software, tools, and management systems should be minimized.

Providers must be able to choose their own implementation mechanisms, ranging from simple over-provisioning to more complex traffic engineering and scheduling methods

Only a small percentage of available network capacity should be allocated to use for IDQ overhead purposes. For a customer link consider the percentage required of a 64kbps capacity link. For other points in the network, consider the aggregate percentage.

Certain information about topology and performance is expected to be sensitive. It may be necessary to restrict the accessibility to this information, or to provide a scheme which hides actual information.

The solution should not decrease the level of security, including making "hard-to-get" information "easy-to-get".

7.1.5 Preserve flexibility

- Supports multiple Service Levels
- Provides for differentiation of services among Providers
- Incrementally deployable

- Deployable as both SP "managed" and "un-managed" services
- Provides for both dynamic and static bandwidth reservations
- Provides for flat subscribed and usage based, and does not prevent destination based billing

The solution must be flexible enough to be able to offer multiple service levels. Service Levels typically include Service Specification (Bandwidth and scope of each Service Class), Report, Cost, Support, etc. The minimum characteristics of service levels should be defined. The number of Service Levels should not be so large as to confuse customers.

While a common minimal level of service is required across SPs, their ability to compete must be maintained. Differentiation is expected by such factors as

- Better than minimum required performance
- Better than minimum required service levels
- Offering of all defined service classes
- Offering of additional service classes
- Better customer support
- Better than minimum required reporting

It is expected that deployment will start in a limited way. Most likely limited to small parts of the few participating SPs offering few Service Classes. Any solution must allow for deployment to be easily increased over time.

The solution must support services that terminate at Provider Edge devices, or Customer Edge devices, or at a customer's host system. Traffic between two PEs is known as edge-to-edge, between two CEs as end-to-end, and traffic between two customer's host systems is known as host-to-host. Managed services may include those offering termination at a CE or a customer's host system.

Static bandwidth reservation is pre-provisioned using traditional SP techniques. For example, a customer may buy 4Mb/s VoIP, 6 Mb/s Low Latency, 8 Mb/s Multimedia, and 30Mb/s Best Effort on a link which is provisioned on a yearly basis. Dynamic bandwidth reservation is provisioned in real-time based upon customer need.

The pricing model for the sender is based on bandwidth per service class. The Service Provider will set those prices and may use a flat rate per unit of bandwidth or a specific rate for specific bandwidth increments. The solution should not prevent a Service Provider's pricing to be different for traffic that is within a region compared with traffic that is destined for other global destinations.

7.1.6 Clearly defined interfaces with other SPs and its customers

- Protect SPs from non-compliant traffic
- Provide interfaces for control, measurement, management, and business processes

Each SP will offer Service Specifications for each Service Class with other SPs and its customers. The Service Specifications include ingress and egress bandwidth for each Service Class. In both cases, each party has obligations about which they should be monitored and receive reports. In order to protect itself from receiving more traffic than contractually agreed, policing must be conducted. In the case of receiving traffic which exceeds the contacted amount, action must be taken to protect an SP. That action must be well specified. Typically obligations during the period when non-compliant traffic is ingressing a SP will differ from "compliant" periods.

Key recommendation: When traffic that is marked for a certain service is received from a customer who has not subscribed to that service, the provider must take steps to ensure it does not interfere with legitimately marked traffic both in the provider who receives it and in subsequent providers.

Key recommendation: Policing using defined methods must occur at all SP edges.

Requirements for control, measurement, management, and business process interfaces are yet to be determined.

7.1.7 Flexible low overhead measurement system

- Highly scalable
- Uses consistent performance parameter measurement metrics
- Use consistent measurement timescales
- Generate measurements of the network impairments metrics which can be concatenated to closely approximate overall performance
- Monitor to assure delivery
- Monitor to determine network compliance
- Monitor for problem resolution
- Generate assured data for prospective customers
- Provide methods for prospective customers to see what performance they could expect if they subscribed

Key choices for a measurement system are

A. Passive measurement of actual User traffic or Active measurement by the use of special probes

B. Performance metrics

C. Timeframes for a time reference (the same start time is used for measurement intervals to allow correlation of information from different providers), for mean inter-probe time, for "roll-up" time (can't have one provider measure delay variation over a month and another measure it over 15 minutes) and reporting times

D. Positioning of measurement points. Imagine a full worldwide mesh of CE-CE probes, this would not be scalable, whereas a network model that segments the network and defines the positioning of measurement points would be scalable if it enabled probes to be re-used.

Key recommendations:

A. Active probes should be used, with each probe being highly leveraged for multiple purposes where possible.

B. One-way metrics should be used. These should include Loss ratio, Mean Delay, statistical Delay Variation, and a metric which measures the amount of loss within a short period of time (suggest we call this metric "Availability").

C. Time should be referenced to UTC including accuracy, the other timeframes should be selected using the criteria below

D. Measurement points should be positioned with either the customer's edge router or the SP's edge router, plus peering points and other locations

The selection of timescales for performance measurement should be determined by the following criteria:

- The measurement overhead traffic must be kept at a low level
- The measurement and scalability requirements must be achievable on current hardware
- The basic timescale must be large enough to contain the start and end of a large number of traffic flows
- The basic timescale must be common and synchronized globally among SPs

- The timescale must be meaningful to network users and capture any productivity or service quality issues they perceive in the network.
- The timescales should not unduly emphasize momentary glitches such as link outages or re-routing events where they do not significantly impact network user experience.

7.1.8 Tools to support operation

It is likely that a solution will require either or both directory based and network based discovery tools. For example, tools will be required to discover the participating SPs, their management systems and network equipment, which service classes they support, and whether a particular service class is supported by all SPs along multiple delivery paths. Discovery of destination customer subscription may also be desirable.

7.1.9 A Management system to support operation

- Manages the initiation, aggregation, storage, analysis and reporting of measurements
- Provides support for billing and settlements
- Provides support for inter-SP communications
- Provides support for directory-based lookup of shared information

These requirements are self-explanatory

7.1.10 Widely Applicable

- to both private and public networks
- independent of the underlying transport mechanism (eg MPLS, ?, etc)
- independent of the underlying method of QoS delivery (eg by overbuilding or traffic engineered)
- independent of unicast or multicast
- supports differing time-zones
- supports any geographical distance
- Easily scalable to many SPs

These requirements are self-explanatory

7.1.11 Clearly Stated Responsibilities

Responsibilities of SPs are expected to differ depending upon whether they are providing service to the customer (terminating) or only other SPs (transit). Example responsibilities are

- Provide information regarding network devices, measurement devices, peering points, and customer subscriptions.
- Support required performance characteristics of each Service Class
- Route IDQ traffic preferentially to other IDQ providers
- Interconnect with majority of other providers that support IDQ
- Supply measurement points
- Monitor measurements taken
- Cooperate in troubleshooting with other IDQ SPs
- Take responsibility for sizing the interconnect with the backbone providers
- Publish reports

7.2 Customer needs

- Commonly understood performance across supported service classes
- Use of consistent metrics which reflect network impact on Users' applications
- "Standard" minimum common reporting
- Consistent provisioning of site-to-site services with QoS
- Similar offered service levels
- Maintain Privacy

7.2.1 Commonly Understood Performance across Supported Service Classes

The offering of common service classes would promote a consistent expectation of performance across locations, providers, and over time.

7.2.2 Use of Consistent Metrics which Reflect Network Impact on Users' Applications

Consistent metrics will promote comparison of offerings, and increase understanding of what values of each are required for User's applications.

7.2.3 "Standard" Minimum Common Reporting

A common minimum report offered by multiple SPs for a particular Service Level would promote ease of understanding no matter which SP was their provider. Additional reporting over the minimum could offer differentiation. Elements of a minimum report should include

- Subscription
- Target Performance
- Measured Performance
- Network Compliance
- Customer Compliance

with incremental content for each successive service level

Information on customer compliance is included to indicate time periods when the SP's performance guarantee was not in effect due to customer non-compliance.

It encourages customers to subscribe to the appropriate bandwidth level for more reliable service

7.2.4 Consistent provisioning of site-to-site services with QoS

A consistent performance experience for applications will promote greater confidence in the offered service.

7.2.5 Similar offered service levels

Common minimum service level offered by multiple SPs at every location which would enable customer multi-homing to multiple SPs and support the ability of the customer to fail-over or distribute traffic to another SP while maintaining the same QoS.

7.2.6 Maintain Privacy

Customers should be given the option of restricting information regarding their subscription, connectivity performance and topology, and traffic usage to others.

8 Network to Network (NNI) Interface specifications

The Multi-Service Provider NNI interface includes support of the following capabilities.

8.1 Data QoS Aspects – Markings

Requirements are extracted from Y.1541 section 5.3.1; (table1 appears after section 5.3.4 of Y.1541). The text below is placed for convenience and can be removed with appropriate references.

The objectives in Table 1 apply to public IP networks, between MPs that delimit the end-to-end IP network. The objectives are believed to be achievable on common implementations of IP Networks.

The left-hand part of Table 1 indicates the statistical nature of the performance objectives that appear in the subsequent rows.

The performance objectives for IP packet transfer delay are upper bounds on the underlying mean IPTD for the flow. Although many individual packets may have transfer delays that exceed this bound, the average IPTD for lifetime of the flow (a statistical estimator of the mean) should normally be less than the applicable bound from Table 1.

The performance objectives for 2-point IP Packet Delay Variation are based on an upper bound on the $1\text{-}10^{-3}$ quantile of the underlying IPTD distribution for the flow. The $1\text{-}10^{-3}$ quantile allows short evaluation intervals (e.g, a sample with 1000 packets is the minimum necessary to evaluate this bound). Also, this allows more flexibility in network designs where engineering of delay buildout buffers and router queue lengths must achieve an overall IPLR objective on the order of 10^{-3}. Use of lower quantile values will result in under-estimates of de-jitter buffer size, and the effective packet loss would exceed the overall IPLR objective (e.g., an upper quantile of $1\text{-}10^{-2}$ may have an overall packet loss of 1.1%, with IPLR=10^{-3}). Other statistical techniques and definitions for IPDV are being studied as described in Appendix II, and Appendix IV discusses IPDV performance estimation.

The performance objectives for the IP packet loss ratios are upper bounds on the IP packet loss for the flow. Although individual packets will be lost, the underlying probability that any individual packet is lost during the flow should be less than the applicable bound from Table 1.

Existing standards specify several metrics and measurement methods for point to point performance. Notable are the ITU-T Y.1540 and Y.1541 standards and the IETF IP Performance Metrics (IPPM) Working Group standards. However, many options and parameters are left unspecified, as are concatenation of performance over multiple network segments, allocation of impairment targets, mapping between IP and non-IP metrics, accuracy, and data handling. Each of these topics must be specified in order to support QoS across multiple heterogeneous Service Providers.

The NGN FG is working to extend the existing standards and to provide standards that cover these additional topics.

Regarding network performance metrics, the IPDV has been modified to reference the mean delay rather than the minimum.

A new metric has been added named Unavailability. Unavailability is significant when a human observer detects a business impacting application failure due to network loss. For a typical application such as telephony, a network is considered unavailable by the user if there is an inability to connect, or a connection is lost. The measurement of unavailability attempts to approximate this view by detecting periods during which network unavailability would have noticeable impacts on applications and individual or business productivity. Unavailability is calculated from the distribution of loss measurements over time.

Table 1/Y.1541 – Provisional IP QoS class definitions and network performance objectives

		QoS Classes					
Network Performance Parameter	**Nature of Network Performance Objective**	**Class 0**	**Class 1**	**Class 2**	**Class 3**	**Class 4**	**Class 5 Un-specified**
IPTD	Upper bound on the mean IPTD (Note 1)	100ms	400ms	100ms	400ms	**1 s**	U
IPDV	Upper bound on the 1-10^{-3} quantile of IPTD minus the minimum IPTD (Note 2)	50ms (Note 3)	50ms (Note 3)	U	U	U	U
IPLR	Upper bound on the packet loss probability	$1*10^{-3}$ (Note 4)	$1*10^{-3}$ (Note 4)	$1*10^{-3}$	$1*10^{-3}$	$1*10^{-3}$	U
IPER	Upper bound	$1*10^{-4}$ (Note 5)					U

General Notes:

The objectives apply to public IP Networks. The objectives are believed to be achievable on common IP network implementations. The network providers' commitment to the user is to attempt to deliver packets in a way that achieves each of the applicable objectives. The vast majority of IP paths advertising conformance with Recommendation Y.1541 should meet those objectives. For some parameters, performance on shorter and/or less complex paths may be significantly better.

An evaluation interval of 1 minute is provisionally suggested for IPTD, IPDV, and IPLR, and in all cases the interval must be reported.

Individual network providers may choose to offer performance commitments better than these objectives.

"U" means "unspecified" or "unbounded". When the performance relative to a particular parameter is identified as being "U" the ITU-T establishes no objective for this parameter and any default Y.1541 objective can be ignored. When the objective for a parameter is set to "U", performance with respect to that parameter may, at times, be arbitrarily poor.

All values are provisional and they need not be met by networks until they are revised (up or down) based on real operational experience

Note 1 – Very long propagation times will prevent low end-to-end delay objectives from being met. In these and some other circumstances, the IPTD objectives in Classes 0 and 2 will not always be achievable. Every network provider will encounter these circumstances and the range of IPTD objectives in Table 1/Y.1541 provides achievable QoS classes as alternatives. The delay objectives of a class do not preclude a network provider from offering services with shorter delay commitments. According to the definition of IPTD in Y.1540, packet insertion time is included in the IPTD objective. This Recommendation suggests a maximum packet information field of 1500 bytes for evaluating these objectives.

Note 2 – The definition and nature of the IPDV objective is under study. See Appendix II for more details.

Note 3 –This value is dependent on the capacity of inter-network links. Smaller variations are possible when all capacities are higher than primary rate (T1 or E1), or when competing packet information fields are smaller than 1500 bytes (see Appendix IV).

Note 4 – The Class 0 and 1 objectives for IPLR are partly based on studies showing that high quality voice applications and voice codecs will be essentially unaffected by a 10^{-3} IPLR.

Note 5 – This value ensures that packet loss is the dominant source of defects presented to upper layers, and is feasible with IP transport on ATM.

Each UDP echo based active probe which crosses the NNI will provide measurements towards all these metrics.

a) Mean delay and

b) Delay variation (90, 99 and 99.9 percentiles)

c) Unavailability

d) Loss Ratio

See FGNGN-OD-000xx, "Performance Measurements and Management for NGN" for further details

The following text and table 2 from Y.1541 section 5.3.6 gives some guidance for the applicability and engineering of the QoS Classes.

Table 2/Y.1541 – Guidance for IP QoS classes

QoS Class	Applications (Examples)	Node Mechanisms	Network Techniques
0	Real-Time, Jitter sensitive, high interaction(VoIP, VTC)	Separate Queue with preferential servicing, Traffic grooming	Constrained Routing and Distance
1	Real-Time, Jitter sensitive, interactive (VoIP, VTC).		Less constrained Routing and Distances
2	Transaction Data, Highly Interactive, (Signaling)	Separate Queue, Drop priority	Constrained Routing and Distance
3	Transaction Data, Interactive		Less constrained Routing and Distances
4	Low Loss Only (Short Transactions, Bulk Data, Video Streaming)	Long Queue, Drop priority	Any route/path
5	Traditional Applications of Default IP Networks	Separate Queue (lowest priority)	Any route/path

Traffic policing and or shaping may also be applied in network nodes.

The following text and table VI.1 from Y.1541 Appendix VI gives some guidance on Per Domain behavior.

A DS Region may contain one or more DS Domains (Network Sections), conforming to Per Domain Behaviors (PDB) [RFC3086]. PDB specifications are work in progress. One or more Per Hop Behaviors (PHBs) may be combined with other Diffserv tools (such as traffic conditioners) to construct Per Domain Behaviors. The currently defined Differentiated Services PHBs are Assured Forwarding (AF) [RFC2597] and Expedited Forwarding (EF) [RFC2598]. The AF specification defines a group of 4 AF classes that should be handled independently.

The following Table VI.1/Y.1541 associates the Y.1541 QoS classes to Integrated and Differentiated Services. This table assumes that all IP packets are in profile, when such a traffic profile is specified for the IP packet stream.

Table VI.1/Y.1541 – Possible Association of Y.1541 QoS classes with Differentiated Services

IP transfer service	IP QoS class	Remarks
Best Effort PDB	Unspecified QoS class 5	a legacy IP service, when operated on a lightly loaded network may achieve a good level of IP QoS
PDBs based on Assured Forwarding	QoS classes 2,3,4	the IPLR objective only applies to the IP packets in the higher priority levels of each AF class. The IPTD applies to all packets
PDBs based on Expedited Forwarding	QoS classes 0 and 1	

Based on the above information, the transmitting SP should appropriately signify or "mark" the QOS class and network performance objectives for the call. The receiving SP should honor the request. This can also be

accomplished in the control or signaling phase of the call or in appropriate markings in the user plane. The exact SLA between the SPs is implementation dependent.

8.2 Configuration of Interfaces (NNI)

8.2.1 Bandwidth

The following text is implied by note 3 in Table 1 of Y.1541

"Inter-network links need to be at least the primary rate (T1 or E1) so that delay objectives can be met".

However, it is recommended that each of these links be T3 or E3 rates since we are referring to optical network environments.

8.2.2 NNI Traffic Shaping Requirement

Traffic Requirements from section 8.7, Rec. Y.1291 shall apply at the NNI.

Traffic shaping deals with controlling the rate and volume of traffic entering the network. The entity responsible for traffic shaping buffers non-conformant packets until it brings the respective aggregate in compliance with the traffic. The resulted traffic thus is not as bursty as the original and is more predictable. Shaping often needs to be performed between the egress and ingress nodes.

There are two key methods for traffic shaping: leaky bucket and token bucket. The leaky bucket method employs a leaky bucket to regulate the rate of the traffic leaving a node. Regardless of the rate of the inflow, the leaky bucket keeps the outflow at a constant rate. Any excessive packets overflowing the bucket are discarded. Two parameters are characteristic to this method and usually user configurable: the size of the bucket and the transmission rate.

The token bucket method, on the other hand, is not as rigid in regulating the rate of the traffic leaving a node. It allows packets to go out as fast as they come in provided that there are enough *tokens*. Tokens are generated at a certain rate and deposited into the token bucket till it is full. At the expense of a token, certain volume of traffic (i.e., a certain number of bytes) is allowed to leave the node. No packets can be transmitted if there are no tokens in the bucket. Yet multiple tokens can be consumed at once to allow bursts to go through. This method, unlike the leaky bucket method, does not discard packets. Two parameters are characteristic to the token bucket method and usually user configurable: the size of the token bucket and the rate of token generation.

The leaky and token bucket methods can be used together. In particular, traffic can be shaped first with the token bucket method and then the leaky bucket method to remove the unwanted busts. Two token buckets can also be used in tandem.

By metering/monitoring the temporal properties (e.g., rate) of a traffic stream against the agreed traffic profile, a meter can invoke necessary treatment (e.g., dropping or shaping) for the packet stream.

Virtual circuits shall be over-engineered to meet the most stringent traffic forecasts between the interconnecting SPs.The exact requirements are service dependent between the interconnecting SPs; the SPs must agree on the use of one or both of the leaky and token bucket mechanisms and agree on

1. size of the leaky or token bucket
2. transmission rate
3. rate of token generation

8.2.3 QOS guarantee mechanism

The exact IP QOS guarantee mechanisms are service dependent. They are described in the subsequent sections. They will form part of the traffic SLA between the interconnecting SPs (Diff Serv./Int. Serv/MPLS)

8.2.4 Scheduling Mechanisms

Requirements from section 8.3 Rec. Y.1291 shall apply.

Queueing and scheduling control which packets to select for transmission on an outgoing link. Incoming traffic is held in a queuing system, which is made of, typically, multiple queues and a scheduler. Governing the queuing system is the queuing and scheduling discipline it employs. There are several key approaches:

– First-in, first-out queuing. Packets are placed into a single queue and served in the same order as they arrive in the queue.

– Fair queuing. Packets are classified into flows and assigned to queues dedicated to respective flows. Queues are then serviced in round robin. Empty queues are skipped. Fair queuing is also referred to as per-flow or flow-based queuing.

– Priority queuing. Packets are first classified and then placed into different priority queues. Packets are scheduled from the head of a given queue only if all queues of higher priority are empty. Within each of the priority queues, packets are scheduled in first-in, first-out order.

– Weighted fair queuing. Packets are classified into flows and assigned to queues dedicated to respective flows. A queue is assigned a percentage of output bandwidth according to the bandwidth need of the corresponding flow. By distinguishing variable-length packets, this approach also prevents flows with larger packets from being allocated more bandwidth than those with smaller packets.

– Class-based queuing. Packets are classified into various service classes and then assigned to queues assigned to the service classes, respectively. Each queue can be assigned a different percentage of the output bandwidth and is serviced in round robin. Empty queues are skipped.

The appropriate scheduling mechanism has to be selected between the interconnecting SPs to ensure IP QOS guarantees employed within their networks.

9 Routing

Requirements of Section 7.2 of Rec. Y.1291 shall be followed. The specific agreement between the interconnecting SPs is service dependent.

QoS routing concerns the selection of a path satisfying the QoS requirements of a flow. The path selected is most likely not the traditional shortest path. It is important to note that QoS routing provides a means to determine only a path that can likely accommodate the requested performance. To guarantee performance on a selected path, QoS routing needs to be used in conjunction with resource reservation to reserve necessary network resources along the path.

QoS routing can also be generalized to apply to traffic engineering. (Concerning slowly-changing traffic patterns over a long time scale and a coarse granularity of traffic flows, traffic engineering encompasses traffic management, capacity management, traffic measurement and modelling, network modelling, and performance analysis.) To this end, routing selection often take into account a variety of constraints such as traffic attributes, network constraints, and policy constraints [IETF RFC 3272]. Such generalized QoS routing is also called constraint-based routing, which can afford path selection to bypass congested spots (or to share load) and improve the overall network utilization as well as automate enforcement of traffic engineering policies.

Path selection, traffic management, capacity management, traffic measurement, network modelling and performance analysis based traffic adjustments are agreements between the interconnecting SPs to hold within the bounds of the min/max bounds of the IP QOS SLA between them.

10 Protocol Mechanisms Required

Requirements from section 12, Rec. Y.1291 shall apply. The appropriate protocol mechanisms from those listed below will be selected by the interconnecting SPs.

To illustrate how QoS building blocks interact and form various QoS approaches, this section describes three standardized approaches: integrated services (*IntServ*), differentiated services (*DiffServ*), and Multi-Protocol Label Switching (MPLS).

10.1 IntServ

Primarily for supporting real-time delay sensitive applications, the *IntServ* (see, e.g., [IETF RFC 1633]) approach is built on the understanding that a flow serviced at a rate slightly higher than its data rate has a bounded delay and the network can guarantee the delay bound of a flow by per-flow resource reservation. With this approach, an application, before sending data, first signals to the network the desired service request, including specifics such as its traffic profile and bandwidth and delay requirements. The network then determines whether it can allocate adequate resources (e.g., bandwidth or buffer space) to deliver the desired performance of the service request. Only after the request is granted can the application start to send data. As long as the application honours its traffic profile, the network meets its service commitment by maintaining per-flow state and by using advanced queuing disciplines (e.g., weighted fair queuing) for link sharing. The building blocks relevant to the *IntServ* approach include admission control, queuing, resource reservation, traffic classification, and traffic policing. In particular, the signalling protocol RSVP is used to reserve resources. The network may accept or reject a reservation request via admission control based on resource availability. A successful reservation request results in installation of states at the RSVP-aware nodes. The building blocks interact by having access to the state information and other provisioned (thus relatively static) data objects.

10.2 DiffServ

The concept behind the *DiffServ* approach is treating a packet based on its class of service as encoded in its IP header. The service provider establishes with each user a service level agreement (or service level specification), which, among other things, specifies how much traffic a user may send within any given class of service. The ensuing traffic is classified (on a per-packet basis) into one of a small number of aggregated flows or classes and policed at the border of the service provider's network. Once the traffic enters the network, routers provide it with differentiated treatment. In contrast to the *IntServ* approach, the treatment is based not on a per-flow basis, but solely on the indicated class of service. The overall network is set up so as to meet all service level agreements. The relevant building blocks (which include buffer management, packet marking, service level agreement, traffic metering and recording, traffic policing, traffic shaping, and scheduling) interact with each other in a relatively static way, primarily through provisioned data objects.

10.3 MPLS

Initially developed for the purpose of interworking between the IP and ATM (or Frame Relay) networks, MPLS [IETF RFC 3031] achieves substantial gains in packet forwarding speed through the use of short, layer-2-like labels. Upon entering the MPLS network, a packet is assigned once and for all a Forward Equivalence Class (FEC), which is encoded as a fixed length string known as a label. When the packet is forwarded to the next hop, the label is sent along with it. At the next hop, the label is used as an index into a

pre-configured table to identify the following hop, and a new label. The old label is replaced with the new label and the packet is forwarded to the following hop. The process continues till the packet reaches the destination. In other words, packet forwarding in MPLS is entirely label driven, whereby packets assigned the same FEC are forwarded the same way. Furthermore, labels are meaningful only to the pair of routers sharing a link, and only in one direction--from a sender to the receiver. The receiver, however, chooses the label and negotiates its semantics with the sender by means of a label distribution protocol. MPLS in its basic form is particularly useful for traffic engineering. To provide explicit QoS support, MPLS makes use of certain elements in the *IntServ* and *DiffServ* approaches. The label distribution protocol, for example, can be based on a resource reservation protocol [IETF RFC 3209]. With it, required network resources along a label switched path can thus be reserved during its set-up phase to guarantee the QoS of packets traveling through the path. In addition, by using the label and certain EXP bits of the shim header that carries the label to represent the differentiated service classes, packets of the same FEC can be subject to *DiffServ* treatment [IETF RFC 3270]. The relevant building blocks for MPLS include buffer management, packet marking, QoS routing, queuing, resource reservation, traffic classification and traffic shaping. They interact through the label-switched-path state information installed in each MPLS node by a label distribution protocol and through provisioned data objects.

The protocol mechanisms to be used between the interconnecting SPs are implementation dependent. Inter-provider agreements on the protocol mechanism or mix thereof would help in efficient traffic flow between the SPs and in adhering to the specific SLAs agreed with.

10.4 Directory Services[2]

To determine endpoint address resolution between interconnecting SPs, there may be a need for some directory function between the SPs. This function may be accessed by all exiting/incoming calls on the interconnecting link. There will be a need to constantly update the directory function by a customer service function agreed between the interconnecting SPs. This function is implementation dependent.

11 Network Performance

The PSTN design strategy is based a highly fault-tolerant high-capacity circuit switching architecture. However, IP network elements vary in size and function and are deployed in a network with redundancy. Therefore, PSTN element requirements are not directly applicable to IP element requirements. IP network design techniques for achieving high-availability include fault-tolerant hardware, fault-tolerant software, system redundancy, and network interface redundancy. Network Performance in the IP network will meet or beat PSTN requirements.

11.1 Service Availability

The scope of this is from the user's PC to a far end server.

ITU-T Rec. E.800 defines QoS as "the collective effect of service performance which determine the degree of satisfaction of a user of the service," and provides a definitional framework that shows the different aspects of QoS.

E.800 has an overall term Serveability with the definition given below

"The ability of a service to be obtained – within specified tolerances and other given conditions – when requested by the user and continue to be provided without excessive impairment for a requested durations.

---

2 This function may not be needed.

NOTE – Serveability performance may be subdivided into the service accessibility performance, service retainability performance and the service integrity performance.

Service availability is defined as occurring when the performance of all of a set of selected performance parameters is deemed acceptable. The performance of a specific parameter is deemed acceptable if its perfomance is greater (or lesser) than that of a pre-specified threshold. The entirety of these selected parameters and their thresholds is called the availability function. The failure of one or more of these parameters results in a transition to the unavailable state. The available state is re-entered when all parameters are once again functioning acceptably.

Agreement has been reached on the estimation af access availability in IP networks based on the state of customer facing ports (available or unavailable) over a defined period of time.[3] The availability will be affected by the reliability of these ports (see next section on reliability).

11.2 Reliability

Reliability is another parameter covered by Rec. E.800.

Reliability is the probability that an item can perform a required function under stated conditions for a given time interval.

IP Network design involves a tradeoff between node reliability, path diversity and redundancy, and restoration times to ensure overall availability

A provisional requirement for reliability of the inter-SP link for IP QOS guarantee is 99.999% for each link.

11.3 Interactions between services

It is required that the underlying IP QOS will ensure that higher layer applications like VOIP and IP VPNs will continue to operate to required service levels without interruption.

12 Service Provisioning

Once an agreement has been reached between the SPs to interconnect necessary provisioning procedures should be undertaken by the interconnecting SPs to ensure Service turn-up by the appropriate date. This will require invocation of new and legacy systems to work harmoniously so the process is automated as in the normal service turn up cases where no service interconnections are required. In this case coordination between the interconnecting SPs will be required to ensure end-to-end cross SP provisioning..

13 Network/Services Management

The necessary IP based and underlying OAM capabilities will be in place to ensure IP QOS SLA guarantees.

A customer care center as shown in Figure 13 between the interconnecting SPs may be needed for customer care and trouble shooting connectivity issues.

Exact agreements are expected to be SP and implementation dependent.

---

3 "Access Availability of Routers in IP-Based Networks," Committee T1 tech. rep. T1.TR.78-2003.

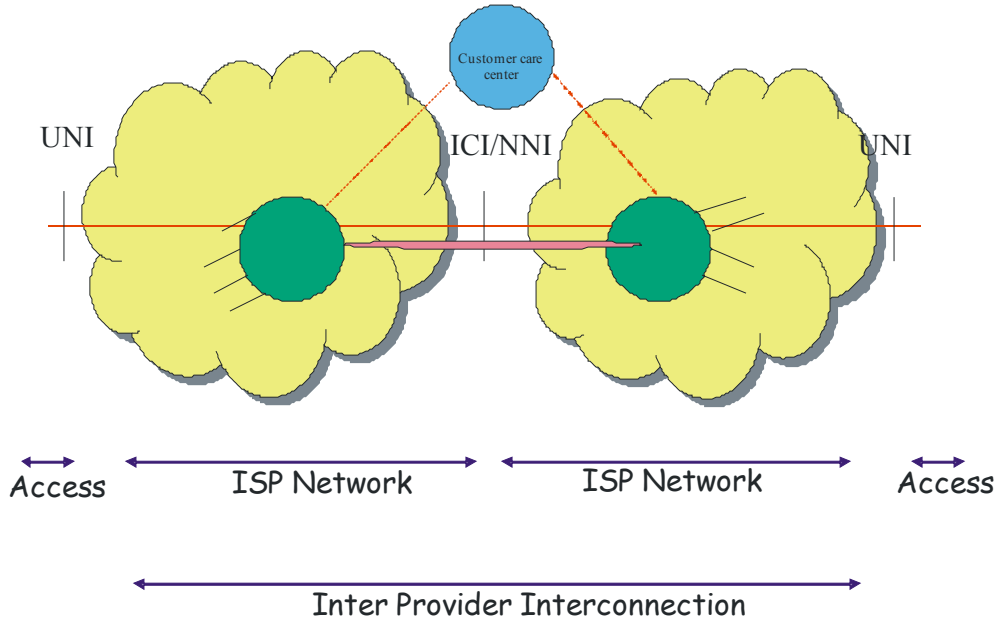


Figure 13 – Administrative Customer Care Function

14 Security

Security policies according to a policy server the terms of which are agreed between the interconnecting SPs will be needed. These will be in user, control and management planes. Exact policies will be service and SP dependent.

Annex A – Service quality criteria

		SERVICE QUALITY CRITERIA						
		SPEED 1	**ACCURACY 2**	**AVAILA BILITY 3**	**RELIA BILITY 4**	**SECURITY 5**	**SIMPLI CITY 6**	**FLEXI BILITY 7**
SERVICE FUNCTION								
SERVICE MANAGEMENT	Sales & Pre-Contract Activities 1							
	Provision 2							
	Alteration 3							
	Service Support 4							
	Repair 5							
	Cessation 6							
CONNECTION QUALITY	Path Establsh. 7							
	Information Transfer 8							
	Path Release 9							
BILLING 10								
NETWORK / SERVICE MANAGEMENT BY CUSTOMER 11								

Figure 1/G.1000 – Matrix to facilitate identification of communications QoS criteria (slightly modified to make it relevant to NGN)

2.9 – Requirements and framework for end to end QoS architecture in NGN*

Summary

This draft provides a general end-to-end QoS architecture framework for NGN to facilitate new applications and services. The purpose is to introduce capabilities that would allow multiple architectural approaches and future innovation.0

Table of Contents

* Status D: The FGNGN considers that this deliverable is not yet mature, requiring discussion and technical input to complete development.

2.9 – Requirements and framework for end to end QoS architecture in NGN

Introduction

The topic of QoS in IP networks has long been the subject of research, development, standardization, and network experience. All indications point to a continuing cycle of experience and innovation. Since each recognized operating agency has a different regulatory environment, service offerings, geographic span, and network infrastructure, there must be flexibility within any global end-to-end architecture that allows each operator to adopt new innovations or to revise existing capabilities on their own time scale.

1 Scope

This Draft provides:

– Requirements for end-to-end QoS architectures

– A general architectural model, and

– A framework consisting of elements common to specific end-to-end QoS architectures in NGN .

Within this framework it is envisioned that a series of new drafts would be created based on new contributions, to serve additional architectural needs like centralized, distributed and hybrid approaches.

[Ed. NOTE: Relationship with general access QoS architecture needs to be clarified. Signaling requirement work in SG11 will be also considered.]

2 References

The following ITU-T Recommendations and other references specified explicitly contain provisions of this Draft. All Recommendations and other references are subject to revision; users of this Draft are therefore encouraged to investigate the possibility of applying the most recent edition of the Drafts and other references listed below.

A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Draft does not give it, as a stand-alone document, the status of a Draft.

1. ITU-T E.860 (2002), Framework of a Service Level Agreement

2. ITU-T E.360.x (2002), QoS Routing and Related Traffic Engineering Methods for IP-, ATM- and TDM-Based Multiservice Networks

3. ITU-T E.361 (2003), Qos Routing Support for Interworking of QoS Service Classes Across Routing Technologies

4. ITU-T Recommendation Y.1001 (2000), A Framework for Convergence of Telecommunications Network and IP Network technologies.

5. ITU-T Recommendation Y.GRM-NGN, General Reference Model for Next Generation Networks.

6. ITU-T Recommendation Y.NGN-FRA, Functional Requirements and Architecture of the NGN.

7. ITU-T J.170 (2002), IPCablecom security specification

8. ITU-T J.174 (2002), IPCablecom interdomain quality of service

9. ITU-T M.1079 (2003), Performance and quality of service requirements for International Mobile Telecommunications-2000 (IMT-2000) access networks

10. ITU-T Y.1221 (2002), IP Packet Transfer Performance Objectives
11. ITU-T Y.1540 (1999), IP Packet Transfer and Availability Performance Parameters
12. ITU-T Y.1541 (2002), IP Packet Transfer Performance Objectives
13. IETF RFC2990 (2000), Next Steps for the IP QoS Architecture
14. IETF RFC3031 (2001), Multiprotocol Label Switching Architecture
15. IETF RFC2475 (1998), An Architecture for Differentiated Services
16. IETF RFC2702 (1999), Requirements for Traffic Engineering Over MPLS
17. IETF RFC3209 (2001), RSVP-TE: Extensions to RSVP for LSP Tunnels
18. IETF RFC3564 (2003), Requirements for Support of DiffServ-aware MPLS Traffic Engineering
19. IETF RFC3270 (2002), Multi-Protocol Label Switching (MPLS) Support of Differentiated Services
20. IETF RFC3272 (2002), Overview and Principles of Internet Traffic Engineering
21. ITU-T Y.1291, An Architectural Framework for Support of Quality of Service (QoS) in Packet Networks
22. ITU-T Y.123.QoS (2003), A QoS architecture for Ethernet-based IP access network
23. Rec. E.800, Terms and definitions related to quality of service and network performance including dependability
24. Rec. I.350, General aspects of quality of service and network performance in digital networks, including ISDNs
25. Rec. I.356, B-ISDN ATM layer cell transfer performance
26. Rec.Y.1540, Internet protocol data communication service - IP packet transfer and availability performance parameters
27. Rec.Y.1541, Network performance objectives for IP-based services
28. Rec. Y.1560, Parameters for TCP connection performance in the presence of middleboxes
29. Rec. Y.1561, Performance and Availability Parameters for MPLS Networks
30. Draft Rec. Y.NGN-GRM, General Reference Model for NGN
31. ITU-T Y.1251, General architectural model for interworking
32. ITU-T Y.1412, ATM-MPLS network interworking - Frame mode user plane interworking
33. ITU-T Y.1411, ATM-MPLS network interworking - Cell mode user plane interworking
34. ITU-T G,1010, End-user multimedia QoS categories
35. GRQ
36. Overview and Principles of Internet Traffic Engineering, IETF RFC 3272

[Ed. NOTE. This section will be updated]

3 Definitions

This Draft defines the following terms:

End-to-End: Within the context of this draft end-to-end means UNI-to-UNI, that is from the User Network Interface (UNI) at the source host side to the UNI at the destination host. Note that end-to-end means from mouth to ear in other Recommendations concerning user perceiving.

Connection-oriented network service: A network service that establishes logical connections between end users before transferring information.

Connectionless service: A service, which allows the transfer of information among service users without the need for end-to-end logical connection establishment procedures.

Relative QoS: This term refers to a traffic delivery service without absolute bounds on the achieved bandwidth, packet delay or packet loss rates. It describes the circumstances where certain classes of traffic are handled differently from other classes of traffic, and the classes achieve different levels of QoS.

Absolute QoS: This term refers to a traffic delivery service with numerical bounds on some or all of the QoS parameters. These bounds may be physical limits, or enforced limits such as those encountered through mechanisms like rate policing. The bounds may result from designating a class of network performance objectives for packet transfer.

Flow [IP flow]: A sequence of packets sent from a particular source to a particular destination to which the common routing is applied. If using IPv4, a flow is identified by IPv4 5-tuple including source/destination IP addresses, protocol ID, source/destination port numbers. If using IPv6, a flow is identified by IPv6 3-tuple including source/destination IP addresses, flow label.

Session: A period of communication between two terminals which may be conversational or non-conversational (for example retrieval from a database).

Interworking: This term is used to express interactions between networks, between end systems, or between parts thereof, with the aim of providing a functional entity capable of supporting an end-to-end communication. The interactions required to provide a functional entity rely on functions and on the means to select these functions.

Interoperability : The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

User: A person or a machine delegated by a customer to use the services and/or facilities of a telecommunications network.

Terminal equipment (TE): Represents the customer's access equipment used to request and terminate network associated connectivity services.

Network provider: The organization that maintains and operates the network components to support services. A network provider may also take more than one role, e.g. also acting as Service Provider.

Service provider: A general reference to an operator that provides NGN services to Customers and other end-users either on a tariff or on a contract basis. A Service Provider may or may not operate a network. A Service Provider may or may not be a Customer of another Service.

[Ed. NOTE. This section will be updated based on the terminology used in this Draft]

4 Abbreviations

This Draft uses the following abbreviations:

IETF Internet Engineering Task Force

ITU-T International Telecommunication Union – Telecommunication Standardization Sector

IP Internet Protocol

AS Autonomous System

RSCF Resource and Service Control Function

LSP Label Switched Path

MPLS Multiple Protocol Label Switching

DiffServ Differentiated Service

RSVP Resource ReSerVation Protocol

QoS Quality of Service

SLA Service Level Agreement

NP Network Performance

CPE Customer Premises Equipment

AN Access Node

ER Edge Router

BR Border Router

BAS Broadband Access server

CPN Customer Premises Network

NGN Next Generation Network

SNMP Simple Network Management Protocol

UNI User-to-Network Interface

NNI Network-to-Network Interface

API Application Programming Interface

[Ed. NOTE. This section will be updated based on the terminology used in this Draft]

5 Conventions

In this draft, "shall" refers to a mandatory requirement, while "should" refers to a suggested but optional feature or procedure. The term "may" refers to an optional course of action without expressing a preference.

6 Requirements

6.1 Generalities

The end-to-end QoS architecture should be designed to provide necessary quality for a variety of services and applications. This architecture should ensure the interworking between different administrative domains with possibly varied architectures to achieve end-to-end QoS services.

The QoS definition is based on TR.NGN.QoS.

The QoS Architecture should take into account:

– NGN general constraints,
– Processes related to service lifecycle,
– QoS mechanisms,
– QoS Interworking,
– QoS Signalling.

The high performance expected from the IP networks evolving to NGN has many requirements besides the QoS. The other considerations closely related to QoS are the following:

– Scalability,
– Security,
– Reliability and Fault Tolerance,
– Mobility.

6.2 NGN general constraints

The QoS architecture should support:

– Different business models.
– Different service types such as Conversational services (e.g. SIP based), Audio-visual services (e;g; VoD, Broadcast TV services), Web services, etc.
– Different access and core transport technologies (xDSL, UMTS, Cable, LAN, WLAN, Ethernet, MPLS, IP, ATM, etc.).
– Firewalls.
– Network Address Translators (NAT).
– Mobility and Nomadicity.
– Priority communications services (e.g., emergency user applications)
– At least one of the recommendations, ITU-T Y.1541 (IP QoS Classes) or 3GPP TS 23.107 (UMTS QoS classes). For details refer to TR.NGN.NHNperf.

6.3 Processes related to service lifecycle

The QoS architecture should support the different processes related to service lifecycle:

– Subscription/Provisioning: customer care (contracts, customer profiles), dimensioning, deployment and network configuration management. *Considering that the deployment of end-to-end QoS will progress in stages, the capacity planning and in particular, the ability to design and allocate bandwidth in advance in management plane is necessary. This function can improve the efficiency of the bandwidth usage in a large scale network*
– Invocation: service and resource controls to support services in real-time (or on-demand).
– After-Sales: measurements and monitoring (network performance report, faults).

6.4 QoS mechanisms

The QoS architecture should support:

– Per-flow, per-session, per-service-class resource QoS control granularity
– Dynamic QoS behaviour (i.e., it should be possible to modify QoS attributes during an active session).
– QoS resource control based on a distributed, centralized or a hybrid approach.
– Admission control and congestion control mechanisms
– Different CPE or CPN intelligence and capability.
– QoS architecture in transport stratum to guarantee transit of packets in control plane.
– QoS architecture in service stratum to prioritize transit of emergency calls and priority calls.

6.5 QoS Interworking

The QoS architecture should support:

– Mechanisms that would allow negotiation between access and core networks that belong to different network providers.

– Inter-working between domains deploying heterogeneous QoS Architectures.

6.6 QoS Signalling

The QoS architecture should support:

– User-initiated and Network-initiated Requests for QoS.

– Path-coupled and path de-coupled QoS signalling.

6.7 Scalability

Ed. NOTE: The current section should be reviewed to focus on requirements.

Scalability is a major concern in new architectures, services and applications of NGN. The fundamental premise of scalability is to provide a system that will not be impacted adversely by growth of hardware, software and number of applications and end-users. It provides essentially a mechanism to gracefully grow the network as necessitated by demand.

NGN must be flexible and have reusable components, be reliable and scalable, and be able to provide QoS support for different applications. In this context scalability refers to the ability to handle additional end-users, services and applications. This means that network performance and QoS parameters do not suffer degradation and end-user perception is not noticeably impacted as network grows. Scalability also affects reliability and system administration. Furthermore, a set of recommended measurements and tests should be defined related to NGN scalability.

Network scalability is often measured by the rate of growth of network connections with the increase of end points. Scalable networks grow linearly as the number of end points, N, increase. Network architectures that grow following an N^2 law do not scale well and could only support a limited set of end points.

The scalability is related to several aspects in the framework as network scales:

1) *Granularity of resource control*

   The granularity of traffic control could be per-flow, per-session or per-service class and so on. For finer granularity, more status information needs to be kept and updated.

2) *Traffic control approach*

   When the network grows, the static configurations will have scalability problems, for instance, the statically configured MPLS TE tunnels will need to be reconfigured and the extra work when more tunnels need to be set up will grow faster than "N". However, dynamic approaches may save a lot of work.

   For dynamic resource control, there could be centralized or distributed frameworks. For centralized approach, scalablity may be an issue. When the network grows it requires that the capability of the centralized devices could be upgraded smoothly to the new set of devices. For distributed approach or other hierarchical approaches, separating the processing capability to multiple equipments, will reduce the burden however there are other considerations beyond scalability (how to keep efficient interactions between the distributed parts) and a network design should consider all the factors involved.However, in the centralized and distributed approaches, the linear relationship between the information that will be kept in the resource control device/devices and the number of network nodes should be kept in an efficient manner.

In DiffServ model, there is no explicit signaling protocols to request resources and there is no admission control function on behalf of the whole network, which makes the DiffServ model scalable. But to provide an assured QoS in DiffServ infrastructure, admission control function and QoS signaling was introduced to the DiffServ domain. Bandwidth utilization of control information in signaling is another factor impacting scalability. This is related to the number and payload of the messages in QoS signalling. For instance, in RSVP, every flow needs a signaling message. To reduce the number of signaling messages into the network, some aggregation RSVP protocol has been proposed.

Flow level forwarding is also possible. Flow state technology recognizes flows, routes the first packet of the flow, dynamically associates state with it and then switches remaining packets in the flow using this state information. This state information is dynamically created and deleted without any explicit signaling because all flow processing is internal. State information allows unique per-flow IP traffic policing, shaping and burst tolerance guarantees, which means individual flow can receive guaranteed bandwidth, delay, priority treatment appropriately.

3) *Equipment capability*

All the QoS-related functions will be implemented in the network equipment. The scalable system design of the router and resource control devices need to be considered. The equipment capability includes the following aspects:

a) Memory of the router and other QoS related controller

The large number of information kept in the memory, for example the network resource status, and flow information, and also the frequent memory access and update could cause scalability problem.

b) CPU capability

An important measurement is the ability to handle large volume of the flow requests that can be processed by the resource control function. Usually, complexity has a relation with scalability, if the algorithm and mechanism has a high computational complexity, it is difficult to provide scalability.

Scalable QoS architectures should consider the above factors. Different approaches in different application environment may have different requirements for scalability. In the networking environment, the functions that relate to QoS control should not be the bottleneck when the network gets overloaded.

6.8 Security

The current section should be reviewed to focus on requirements.

The QoS architecture described in this draft enhances the security of IP networks. And it does not raise any new security issues to IP networks.MPLS technology can be used to implement network resource isolation between the different service classes. It prevents from the vulnerable best-effort traffic intruding into the reserved resources of Logical Bearer Network (LBN).

Resource requests are initiated by service control function not by hosts, which prevents from the malicious resource requests and the resulting illegal excessive resource reservation, exhaustion and even DoS (denial of service). All of resource requests are triggered by the service requests that have passed the end-user authentication and authorization. Should also cover resource reservation by hosts.Admission control is helpful against fabrication attacks, unauthorized traffic and the resulting congestion. Traffic marking can be done and checked edge routers. And the mark is trusted and reused by core routers. Initial markings can be done by hosts.QoS (resource control) signalling can be out-of-band and path-decoupled, which can be delivered on the dedicated link with security encryption. Access nodes, edge routers and service control function should protect themselves from DoS attacks.The conventional network security mechanisms such as firewalls, intrusion detection software (IDS) and proxies are used against network attacks. If needed,

authentication and integrity mechanisms can be used to protect UNI and NNI from interception, modification and fabrication attacks.

[Ed. NOTE*:* This section will describe the requirements for security and is subject to change. *Contributions are invited.*]

6.9 Reliability and Fault Tolerance

The current section should be reviewed to focus on requirements.

This section is about reliable service protection and rapid service restoration from the failure of an end-to-end QoS architecture. In user/data plane, the reliability and OAM function of routers is of much concern. In control and management plane, the reliability and backup of centralized admission control and resource management entities is of much concern. The interaction between different sub-layers may also make effects on the systematic reliability.

In the end-to-end QoS architecture described in this draft, the key function physical entities could be multihomed for redundancy backup. That is, a AN could be connected to multiple ERs; an ER/AN could be connected to multiple RCFs in a domain; a SCF could be connected to multiple RCFs; a RCF could be connectted to multiple RCFs in other domains. The redundancy of the physical entities could be more or less according to the network requirements. The data consistency check by background process is used for avoiding the resource deadlock.Routers should support MPLS OAM mechanisms at least including MPLS LSP fast failure detection and protection switching in conformance to ITU-T Y.1711 and Y.1720.If a LSP is detected in failure, all service flows borne on the LSP should be rerouted rapidly if not receiving the call release form SCF. If the failure LSP is configured with one or more backup LSP, these flows traffic should be switched into the backup LSP rapidly and reliably. If the failed LSP is configured without any backup LSP, RCF should immediately select the new paths for these flows traffic and release the previously selected paths resource. It is desired to seek the equivalent path to the previous failure path in the same domain for a service flow as much as possible. For the fast path reselection, a routing matrix table may be used to calculate and store the equivalent paths for a service flow so that the path can be recalculated and switched partially instantly according to the service type, available resource, policy, specific QoS requirement and so on.

If needed, the key function physical entities could be installed with one or more backup entities working in the active-standby mode or in the load-balancing mode, such as RCF, Edge Router and Transit router. The cooperation and interaction between multi-layer protection mechanisms is for further study.

[Ed. NOTE: This section will describe the requirements for reliability and is subject to change. *Contributions are invited*.]

6.10 Mobility

In a mobile environment, the establishment of end to end QoS means that all hops in the path provide required QoS levels. The signalling to setup QoS enabled flows shall provide the capability to coordinate individual network QoS and shall ensure that end to end QoS is attained.

Due to the inherent nature of mobile systems, QoS signalling should be optimized such that resources for QoS enabled flows can be reserved, and committed very rapidly. The process of coupling of the newly allocated links to the existing links is part of the end to end setup process, and the QoS signalling framework shall support seamless treatment of the packets during this setup process. Both path coupled and path decoupled signalling shall be supported in mobile environments.

Mobility of end user terminals places unique demands on maintenance of QoS enabled flows across network boundaries. When terminals transition to a new network attachment point, the new network segment(s) perform some admission control. The admission control shall occur such that when the transition between

current and new network occurs, that the flows handed into the new network are treated with the required QoS.

Networks shall support a means to negotiate QoS attributes in a manner such that transition of the user's QoS enabled flows remain at a specified minimum level of service. When moving across network domain boundaries, the negotiated or minimum QoS shall be maintained within a set of configurable limitations. Maintenance of QoS for flows shall be coordinated such that the end user is assured of their prescribed level of QoS (i.e., specification of peak rate, delay, jitter, packet loss, etc.) for the duration of the session, especially important when carrying time sensitive bearer streams, or critical signalling streams.

The QoS level supported should be able to be modified during a session without the explicit need to disable, and re-establish the IP flow. In the newly configured flows due to changes in the underlying characteristics of the network, modification of the QoS support may be required. The network segment(s) involved in a change during a session should provide the newly requested QoS without interruption in the delivery of packets in the flow.

In NGN systems that support mobility, coordination of QoS policies and charging agreements should be in place so that the application is not required to send additional requests for QoS when transitioning between networks. If negotiated QoS is not attainable when moving to a new network attachment point, several alternative options may be considered.

In order to protect the NGN from fraud and other security threats, QoS requests shall be authorized prior to commitment of QoS resources in a new target network. The authorization may occur in advance of the actual transition to the new network, or may occur at the time of transition.

Performance information pertinent to QoS in a mobile environment include resource usage data, congestion performance data, and admission performance data for all network segments involved in the transport of QoS enabled flows.

Security is a critical part of NGN, and securing multiple networks involved in a QoS enabled session is no exception. When terminals are transitioning into a new network, requests for QoS shall be authorized such that valuable QoS traffic classes are not used in a fraudulent manner. The NGN should validate the QoS requests from terminals coming into a new network. The NGN should police QoS enabled flows to ensure they are not being used for transport of data beyond the agreed QoS parameters.

7 QoS Framework Model

7.1 Framework Model

In order to provide a global and homogenous view of functions needed to support end-to-end services in NGN, a framework model is useful. This model should allow the possibility to identify the different processes and functions implied in QoS both in service and transport stratum.

This model is not an architecture model. The mapping of this model on a functional architecture is out of scope of this document. The decision to standardise or not the functions identified in this model is also out of scope of this document

The framework is based upon the customer-provider relationship. The provider provides a service to the customer. The customer could be either an end-user or a provider itself that plays the customer role. A customer sends a request to initiate a demand to the provider. The framework (Figure 7-1) introduces horizontally three processes, and vertically six levels to structure functions and data. A seventh vertical level is devoted to network element functions also called transport functions.

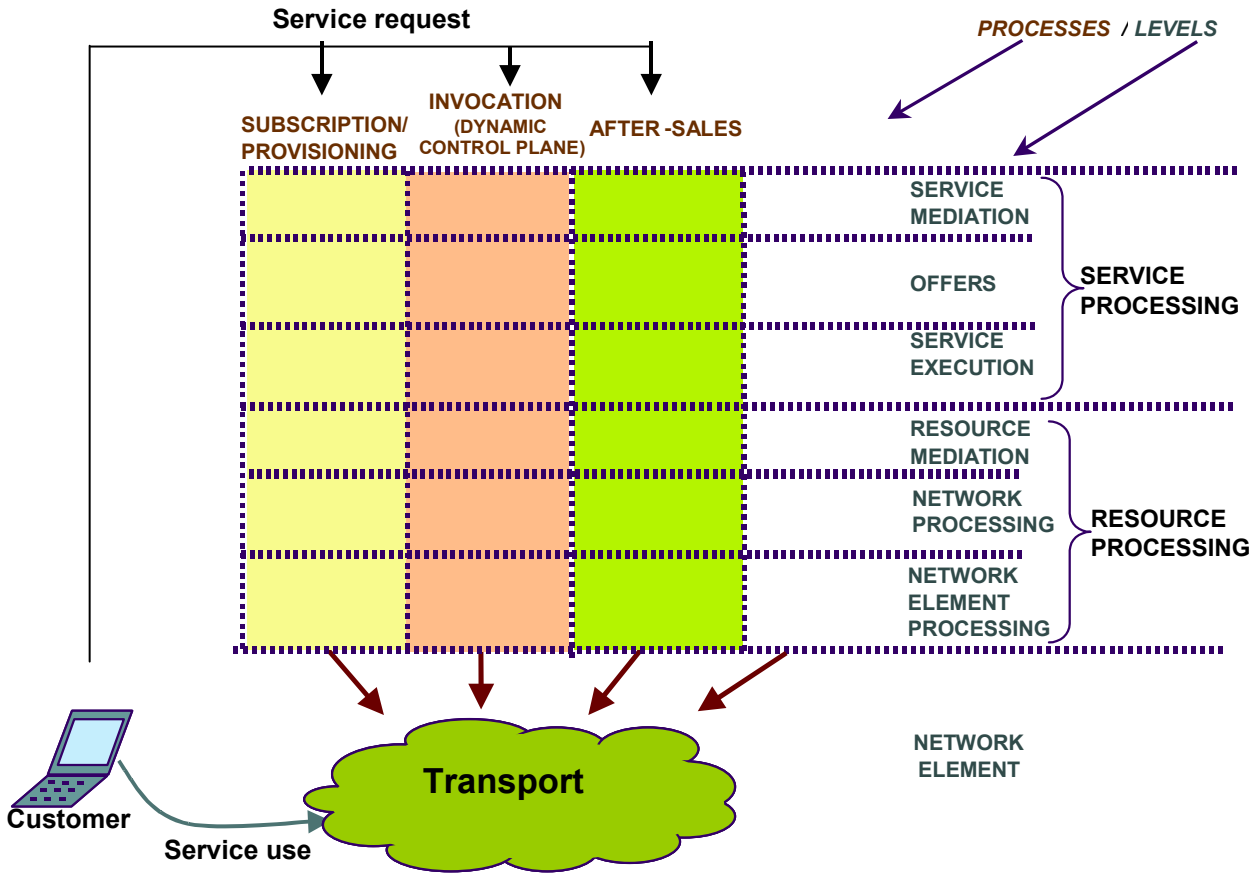


Figure 7-1 – Framework model

7.1.1 Processes

Processes are related to service lifecycle. They structure actions undertaken by providers to answer to customers' requests. The proposed processes are the following:

1) **Subscription/Provisioning**: this process deals with actions that follow customers' subscriptions: customer care (contracts, customer profiles), dimensioning, deployment and network configuration management.

2) **Invocation**: following a service invocation request, this process is in charge of service and resource controls to support services in real-time (or on-demand).

3) **After-Sales**: network performance report, quality of services and faults are handled by this process. It also manages measurements and monitoring. Customers might ask for their QoS information.

In this framework, two management processes are identified (Subscription/Provisioning, After-Sales), and one process which corresponds to the dynamic control plane (Invocation).

7.1.2 Levels

Each process is divided in two parts: Services Processing and Resources Processing, each gathering three levels. The proposed levels are the following:

1) **Service Mediation or Front Office**: this optional level is intermediary between the customer and service offers. It manages catalogues of service providers, for example in the form of "yellow pages" indicating the main attributes of provided services. It can deal with user requests to direct them to the appropriate service providers.

2) **Offers or Back Office**: this level is intermediary between the service mediation and service execution. It proposes offers, i.e. bundles of one or more services to the customer. It also deals with the customer's subscription, the customer's identification and authentication in order to allow him to use the subscribed services in an offer.

3) **Service Execution**: this level is in charge of the planning and the development of services. In the Invocation process, it ensures the execution of a telecommunications service that is dynamically requested by the customer.

4) **Resource Mediation**: this level is intermediary between Service Execution and resource processing. It first ensures the adaptation between service instance and resources by translating service parameters into resource parameters. This level is then in charge of resource positioning in order to support the customer's service. It identifies the sub-networks in accordance with the needed QoS. This level makes the Resource Processing independent from the Service Processing and therefore is particularly relevant in NGN architectures.

5) **Network Resource Processing**: this level is in charge of network resource deployment in order to meet demands of the customer's service. It identifies and monitors resources required to support the service. It computes topological paths (nodes, interfaces/links) and constraints to transfer flows.

6) **Network Element Resource Processing**: this level is in charge of resource network element deployment. It identifies and monitors resources at the Network Element level (matrix connection, interface, port, etc.). These functions are in charge of two main actions in the Invocation process: to select physical paths and to route data.

7) **Network Element or Transpor**t: this level corresponds to transport functions. An example is termination functions (traffic filtering, policing, etc.).

These levels are functionally split and Reference Points are found at boundaries.

7.2 Application to QOS

The previous Framework Model could be applied to QoS (Figure 7-2).

Following a customer's subscription request, in the Subscription/Provisioning process:

1) The **Offers** level functions manage service subscription. It formalizes QoS contract negotiated between the customer and the provider.

2) The **Service Execution** level functions activate the QoS contract and orders the Resource Mediation level.

3) The **Resource Mediation** level functions manage information related to end-to-end resource performances (connection, access network, etc.). It binds QoS characteristics and network resource performances.

4) The **Network Resource Processing** level functions manage network resource configuration and takes into account QoS constraints to dimension necessary resources in macroscopic way: interface, buffer, etc.

5) The **Network Element Resource Processing** level functions manage network element configuration parameters and maintains provisional states of resource occupation.

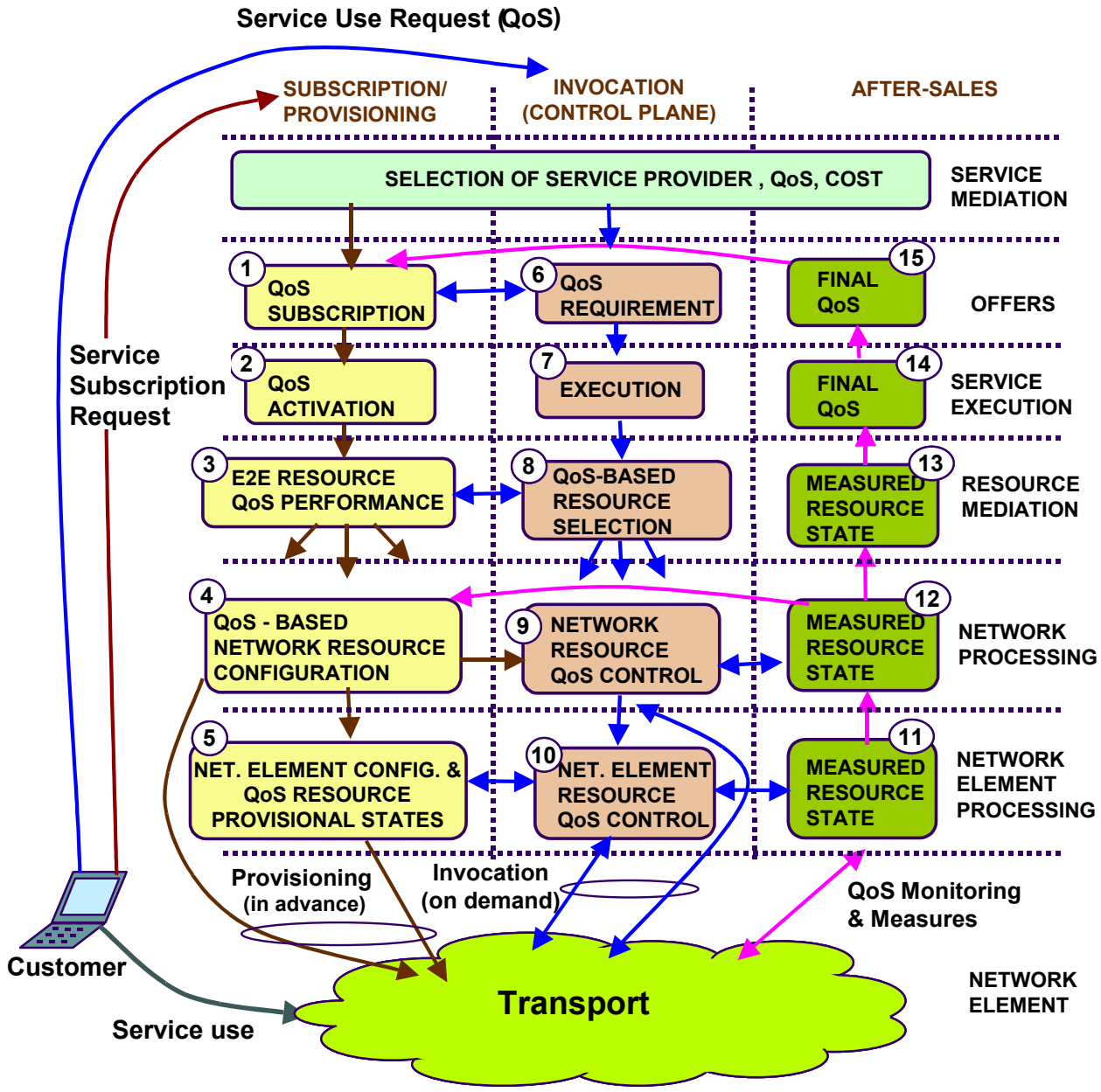


Figure 7-2 – QoS Framework Model

Following a customer's service invocation (or use) request, in the Invocation process:

6) The **Offers** level functions control the correspondence between the QoS subscribed by the customer and the QoS requested by the customer.

7) The **Service Execution** level function handles QoS data suitable to the customer's request.

8) The **Resource Mediation** level functions select the end-to-end resource support (access network, sub-networks, core network, etc.) corresponding to the above QoS constraints, with respect to resource performances and the state of resources managed in the Subscription/Provisioning process.

9) The **Network Resource Processing** level functions control and includes an admission control on the basis of QoS constraints with regards to the estimated network resources state, obtained by QoS monitoring and measures in the After-Sales process, and potentially to the amount of reserved resources.

10) The **Network Element Resource Processing** level functions control and includes an admission control on the basis of the real resources states node per node. This function is vital to guarantee QoS on-demand.

At the resources level, flows are switched/forwarded in accordance with the traffic contract.

Finally, in the After-Sales process (11 to 15), based on the network monitoring and measurements, are obtained information about the estimated (or operational) state of resources (residual bandwidth, queue occupation, etc.), and the QoS experienced by the customer's service use. All this information would be used to improve the resource planning and the QoS offered to customers.

In order to support to the absolute QoS, it would be useful to calculate the real state of reserved resources. Thus the Reserved Resource State database, previously identified in the Subscription/Provisioning process, is essential to provide absolute QoS.

Processes are related to service lifecycle. They structure actions undertaken by providers to answer to customers' requests. The proposed processes are the following:

1) Subscription/Provisioning: this process deals with actions that follow customers' subscriptions: customer care (contracts, customer profiles), dimensioning, deployment and network configuration management.

2) Invocation: following a service invocation request, this process is in charge of service and resource controls to support services in real-time (or on-demand).

3) After-Sales: network performance report, quality of services and faults are handled by this process. It also manages measurements and monitoring. Customers might ask for their QoS information.

8 Generic reference Architecture

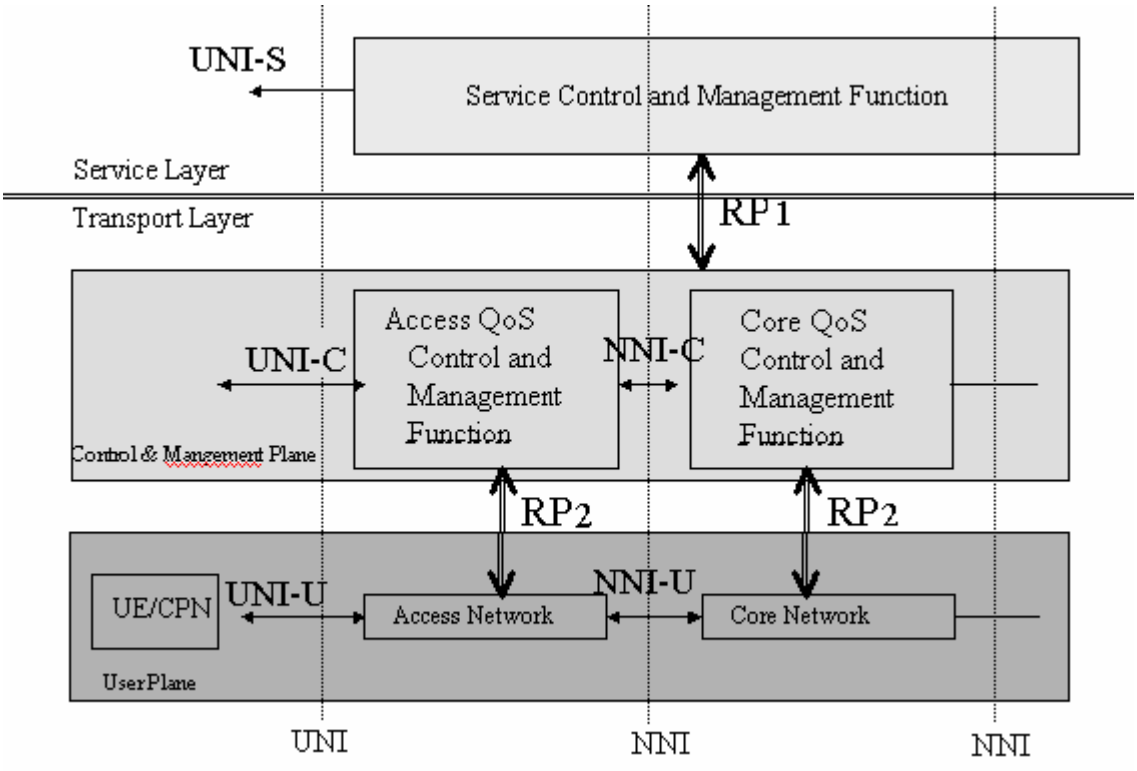


Figure 8-1 – General reference model for end-to-end QoS architecture

This section provides a general framework architecture that will be used as a guide to specific architectural needs that will be addressed in subsequent drafts that will follow this. To motivate innovation and creation of new applications and to address the needs of users and providers of application and networks several types of architectures are envisioned such as centralized, decentralized and possible combinations of these two.

Based on the two-layered NGN architecture, the general reference model of end-to-end QoS architecture is depicted as Figure 8-1. It is designed to enable different technologies in CPE, access network and core network. The general reference model covers multiple administrative domain and multiple planes.

There are several logical planes involved: service control and management plane, resource control and management plane and user plane. Between these planes, two reference points are defined. Vertical reference points include RP1 and RP2. Horizon reference points include the UNI and NNI.

Scenario1 – Centralized Resource control inside a network:

In this scenario, the admission control and the resource control is done in a single functional entity, and the resource status information is gathered from each routers, and kept in the information base as a basis for admission control. There are no resource information sent between routers, and the configuration is done by protocols like COPS, or Diameter.

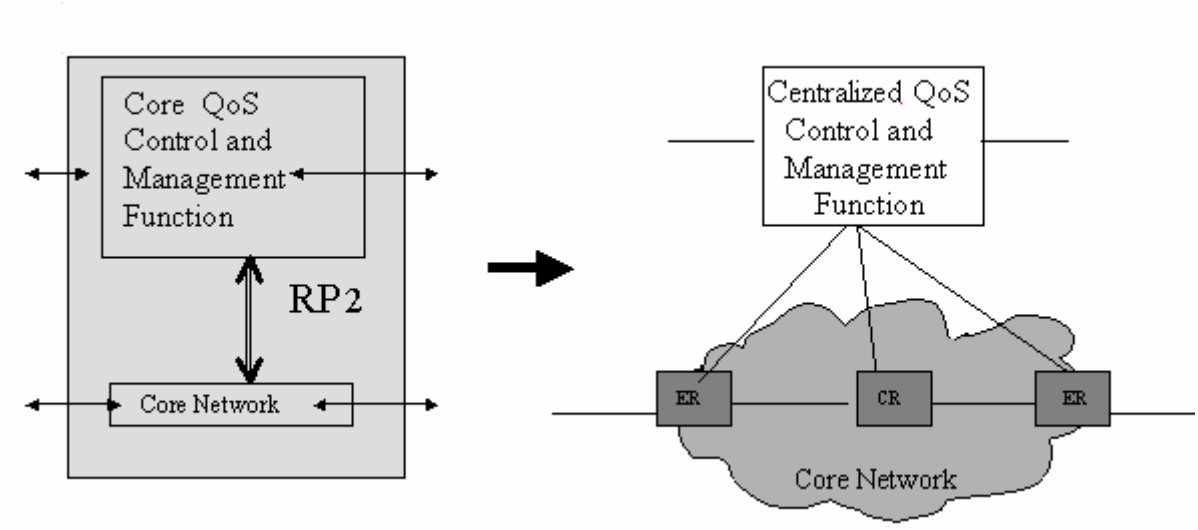


Figure 8-2 – Centralized Resource control

Scenario 2 – Distributed resource control

In this scenario, the admission control and resource allocation is implemented in the edge of the network. Edge routers perform admission control based on the resource information they get from other edge routers. And to get a whole picture of the resource usage inside a network, the interaction between the edge routers could be done by the extended routing protocols.

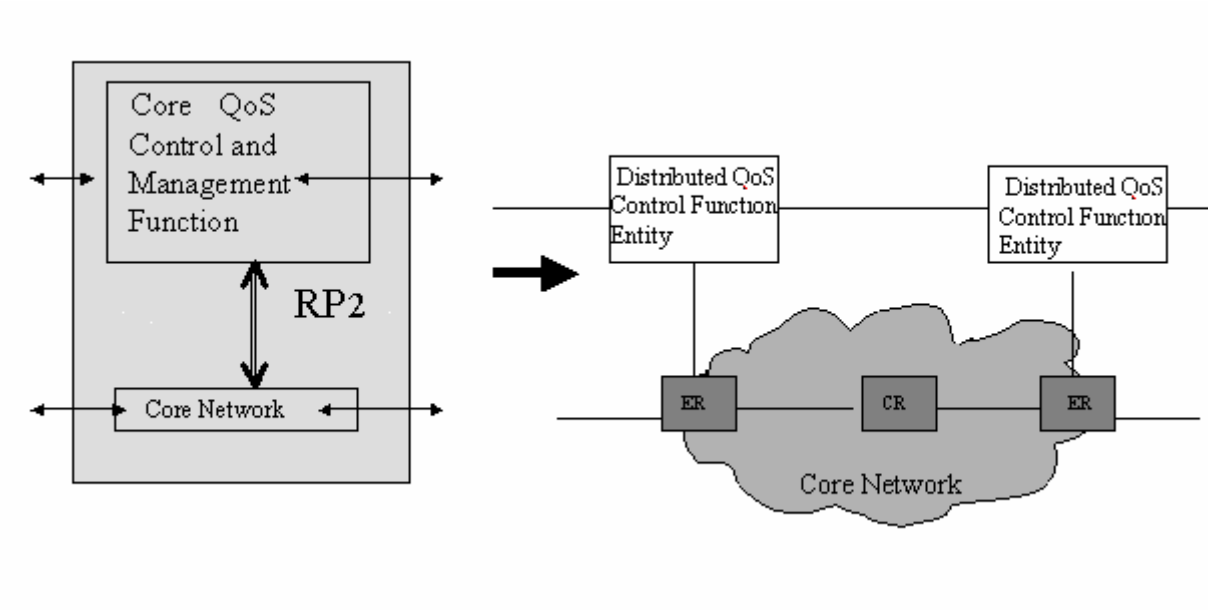


Figure 8-3 – Distributed Resource control

Scenario 3 – Hybrid Resource control

In this scenario, the admission control and resource allocation is implemented in a hierarchical way. Edge routers could do the admission control and resource allocation with the guidance by a centralized function entity which is in charge of the whole network resource allocation. Usually, centralized function entity will perform coarse-grain resource allocation, for instance, the resource allocation for large pipes. Edge routers usually implement the fine-grained resource control, for instance, processing the per-flow/per-session based resource request. Centralized function entity could re-adjust the coarse grain resource allocation based on the usage of each pipe. Other alternative cases can be obtained by edge routers using resources that are updated by a centralized control function periodically.

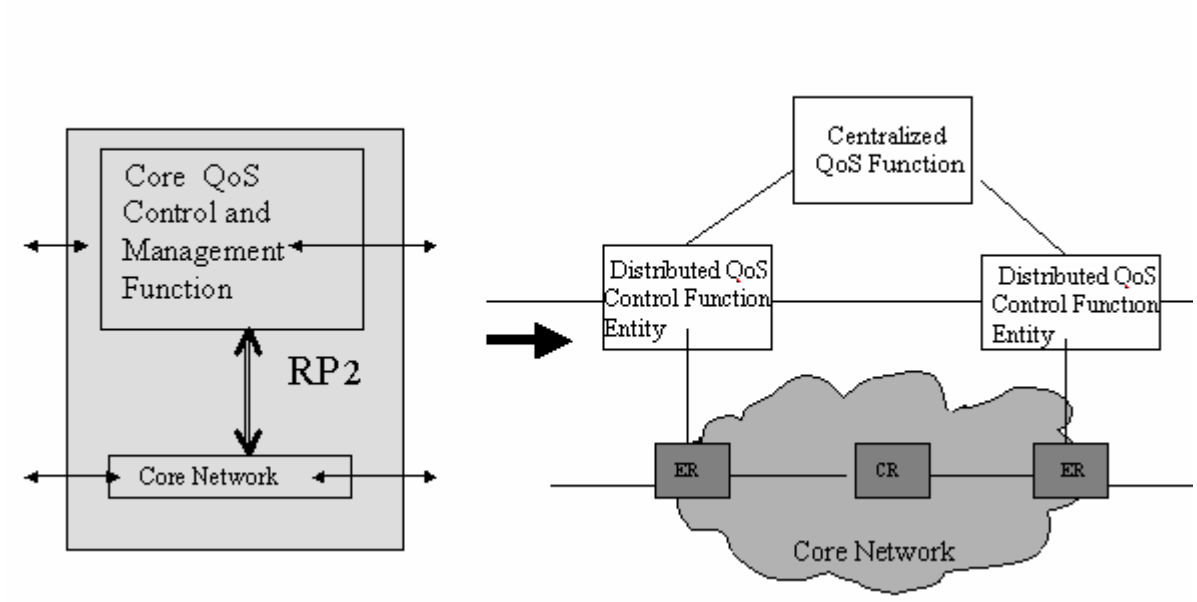


Figure 8-4 – Hybrid Resource control

The detailed description of implementation is beyond the scope of this draft.

8.1 Control and Management functions

8.1.1 Access QoS Control and Management

The Access QoS Control and Management Function is to process the resource requests for different kinds of access networks, and perform admission control and resource allocation in the access network, and also is responsible for the interaction between other QoS Control and Management Functions. It also includes the monitoring function to verify the services provided to the users. It may receive the resource requests from the reference point RP1, i.e. from the general Service control and management function, and it could also get the request from the horizon UNI-C which is directly from the user.

Different scenarios and the interaction to core network will be elaborated in TR-ipaqos.

8.1.2 General Service Control and Management function

General Service Control and Management Function includes both the service control and service management, and these two functions could be separated. Service control function includes functions for dealing with different services, like call/session control function, media service control function, data service control function, VPN service control function and other new value-added service control functions.

Service management function mainly includes service provisioning function, service policy management function, registration management function, user database management function, AAA function and OAM function.

8.1.3 General Service Control and Management Function

This function will do the mapping from the service request to resource requests if there is no explicit QoS parameters in the request. It also includes QoS- related charging and billing functions. Function entities for CPN/UE.

TBD

8.2 Generic Functions for End-to-End QoS Support

This section describes the generic functions required for end-to-end QoS support.

Editor's NOTE: Decomposition of the functions shown in Figure 1 should drive the identification of additional generic functions in this section. Contributions are invited.

8.2.1 Management Functionalities for QoS support

1. SLS Management Functions

SLS Management is the module that deals with flows and traffic characteristics. Its main functionality consists of provisioning of the SLS and monitoring of the enforced SLS to ensure that the expectation is met. If the SLS management is performed between a customer and a provider, it checks customer profiles to verify the requested services for compliance.

In case the management is performed between two providers, SLS checks the interprovider agreements.

SLS management interacts with other control plane functional entities such as an admission control and provisioning functional entities to provide expected services to traffic based on the contract.It also retrieves non-compliance information and forwards reports. It provides a set of rules to traffic conditioning mechanisms such as marking, shaping and policing.

2. Policy Management

Policy management is a module that deals with network provider's policy for routing, security, resource, etc.

3. Capacity Management

Capacity management is a module for maintaining transport network node capacities such as buffer size, link bandwidth, scheduling method.

4. Monitoring

Monitoring is a module for monitoring transport network including both path monitor and node monitor. The monitoring results should be able to be accessed by other modules to provide information about network status.

5. Traffic Engineering (TE)

Traffic Engineering is a general and generic term that is used in different contexts and summarizes basic principles to enhance networking experience of users and service providers and application providers. In this draft it is used in a somewhat more restricted sense for providing functionalities that are more modular and automatic. However, since it is a set of principles related to the measurement, characterization, modeling, and control of network traffic, the modules included can always be flexible since new applications and methodologies can be introduced. The basic principle is 'optimization' of both traffic and network resources in some sense to provide economic and reliable networking and related controls are provided in the control plane. In this context restoration and protection of paths also falls in this framework.

- **QoS Route Management**

QoS route management may be based on a multiple set of constraints such as carrier preference, available bandwidth, various performance parameters, impairment, security requirements, cost etc.A set of paths can be calculated for different types of traffic, a selection can be made based on multiple considerations and request is made to make appropriate reservations. *QoS route management can calculate routes satisfying certain QoS constraints (such as bandwidth or delay) in advance in management plane.*

In case the requested resources are not available it provides information to session function in service stratum for further instructions.

The QoS based routing is more generic and routes can be computed in a distributed manner taking into account other network constraints and network conditions. The path selected is most likely not the traditional shortest path since factors such as traffic, network and policy constraints are taken into consideration in routing decisions to accommodate the requested performance. To guarantee performance on a selected path, QoS routing needs to be used in conjunction with resource reservation to reserve necessary network resources along the path.

The routes can be provisioned in advance for real-time traffics. The capacities of routes are determined in accordance with off-line performance analysis and traffics are assigned to these routes.

- **Traffic Data Management**

The data collected by network elements and monitoring mechanisms needs to be analyzed and managed for optimization objectives and involve a continual and iterative process of network performance improvement. The traffic data analysis and management can be proactive, that is acts to prevent foreseen performance degradations using the appropriate control functions or reactive. In the latter case, the control system responds to the situation as it is occurring or just after it occurred to prevent similar situations in the future. Therefore the data obtained using monitoring as well as historical data is very crucial together with the algorithms deployed.

- **Reliability Management**

Reliability management is a module to check network fault to guarantee high availability. If fault is detected, either protection or restoration procedure is induced in order to guarantee recovery within 50 ms

- **Anomaly Management**

Anomaly management provides mechanisms to detect network and traffic anomalies based on network traffic analysis. This involves protocol analysis and marked increase or decrease of bandwidth utilization or certain type of traffic in relation to normal levels. Once this module detects anomaly, it should be able to control the detected anomaly traffic.The purpose is to provide mechanisms to prevent and in cases this is not possible to localize the anomalous behaviour. In cases the anomalous behaviour is localized the route management is invoked to provide routes that avoid potential hot spots.

8.2.2 Service Control and Management Functions

- **Session Functions**

Session Functions provide Session Control/Service Control functions related to the capabilities requested on the demanded services. This includes invocation of various service logic in support of the requested services including QoS related activities and security.

- **Service Mediation Functions**

Service Mediation functions provide and manage a set of available services to the user and acts like a intermediary between the user and service providers. It manages catalogues of service providers, for example in the form of "yellow pages" indicating the main attributes of provided services. It can deal with user requests to direct them to the appropriate service providers to find an appropriate set of service offers within the criteria of user demands.

8.2.3 Generic Controls

- **Resource Mediation Functions**

Resource Mediation is an intermediary between service mediation and resource processing. It first ensures the adaptation between service instance and resources by translating service parameters into resource parameters. It identifies the networks in accordance with the required QoS derived from service parameters given by a Service stratum function. It responds to the requests from Service stratum functions on the degree of availability of resources. This entity makes the Resource Processing independent from the Service Processing.

- **Policy Control**

Policy control is a module to control policy, which is a set of rules that specify network should apply to users, flows, or services for routing, security, resources, etc.

TBD

8.3 Reference points

For a specific end-to-end QoS solution, it is not necessary that all the reference points must be involved, it depends on the specific procedure the QoS architecture is using. Some reference points could be merged due to the merge of several functional entities in a single equipment.

8.3.1 Vertical Reference Points

From a vertically view, there are two reference points, RP1 and RP2.

RP1 is a reference point between service control plane and resource control plane. It maps between the service control and resource control. It conveys the QoS request for admission control and resource allocation. It also provides some feedback from resource control to service plane, for instance, some information used as the basis for accounting and charging.

RP2 is a reference point between resource control and user plane. It maps between the resource control to the data transport. It conveys the configuration information from the control plane to the routers, and also will give some feedback from user plane to report to control plane.

The vertical reference points will be elaborated in TR-racs.

8.3.2 Horizon reference points

From a horizontal view, there are two kinds of interfaces: UNI, and NNI. UNI and NNI deal with the information transmitted end-to-end. Both of them cover several vertical planes.

User and network interfaces could be divided into three sub-layer as UNI-C, UNI-U and UNI-S according to the planes it covers.

UNI-User plane: It mainly deals with the data transport interface. A CPE sited on a CPN is connected to provider's network through this media interface. The interface between a CPE to the network provider's network might be wireless or wireline, such as xDSL, HFC, Ethernet and etc.

UNI-Service plane: This interface mainly deals with the user service request initiated from user to the service control function entities though signaling interfaces. Because of diversity of applications, the interface protocols used for this interface are various, such as SIP/SDP, H.323/H.245.

UNI-Control Plane: This interface will deal with the specific QoS requests from user CPE to the network resource control function after the prior authorization for the service from the Service control function. Some data services with QoS requirements but now without service signaling designed, like point-to-point or point-to-multipoint data delivery service, User CPE could map the application to the QoS requirements and can initiate a QoS request through RSVP, NSIS (that IETF is studying), or other protocols.

NNI-User plane: It mainly deals with the data transport interface between two networks. Access network or core network is connected with core network through this interface. It might be Ethernet, POS, ATM and etc.

NNI-Service plane: This interface mainly deals with the service request between two service control and management functions through signaling. Protocols used for this interface could be SIP/SDP, H.323/H.245.

NNI-Control plane: This interface will deal with the resource requests between two resource control and management functions. Protocols used for this interface could be RSVP, NSIS (that IETF is studying), or other protocols.

8.3.3 Examples for possible candidate for reference points

Table 3 – Possible protocols for reference points

Reference Point	Possible candidate protocols examples
RP1	RSVP, IETF NSIS (still not finalized), etc.
RP2	COPS-PR, Diameter, H.248, SNMP etc.
UNI-C,NNI-C	QoS signaling protocols, like RSVP, IETF NSIS , etc.
UNI-S, NNI-S	Call/Session control protocols, Like SIP/SDP,H.323/H245.

Some possible candidate protocols for these reference points are listed in Table 8-1.

In Figure 8-1, a generic end-to-end QoS architecture is introduced to provide service and resource control functions in an abstract setting. In this setting a user application creates a set of low level requirements related to QoS, Security etc. This process can be implemented using a user process and the network access can be achieved by a gateway which can be provided by various types of network providers, access network providers or by another application provider. These requirements are signaled to a service and resource control function by the User Gateway. A user gateway functions as an agent with generic functions and acts as a proxy functional entity that creates resource and service allocation requests and oversees the validation process. Generic QoS Control and Management Function in this abstract setting is responsible to provide admission control, service control functions as well as allocation of resources based on the general constraint based requirements. Path selection based on QoS parameters and network route optimization are functions provided among other functions, such as Monitoring, SLS, Policy management, security, authentication etc.. Since this is a generic architecture, implementation details are not provided here. Some of the possible implementations are distributed, centralized or hybrid resource and service control. After the resources are determined and requested service level requirements are satisfied and the necessary resources are allocated, the provided services and resources are guaranteed. This guarantee mechanism is provided by a framework that establishes measurement and validation mechanisms for each resource request across entities. In addition to these a synchronization mechanism is provided to have the network measurement, resource allocations and other necessary data to be synchronized across the network.

9 Interfaces and Functional Information Model

[Ed. NOTE: This section will describe interfaces and relevant requirements as well as Functional Information Model based. Signaling documents in SG11 will be referred and considered.Contributions are invited]

9.1 UNI

9.2 NNI

10 QoS mechanisms

Some of the proposed mechanisms are provided below:

Admission Control

Resource Control and Reservation

Parameter Tuning

TE

- QoS Routing Constraint-based routing
- Traffic Data Analysis
- Anomaly Analysis

Traffic Conditioning

- Marking
- Shaping
- Policing

Congestion Avoidance

SLS Management

Capacity Management

Monitoring Measurement

Reliability Management

Policy Management

A QoS enabled node will have the general architecture shown in Figure 10-1. The focus of this section is on the forwarding path that is depicted by the bottom layer of Figure 10-1. The functionality illustrated in this layer includes packet classifier, policer, marker, the forwarding engine and the queue manager. Not all these functions will exist at every node in the network. The presence or absence of a certain function depends on whether the node is located at the edge or at the core of the network.

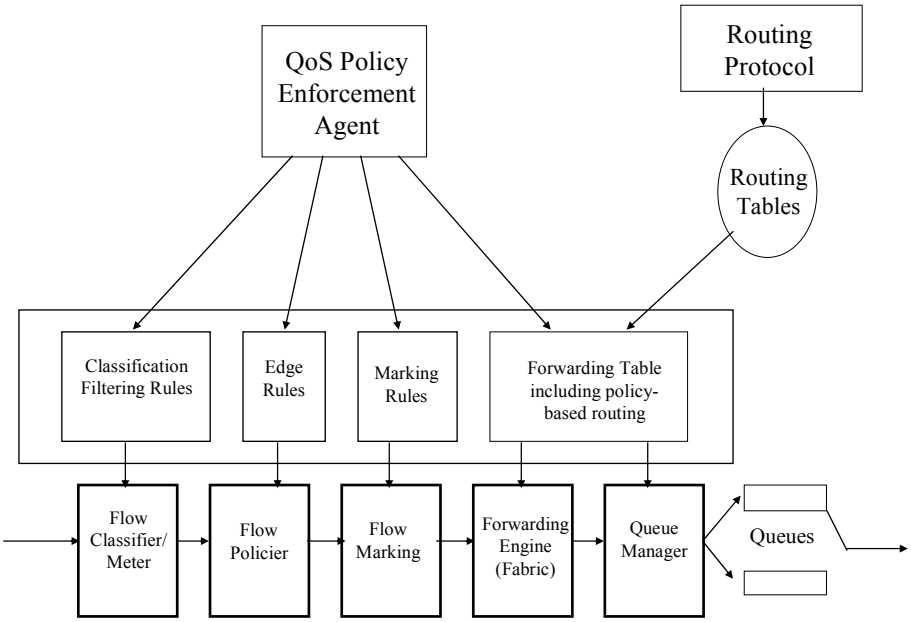


Figure 10-1 – General Nodal Architecture

Edge nodes are likely to include all the functions shown at the bottom layer of Figure 6. The Edge node is the place where flow classification, policing, shaping, and marking take place. The execution of these functions requires the availability of per flow state at the edge. These functions are driven by policies enforced by a policy enforcement agent resides at the node. The policy enforcement agent is likely to communicate with a network management entity (or a policy manager). This policy manager supervises the operation of the sub-network.

The design of the core nodes includes a subset of the functions shown in at the bottom layer of Figure 6. Classifications, policing, and marking are not necessary functions at the core nodes. Hence those nodes are relieved from the burden of keeping per flow state. This makes the network architecture scalable to a large number of flows.

Traffic conditioning function is required at the edge of the network. The requirements of the traffic conditioning function are:

- Ability to enforce multiple traffic parameters that might include committed rate, excess rate, and burst sizes, and,
- Ability to drop or re-classify and remark non-conformant traffic

Leaky bucket and time sliding window are two possible implementations of the metering function. The leaky bucket algorithm in particular has seen a wide deployment in the context of ATM switches because of its ease of implementation. Several metering/marking algorithms based on leaky bucket algorithm are available. Among those are FR algorithm in ANSI 606, RFC 2697 and *RFC 2698.*

In addition to the metering function, shaping might be needed at the network egress. Its value stems from its ability to avoid unnecessary traffic loss due to traffic characteristics mismatch as traffic crosses network boundaries. A requirement of the shaping function is the ability to pace packets according to a contracted rate and shape.

The implementation of the shaping function requires the support of per flow queues at the egress nodes. One possible implementation of the shaping function is based on buffered leaky bucket with a bucket size in the order of one packet. Such an implementation is usually referred to as peak-rate shaping.

Shaping function at the core nodes is not recommended. Shaping is a non-work conserving queuing discipline in the sense that the link could go idle while packets are sitting in the buffer. Therefore shaping could have some negative effects on the throughput of the network and packet delays.

Requirements of the queue manager entity are:

- A class queue with sufficient number of classes to support various services.
- Minimum bandwidth assurances per class
- Minimum buffer allocation for each class queue to avoid the buffer starvation
- Support of active queue management mechanisms such RED or WRED for TCP flows
- Support for simple discard thresholds for non-TCP flows, e.g. real-time traffic utilizing the UDP protocol.

[Ed. NOTE: This section will describe QoS mechanisms that are needed in the generic and specific architecture interfaces Contributions are invited]

10.1 QoS notification scheme between the CPEs

Speech and voice band media signals that have real-time properties are transmitted over IP-based networks between the CPEs using RTP/RTCP. The QoS parameters such as delay, packet-loss and jitter of RTP packets are included in the RTCP reports. The CPEs which receive RTP packets and the RTCP reports are able to reconstruct the sender's packet sequence and to maintain the QoS of media signals.

The QoS notification scheme based on the RTP/RTCP is not only applicable to QoS control mechanisms of end to end CPEs themselves but also to performance measurements and monitoring schemes of nodes located among the CPEs in NGN. Considering this feature of the RTP/RTCP, some example approaches of obtaining QoS parameters and schemes at CPEs connected to the NGN are shown in the Appendix 2.

10.2 QoS mechanisms in CPN

An end-user can be in a "private" network (e.g. LAN of an enterprise or a university) that establishes connections to the Access network or in a private network that is maintained by the end-customer. Due to administration and maintenance reasons these networks are not open to general public and more confidentiality is guaranteed within these "private" networks compared to other public networks. These "private" networks are called CPN (Customer Premises Network).

The CPN may offer additional private applications and data transport services for their end users. The CPN interconnects end-customers to an access network and groups the end-customers. It represents a group of end-customers in terms of a common policy and "hides" the individual user (end-customer) to the Access network.

The CPN is a key component of the whole network. When one end-user in a CPN communicates the other end-user in another CPN, the traffic between them has to go through at least two CPNs. For providing end-to-end QoS support, some QoS mechanisms are provided in the CPN. On the other hand, because the CPN is a "private" network, for administration and maintenance reasons one could add a "CPN QoS control and Management Functionality" in every CPN, and this will be responsible for the resource management within the CPN. If necessary, the "CPN QoS control and Management Functionality entity" could cooperate with the network "QoS Control Function Entity".

10.3 QoS mechanisms in access network

[Ed. NOTE: This section will describe QoS mechanisms in access networks. It is related to the findings of general access network QoS mechanisms that is being developed under Y.ipaqos]

10.4 QoS mechanisms in core network

[Ed. NOTE: This section will describe QoS mechanisms in core networks. It will contain some of the material listed in NGN-WD-87 listed under Y.e2eqos. Contributions are invited]

10.5 Interdomain and Interworking QoS mechanisms

[Ed. NOTE: Me3chanisms of the QoS architecture relevant to be given to ensure the interworking between different domains, different technologies and different authorities. Contributions are invited]

11 Interaction with AAA system

[Ed. NOTE: This section will describe interaction of the architecture with AAA systems. It will contain some of the material listed in NGN-WD-87 listed under Y.e2eqos. Contributions are invited]

12 Interaction with network management system

[Ed. NOTE: This section will describe interaction of the architecture with NMS. Contributions are invited]

13 Other considerations

13.1 Business Considerations

The general model shown in Figure 1 allows users to access the networks and other users through a User Gateway functionality to provide various services. This is a generic device that allows various access network realizations and transport networks to provide end-to-end services. These gateways can be provided by different types of network providers (mobile, fixed access, or other types of service providers). Depending on the provider supplying the User Gateways, there will be different requirements and functionalities. Service control, admission control and resource and QoS support will be based on these. New business models are needed for each case since the access and transport collaboration is quite different in fixed and wireless providers. This will involve service agreements and requirements, security issues, and revenue sharing as well as service verification among network entities. The mechanisms can support the centralized versions as well as totally distributed and hybrid implementations. Enabling peer-to-peer applications are also important consideration in any end-to-end architecture scenarios. One important

consideration of many of these applications is to have charging and revenue sharing mechanisms and the provided architecture have functional blocks that can address each of these issues.

[Ed. NOTE*: This section will describe general business considerations relevant to this framework draft.* The following text provides a non-exhaustive list of gradual deployment scenarios. Eventually a separate document on deployment strategies triggered by the text below may be formed when this document is finalized.Additional Contributions are invited.]

Phased deployment for end-to-end QoS

The issues regarding QoS inside the networks have been studied for years, with increasing importance with the development of next generation networks. To keep the Capex low, it is important to deploy QoS services in the current network in a progressive manner. The following is a guideline for a phase-in deployment.

1) *From access to core network*

The deployment of QoS mechanisms should start from the access network to the core network. Access network has been the bottleneck for traffic and hence QoS mechanisms should be deployed first. In the phase-in approach, the end-to-end QoS issue can be divided into two stages:

- In the first stage, resource control and management functions could be introduced in access network while assuming core network is over-provisioned.

  In this case, for an end-to-end QoS assurance, the inter-domain and inter-provider QoS signalling is not needed because the resource control is local. Only the protocols inside the access network need to be considered. The interaction between the access and core network will only be the interactions on the transport layer with unified service classes specifications and mappings.
- In the second stage, the QoS signalling function (i.e. resource controllers) between the access and core networks can be considered. For the core network, the capacity planning tools and traffic engineering mechanisms needed to be in place when such interactions are to be taken place.

2) *From intra- provider to inter-provider*

To improve and implement the QoS mechanism inside a provider's network, there are a wide range of mechanisms to choose, such as DiffServ, MPLS-enabled network with separated or embedded resource controller. Once theissues regarding the intra-provider is resolved, the inter-provider situation can be addressed.

For inter-provider consideration, new features need to be added such as the QoS signalling.

3) *From the transport network equipment to the control layer*

Part of the QoS implementation is based on the transport network equipment. The phase-in approach for QoS is to make the transport network equipment ready as first priority, for example, to keep the wire-rate QoS processing including classification, differentiated queuing and scheduling. Once proper equipment is in place, control functions can be added to co-ordinate the service layer requirement and transport network capabilities.

4) *From pre-provisioning to dynamic per-session QoS assurance*

Deploying the dynamic session-based QoS resource control may be impractical initially. Involved technologies are the usual hurdles in network reliability, network scalability, and service marketability. The first stage in the phase-in approach should consider pre-provisioning the network resource. The pre-provisioning approach to QoS will simplify the admission and resource control function and hence improve network reliability and scalability.

Dynamic per-session based resource allocation can be implemented when the protocols are standardized and when there is market demand.

At any stage, the carriers can decide if more QoS mechanisms are needed with proper investment and financial considerations.

Appendix I

Scalability consideration

The following components and methods need to be considered for scalable systems and scalability requirements.

Number and size applications

Number of client systems supported

Number of concurrent users

Load growth and application load profiles

Geographical distribution of load

Load distribution by time (daily, time of day, seasonal etc.)

Load balancing strategies

Administration and maintenance considerations

Caching and replication methods

Multicast mechanisms used to increase scalability

Number of simultaneous connections,

Size of data and control messages exchanged,

Usage of multi-threading,

Distribution and managing objects

For the distributed resource layer: network capacity, hardware configuration, replication mechanisms, fault-tolerance, transport layer, and bridging technologies.

Middleware products and their performance

Number and arrangement of servers

Authentication and user profile management

Hardware and software limits of each product (CPU, buffers. etc.)

Configuration and tuning used in basic hardware and software (routers, gateways, softswitches etc.)

A detailed example study providing guidance needs to be developed that shows the impact of these factors on scalability.

In addition several other important factors that help provide scalable systems with necessary QoS support need to be will developed such as:

Scalability testing

Monitoring and Measurements

Performance : response time, throughput, etc

Device, OS, application server, DB, I/O, and middleware limits- configuration parameters

Load Balancing

Methods of load balancing-measurement based auction based

Replication and cashing

Distributed and centralized schemes

Multicasting schemes

Modelling, Analysis and Simulation

The usage of modelling, analysis and simulation should be investigated on the determination of scalability requirements of NGN applications and architectures.

Appendix II

A sample measurement methodology of QoS parameters based on RTP/RTCP

Definition of QoS parameters based on RTP/RTCP

RTCP packets are periodically transmitted for the feedback on the quality of data distribution using RTP packets. However there are several kinds of packets in RTCP, the Packets of Sender Report (SR) and Receiver Report (RR) are used for monitoring the quality of service. Please note that the granularity of QoS parameters can be adjusted by the period of the communication of RTCP packets.

SR RTCP packet mainly includes,

1) SSRC of sender: identify source of data
2) NTP timestamp: when report was sent
3) RTP timestamp: corresponding RTP time
4) Packet count: total number sent and RR RTCP packet mainly includes,
    1) SSRC of sender: identify the source to which this RR block pertains
    2) fraction lost: since previous RR (SR) sent
    3) cumulative number of packets lost: long term loss
    4) highest sequence number of received: compare losses
    5) interarrival jitter: smoothed interpacket distortion
    6) LSR: time when last SR received
    7) DLSR: delay since last SR

Sending and Receiving CPEs should calculate the following QoS parameters by Sender/ Receiver reports of RTCP.

a) Delay (Sender Report: SR)
    1) Delay

        Value derived from the RTCP RTT (Round Trip Time) divided by 2.
    2) Mean Delay

        Mean value of delay for the current reported time interval.
    3) MaxDelay

        Largest value of delay during a call (this value is renewed in each reported time interval).

b) Packet Loss (Receiver Report: RR)
    1) CumulativeNumberOfPacketsLost

        Cumulative number of packets lost of last sent RTCP Receiver Report.
    2) MaxPacketLostRate

        Maximum value of difference between Cumulative number of packets lost of last sent RTCP Receiver Report of last time interval and last sent RTCP Receiver Report of currently reported timer interval per second.

c) Jitter (Receiver Report: RR)
    1) InterarrivalJitter

Indicating the *Interarrival Jitter* of sent *RTCP Receiver Report* in timestamp units.

2) MeanJitter

Average value of ***CalculatedJitter*** calculated from all sent *RTCP Receiver Reports* for the current reported time interval.

3) MaxJitter

Largest value of ***CalculatedJitter*** from all sent *RTCP Receiver Reports* during a call (this value is renewed in each reported time interval).

4) Standard deviation of jitter

Standard deviation value of ***CalculatedJitter*** calculated from all sent *RTCP Receiver Reports* for the current reported time interval.

Calculation schemes

A. Delay (Sender Report: SR)

A calculation scheme to provide information of QoS parameters based on RTP/RTCP is shown in Figure II-1. In this figure, for example, the delay value (QoSx) is calculated in the CPE. A calculation interval of QoSx based on the RTCP packets' interval should be defined in the profile of CPE.

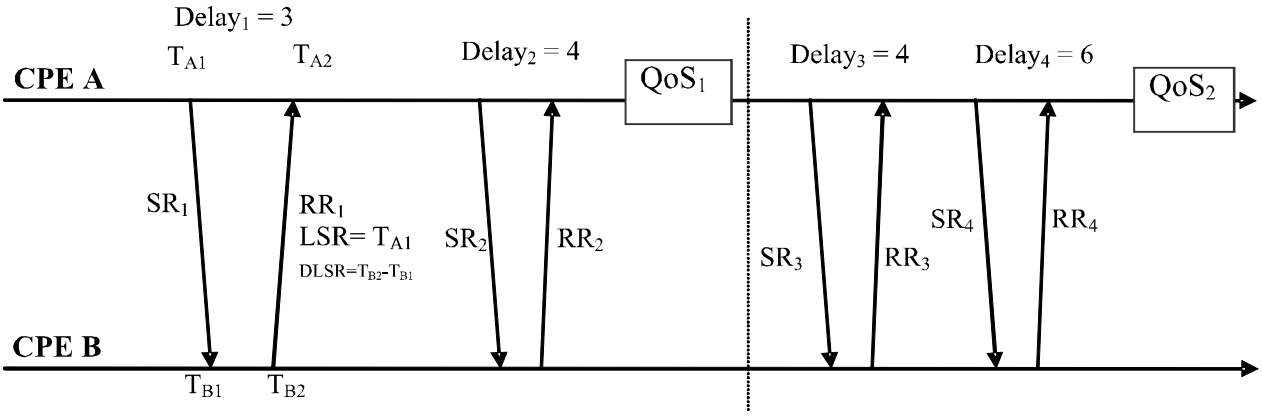


Figure II-1 – Calculation scheme for Delay value

Delay $= Delay_1$

$= (T_{A2} - LSR - DLSR) / 2$

$= \{ T_{A2} - T_{A1} - (T_{B2} - T_{B1}) \} / 2$

QoS_1:

Delay = Delay2 = 4,

MeanDelay = (3 + 4) / 2 = 3.5

MaxDelay = Max (3, 4) = 4

QoS_2:

Delay = Delay4 = 6

MeanDelay = (4 + 6) / 2 = 5

MaxDelay = Max (4, 6) = 6

B. Packet Loss (Receiver Report: RR)

A calculation scheme to provide information of QoS parameters based on RTP/RTCP is shown in Figure II-2. In this figure, for example, the Packet Loss value (QoSx) is calculated in the CPE. A calculation interval of QoSx based on the RTCP packets' interval should be defined in the profile of CPE.

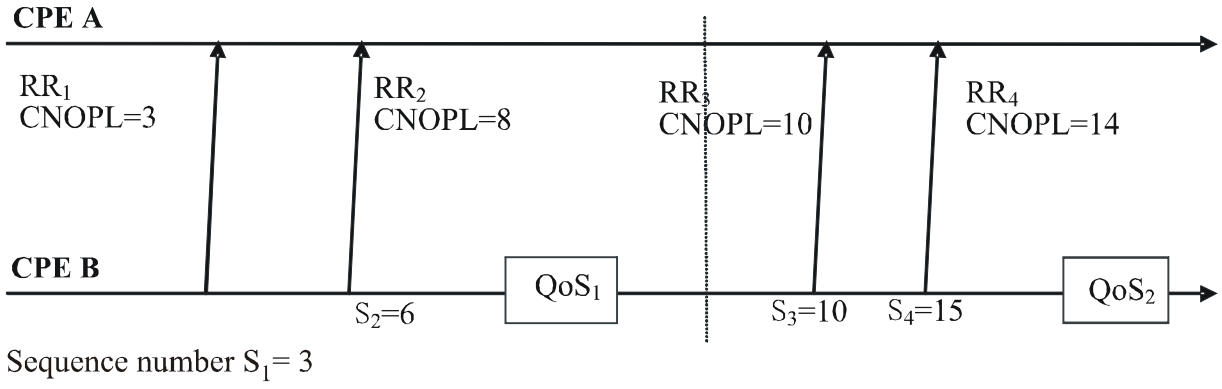


Figure II-2 – Calculation scheme for Packet Loss value

QoS_1:

CNOPL = CNOPL of RR2 = 8

MaxPacketsLostRate

= (CNOPL of RR2 – CNOPL of RR1) / (S2 – S1) = (8-3) / (6-3) = 1.67

QoS_2:

CNOPL = CNOPL of RR4 = 14

MaxPacketsLostRate

= Max((CNOPL of RR3 – CNOPL of RR2) / (S3 – S2), (CNOPL of RR4 – CNOPL of RR3) / (S4 – S3))

= Max((10 – 8) / (10 – 6), (14 – 10) / (15 – 10))

= Max (0.5, 0.8)

= 0.8

C. Jitter (Receiver Report: RR)

A calculation scheme to provide information of QoS parameters based on RTP/RTCP is shown in Figure II-3. In this figure, for example, the Jitter value (QoSx) based of RFC 3550 is calculated in the CPE. A calculation interval of QoSx based on the RTCP packets' interval should be defined in the profile of CPE.

QoS_1:

InterarrivalJitter = $S.jitter_2 >> 4 = 7$

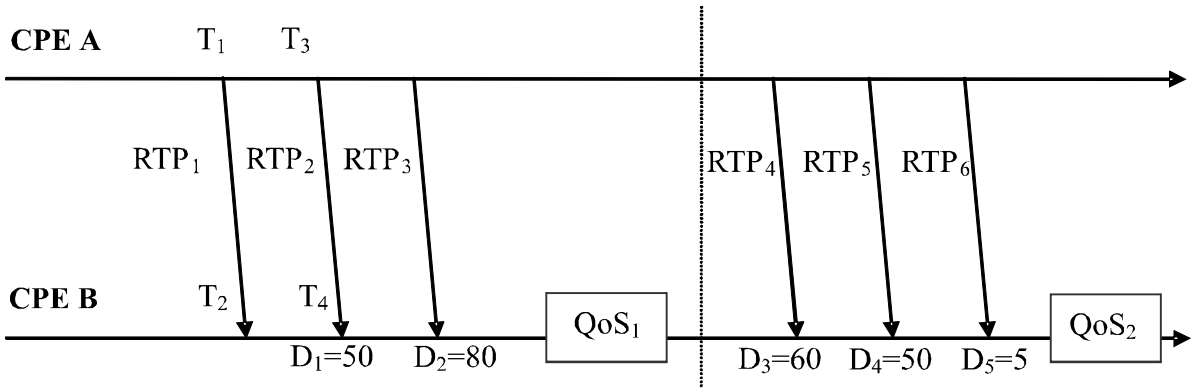
1) $S.jitter_1 = 0 + (50 – ((0 + 8) >> 4)) = 0 + (50 – (0)) = 50$

2) $S.jitter_2 = 50 + (80 – ((50 + 8) >> 4)) = 50 + (80 – (3)) = 127$

MeanJitter = (50 + 80) / 2 = 65

MaxJitter = Max (50, 80) = 80

Standard deviation of jitter = this value is calculated based on Dx and Mean Jitter values.



$Transit_1 = T_2 - T_1$, $Transit_2 = T_4 - T_3$

$D_1 = |Transit_2 - Transit_1|$

Intrarrival Jitters=$S.jitter_1 += D_1 - ((S.jitter_0=0 + 8) >> 4)$;

Figure II-3 – Calculation scheme for Jitter value

QoS_2:

InterarrivalJitter = $S.jitter_5 >> 4 = 13$

1) $S.jitter_3 = 127 + (60 – ((127 + 8) >> 4)) = 127 + (60 – (8)) = 179$
2) $S.jitter_4 = 179 + (50 – ((179 + 8) >> 4)) = 179 + (50 – (11)) = 218$
3) $S.jitter_5 = 218 + (5 – ((218 + 8) >> 4)) = 218 + (5 – (14)) = 209$

MeanJitter = (60 + 50 + 5) / 3 = 38

MaxJitter = Max (60, 50, 5) = 60

Standard deviation of jitter = this value is calculated based on Dx and Mean Jitter values.

References

[1] IETF RFC 3550, "A Transport Protocol for Real-Time Applications", July 2003.

[2] IETF RFC 3611, "RTP Control Protocol Extended Reports (RTCP XR)", November 2003.

[3] ITU-T Rec. Y.1540, "Internet protocol data communication service -IP packet transfer and availability performance parameters", December 2002.

[4] ITU-T Rec. Y.1541, "Network performance objectives for IP-based services", May 2002.

[5] IETF RFC 2330, "Framework for IP Performance Metrics", May 1998.

Annex A

Supplementary material to be inserted into the main document

[Ed. NOTE: There is no concensus on the status of this Annex, however this is maintained in the hope of using it in the main body of this draft]

This part copies some sections from TRQ document with minor modification, and needs editing and further development,user/TE needs to beclarified]

QoS signalling requirements are expressed in terms of attributes include the following:

- the network QoS Class (i.e., Y.1541 [7]/Table 1);
- the network capacity required, at both the application and network (i.e., Y.1221 [9]) levels;
- the reliability/priority with which the service is to be sustained; and
- other elements of QoS.

Note that the complete set of classes for reliability/priority is yet to be defined.

This document recognises that an automated system for obtaining User-to-User QoS on IP Networks, and on combinations of various network technologies, will require standard signalling protocols for communicating the requirements among the major entities. For the purposes of this document, these entities are defined as:

1) Users and their end Terminal Equipment (TE); and
2) Network Service Providers/Operators and their equipment, especially equipment implementing the inter-working and signalling function between networks, and between users and networks.

Requirements

Authentication of User and Network Peers is a prerequisite for QoS signalling. Authentication may be accomplished by static extension of the zone of trust, or through an Authentication Protocol, which is beyond the scope of these requirements.

User-Network Signalling

The following requirements apply to QoS Signalling between Users (or their terminal equipment) and the responsible network entity. Attributes of a User QoS Request

It shall be possible to derive the following service level parameters as part of the process of requesting service: (Some of these may not be explicitly communicated by the user.)

1) QoS class from Y.1541 [7][4]
2) peak rate (Rp)
3) peak bucket size (Bp)
4) sustainable rate (Rs)
5) sustainable bucket size (Bs)

[4] The values of IP Loss Ratio, IP Transfer Delay, and IP Delay Variation as specified in Y.1221 [9] may be derived by specifying the QoS class from Y.1541 [7] as a signalling parameter.

6) maximum allowed packet size (M)

It should be possible to derive the following service level parameters as part of the process of requesting service:

1) the Reliability/Priority with which the service is to be sustained, and

2) other elements of QoS.

Note that the complete set of classes for Reliability/Priority is to be defined.

Users must be able to initiate requests for service quality. Such requests may have the following attributes if the TE has this ability:

- the network QoS Class (e.g., Y.1541 [7]/Table 1);
- the network Capacity required, at both the application and network (e.g., Y.1221 [9]) levels;
- the Reliability/Priority with which the service is to be sustained; and
- other elements of QoS.

Note that the complete set of classes for Reliability/Priority is to be defined.

Optional attributes include the user Application type and quality from among several quality categories, when such categories are available. The type of application may be completely specified from the chosen quality category.

Terminal Equipment (TE) may compose the detailed request on the user's behalf, possibly based on configurations set by the user or equipment installer. Many TE may have the flexibility to match the user's request for application quality with network QoS classes by selecting parameters such as source coder type and packet size.

Omitting Attributes of a User QoS Request

Network QoS Class, Capacity, and Reliability/Priority are required attributes; others are optional. The Network Provider may assign default values for omitted attributes.

For example, Speech quality categories have been defined in ITU-T Rec. G.109 [12], but there is no comparable standard range of quality categories for Web browsing, financial transactions, or many other applications of networks (each is associated with a limited quality range in new ITU-T Rec. G.1010 [13). ITU-T Rec. P.911 [14] tabulates quality categories for Multimedia Communication (also known as video/audio/data conferencing) and Television applications. Users may simply wish to make requests for capacity, network QoS class, and reliability.

A user/TE may make a service request without providing explicit QoS parameters.In case where explicit QoS request is initiated by TE the following requirements apply.

Form of a Verifiable User QoS Request

The QoS requests made by the user/TE must be in terms that the network understands, especially the parameters for Network QoS. The Network QoS Classes and Network Capacity specifications in the signalling protocol must contain values that are verifiable by users (the classes in Y.1541 [7] meet that requirement). TE may conduct measurements to ensure that the committed performance and capacity levels are achieved by the network(s).

Special Case of User QoS Request to support Voiceband Channels

When the user/TE request is for a voiceband channel (to support speech or voice band modems), the QoS request (or other associated message) should contain the preferred voiceband codec and packet size. Other

optional parameters may be included to indicate, for example, the use of silence suppression, the need for network echo cancellation, and alternate codecs/packet sizes.

Many of the capacity attributes will be determined by this codec choice. Also, the network operation benefits from knowledge of the codec when the need for voice transcoding can be identified (and possibly avoided). However, much of the negotiation of application parameters takes place beyond the network's purview.

Flow Control for User QoS Requests and Re-requests

The TE must wait X seconds before re-submitting a request, and may have a maximum of Y simultaneous requests outstanding. Time-outs for re-submission will increase exponentially. The protocol must be "congestion-aware," using failed requests as implicit indications of congestion or using explicit notification of congestion, if available.

Network Response to User QoS Requests

Network Service providers should be able to communicate the following messages and attributes (in the case of user-network interaction):

1) An Identification Code for the request exchange, to be used in this response and all messages that follow (such as User ACK, or Release, and also in Network-Network messages). When used together with other information, such as Src address, each request can be uniquely referenced.
2) The simple acknowledgement and acceptance of user/TE requests.
3) The performance level expected. The ability to achieve a performance level that is better than an aspect of the QoS Class response, if the network operator desires. This indication may be made for a single performance parameter, or for a combination of parameters.
4) The ability to reject a request and, at the same time, to offer a modified service level that can be met. The response may modify the request and may include commitments to an alternate QoS Class, a lower capacity, and other indications such as those in item 3.

The processing of each request and determination of acceptance require considerable work on behalf of the network provider/operator. Networks may wish to indicate a maximum time interval for which the response is valid.

User Answer to Network QoS Response

The final decision to accept or reject an offered service is left to the user/TE. This completes a Request-Offer-Answer exchange.

QoS Signalling at the Network – Network Interface

Network-network interfaces include the QoS related interfaces between network providers and between service provider and network providers in case that they have different ownership.

[Ed. NOTE: This part needs to be further clarified

This section treats the case where multiple networks co-operate to realise the end-to-end connectivity desired. Beyond the applications considerations mentioned above, network providers/operators primarily deal with Network QoS Classes, Network Capacity, and Reliability. Network-network signalling is the principal way for networks to determine multi-network compliance with QoS classes, since fixed performance allocations are not currently possible on IP Networks.

Network - Network signalling shall support the determination of the QoS Class offered to the user/TE, by communicating both the Network QoS Class requested, and the extent to which each specified parameter is already consumed. This implies that each network knows the performance from the entrance node to the (most likely) exit node(s) for the network that has the best opportunity to complete the end-end path. Policies

may also determine the next network chosen. The best-next network receives the network-network signalling request.

Networks shall determine if the desired capacity and reliability are available to support the specified Network QoS Class from entrance to exit node(s).

Attributes of a Network QoS Request

The attributes of the network's request are:

- the network QoS Class (e.g., Y.1541 [7]/Table 1), along with the consumption of individual objectives that are specified by the class;
- the network Capacity required, at both the application and network (e.g., Y.1221 [9]) levels;
- the interconnecting point(s), where user/TE traffic will leave the requesting network and enter the next network;
- the Reliability/Priority with which the service is to be sustained; and
- other elements of QoS.
- Note that the complete set of classes for Reliability/Priority is yet to be defined.

Optional attributes include the user Application type and the quality category, when such categories are available and meaningful.

Omitting Attributes of a Network QoS Request

Network QoS Class, Capacity, and Reliability/Priority are required attributes; others are optional.

Performance Requirements for QoS Requests and Re-requests

An important aspect of the requirements for a signalling protocol is the performance requirement associated with that protocol. The most important areas where signalling performance requirements need to be established is the average / maximum latency for the establishment of service and the average / maximum latency for the re-establishment of service in the event of a network failure. The latency requirements described above for the signalling protocol depend on the performance characteristics of the underlying transport network. Because of this, performance requirements for the transport network must be specified along with the latency requirements for the signalling protocol. The combination of these factors leads to the following formal performance requirements for the signalling protocol.

1) Networks designed to meet the signalling protocol requirements specified in this section should be capable of supporting the network performance objectives of QoS class 2 in Y.1541 [7].
2) The average delay from the time of a UNI or NNI request for service to the acceptance or rejection of this service request by the network should be <800 msec.
3) The maximum delay from the time of a UNI or NNI request for service to the acceptance or rejection of this service request by the network should be <1500 msec.
4) The average delay from the time of a network failure to the time of re-establishment of service at any UNI or NNI interface should be <800 msec. (This does not address restoration of failed links.).
5) The maximum delay from the time of a network failure to the time of re-establishment of service at any UNI or NNI interface should be <1500 msec.

Response to a Network QoS Request

Network providers shall be able to respond with the following messages and attributes (in the case of network-network interaction):

1) The ability to correlate all responses and subsequent requests to the original request is required. An Identification Code is one example.
2) The simple acknowledgement and acceptance of requests.
3) The ability to indicate a performance level that exceeds an aspect of the request/response is required, but the indication to other entities is a network option.
4) The terminating network supporting the destination UNI shall offer a modified service level if the original service level cannot be met. The modified service may include commitment to an alternate QoS Class, a lower capacity, etc.

It is possible that a chain of network-network QoS requests will encounter a network that does not support the QoS signalling protocol or QoS Classes in general. If this network is an essential section of the end-to-end path, then several results are possible. One is to reject the request, but at the same time offer an Unspecified Class (e.g., Class 5 of Y.1541 [7]), possibly with the indication of some additional parameter values.

When making entrance-to-exit performance commitments, only one of the interconnecting links will be included for all networks, except the first network which shall include both the link to the UNI and the link to the NNI (subsequent networks will include the exit link to the next interface, either NNI or UNI).

Accumulating Performance for Additional Requests

Signalling must communicate the consumption of the network (source-UNI to destination-UNI) QoS objectives.

QoS Release

Users and Networks shall be able to signal when a previously requested network resource is no longer needed.

Performance

For reasons of signalling performance, the following areas should be addressed:

– the number of messages required to establish, maintain and clear QoS requests should be kept to a minimum; and
– the format of the IP Signalling Protocol information should be chosen to minimize message-processing delays at the endpoints.

Symmetry of information transfer capability

The QoS Signalling protocol shall support symmetric QoS Requests.

Asymmetric QoS Requests are optional. That is, the end-to-end requests may be bi-directional where the information transfer capability in each direction might be different.

Contention resolution

The QoS Signalling protocol shall be able to resolve all contentions with respect to resource allocation and collision.

Error reporting

The QoS Signalling Protocol shall include mechanisms for detecting and reporting signalling procedural errors or other failures detected by the TE/Network. Service failures may also be reported to the User.

Unrecoverable failures

The TE and Network Entities shall include mechanisms for returning the QoS protocol instance to a stable state after detection of unrecoverable failures.

Forward and backward compatibility

The QoS Signalling Protocol shall include a forward compatibility mechanism and backward compatibility rules.

Parameters and values for Transport connections

The signalling protocol(s) at UNI and NNI interfaces should be capable of specifying the following additional parameters as part of the process of requesting service:IP header fields: source + destination address (RFC 791 [1], RFC 2460 [2]);Source + destination port as specified in RFC 768 [4] and RFC 793 [5].

User-Initiated QoS Resource Modification

If the QoS request is initiated by User/TE explicitly, the following requirements apply.

Either User may be able to modify the resources associated with an active Transport connection, represented by the information contained in the Transport Connection messages.

Collision of connection resource modification requests shall be avoided by the Served User.

Modification shall be performed with no loss of IP transport contents.

The use of the preferred Transport Connection messages is to avoid the need for subsequent modification of the connection resources immediately after the establishment.

User/TE (IP Endpoints) should determine, through the use of end-end application level capability signalling, the ability and support to use resources beyond those currently in use. The support / lack of support of the capability to modify Transport Connection messages, for a Transport connection must be indicated by the originating IP Endpoint. The terminating IP Endpoint must indicate the support / lack of support of the modification capability of the Transport Connection messages. Only when both Endpoints indicate modification support can modification be attempted.

This capability uses the following objects:

1) Transport Connection message Modification Support Request,
2) Transport Connection message Modification Support Response.

Emergency Service

Requirements for support of Emergency Services may be specified in a future version of this document. The protocol will identify reserved objects, bits, etc. This topic is treated in general under reliability and priority attributes.

Reliability/Priority Attributes

Reliability/Priority attributes are the same for User-Network and Network-Network signalling requirements. Reliability for a service can be expressed in the form of a priority level with which that service requires a particular type of network function (e.g., Connection Admission Control Priority). Hence, reliability can be requested in the form of a Priority Class for that specific network function. Two types of network functions apply for Reliability/Priority classes: Connection Admission Control and Network Restoration. As an example, emergency services can signal for the highest available connection admission control priority during emergency conditions.

No formal standards exist with respect to the qualitative (e.g., number of priority classes) or quantitative (e.g., time-to-restore) aspects of reliability. From the viewpoint of signalling, there should be a limited number of Priority Classes for all network functions in order to ensure scalability (e.g., 4 classes). The signalling protocol needs to be able to provide the capability to effectively convey these priority requests once priority level attributes are established in standards forums.

2.10 – The Qos Architecture for the Ethernet Network*

Introduction

From the NGN requirements, the Ethernet network can be a best candidate as future packet transport mode. For the specific requirements from control-/management views of NGN, The QoS architecture for the Ethernet network has to consider the following concerns.

– Flexible Connection Configuration and bandwidth allocation
  - Dynamic provisioning for end-to-end connectivity
  - Priority, access control, and security protection, etc.
  - TE/QoS handling for acceptable end-to-end quality
– End-to-end/segment OAM and Protection & Restoration
  - End-to-end OAM, segment OAM
  - Segment-wise 1+1 Protection & Restoration (P&R), end-to-end P&R
– L1/L2/L3 VPN services
  - Access control, QoS, and security according to VPN services
– Support integration of L2 ~ L7 switching capabilities
  - TE/QoS, routing, and control processing, etc.
  - Binding of the MAC address and VLAN ID. Furthermore, if possible, binding between Ethernet MAC and high layer services.

The Ethernet-based NGN is broadly characterized as employment of IP protocols for control of Ethernet data flows. In underlying hardware layer, most data link feature and interface defined in IEEE 802.3 will not be altered. However, intelligent signaling and routing protocols of NGN will be necessary in replacement to simple bridge control algorithms [STP][MSTP].

The overall scope of the Ethernet network will cover not only the area of customer's local network but provider's access network and core network that employ Ethernet technology.

* Status D: The FGNGN considers that this deliverable is not yet mature, requiring discussion and technical input to complete development.

Table of Contents

2.10 – The QoS Architecture for the Ethernet Network

1 Scope

The scope of this draft includes

- Service definitions and requirements of the Ethernet based NGN
- Reference Model of QoS Architecture for the Ethernet based NGN
- QoS Procedures for the Ethernet based NGN

2 References

[1] ITU-T Recommendation I. 371, Traffic control and congestion control in B ISDN

[2] ITU-T Recommendation G.8080, Architecture for the Automatically Switched Transport Network

[3] ITU-T Recommendation G.8010/Y.1306(2004), Architecture of Ethernet layer networks

[4] ITU-T Recommendation G.8011/Y.1307(2004), Ethernet over Transport – Ethernet services framework

[5] ITU-T Recommendation G.8011.1/Y.1307.1(2004), Ethernet private line service

[6] ITU-T Recommendation G.8012/Y.1308(2004), Ethernet UNI and Ethernet NNI

[7] TU-T Recommendation G.8021/Y.1341(2004), Characteristics of Ethernet transport network equipment functional blocks

[8] ITU-T Recommendation Y.1291(2004), An architectural framework for support of Quality of Service in packet networks

[9] ITU-T Recommendation Y.1710(2002), Requirements for Operation & Maintenance functionality for MPLS networks

[10] ITU-T Recommendation Y.1711(2004), Operation & Maintenance mechanism for MPLS networks

[11] ITU-T Recommendation Y.1711-Corrigendum 1(2005), Operation and maintenance mechanism for MPLS networks Corrigendum 1

[12] ITU-T Recommendation Y.1712(2004), OAM functionality for ATM-MPLS interworking

[13] ITU-T Recommendation Y.1720(2003), Protection switching for MPLS networks

[14] ITU-T Recommendation Y.1720-Erratum(2004), Protection switching for MPLS networks

[15] ITU-T Recommendation Y.1730(2004), Requirements for OAM functions in Ethernet-based networks and Ethernet services

[16] ITU-T FGNGN-ID-797, Draft FGNGN-FRA version 5.1

[17] IETF RFC2284(1998), PPP(Point-to-Point Protocol) Extensible Authentication Protocol (EAP)

[18] IETF RFC3748(2004), Extensible Authentication Protocol (EAP)

[19] IETF RFC3031(2001), Multi-protocol Label Switching Architecture

[20] IEEE Standard 802.1q, Virtual Local Access Network

[21] IEEE Standard 802.1p, LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization

[22] IEEE Standard 802.1D(1998), Media Access Control(MAC) Bridges

[23] IEEE Standard 802.1Q(2003), Virtual Bridged Local Area Networks

[24] IEEE Standard 802.1s(2002), Multiple Spanning Trees

[25] IEEE Standard 802.1w(2001), Rapid Reconfiguration of Spanning Trees

[26] IEEE Standard 802.1x(2001), Port Based Network Access Control

[27] MEF 1.0(2003), Metro Ethernet Forum, Ethernet Service Model, Phase 1

3 Abbreviations

A-BGF Access Border Gateway Functional entity

ABR Available Bit Rate

ABT Available Block Transfer

AF Assured Forwarding

ANF Access Node Functional entity

APS Automatic Protection Switch

ATM Asynchronous Transfer Mode

A-TRCF Access Transport Resource Control Functional entity

BE Best Effort

BGF Border Gateway Function

BW Bandwidth

CAC Connection Admission Control

CBR Constant Bit Rate

CBS Committed Burst Size

CIR Committed Information Rate

CL-PS Connectionless, Packet-Switched

CO-CS Connection Oriented, Circuit-Switched

CO-PS Connection Oriented, Packet-Switched

COS Class of Service

CPE Customer Premises Equipment

CPN Customer Premise Network

C-TRCF Core Transport Resource Control Functional entity

DF	Default Forwarding
EAP	Extensible Authentication Protocol
EAPOL	EAP over LANs
EBS	Excess Burst Size
EF	Extended Forwarding
EIR	Excess Information Rate
ENF	Edge Node Functional entity
E-PHB	Ethernet Per Hop Behavior
EPL	Ethernet Private Line
E-NNI	Ethernet Network Node Interface
E-UNI	Ethernet User Network Interface
EVC	Ethernet Virtual Circuit
EVPL	Ethernet Virtual Private Line
FRS	Frame Relay Service
GCRA	Generic Cell Rate Algorithm
GFP	Generic Framing Procedure
GFR	Guaranteed Frame Rate
GMPLS	Generalized Multi-Protocol Label Switching
GS	Gold Service
IBCF	Interconnection Border Control Functional entity
I-BGF	Interconnection Border Gateway Functional entity
IP	Internet Protocol
I-TRCF	Interconnection Transport Resource Control Functional entity
LSP	Label Switched Path
MAC	Media Access Control
MBS	Maximum Burst Size
MPLS	Multi-Protocol Label Switching
MSTP	Multiple Spanning Trees Protocol
NGN	Next Generation Network
PAE	Port Access Entity
PCR	Peak Cell Rate
PDF	Policy Decision Function
PPP	Point-to-Point Protocol

RACF	Resource and Admission Control Functions
RADIUS	Remote Authentication Dial In User Service
R-BGF	Residential Border Gateway Functional entity
SCF	Service Control Functions
SCP-FE	Session Control Proxy Functional Entity
SCR	Sustained Cell Rate
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
SONET	Synchronous Optical Network
STP	Spanning Tree Protocol
TDM	Time Division Multiplex
TRCF	Transport Resource Control Function
UBR	Unspecific Bit Rate
UNI	User to Network Interface
VBR	Variable Bit Rate
VLAN	Virtual Local Area Networks
VID	VLAN Identifier
VPLS	Virtual Private LAN Service
VPN	Virtual Private Networks

4 Terms and Definitions

- Ethernet-User Network Interface (E-UNI): An interface between a user (an end user or a private customer network) and an Ethernet network owned by a public carrier.
- Ethernet-Network Network Interface (E-NNI): An interface between two public carrier Ethernet networks.
- Ethernet Virtual Circuit (EVC): A bi-directional connection between two E-UNIs that acts as though it is a direct connection even though it may physically be circuitous.

5 Service Definition and Requirements for the Ethernet based NGN

5.1 Ethernet based NGN Service Definitions

The key idea of the Ethernet-based NGN is to keep the same frame format as Ethernet. There is no format conversion during end-to-end delivery of packets. But, without change of the basic frame format, the control-/management field can be encoded inside the network like the VLAN [20], [21]. The Ethernet-based NGN means the network using the Ethernet technology though any physical media including fixed and wireless

environments. The Ethernet is a transfer medium of the core network as well as the user interface. The Ethernet-based control-/management functions satisfy the service requirements of the NGN.

5.2 Ethernet based NGN Service Requirements

The service requirements of the Ethernet-based NGN can be divided into end user requirements and network provider requirements.

– End User and application requirements
  - Keep the same Ethernet frame format for fixed and wireless interfaces. The different frame format like RPR frame of IEEE 802.17 is not allowed at the user interface.
  - It requests that there is no change of the existing operating system or device drivers of the Ethernet interface to support data, audio, and video applications at the end user system.
  - It operates auto-discovery capability like ARP/RARP. The same discovery function can be extended for global VPN services like VPLS, Ethernet virtual connection (EVC) or Ethernet relay, etc.
  - Depending on applications, the end user may request the relevant QoS/TE capability.

– Network Operator requirements
  - The equivalent capabilities with SONET/SDH including the OAM, protection & restoration, and load sharing capabilities. The additional field of the Ethernet frame may be encoded like VLAN header.
  - The provider provisioned VPN capability. The existing VLAN can be extended or changed to support the NGN core network.
  - Auto-configuration like neighbour discovery
  - Access control based on MAC address and (or) VLAN ID including security

6 Reference Model of QoS Architecture for the Ethernet based NGN

6.1 Introduction

As the MAC layer protocol, the Ethernet can support all the layer 2 and 3 protocols like IPv4, IPv6, ATM, PPP, and MPLS, etc. Also, the layer 1 protocols like SONET/SDH, TDM, and wireless links are used to deliver the Ethernet frames. But, in views of Ethernet service, the high layer protocols (e.g., IP, ATM, PPP, or MPLS, etc) can encapsulate the Ethernet frame, which looks like a kind of high layer service.

The Ethernet-based NGN are depending on the QoS/TE capabilities of each layer. For example, the QoS/TE capability of IP over Ethernet over SDH is depending both on IP QoS/TE (layer 3), Ethernet QoS/TE (layer 2), and SDH QoS/TE capabilities (layer 1). Therefore, the QoS/TE mappings between different layer protocols are important. Normally, the higher layer has more accurate QoS/TE capabilities rather than the lower layer. It means that the IP QoS class has to be more accurate rather than the Ethernet QoS.

The example of layer model of QoS/TE capabilities are shown in Figure 1/TR-enet.

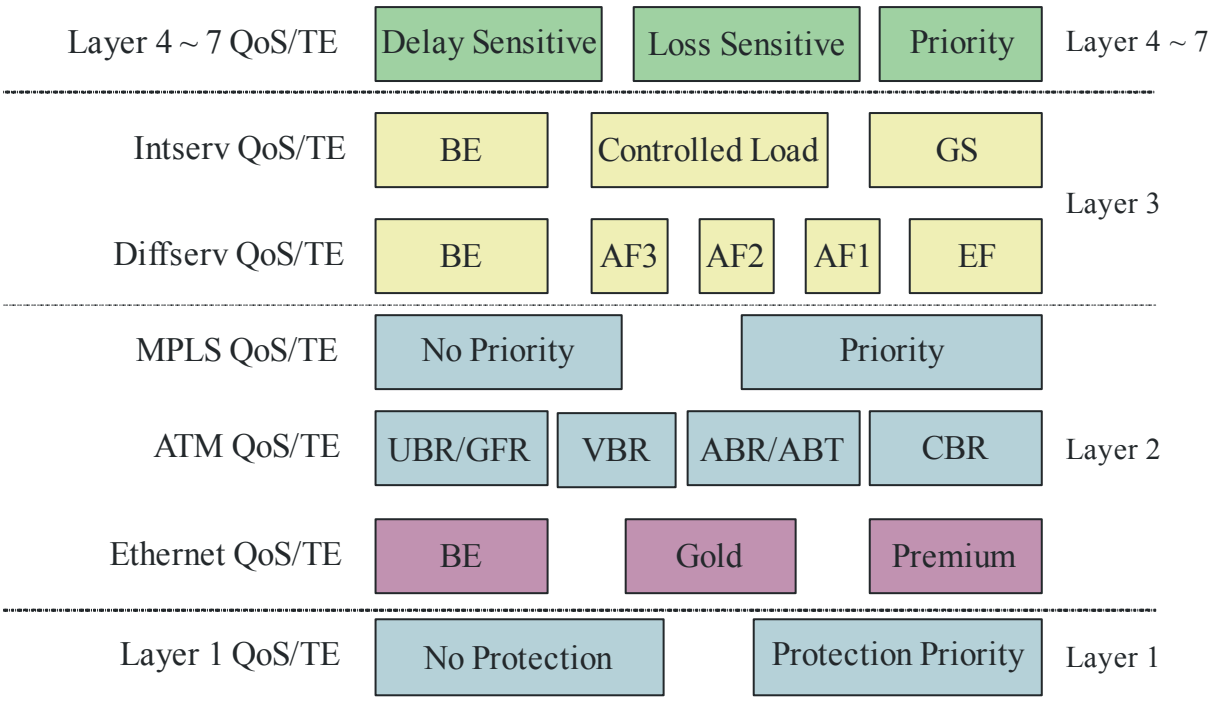


Figure 1/TR-enet – Example of QoS/TE mapping relating to Ethernet-based QoS/TE

NOTE – The protocols in a layer do not have a hierarchy in the Figure 1/TR-enet and need clarification.

In order to reserve the bandwidth between end users, the end-to-end signaling protocol have to operate both for the Ethernet layer and the upper layer protocols.

6.2 Reference Architecture

Figure 2/TR-enet shows Ethernet service architecture as defined in ITU-T Recommendation G.8010. The interface between the customer and the provider is an Ethernet User to Network interface (E-UNI). Ethernet services could be offered by concatenating a number of providers' networks. Network to Network Interface (NNI) defines the interface between different provider networks.

Following Figure 2(a) shows the case of single service provider with a simple network. And the Figure 2(b) indicates the case that there are multiple service providers. In the Figure 2 (a) and (b), the functional entity TRCF may include the functional entities of A-TRCF and C-TRCF. Figure (c) is the case of single service provider with a big network. In the case of a big network, the service provider's network has a complex form which consists of access and core. And each of them may be controlled by separate TRCFs.

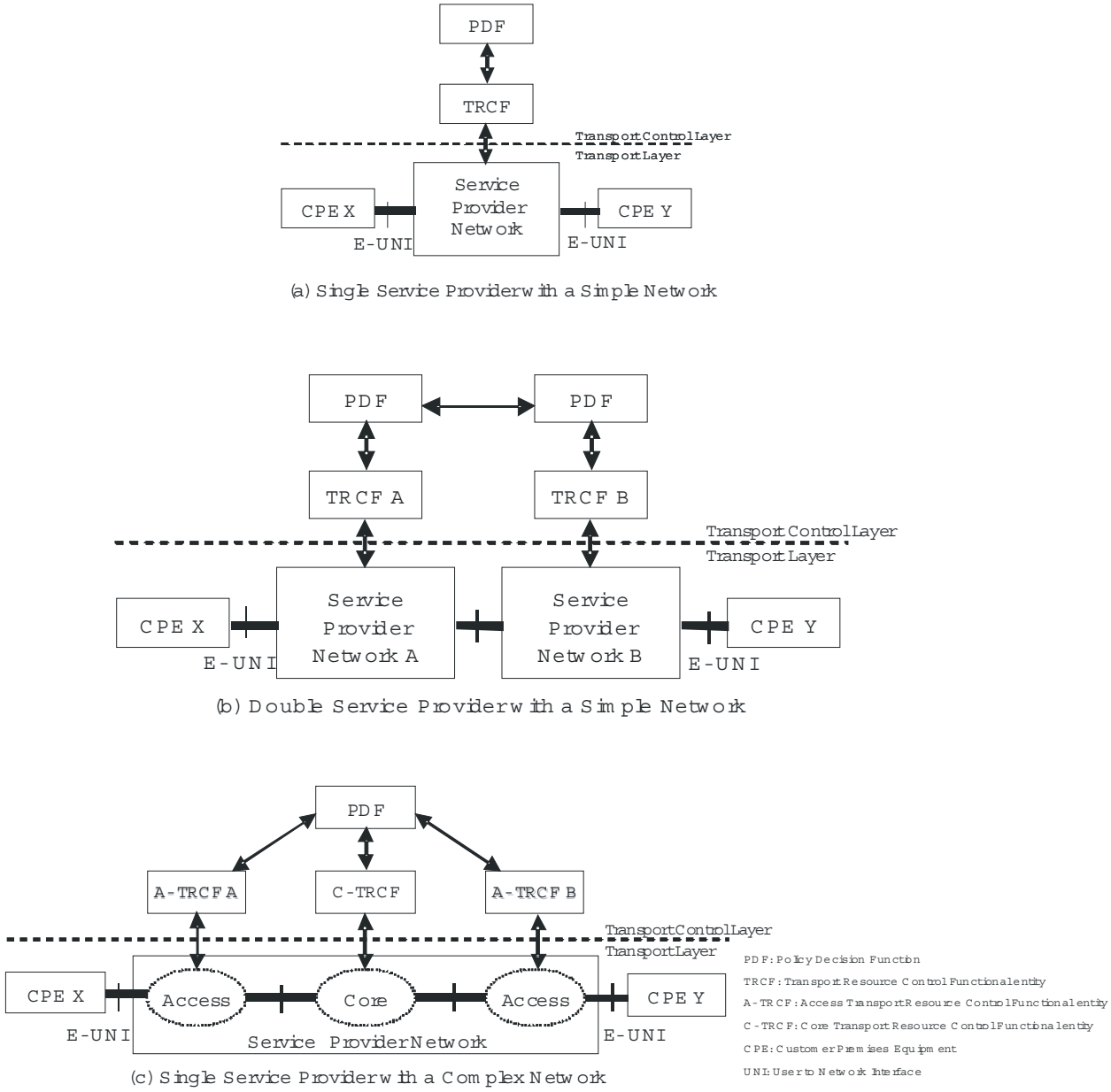


Figure 2/TR-enet – Ethernet Service Architecture

The E-UNI is an Ethernet interface at both the physical layer and the medium access control (MAC) layer. Across the UNI Ethernet frames as defined in IEEE 802.3 or IEEE 802.1Q are exchanged between the user and the provider. Ethernet frames may be untagged or tagged with VLAN Tag control information. VLAN Tag control information consists of the VLAN ID (VID) and the user priority bits (commonly referred to as the p-bits) as shown in Figure 3/TR-enet.

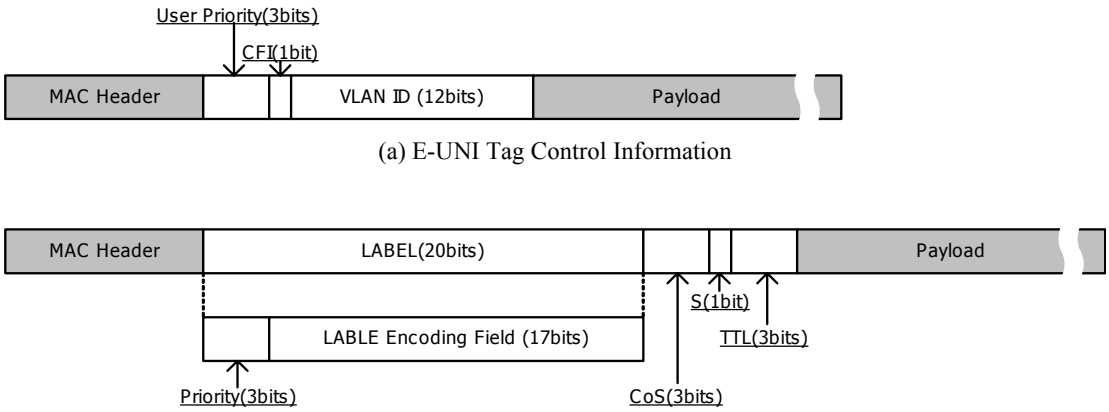


Figure 3/TR-enet – Ethernet Tag Control Information

The frames which are defined in IEEE802.1Q are not enough to support various kinds of requirements such as guaranteeing quality of service and traffic engineering over the core network. So the tagged frames for the E-NNI may need to contain the information of priority, security, and traffic engineering parameters and so on. In the case of E-NNI, it is better to follow the tag frame format of MPLS/GMPLS because of easy migration. And the Label should have the 3bit Priority field to be mapped from the E-UNI 802.1p field. And also other fields related to traffic engineering are need according to the service provider's policy.

Note that the Label Encoding Field in the Figure 3 might be used for Service Level Agreement, Security, Bandwidth for traffic engineering, and/or Applications as the policy of service providers

Ethernet frames are transported inside the transport network using the native transport technology deployed. The transport technology may be either CO-CS (Connection Oriented, Circuit-Switched), CO-PS (Connection Oriented, Packet-Switched), or CL-PS (Connectionless, Packet-Switched). Examples of the different transport technologies that are currently deployed are given in Table 1/TR-enet.

Table 1/TR-enet – Examples of Transport Technologies and Services

Technology	Examples
CO-CS	SONET, SDH
CO-PS	ATM, FR, MPLS
CL-PS	IP, Ethernet

For CO-CS, Ethernet frames are encapsulated using the Generic Framing Procedure (GFP), G.7041 frame encapsulation. Ethernet frames are then transported in a transparent way across the circuit-switched networks.

For packet-switched transport Ethernet frames are to be encapsulated and forwarded using the native transport technology, e.g. ATM.

6.2.1 Ethernet Virtual Circuit (EVC)

The main service instance is the Ethernet Virtual Circuit (EVC). The EVC extends between two UNI. Across the UNI one or more VLAN ID are mapped to the same EVC. An EVC may support multiple Classes of Services as identified by the p-bits. The multiple service classes could differ in their QoS requirements. Each of those service classes is considered a separate CoS instance.

From the class of service perspective, an EVC can have one of three possible types:

- Single Class of Service EVC in which all frames belonging to the EVC are treated in the same way and are subjected to the same bandwidth profile
- Multi-CoS EVC with single bandwidth profile in which frames may be treated differently according to their classes of service but all frames are subjected to the same bandwidth profile.
- Multi-CoS EVC with multiple bandwidth profiles, in which frames are treated differently according to their classes of service and frames belonging to a particular class of service are subjected to a single bandwidth

6.2.2 Ethernet User Network Interface (E-UNI)

E-UNI is the interface between the end customer and the network. A single UNI may support more than one EVC destined to different destinations. Similar to the EVC, from the QoS perspective E-UNI can be one of three types:

- Single Class of Service E-UNI in which all frames belonging to the E-UNI are treated in the same way and are subjected to the same bandwidth profile
- Multi-CoS E-UNI with single bandwidth profile in which frames may be treated differently according to their classes of service but all frames are subjected to the same bandwidth profile.
- Multi-CoS E-UNI with multiple bandwidth profiles, in which frames are treated differently according to their classes of service and frames belonging to a particular class of service are subjected to a single bandwidth

6.2.3 Ethernet Network Network Interface (E-NNI)

E-NNI is the interface between network providers A single NNI may support more than one EVC destined to different destinations. Similar to the EVC, from the QoS perspective E-NNI can be one of three types:

- Single Class of Service E-NNI in which all frames belonging to the E-NNI are treated in the same way and are subjected to the same bandwidth profile
- Multi-CoS E-NNI with single bandwidth profile in which frames may be treated differently according to their classes of service but all frames are subjected to the same bandwidth profile.
- Multi-CoS E-NNI with multiple bandwidth profiles, in which frames are treated differently according to their classes of service and frames belonging to a particular class of service are subjected to a single bandwidth.

An OAM and fault handling of E-NNI may use policies as inputs. For examples, protection and restoration behaviour may differ depending on policies for each connection and/or EVC. And the information can be exchanged by the tag field of the frames.

OAM and fault handling includes following functions.

– Transfer of performance information

– Transfer of fault information

– Performance monitoring

– Fault management

E-NNI has to support 8 classes of service to be mapped with E-UNI classes which are using 802.1p format.

6.3 QoS Provisioning and Mapping

6.3.1 Ethernet Traffic Management Functions

Figure 4/TR-enet shows architecture for Ethernet traffic management. Figure shows both the control and data plane functions.

The control plane functions are those concerned with metering configuration based on the Bandwidth Profile parameters, mapping of Ethernet connections to the corresponding core connections, and resource allocation and admission control, if necessary.

The data plane is concerned with manipulating Ethernet frames based on the results of a classifier, meter, and marker. Conformance of Ethernet frames received at the UNI is verified using a metering function. Based on the output of the meter an Ethernet frame may be colored, recolored, or dropped according to its conformance. Frames are then marked with the appropriate core forwarding class and proceed to the network.

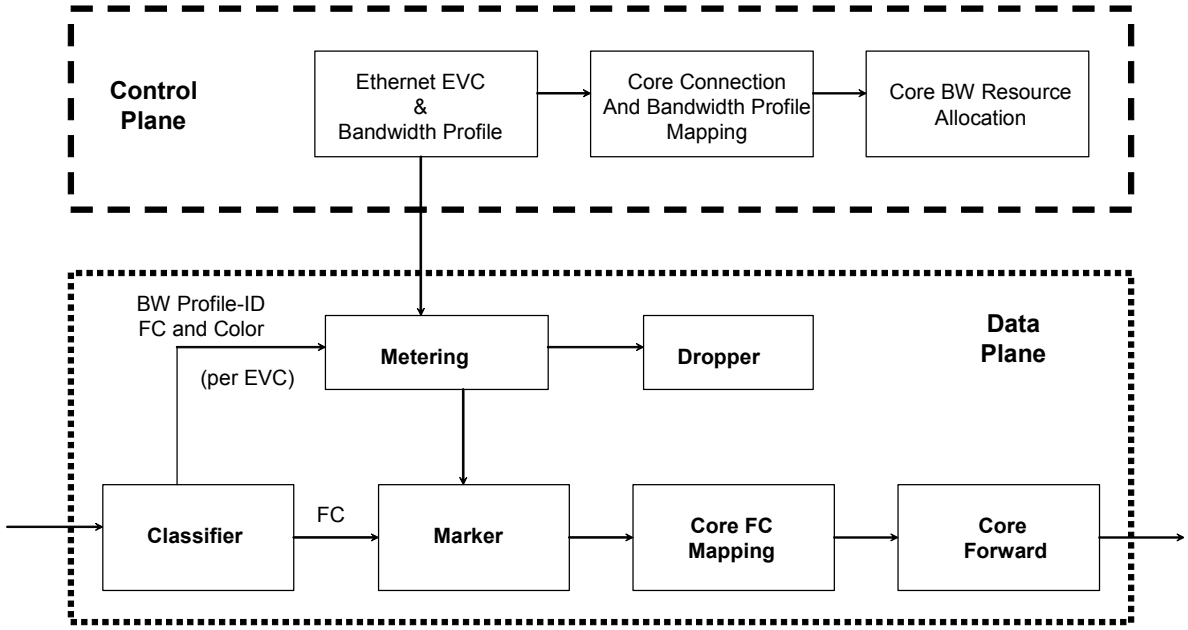


Figure 4/TR-enet – Architecture for Ethernet Traffic Management

Traffic management mechanisms can also be divided to those mechanisms implemented at the edge of the networks at the interface between the customer and the provider, and to those mechanisms implemented inside the network to ensure that traffic volume do not exceed capacity and to treat frames based on their performance requirements. This contribution addresses the mechanisms at the edge as well as inside the network. The resulting service as seen by a subscriber is the result of combining these mechanisms at the two places.

6.3.2 Definition of Edge Traffic Management Functions

Traffic management mechanisms at the provider edge are usually concerned with ensuring that customer submitted traffic (**classification**) adheres to certain traffic pattern (**conformance definition**) and within the parameter values (**traffic parameters**) that are agreed upon between customer and provider.

Actions must be taken when customer's traffic exceeds the assigned parameter values. These actions (**edge rules**) usually involve dropping the excess traffic or mark the excess frame with discard eligibility flag.

The main components of the edge mechanisms are collectively referred to as **traffic conditioning** as was described in the IP differentiated service architecture. In its general form the traffic conditioning function in consists of a classifier, metering, marker, dropper, and shaper functions. The following describes each of the edge functions as identified above.

6.3.3 Classification

Classification is the first step in traffic conditioning to identify sequences of frames (or flows) and correlate those sequences with the traffic parameters, conformance, actions and network behaviour.

Classification can be based solely on L2 (Ethernet) quantities or make use of elements of higher layers, e.g. IP. Classification can also be based on an EVC or the entire UNI.

Ethernet frames may be tagged or untagged. Tagged frames will contain the Tag control information field as shown in Figure 2/TR-enet. Both the VID and the user priority bits can be used for flow classification. For instance, frames with certain VID values are assigned certain traffic parameters and network behaviour. VID values might be mapped or encapsulated to LABEL to cross core networks with containing original information. This mapping procedure is done on network edge router or access gateway by referring mapping table.

6.3.4 Ethernet Traffic Parameters and Conformance Definition

Service traffic parameters are usually associated with rate parameters and the associated measuring period. The measuring period can be stated explicitly in seconds, i.e. rate parameters are measured over a time window of fixed length. Alternatively the measuring period can be stated in terms of the amount of traffic expected back to back at a given rate.

The MEF in its traffic management draft defines CIR and EIR. Associated with CIR and EIR are the committed burst size (CBS) and excess burst size (EBS). Frames may arrive at the access rate (AR) as long as they are within their burst sizes. Otherwise frames are declared non-conformant relative to the conformance definition. The MEF defined parameters bear some similarity to FRS parameters in the sense that both the CIR and the EIR concepts are used. However they differ from FRS parameters in the absence of a specified time period over which parameters may be measured.

The function of the conformance definition is to determine the conformance of incoming frames to the service parameters. The conformance definition is a deterministic algorithm that provides a deterministic upper bound, or deterministic envelope, on the amount of traffic admitted to the network. A deterministic upper bound is necessary for proper engineering of network resources needed to satisfy the performance requirements.

The conformance definition defined at the MEF is shown in Figure 5. Frames conformance can be defined by making use of the conformance definition. For instant frames conformant to CIR and CBS are those that are conformant to TBRA (CIR, CBS). In a similar way frames conformant to EIR are those conformant to TBRA (EIR, EBS). Figure 5/TR-enet shows an arrangement for rate conformance for both CIR and EIR.

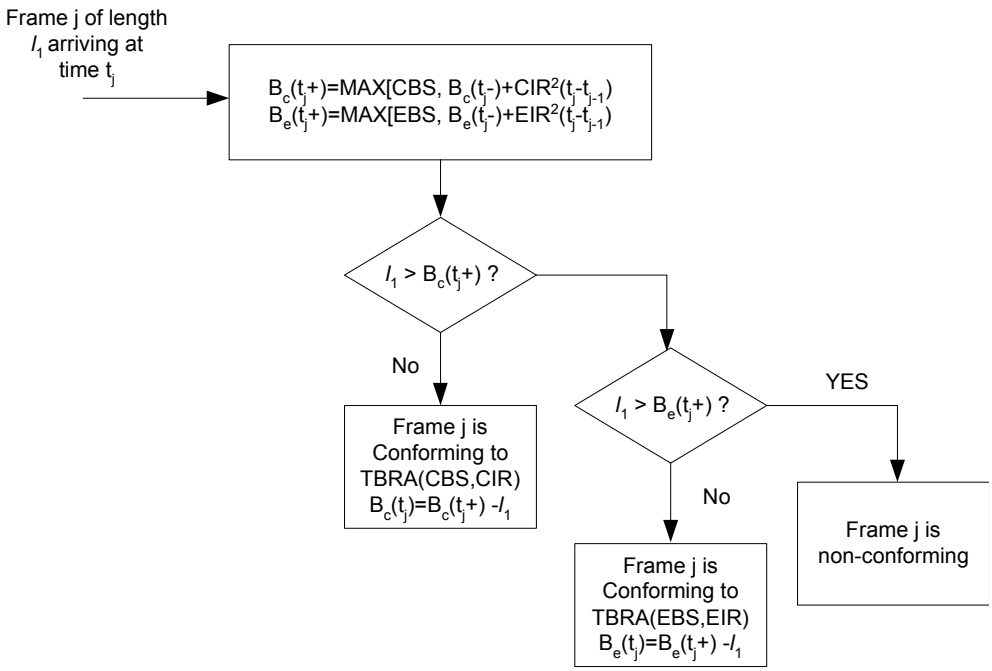


Figure 5/TR-enet – Ethernet Metering and Marking Algorithm

NOTE – Traffic parameters and control mechanisms of Ethernet comes from those of ATM and FR.

6.3.5 Edge Rules

Frames that deemed non-conformant according to some conformance definition must be acted upon in certain way. There are usually two actions associated with non-conformant frames. Those are drop or marking.

With dropping, non-conformant frames are not allowed to progress further beyond the edge node of the provider network. Non-conformant frames are dropped or alternatively no excess traffic is allowed to the network.

With marking, non-conformant frames are marked for discard eligibility. Discard eligible frames are allowed to the network with the understanding that no performance assurances are extended to them. Discard eligible frames are to be dropped first when the network is in a congestion state. The volume of the discard eligible frames is usually limited, e.g. by EIR in order not to overwhelm network resources and negatively impact upper layer performance.

The choice between dropping and marking has a significant impact on the service offered. For instance there are three flavours of VBR service based on whether tagging is allowed by customer and at the network edge.

6.3.6 Network Traffic Management Mechanisms

The provider network should be equipped with traffic management capabilities that allow performance objectives to be satisfied on a frame by frame basis. Traffic management mechanisms inside the provider network are those related to transmission scheduler, buffer management, and admission control. Transmission Scheduling and buffer management are often referred to as forwarding classes.

The traffic engineering should be supported over the end to end transfer. However it is very difficult to offer continuous traffic engineering for the reason of different parameters of UNI and NNI. So a layer 2 parameter mapping should be done at the edge routers or access gateway. A different parameter mapping example between UNI and NNI is shown below.

Table 2/TR-enet – TE parameter mapping table

UNI	NNI
802.1p(3bits)	LABEL Priority (3bits)
VLAN ID(12bits)	LABEL_BW LABEL_SLA LABEL security

Basically traffic classes could be aggregated or divided during bridging the different network interfaces. The traffic classification depends on service provider's policy.

6.3.7 Ethernet Per Hop Behaviours (E-PHB)

Transmission scheduling and buffer management are usually referred to as the nodal behaviour (in the context of the IP differentiated service, they are referred to as the per hob behaviour (PHB)). Transmission scheduling has to do with what frame has to be transmitted first and what portion of the transmission facility has to be reserved for a particular flow or group of flows. Buffer management is concerned with the accepting of incoming packets to nodal buffer based on the current buffer fill and the packet discard eligibility.

Broadly speaking there are two main techniques for identifying the type of behaviour applied to each packet, a stateful and a stateless approaches. The stateful approach is one based on a connection identifier that determines which connection the incoming packet belongs to and what type of behaviour should be applied to it. Example to that is the ATM/MPLS traffic management where the MPLS label is used to define the connection and the service category it belongs to, e.g. CBR connection. This method requires the keeping of context tables inside the node that correlate, among other things, the label to its service category.

The second method is the one applied for the IP differentiated services where the packet carries in its header an indication of what type of treatment should be applied to it, e.g. priority treatment. All packets with the same bit pattern receive the same treatment by the node. This technique is perceived to be more scalable than the first one.

In this section we extend the differentiated service approach to Ethernet. As shown in Figure 2/TR-enet, Ethernet frame header included 3 bits that are called user priority bits. Those bits can be used in a variety of ways to support a number of Ethernet per hop behaviours (E-PHB). Similar to differentiated service PHB, E-PHB may include:

- Ethernet Extended Forwarding (E-EF) that is suitable for implementing services that require frames to be delivered within tight delay and loss bounds. No reordering of frames is allowed.
- Ethernet Assured Forwarding (E-AF) that defines a number of classes with a number of discard precedence associated with each class. No reordering of frames is allowed.
- Ethernet Default Forwarding (DF) that is suitable for implementing services with no performance assurances, e.g. best effort. No reordering of frames is allowed.

Table 3/TR-enet shows an example how to use the user-priority bits to defines E-EF, three E-AF classes, and E-DF.

Buffer management includes provisions required to handle short and long term congestion. Short term congestion is handled by supplying the adequate amount of buffering needed to buffer incoming frames during those brief periods when frame input rate to the node exceeds the nodal capacity. Long term congestion is handled by dropping packet based on their discard eligibility. Nodal discard algorithm may include active queue management or simple drop thresholds based on supported applications.

Table 3/TR-enet – Ethernet Per Hop Behaviours (E-PHB)

Ethernet p-bits	E-PHB	Example Application
111	E-EF	Emergence Service
110	E-AF31	Voice(Bearer)
101	E-AF32	Video Conferencing
100	E-AF21	Voice Control
011	E-AF22	Critical Data
010	E-AF11	Streaming Video
001	E-AF12	Medium Data
000	E-DF	Best Effort Data

6.3.8 Admission and Congestion Control

The main function of admission control is to limit the number of connections accepted by the network. This in turn will limit the amount of traffic submitted to the network and consequently offers a better opportunity for meeting the QoS requirements of the accepted connections.

Admission control is based on connection traffic parameters and QoS requirements. As mentioned before the importance of the traffic parameters is that it imposes a deterministic upper bound on connections traffic, hence allows for accurate prediction of the required resources.

6.3.9 Ethernet QoS Services

Editor's note: Need to check whether there is a consistency with MEF or not.

Edge mechanisms together with the network forwarding classes are combined together to define a set of Ethernet QoS services. A number of service categories could be defined by specifying traffic parameters, edge rules, and the network forwarding class. Table 4/TR-enet shows a number of Ethernet QoS services.

Table 4/TR-enet – Ethernet QoS Services

Ethernet QoS Service	Traffic Parameters	Edge Rules	Forwarding Class
Premium Service	CIR > 0 CBS > 0 EIR = 0 EBS = 0	Drop non-conforming frames	E-EF
Gold Service	CIR > 0 CBS > 0 EIR > 0 EBS > 0	Admit non-conformant frames up to EIR. Excess frames are assigned high discard precedence	E-AF with Minimum bandwidth assurances No delay bound Drop excess frames first when congested
Best Effort Service	CIR = 0 EBS = 0 EIR > 0 (possibly equal physical rate) EBS > 0 (large)	All frames are admitted with high discard precedence	E-DF Small bandwidth assurances No delay bound Drop first when congested

The premium service is useful for those applications that require stringent bounds on both the frame loss and the frame delay. The service doesn't allow excess frames (defined as frames that are non-conforming to CIR) to the network. It is most suitable for EPL application as defined in G.8012.1 on SDH networks. In this case frame discard precedence is invisible to the nodal mechanism and there is nothing to be gained from allowing frames to the network with different discard precedence.

The Gold service provides some bandwidth assurances but not any delay bounds. In that respect it is similar to the traditional Frame Relay service or the ATM nrt-VBR service category. Gold service could be useful for EVPL application that require some bandwidth assurance but does not care about delay.

6.3.10 Ethernet Traffic Grooming

To support guaranteed QoS over Ethernet, the traffic grooming is required. An access node (or edge router) has to be connected to core MPLS/GMPLS routers. So the traffic grooming functionality should be same or part of the MPLS/GMPLS traffic grooming technology for compatibility. The MPLS traffic grooming functionalities could be referred G.8080, which recommendation provides the sorts of traffic grooming techniques over optical networks.

6.4 VPN configuration based on Ethernet

VPLS delivers a multipoint-to-multipoint Ethernet service that can span one or more metro areas and that provides connectivity between multiple sites as if these sites were attached to the same Ethernet LAN. In contrast to the current Ethernet multipoint-to multipoint service offering that is delivered upon a service provider infrastructure composed of Ethernet switches, VPLS uses the MPLS service provider infrastructure. From the service provider's point of view, use of MPLS routing protocols and procedures instead of the Spanning Tree Protocol and MPLS labels instead of VLAN IDs within the service provider infrastructure results in significant improvements in the scalability of the VPLS as a service.

As previously mentioned, most providers delivering Metro Ethernet services today have constructed their networks exclusively for Ethernet services. Therefore, to keep costs low, they have deployed implementations using Layer 3 and Layer 2 switches. Unfortunately, what they are finding is that all they can deliver is Ethernet bandwidth, as it has been virtually impossible to turn on services due to the performance of these low-powered platforms. This approach of more bits for less revenue leads to a commoditized business model. Furthermore, since the networks are based on Ethernet with Spanning Tree Protocol and VLAN-Ids, there are fundamental scaling limitations to the technology used to deliver any kind of service.

6.5 L4 ~ L7 Switching Capabilities using Ethernet

While the L3 switch performs IP-based routing, the Layer 4/Layer 7 switch forwards packets from the switch to appropriate destinations based upon the upper layer information. Unlike the L2 or L3 switching, we can not switch at Layer 4, but can utilize the upper layer information to make switching decision. Through the analysis of TCP/UDP port information, (HTTP, FTP, Telnet, SMTP, POP3, etc.) the L4 switch delivers the packets with the same destination IP address to different destinations. Furthermore, Layer 4 information can be used to prioritize and queue traffic. The L7 switching looks inside the application layer field to make forwarding decision. Depending on the contents, such as HTTP contents, cookie information, FTP file names and email titles, traffic can be directed to different paths. Major benefits that the L4/L7 switch provides include load-balancing, failover of various servers, and network security by preventing a monopoly of network resources.

To support L4/L7 switching capabilities, binding of the Ethernet MAC address and high layer service is required. Multiple Ethernet MAC address can be assigned to the same destination IP address and/or port number. By examining the information on high layer, a mapping rule given by a switch operator finds a proper destination Ethernet MAC address.

6.6 Access Control using Ethernet

6.6.1 Introduction

Network access control makes use of the physical access characteristics of LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails. A port in this context is a single point of attachment to the LAN infrastructure. Examples of ports in which the use of authentication can be desirable include the Ports of MAC Bridges, the ports used to attach servers or routers to the LAN infrastructure.

6.6.2 Relationship among the Supplicant, Authenticator, and Authentication Server

Figure 6/TR-enet illustrates the relationship among the Supplicant, Authenticator, and Authentication Server, and the exchange of information among them.

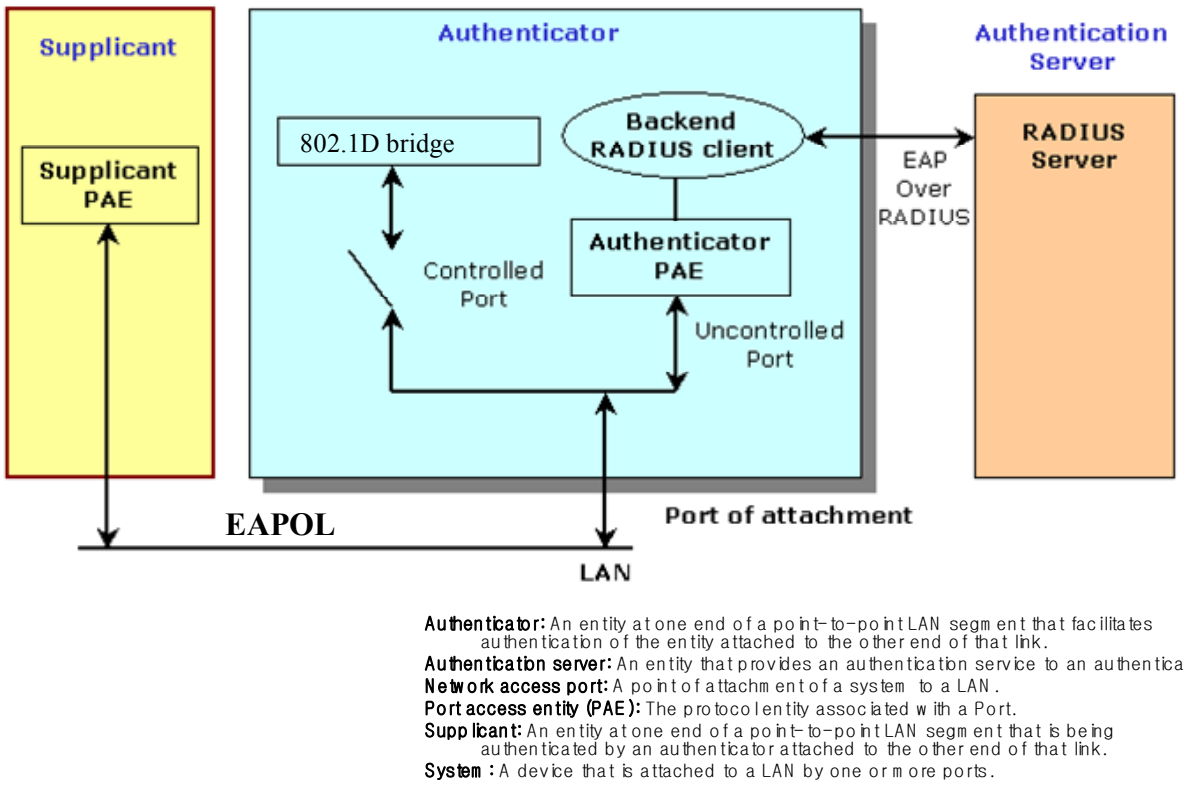


Figure 6/TR-enet – Authenticator, Supplicant, and Authentication Server roles

In this illustration, the Authenticator's controlled Port is in the unauthorized state and is therefore disabled from the point of view of access to the services offered by the Authenticator's system.

For the authentication protocol between the Supplicant and the Authentication Sever, EAP (Extensible Authentication Protocol) is used. Over LAN segment, EAP information is encapsulated in a LAN frame with EAPoL (EAP over LAN) protocol, and delivered to the bridge. The bridge incorporates EAP portion of the EAPoL frame into RADIUS message, and sends the RADIUS message to the corresponding Authentication Server. The bridge, which is the Authenticator, acts as a RADIUS client for the Authentication Server.

– In the Supplicant role, the PAE is responsible for responding to requests from an Authenticator for information that will establish its credentials. The PAE that performs the Supplicant role in an authentication exchange is known as the Supplicant PAE.

– In the Authenticator role, the PAE is responsible for communication with the Supplicant, and for submitting the information received from the Supplicant to a suitable Authentication Server in order for the credentials to be checked and for the consequent authorization state to be determined. The PAE that performs the Authenticator role in an authentication exchange is known as the Authenticator PAE.
– The Authentication Server performs the authentication function necessary to check the credentials of the Supplicant on behalf of the Authenticator and indicates whether the Supplicant is authorized to access the Authenticator's services.

6.6.3 Protocols and operations

Protocols and operations for network access control should refer to IEEE specifications [26].

7 QoS Procedures for Ethernet based NGN

7.1 Overview

Users can select or request their own QoS/TE with relevant parameters to network provider. CAC and UNI/NNI procedures require the knowledge of certain parameters to operate efficiently: they should take into account the network service provider's transfer capability, the source traffic descriptor, the requested QoS classes.

A network service provider's capability, a source traffic descriptor, and associated a QoS class are declared by the user at connection establishment by means of signalling or subscription.

For a given network service provider's connection, the source traffic descriptor belonging to the traffic contract and all parameter values of this source traffic descriptor are the same at all standardized interfaces along the connection.

In order for QoS commitments to be met, a conformance definition is specified at the AAA server for any given network service provider's transfer capability. A conformance definition also pertains at each standardized network to network interface. A traffic contract may apply to an Ethernet virtual flow. As a consequence, conformance definition at an interface applies at the level where the traffic contract is defined. Additionally, a traffic contract for a connection may imply a cell flow on the connection of the reverse direction of a communication. In such a case, a conformance definition also pertains for the reverse connection.

The Connection Admission Control (CAC) and User to Network Interface/ Network to Network Interface (UNI/NNI) procedures are operator specific. Once the connection has been accepted, the value of the CAC and UNI/NNI parameters are set by the network on the basis of the network operator's policy.

7.2 QoS Procedures

For guaranteeing QoS in IP-based Ethernet access network, the following requirements should be also met.

1) Network topology and resource status collection;
2) Resource request with specific QoS requirements;
3) Admission control and Resource allocation;
4) Service flow identification, classification and marking;
5) Packet forwarding through UNI on the basis of Ethernet-layer priorities defined in IEEE 802.1p or through NNI attaching Label per flow.

For relatively guaranteeing QoS of connectionless services in IP access network, the same QoS mechanisms can be used. SLA negotiation between customer and provider is viewed as a static and manual service request for data delivery quality, and network administrators serve as SCF. Admission control and resource allocation may be done only based on SLA/policy. Packets are also forwarded on the basis of Ethernet-layer priorities defined in IEEE 802.1p. Considering automation and security of SLA management, maybe a path-decoupled signaling protocol needs to be developed for dynamic SLA negotiation and policy decision.

7.3 QoS Mapping procedure

The requirements between a user side and a service provider side are different. And the network abilities which can afford to support guaranteeing certain specific quality of service are different as well. So the definition of quality of service must be mapped from one network to the other networks to support end-to-end quality of service.

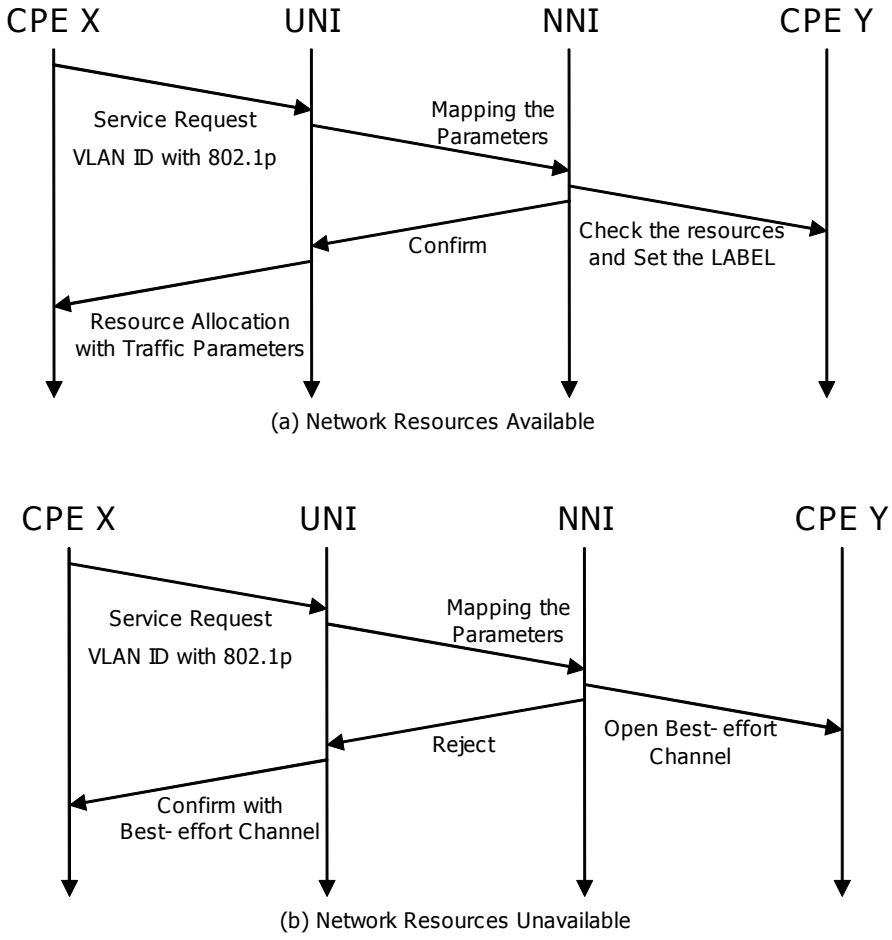


Figure 7/TR-enet – QoS Mapping procedure

Figure 7/TR-enet shows the QoS mapping procedure for the access gateway. First of all, the NRCF as access gateway has to reserve available bandwidth to the core network before arriving the clients' call. If a user's request is received, the access gateway looks into the authority of the user. A validated user is proved, the Access gateway discriminate flow type. By the flow classes, that NRCF gives CPE the priority information for the priority scheduling. Because the client information is not given to CPE initially. The incoming packets are switched in the access gateway and stored at the different buffers by the classes. According to the network service provider's policy and network circumstance, the stored packets classified in the buffered are attached to label to be sent through the Ethernet-based core network. For example, the priority bits through the interface, UNI, should be mapped into the same priority bits to the corresponding LABEL in the NNI. And other parameters such as bandwidth and delay limits are also mapped into the proper position in the LABEL by network providers' policy.

7.4 Resource allocation mechanism

Figure 8/TR-enet introduces the procedure of resource allocation mechanism, which is based on the Figure 2/TR-enet.

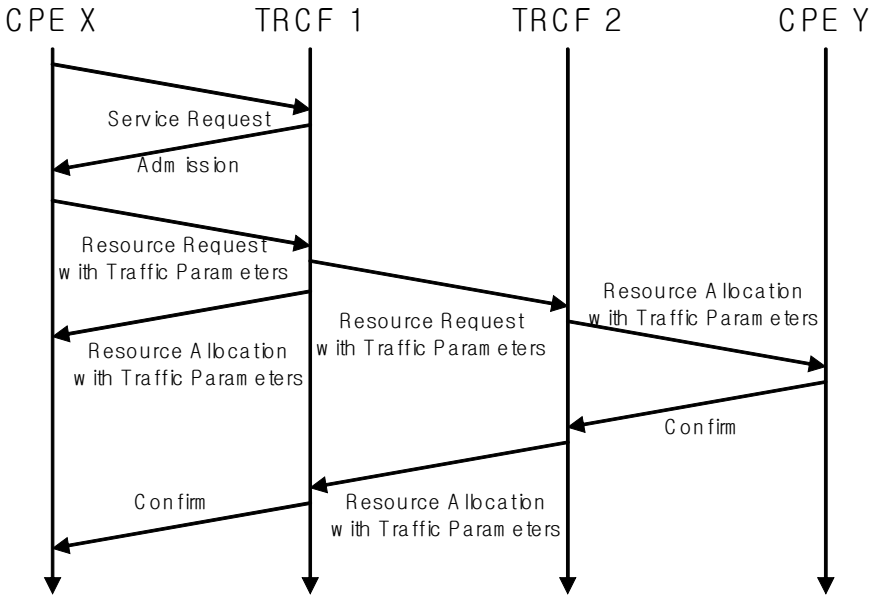


Figure 8/TR-enet – Resource allocation mechanism

(1) Service Request: The CPE sends a service request to MNF through the NRCF. A resource request is triggered by the service request. Service requests are various and application-specific.

(2) Resource Request with specific QoS requirements: CPE sends a resource request containing the parameters such as the IP address of the customer terminal, flow description, bandwidth demand and priority to NRCF.

(3) Admission Control and Resource Allocation: NRCF finds the path of a flow according to the MNF and IP address of the source terminal, and judges whether or not there is enough network resource for the flow access. If there is, NRCF sends an access admission response to CPE and marks this part of resource as occupied in network topology and resource database; if there is not, the access is denied and the admission control procedure terminates.

(4) QoS Parameters Configuration: NRCF sends the flow description, bandwidth and priority of 802.1p back to CPE X though an UNI interface. If the service is bi-directional, NRCF should also configure flow description, bandwidth limitation and priority of the flow in LABEL to next NRCF though a NNI interface.

(5) Flow Identification, Classification, Marking and Forwarding: NRCF identifies a service flow according to flow description, classifies the flow packets, limits the bandwidth of the flow, marks and forwards packets according to priority. The intermediate devices forward packets according to priority too. Unidentified packets, which don't match any flow description configured in NRCF, are not assured to be forwarded with their original priority if any value is set and may be treated as best-effort packets. If the service is bi-directional, other next-hop NRCFs perform same processes with that.

8 Operation and Management for the Ethernet based NGN

8.1 Introduction

The OAM functionality needs to ensure reliability and performance for the Ethernet-based NGN. User-plane OAM tools are required to verify that the Ethernet-based NGN maintain correct connectivity, and are thus able to deliver customer data to target destinations with both, availability and QoS (Quality of Service) guarantees, given in SLAs (Service Level Agreements).

8.2 Requirements for OAM functionality

The OAM requirements of the Ethernet-based NGN are very similar to those of the MPLS-based networks [Y.1730]. The difference of the Ethernet-based NGN from the MPLS-based networks is using VLAN ID in the access area instead of LABEL to distinguish traffic flows.

So network operators may map which functions to use into which labels and/or VLAN IDs they apply to. And the network border equipment may have mapping algorithm VLAN IDs into corresponding LABELs.

8.3 OAM mechanism

The OAM mechanism for Ethernet-based NGN is based on MPLS OAM mechanism [Y.1711] except for stack encoding. When the core network a packet comes to the core network, an access area from the LABEL should be mapped into the corresponding VLAN ID and vice versa. This means that the access area of Ethernet-based NGN should be able to be operated and managed by the core OAM mechanism or should be able to exchange the OAM information to control the access area under an agreement between the service providers.

9 Ethernet Protection and Restoration

Protection and restoration mechanisms require relatively more time to recover, and using higher levels of recovery mechanisms may require more resources. But there are limitations and disadvantages in the Ethernet layer protection, particularly in the optical network, e.g., complicated implementation, cost, instability due to duplication of functions, etc.

The study of specific recovery mechanisms is out of the scope of this document. The motivation for Ethernet protection and restoration is to provide the desired level of service in the most cost-effective manner. The most proper method for this protection and restoration is employing GMPLS system. The recovery mechanism that has higher priority is triggered first to recover failures. Usually, it is expected that lower layer recovery mechanism is closer to the failure, so it has higher priority. One of the most popular coordination mechanisms is the hold-off timer. The hold-off time is the waiting time until taking MPLS-based recovery action after the detection of a failure. It allows time for the lower layer protection to take effect. If MPLS-based recovery is the only recovery mechanism desired, then the hold-off time may be zero.

Assuming that we have SONET Automatic Protection Switch (APS) link protection, for example, during the hold off time, GMPLS LSP path protection waits for the APS protection to switch. If the SONET APS succeeds protection within the hold-off time, then the hold-off timer is reset and no further protection is needed. The original LSP can remain there. From this point of view, the link layer protection provides a means of LSP protection. If the hold-off time expires, the LSP protection and restoration is triggered. The coordination mechanism introduces a tradeoff between rapid recovery and creation of a race condition where several layer protection mechanisms respond to the same fault. GMPLS widens the application scope of MPLS, and people propose using GMPLS to build a unified control plane to manage all kinds of network nodes including Ethernet nodes for NGN. The GMPLS LSP protection and restoration has been an important recovery mechanism for network survivability.

9.1 Protection

Protection is a mechanism for enhancing availability of a connection through the use of additional, assigned capacity. Once capacity is assigned for protection purposes there is no rerouting and the SNPs allocated at intermediate points to support the protection capacity do not change as a result of a protection event. The control function, specifically the connection control component, is responsible for the creation of a connection. This includes creating both a working connection and a protection connection, and providing connection-specific configuration information for a protection scheme. For transport function protection, the configuration of protection is made under the direction of the management function. For control function protection, the configuration of protection is under the direction of the control function rather than the management function. Like the GMPLS protection, when a failure occurs, the nodes involved in the recovery need not notify the end-nodes of the route (path) in the 1+1 protection mechanism; but in the M:N, 1:1 and 1:N protection mechanisms, the nodes neighboring the failure must notify the end nodes so that the end-nodes will switch the traffic. So the 1+1 protection mechanism provides fast recovery because it does not need fault notification time. However, the other mechanisms utilize the resources more efficiently.

9.2 Traffic Restoration

Restoration is broadly defined here as the mitigating response from a network under conditions of failure. Potential methods for failure recovery include Automatic Protection Switching for line/path protections and shared mesh restoration methods. There are two types of network failures:

- Node Failure: Failure of a network element (e.g., router card) in a network node or office. This type of failure is typically dealt with by designing redundancy features in network elements to minimize failure impact. Catastrophic failures such as power outages and natural disasters however may take down an entire network node. In which case, through traffic can be re-routed over spare links designed around the failed node.
- Transport Link Failure: Failure of a link (e.g., T1, OC-3) connecting two network nodes. Typically links can fail due to link element failure (e.g., line card) (which can then take down a single link) or, more seriously, a fiber cut (which can then disrupt a large number of links). Service providers can design additional spare capacity to mitigate the impact of such failures and restore traffic flows until the failure is repaired.

As in the case of admission control, certain traffic streams related to the critical services may require higher restoration priority than others. A service provider needs to plan for adequate levels of spare resources such that QoS SLAs are in compliance under conditions of restoration. Typical parameters for measuring service restorability are time-to-restore and the percentage of service restorability.

9.2.1 Local Restoration

Local restoration eliminates the need to propagate fault information across networks. But its application is limited. A local restoration requires the following procedure :

(1) The failure detection mechanism detects the failure.

(2) The fault localization mechanism localizes the failure. Meanwhile, the node that is the immediate upstream node of the failure knows about the failure.

(3) The node initiates the process to establish a new path or path segment that bypasses the failure.

(4) And the node switches the traffic to the alternate path.

9.2.2 Local Rerouting

Local restoration eliminates the need to propagate fault information across networks. But its application is limited.

9.2.3 Global Restoration

Compared to end-to-end path protection, the end-to-end path restoration is slow because the fault notification and the routing information synchronization would take seconds. So it may not be required to work for real-time applications such as voice. It is resource efficient, because the alternative LSP is established on demand and the resource is allocated on demand.

10 Security Consideration

-TBD

2.11 – Functional Requirements and Architecture for Resource and Admission Control in NGN*

Table of Contents

* Status D: The FGNGN considers that this deliverable is not yet mature, requiring discussion and technical input to complete development.

2.11 – Functional Requirements and Architecture for Resource and Admission Control in NGN

1 Scope

This document provides the high-level requirements, scenarios, functional architecture and decomposition for the Resource and Admission Control in next generation networks. The reference points and interfaces between the functional entities are described. The procedures for the control of Quality of Service (QoS), Network Address and Port Translator (NAPT) Control and NAT traversal, Firewall Control are described.

Network management is outside the scope of this document.

2 Reference

Editors' note: The final version of references must be released documents.

[1] ITU-T Y.2001, General overview of NGN

[2] ITU-T Y.2011, General principles and general reference model for Next Generation Networks

[3] ITU-T draft Y.FRA-NGN, Functional requirements and architecture of the NGN

[4] ITU-T Y.1291, An architectural framework for support of quality of Service (QoS) in packet networks

[5] 3GPP TS 23.228 Release 6, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2

[6] 3GPP TS 23.207 Release 6, End-to-end Quality of Service (QoS) concept and architecture

[7] 3GPP TS 29.207 Release 6, Policy control over Go interface

[8] 3GPP TS 29.209 Release 6, Policy control over Gq interface

[9] ITU-T TR Q.sup51, Signalling requirements for IP QoS

[10] ITU-T Recommendation E.106 (2003), International Emergency Preference Scheme (IEPS) for Disaster Relief Operations

[11] RFC 2205, Resource ReSerVation Protocol (RSVP) Version 1 Functional Specification

[12] RFC 3261, Session Initiation Protocol (SIP)

[13] RFC 2327, SDP: Session Description Protocol

[14] RFC 2475, An Architecture for Differentiated Services (DiffServ).

[15] RFC 3312, Integration of Resource Management and Session Initiation Protocol (SIP)

[16] IETF RFC 2246 (1999), The TLS Protocol Version 1.0.

[17] IETF RFC 2401 (1998), Security Architecture for the Internet Protocol.

[18] IETF RFC 2402 (1998), IP Authentication Header.

[19] IETF RFC 2403 (1998), The Use of HMAC-MD5-96 within ESP and AH.

[20] IETF RFC 2404 (1998), The Use of HMAC-SHA-1-96 within ESP and AH.

[21] IETF RFC 2405 (1998), The ESP DES-CBC Cipher Algorithm With Explicit IV.

[22] IETF RFC 2406 (1998), IP Encapsulating Security Payload (ESP).

[23] IETF RFC 2407 (1998), The Internet IP Security Domain of Interpretation for ISAKMP.

[24] IETF RFC 2408 (1998), Internet Security Association and Key Management Protocol (ISAKMP).

[25] IETF RFC 2409 (1998), The Internet Key Exchange (IKE).

[26] IETF RFC 2410 (1998), The NULL Encryption Algorithm and Its Use With IPsec.

[27] IETF RFC 2411 (1998), IP Security Document Roadmap.

[28] IETF RFC 2412 (1998), The OAKLEY Key Determination Protocol.

[29] IETF RFC 3168 (2001), The Addition of Explicit Congestion Notification (ECN) to IP.

[30] IETF RFC 4109 (2005), Algorithms for Internet Key Exchange version 1 (IKEv1).

[31] Guidelines for NGN Security Release 1.

3 Definitions and Terms

<Check in ITU-T Terms and definitions database under http://www.itu.int/sancho/index.htm if the term is not already defined in another draft. It could be more consistent to refer to such a definition rather than refined it>

This draft defines the following terms:

Absolute QoS: Traffic delivery with numerical bounds on some or all of the QoS parameters. These bounds may be physical limits, or enforced limits such as those encountered through mechanisms like rate policing. The bounds may result from designating a class of network performance objectives for packet transfer.

Relative QoS: Traffic delivery without absolute bounds on the achieved bandwidth, packet delay or packet loss rates. It describes the circumstances where certain classes of traffic are handled differently from other classes of traffic, and the classes achieve different levels of QoS.

Gate: Packet filtering to enforce the policy decision for a specific media flow based on flow classifier (e.g. IPv4 5-tuple) and flow direction.

Gate Control: Enable (open) or disenable (close) the gate for a media flow. When a gate is open, the packets in the flow are passed; when a gate is closed, all of the packets in the flow are blocked and dropped.

Media Flow: A unidirectional or bidirectional media stream of a particular type, which is specified by two endpoint identifiers, bandwidth and class of service.

Firewall working mode selection: Choose the packet inspection mode of packet-filtering-based firewall for accepting or rejecting the packets of a media flow based on related service security level requirement. There are four packet inspection modes for packet-filtering-based firewall: static packet filtering, dynamic packet filtering, stateful inspection, and deep packet inspection. The static packet filtering firewall is the default packet inspection mode applied for all flows.

Editor's note: The definition of NAPT control and NAT traversal is required

4 Abbreviations

This draft uses the following abbreviations:

IETF	Internet Engineering Task Force
3GPP	3rd Generation Partnership Project
QoS	Quality of Service
NAPT	Network Address and Port Translation
FW	Firewall
IP	Internet Protocol
MPLS	Multiple Protocol Label Switching
DiffServ	Differentiated Service
RSVP	Resource ReSerVation Protocol
SLA	Service Level Agreement
CPE	Customer Premises Equipment
CPN	Customer Premises Network
NGN	Next Generation Network
SCF	Service Control Functions
RACF	Resource and Admission Control Functions
NACF	Network Attachment Control Functions
PDF	Policy Decision Functional entity
TRCF	Transport Resource Control Functional entity
BGF	Border Gateway Functional entity
TDR	Telecommunications for Disaster Relief
ETS	Emergency Telecommunications Service

Editor's Note: The SCF used in the context represents the abstract view of service control stratum. Further alignment is needed with WG2.

5 Overview and requirements

5.1 Overview

In the NGN Architecture [1][2], the Resource and Admission Control Functions (RACF) provide QoS [4] resource control functions (including resource reservation, admission control and gate control), and border gateway control functions (including NAPT/Firewall control and/or NAT traversal Functions) over access and core transport networks.

Within the NGN architecture, the RACF act as the arbitrator for QoS-related transport resource negotiation and reservation between Service Control Functions and Transport Functions based on user profiles, SLAs,

operator network policy rules, service priority, and resource availability within access and core transport. Figure 1 depicts a schematic view of the RACF in the overall NGN architecture.

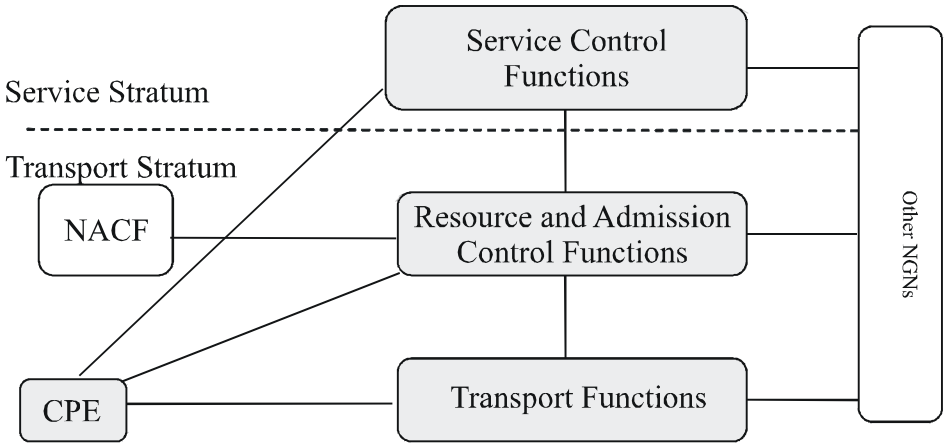


Figure 1 – RACF within the NGN architecture

Notes:

1. The definition of the reference point between CPE and RACF is for further study.

The RACF interacts with Service Control Functions and Transport Functions for a variety of applications (e.g. SIP [12] call, Video Streaming etc.) that require the control of NGN transport resource, including QoS control and NAPT/FW control and NAT Traversal.

The RACF interact with Transport Functions for the purpose of controlling one or more the following functions in the transport layer: Packet filtering; Traffic classification, marking, policing, and priority handling; Bandwidth reservation ; Network address and port translation; Firewall.

The RACF interact with Network Attachment Control Functions (NACF, including network access registration, authentication and authorization, parameters configuration) for checking QoS-related user profile held by them.

For those services across multiple providers or operators, Service Control Functions, RACF and Transport Functions may interact with the corresponding functions in other packet networks.

5.2 High-level requirements

The Resource and Admission Control functional architecture shall meet the following high-level requirements:

(1) Controls the QoS-related transport resources within packet networks and at the network boundaries in accordance with their capabilities.

(2) Shall support different access and core transport technologies (e.g. xDSL, UMTS, CDMA2000, Cable, LAN, WLAN, Ethernet, MPLS, IP, ATM, etc.), while hiding network technological and administrative details (e.g. network topology, connectivity, control mechanisms etc.) from the Service Control Functions.

(3) Support of different CPE intelligence and capability. For example, Some CPE may support transport layer QoS signalling (such as PDP context [6], RSVP [11] etc.), while others may not.

(4) Support of resource and admission control across multiple administrative domains.

(5) Act as the arbitrator for resource negotiation between Service Control Functions and Transport Functions in the access and core networks.

(6) Support of both relative QoS control and absolute QoS control.

(7) Shall be capable to verify resource availability within its purview. The verification may be loose or strict, depending on whether the request is for relative or absolute QoS. RACF may act to reserve resources following notifications that resources are available.

(8) Shall support QoS differentiation over various categories of packet traffic including packet-type flows (i.e. different packet-type flows may receive different QoS treatments) and user designations (i.e. different user traffic may receive different QoS treatments depending on the user's classifications).

(9) Shall support QoS signalling [9]. This may include the ability to perform admission control based on estimated performance achieved along the path, compliant with QoS objectives.

(10) Shall only operate on authorised requests for QoS, for example, using information derived from user profiles, service priority, and operator network policy rules.

(11) Should be able to export information to support charging based on resource usage and/or QoS treatments.

(12) Should support methods for resource-based admission control, which may require one or more of the following:

- Accounting based, which admits service requests according to the knowledge of how much bandwidth (or how many sessions) has already been assigned for.
- Out-of-band measurement, which admits service requests based on measured network resource availability through periodic polling of routers or switches
- In-band measurement, which admits service requests based on the measured network performance through active probes or other in-band performance metrics
- Reservation based, which admits service requests only if an explicit request for the required bandwidth reservation is successful

(13) Shall support dynamic near-end NAPT control and firewall control.

(14) Shall support far-end (remote) NAT traversal.

(15) When different transport QoS mechanisms across network domains are involved, shall control the related transport interworking function.

(16) Should have access to and make use of information provided by network management on performance monitoring to assist in making admission decision.

(17) Should have access to and make use of information provided by the survivability functionality to support end-to-end QoS when Transport Function detects and reports a failure.

(18) Should make use of the service priority information for priority handling (e.g., admission control based on service priority information). This includes passing of service priority information between entities where applicable.

(19) Should support the selection of static provisioned resource separation among different types of NGN services at the network boundary.

6 RACF Mechanisms and Scenarios

6.1 QoS Resource Control Mechanisms and Scenarios

6.1.1 QoS Resource Control Mechanisms

QoS Capability of CPE:

According to the capability of QoS negotiation, the CPEs can be categorized as follows:

(1) Type 1 – CPE without QoS negotiation capability (e.g., vanilla softphone, gaming consoles)

The CPE does not have any QoS negotiation capability at either transport or service stratum. It can communicate with Service Control Functions for service initiation and negotiation, but cannot request QoS resources directly.

(2) Type 2 – CPE with QoS negotiation capability at the application layer (e.g. SIP phone with SDP[13]/SIP QoS extensions [15])

The CPE can perform application layer QoS negotiation (such as bandwidth) through application layer signalling, but is unaware of QoS attributes specific to the transport. The (application) service QoS concerns characteristics pertinent to the application such as media type and bandwidth etc.

(3) Type 3 – CPE with QoS negotiation capability at the transport layer (e.g. UMTS UE)

The CPE supports RSVP-like protocol or other Layer-2 QoS-aware signalling protocols (e.g. 802.1p, PDP context, ATM PNNI/Q.931 etc). It is able to directly perform transport layer QoS negotiation throughout the transport facilities (e.g. DSLAM, CMTS, SGSN/GGSN etc). The transport QoS concerns characteristics pertinent to the specific transport technology such as Y.1541 IP QoS class and DiffServ DSCP [14].

Resource Control Modes:

In order to handle different type of CPEs, the RACF shall support the following QoS resource control modes:

- Push Mode: The SCFs issue a request to the RACF for QoS resource authorization and reservation, and the RACF pushes the admission decisions to Transport Functions for policy and resource enforcement
- Pull Mode: The SCFs issue a request to RACF for QoS resource authorization, and QoS resource reservation and the admission decisions are requested by Transport Functions upon receiving transport-layer QoS signaling messages

The Push mode is particularly suitable for the first two types of CPEs. For type 1 CPEs, the SCFs determine the QoS requirements of the requested service on behalf of CPEs; for type 2 CPEs, SCFs extract the QoS requirements from application layer signalling. The Pull mode is suitable only for the third type of CPEs, which can explicitly request the QoS resource reservation through transport-layer QoS signaling.

Resource Control States:

Regardless of QoS negotiation capability of a particular CPE and the use of a particular resource control mode, the act of QoS resource control has three logical states:

- Authorization (Authorized): The QoS resource is authorized based on operator specific policy rules. The authorized QoS form the boundary of maximum amount of resource for the resource reservation.

- Reservation (Reserved): The QoS resource is reserved based on the authorized resource and resource availability. The reserved resource can be used by the best effort media flows when the resource has not yet committed at the transport functions.
- Commitment (Committed): The QoS resource request is committed based on the reserved resource for the requested service flows when the gates is opened as well as other admission decisions (e.g. bandwidth allocation) for the requested service flows are enforced at the transport functions.

In general, the resource control shall be based on the following criteria:

- The amount of committed resources is not greater than the amount of reserved resources.
- The amount of reserved resources is not greater than the amount of authorized resources.

Note that the amount of committed resources typically equals to the amount of reserved resources.

Resource Control Schemes:

Given the variation of application characteristics and performance requirements, the RACF architecture supports the following resource control schemes:

- Single-Phase Scheme: The three logical states including authorization, reservation and commitment are performed in one phase. The requested resource is immediately committed upon successful authorization and reservation. The Single-Phase Scheme is suitable for client-server applications to minimize the delay between the service request and the ensuing reception of content.
- Two-Phase Scheme: Authorization and reservation are performed in one phase, followed by commitment in a separate phase. Or Authorization is performed in one phase, followed by reservation and commitment in a separate phase. The Two-Phase Scheme is suitable for interactive applications, which have stringent performance requirements and need to have sufficient transport resources available.
- Three-Phase Scheme: The authorization, reservation and commitment are performed in three phases sequentially. The Three-Phase Scheme is suitable for network-hosted services in an environment where transport resources are particularly limited.

Information for Resource Control:

The RACF shall perform the resource control based on the following information:

- Service Information: A collective of data provided by SCFs for resource control request, which is derived from service subscription, application QoS requirement and service layer policy.
- Network Information: A collective of data collected from the transport networks, which may consist of network resource availability and local network policy.
- Transport Subscription Information: A collective of data provided by NACF, which includes the transport subscription profile such as the maximum bandwidth per subscriber.

The RACF may use the soft-state or hard-state approach in support of resource control per the network complexity, scalability and performance requirements.

6.1.2 QoS Resource Control Scenarios

On account of different QoS capabilities of CPEs and access transport networks, two QoS resource control scenarios using either the push mode or the pull mode are identified and can be applied to different types of network environment.

Scenario 1: QoS resource control scenario using the push mode.

The QoS resource control scenario using the push mode is applied to CPEs and/or access transport networks that do not support path-coupled QoS signaling in the transport layer, such as CPE type 1 and CPE type 2.

The CPE type 1 does not have any QoS negotiation capability, therefore it cannot initiate an explicit QoS request. The Service Control Functions (including IMS [5] and non-IMS) are responsible for 'determining' the QoS needs of the user requested service, and requesting QoS resource authorization and reservation from the RACF.

The CPE type 2 supports QoS negotiation at the application layer, therefore it can initiate an explicit application QoS request through the application layer signaling with QoS extensions (e.g. SDP/SIP extensions for delivering application QoS requirements) or through a dedicated application layer QoS signalling used for those application signalling protocols without QoS extensions or difficult to be extended. The Service Control Functions (e.g. P-CSCF in IMS) are responsible for 'extracting' the application QoS requirements and requesting QoS resource authorization and reservation from the RACF.

In this scenario the single-phase or two-phase resource control scheme can be used if the service control functions require the resource commitment to be performed in a separate phase.

Figure 2 depicts the high-level QoS resource control steps for Scenario 1.

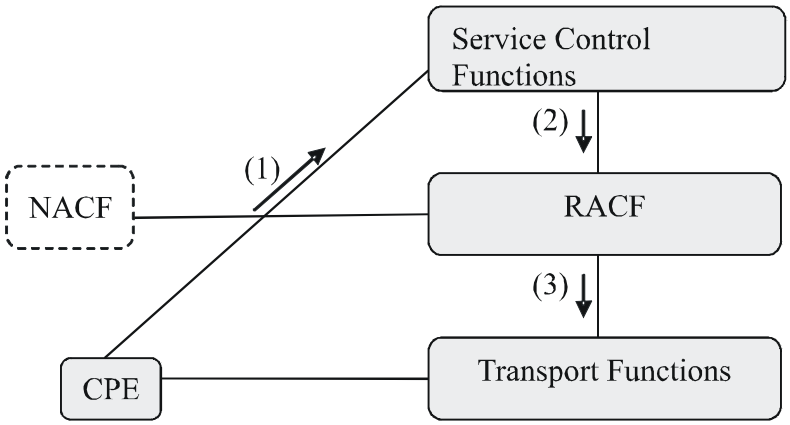


Figure 2 – The flow diagram for Scenario 1

(1) The CPE requests an application-specific service by sending a "Service Request" （e.g. SIP Invite, HTTP Get, etc.）to the Service Control Functions or also sends a dedicated application layer QoS signalling request. The Service Request may or not contain any explicit (application) service QoS requirement parameters.

(2) The Service Control Functions extract or determine the service QoS requirement parameters (e.g. media type, bandwidth etc.) of the requested service, and then request QoS resource authorization and reservation from the RACF by sending a 'Resource Reservation Request' which contains the explicit QoS requirement parameters.

(3) The RACF checks authorization and makes admission control based on user profile in the NACF, on operator specific policy rules and on resource availability. If admitted, the RACF installs the gate control, packet marking and bandwidth allocation decisions to the Transport Functions.

Scenario 2: QoS resource control scenario using the pull mode.

The QoS resource control scenario using the pull mode is applied to CPEs and/or access transport networks that support path-coupled QoS signaling in the transport layer, such as CPE type 3.

The CPE type 3 supports a dedicated path-coupled transport layer QoS signalling (e.g. PDP context, RSVP) which passes only through the nodes on the data path, therefore it can initiate an explicit QoS request (actually a resource reservation request) directly to the Transport Functions. But the QoS resource reservation needs prior authorization via the Service Control Functions.

In this scenario the two-phase or three-phase resource control scheme can be used if the service control functions require the resource commitment to be performed in a separate phase. And the coordination between the application layer signalling and the dedicated path-coupled transport layer QoS signalling is necessary.

Figure 3 depicts the high-level QoS resource control steps for Scenario 2.

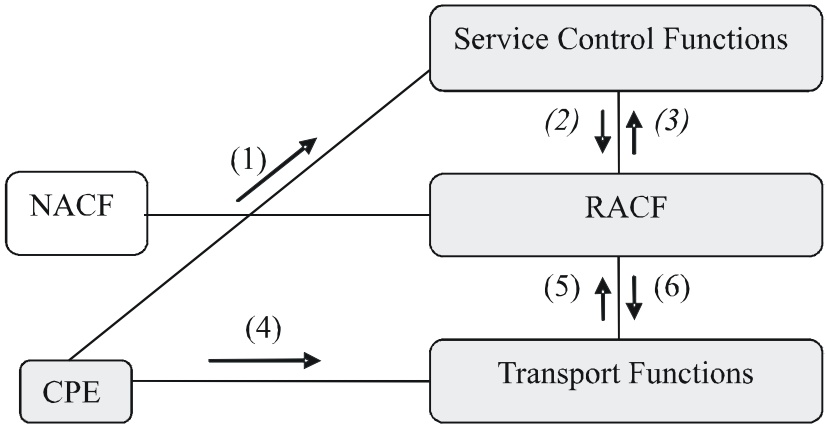


Figure 3 – The flow diagram for Scenario 2

(1) The CPE requests an application-specific service by sending a "Service Request" （e.g. SIP Invite）to the Service Control Functions. The Service Request may or not contain any explicit (application) service QoS requirement parameters.

(2) The Service Control Functions extract or determine the service QoS requirement parameters (e.g. media type, bandwidth etc.) of the requested service, and then requests authorization from the RACF by sending a 'Resource Authorization Request' that contains the explicit QoS requirement parameters.

(3) The RACF checks authorization based on operator specific policy rules. If authorized, an authorization token is assigned to this service and informed to the CPE. The token may be optional.

(4) The CPE initiates an explicit 'QoS Request' (actually a resource reservation request) directly to the Transport Functions through a dedicated path-coupled transport layer QoS signalling. This QoS Request contains the explicit transport QoS requirement parameters for an application-specific service. And it may also contain the authorization token assigned at the first phase.

(5) On receipt of the 'QoS Request', the transport function at the network edge requests reservation and admission control from the RACF by sending a 'Resource Reservation Request' which may contain the authorization token.

(6) The RACF makes reservation and admission control based on user profile held in the NACF, operator specific policy rules and resource availability. If admitted, the RACF installs the gate control, packet marking and bandwidth allocation decisions to the Transport Functions.

6.2 NAPT Control and NAT Traversal Mechanisms and Scenarios

6.2.1 NAPT Control and NAT Traversal Scenarios

The RACF shall provide the control function in support of the following NAPT scenarios.

Near-end NAPT:

In order to hide transport network addresses between different network segments/domains as a security measure or use private addresses due to the shortage of public addresses, near-end NAT devices controlled by operators are required to perform the address and/or port translation (NAPT) at the border of access-to-core and/or the border of core-to-core. All NAPT techniques in support of Network Address Hiding ultimately involve the installation of bindings in NAPT devices, and the modification of the application signalling messages to reflect the bindings created by NAPT.

Far-end (remote) NAPT:

The far-end (remote) NAT devices are widely deployed in enterprise and residential networks to protect the customer premises networks. Both signalling and media of the application have to go through such NAT devices, if exist. By default the application assumes CPE's local network address is unique and reachable globally; therefore, the application signalling uses this local address to setup end-to-end connection. However, the-far end NAT has broken those properties because the network address of media packet will be changed by the far-end NAT. Therefore, the application doesn't work through the far-end NAT, and NAT traversal mechanisms are required. All NAT traversal techniques ultimately involve the modification of the application protocol messages to reflect the address mapping necessitated by the far-end NAT.

6.2.2 NAPT Control and NAT Traversal Mechansms

The RACF shall interact with SCFs and Transport Functions to control the NAPT and NAT Traversal. Both NAPT and NAT Traversal can be supported by one set of functions. The pertinent functions are distributed in the SCFs, RACF and Transport Functions:

- NAPT Proxy Function (NPF): modifies the address and/or port in the message body of application signalling to reflect the address binding information created by NTF, which is a service stratum function.
- NAPT Control Function (NCF): generates the address binding information, performs the NAPT policy control and gate control (i.e., instruct the opening/closing of a "gate").
- NAPT Processing Function (NTF): enforces the NAPT translation and media relay to change the address and port in the media packet, which is a transport stratum function.

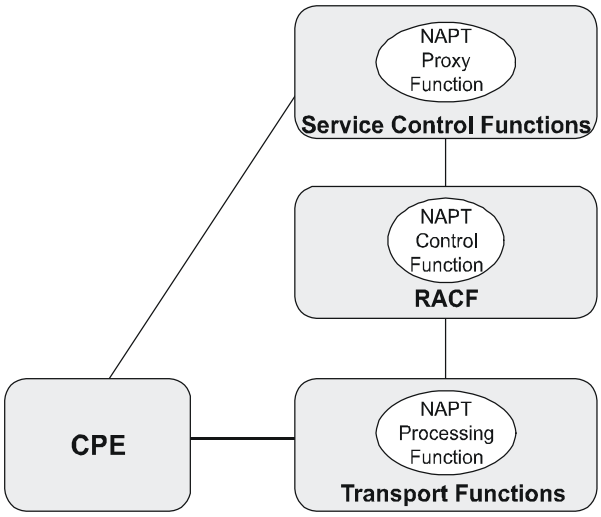


Figure 4 – NAPT and NAT Traversal Control Mechanisms

The RACF shall provide the NAPT and NAT Traversal control function for address/port binding, NAPT policy control and gate control; and interact with NAPT Proxy Function in SCFs for modifying the message body of application signalling, and interact with NAPT Processing Function in the transport functions for requesting network address/port translation information.

7 Functional Architecture

The Figure 5 shows a generic Resource and Admission Control functional architecture in NGN.

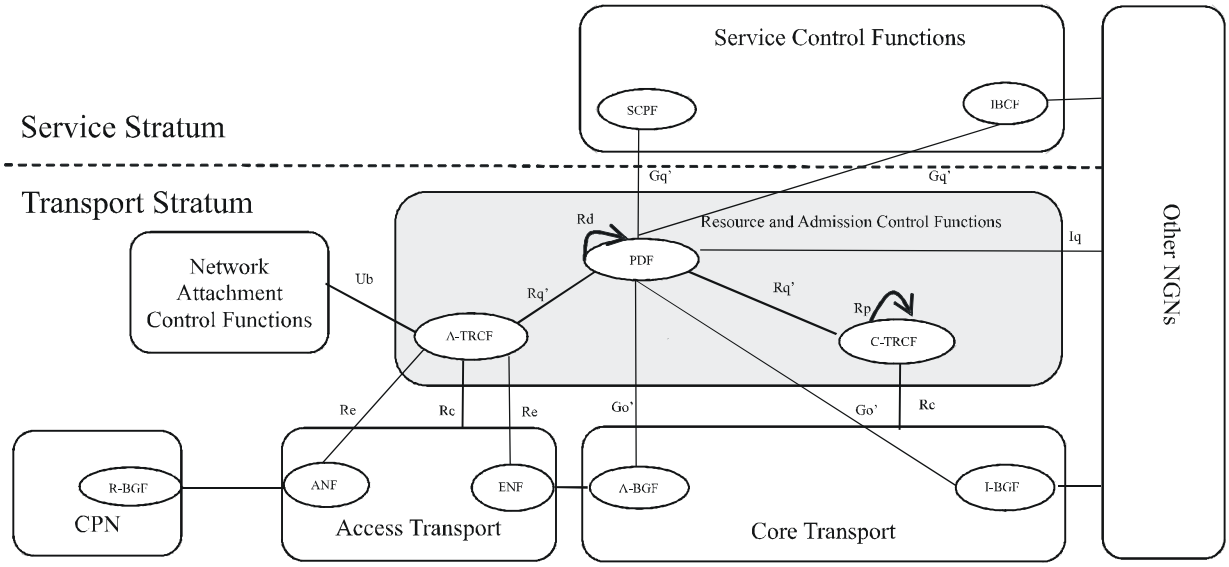


Figure 5 – Resource and Admission Control functional architecture in NGN

Editor's notes: NGN should allow both IPv4 and IPv6, so the NAT effects on this architecture and reference points (Gq', Go' and Rq') shall be considered as a whole. The figure and related text also require clarification.

In Figure 5, there are mainly the following functional entities involved in. A functional entity is an entity that comprises a specific set of functions at a given location.

R-BGF – Residential Border Gateway Functional entity

CPN – Customer Premises Network

ANF – Access Node Functional entity

ENF – Edge Node Functional entity

SCPF – Session Control Proxy Functional entity

IBCF – Interconnection Border Control Functional entity

PDF – Policy Decision Functional entity

A-TRCF – Access Transport Resource Control Functional entity

C-TRCF – Core Transport Resource Control Functional entity

A-BGF – Access Border Gateway Functional entity

I-BGF – Interconnection Border Gateway Functional entity

Editor's note: How the functional entities are called should be aligned with WG2. The term "subsystem" in the draft needs to be replaced with the one agreed by WG 2.

7.1 Overview

Service Control Functions present the functional entities in different service subsystems of NGN that request the QoS resource and admission control for the media flow of a given service via the reference point Gq'. For session-based services, they are SCPF and IBCF [3]. SCPF acts as the access point for session services and with user service access control. IBCF acts as the interconnection point for session services between two operator's networks.

Network Attachment Control Functions (NACF) present the functional entities that provide user access network management and configuration based on user profiles.

A core transport infrastructure is shared among multiple service subsystems and even possibly shared among multiple service providers. The transport resource separation mechanisms (i.e. L1/L2/L3 VPN) may be used among service subsystems for security and network performance.

Border Gateway Function (BGF) is a packet-to-packet gateway function at the boundary between different packet networks. There may be one or multiple A-BGF to different service subsystems, and one or multiple I-BGF used to interconnect with other core networks. ANF, ENF, A-BGF and I-BGF in the transport layer are the key injection nodes in support of dynamic QoS control, and NAPT Control and NAT traversal.

The RACF consists of two types of resource and admission control functional entities: PDF (Policy Decision Function) and TRCF (Transport Resource Control Function).

- The PDF is a functional entity for the final decision for a QoS resource request in terms of the network resource and admission control based on operator policy rules, service information, and resource availability checking result. It controls the gates (packet filtering) in the BGF at the network boundary at the media flow level. The PDF is transport technology-independent. It is independent of Service Control Functions as well. The policy rules used by PDF are service-based. One PDF may serve for multiple service subsystems and service providers.
- The TRCF is a functional entity for the resource availability check for a QoS resource request within a single network segment based on network topology, network resource utilization and element resource availability. It controls the transport resource at the aggregation and element level. The TRCF is service-independent and transport technology-dependent, which is located in a network provider's domain. The policy rules used by TRCF are transport technology specific. There may be multiple TRCF instances in a large scale core network to control different sub-networks.

PDF provides a single contact point to Service Control Functions and hides the details of transport functions from Service Control Functions. The PDF asks the TRCFs in the involved access and core transport networks through the reference point Rq' to check the resource availability for the requested QoS resource along its end-to-end media flow path.

Multiple PDF instances can be interconnected with each other through the reference point Rd within the same network operator's domain. If there are multiple TRCF instances in an involved core network, the PDF may only contact one designated TRCF instance, and then these TRCF instances communicate with each other through the reference point Rp to check the edge-to-edge resource availability in the involved core network for the requested QoS resource.

All the entities in Figure 5 are functional ones. The implementation and physical configuration of the PDF and TRCF functional entities are flexible, which can be distributed or centralized and can be a stand-alone box or a module in an integrated box. A network administrative domain shall contain at least one PDF. So, the PDF may be part of the Access Network or part of the Core Network or be present in both Access and Core Network, depending of the business model and implementation choices.

7.2 Functional entity descriptions

7.2.1 Service Control Functions

Service Control Functions in different service subsystems can interact with PDF via the Gq' reference point. It makes requests for bearer resources and may receive notifications when resources are reserved and released.

- Service Control Functions (SCFs) provide information to the PDF to identify media flows and their required QoS resource (e.g. service QoS class, bandwidth).
- The SCFs may provide service priority information to the PDF to facilitate appropriate priority handling (e.g. priority processing of the resource request, resource pre-emption if needed).
- The SCFs may request resource usage information through the PDF for charging.
- The SCFs may provide related service information to the PDF to facilitate appropriate dynamic firewall working mode selection.
- The SCFs shall indicate whether the resource should be committed (i.e. opening gate and allocation bandwidth) immediately when resources are reserved. Alternatively, the SCF may request the resource commitment later, after resources are reserved.
- In the case where a NAPT function is required, the SCF shall request address binding (mapping) information and shall do any modifications that may be required to address information within application signalling (e.g. SDP/SIP).
- In the case where the pull mode along with a path-coupled resource reservation mechanism is used the SCF shall indicate to the PDF whether it would be notified when resources are reserved, modified and released.
- When an authorization token mechanism is used the PDF may supply the SCF with one or more authorization tokens which the SCF shall include in application signalling to the CPE.

7.2.2 Network Attachment Control Functions

Network Attachment Control Functions (NACF) present all the functional entities that provide user access network management and configuration based on user profiles,

The network attachment control functions provide the following functions:

- Dynamic provision of IP address and other user equipment configuration parameters.
- Authentication of user access network, prior or during the IP address allocation procedure.
- Authorisation of user access network, based on user profiles.
- Access network configuration, based on user profiles.
- Location management.

The A-TRCF interacts with the NACF via the Ub reference point, which makes requests for the binding of the logical/physical port address to an assigned IP address.

7.2.3 Resource and Admission Control Functions

7.2.3.1 Overview

Function	Description	Location
QoS and Priority Mapping - Technology Independent (QMTI)	Maps the service QoS parameters and priority received from the SCF to network QoS parameters and priority	PDF
Firewall Working Mode Selection– (FWMS)	Selects the working mode of the firewall based on the related service information	PDF
Final Decision Point (FDP)	Makes the final admission decisions (including priority considerations) in terms of network resources and admission control, based on request information from the SCF	PDF
Networks Selection (NS)	Locates core networks, the A-BGF and I-BGF that are involved to enforce the final admission decisions	PDF
Core Network Path Selection (CNPS)	Chooses the technology independent core network ingress path at the network boundary based on the service information and policy rules	PDF
IP Packet Marking Control (IPMC)	Decides on the packet marking and remarking of flows	PDF
NAPT Control (NAPTC)	Controls network address translation for both near-end NA(P)T and far-end NA(P)T	PDF
IP Gate Control (IPGC)	Controls the opening and closing of a gate. An IP gate is identified by, for example, an IP flow 5-tuple.	PDF, A-TRCF
QoS Mapping - Technology Dependent (QMTD)	Maps the network QoS parameters to transport (technology dependent) QoS parameters.	TRCF
Technology Dependent Decision Point (TDDP)	Makes technology-dependent and resource-based admission decisions.	TRCF
Technology-Dependent Gate Control (TDGC)	Controls the opening and closing of a gate. A technology-dependent gate is defined by, for example, an IP 5-tuple and additional link-layer attributes	A-TRCF
Technology Dependent Marking	Decision on the marking and remarking of flows at the link layer	A-TRCF
Network Topology Maintenance (NTM)	Collects and maintains the transport network topology	TRCF
Network Resource Maintenance (NRM)	Collects and maintains the transport resource status information	TRCF
Element Resource Control (ERC)	Controls the resources at the aggregation and element level, such as control of DiffServ PHB (including policing, shaping, etc.) of relevant transport elements	TRCF

Editor's notes: Further contributions are invited to clarify the following items:

1. IPGC, TDGC

2. IPMC

3. ERC

In addition, contributions are invited to define the terms "technology dependent" and "technology independent."

7.2.3.2 Policy Decision Functional entity (PDF)

The PDF entity handles the QoS resource requests received from SCFs via the Gq' reference point or from A-BGF/I-BGF via the Go' reference point in the Core Network. The PDF contains the following functions:

- QoS Mapping - Technology Independent (QMTI): This function maps the service QoS parameters and priority received from the SCFs via the Gq' reference point to network QoS parameters and priority based on the operator network policy rules, and accommodate the diversity of service QoS parameters and priority.
- Firewall Working Mode Selection (FWMS): Selecting the working mode of the firewall based on the related service information.
- Network Selection (NS): This function locates core networks that are involved to offer the requested QoS resource. It locates A-BGF and I-BGF that are involved to enforce the final admission decisions.
- Final Decision Point (FDP):
  - This function interacts with one of the A-TRCF (respectively C-TRCF) in the involved access network via the Rq' reference point to check if there is the requested QoS resource available within the involved access network (respectively within the involved core network).
  - Then the FDP makes the final admission decisions based on user access network profiles, operator specific policy rules, service priority information, and resource availability for the media flow of a given service.
  - The FDP indicates the loss of connectivity: It informs SCPF that the transport resource previously granted is lost. SCPF may request PDF to relinquish all resource relative to the session.
- IP Packet Marking Control (IPMC): This function takes decisions on packet marking and remarking of flows. The marking may consider the priority of the flow and traffic engineering parameters.
- NAPT Control (NAPTC): This function interacts with A-BGF and I-BGF and SCF to provide the address binding information for the NAPT Control and NAT traversal at the A-BGF and I-BGF as needed.
- IP Gate Control (IPGC): This function controls A-BGF and I-BGF to install and enforce the final admission decisions via the Go' reference point (e.g. opening or closing the gate), which is located at the core network boundary and connected to an access network. The decision whether to enable or disable the forwarding of IP packets is based on a set of IP gates (packet classifiers, e.g. IP 5-tuple) that identify the media flows.
- Interact with A-BGF and I-BGF to request resource usage information and respond to SCF.
- Core Network Path Selection (CNPS): Chooses the technology independent core network ingress path for a media flow based on the service information and policy rules at the involved BGF.

The PDF can be stateful or stateless depending on the complexity of the specific network environment, application characteristics and deployment architecture. In order to be stateless, the PDF shall generate a transaction state index for each resource control request from SCFs, which can be stored in the SCFs, TRCF or BGF and used to retrieve the state information together with pertinent information flows.

7.2.3.3 Transport Resource Control Functional entity (TRCF)

TRCF is a collective of transport technology dependent resource reservation and admission control functions that are dispersed over transport network segments. The main functions of TRCF are as follows:

- Resource status monitoring and network topology collection

  TRCF collects and maintains the network topology and resource status information. The resource status information may be specific to the resource-related admission control scheme being used by

TRCF whether it is accounting, out-of-band measurements, in-band measurements, or reservation-based.

- Resource based admission control

  On receipt of the resource availability checking request from PDF, indicating QoS characteristics (e.g. bandwidth), the TRCF shall use the QoS information received from the PDF to perform resource based admission control, i.e. the TRCF checks and computes the transport resource availability on the basis of the resource status information and transport network policies, updates the resource allocation status, and then returns the checking confirmation to PDF.

- Transport dependent policy control

  Transport dependent policies are a set of rules that specify what network policies should be applied to a particular transport technology. The TRCF ensures that request from the PDF (of an particular network service provider) matches the transport specific policies (e.g. access link policies, core transport network policies), as multiple PDF can request resources from the same TRCF.

The TRCF combines the requests from the PDFs that have requested resources to ensure that the total of the requests match the capabilities of the particular transport network.

The TRCF entity has the following basic functions:

- QoS Mapping - Technology Dependent (QMTD): This function maps the network QoS parameters and classes received from the PDF via the Rq' reference point to transport (technology dependent) QoS parameters and classes per the specific transport policy rules, and accommodate the diversity of transport technologies.
  - When mapping network QoS parameters to Transport (Technology Dependent) QoS parameters, TRCF considers the underlying transport technology. A set of network QoS parameters may be mapped to different sets of Transport (Technology Dependent) QoS parameters based on transport technologies. TCRF has knowledge on the QoS related features of underlying transport network and map the network QoS parameters to the best matching Transport (Technology Dependent) QoS parameters for given transport technology. The mapping policy needs to be provided and that should depend on underlying transport technology of the network segment.
- Network Topology Maintenance (NTM): This function collects and maintains the transport network topology information via the Rc reference point.
- Network Resource Maintenance (NRM): This function collects and maintains the transport resource status information via the Rc reference point.

7.2.3.3.1 Access Transport Resource Control Functional Entity (A-TRCF)

In addition to the basis TRCF functions, the A-TRCF entity has the following specific functions:

- Technology-Dependent Gate Control (TDGC): This function controls ANF/ENF to install and enforce the packet filtering decisions at media flow level via the Re reference point. A technology-dependent gate (packet filtering) is defined by, for example, an IP 5-tuple and additional link-layer attributes.
- IP Gate Control (IPGC): This function controls the packet filtering and marking of ANF/ENF at media flow level via the Re reference point only when access networks support IP layer capability.
- Technology Dependent Decision Point (TDDP): This function receives and responds the QoS resource availability check requests from PDF via the Rq'reference point. This function computes the requested QoS resource availability based on the access network topology and resource status information database.

- Technology Dependent Marking (TDM): This function takes decisions on marking and remarking of flows at the link layer. The marking may consider the priority of the flow and traffic engineering parameters.
- Element Resource Control (ERC): This function controls the transport resource in the access network at the aggregation and element level (e.g. configuration of the L2/L3 QoS-related parameters and behaviours in a transport element, per-aggregation resource reservation). It receives requests for decisions and handles them.

The A-TRCF shall interact with NACF to retrieve the transport user profile via Ub reference point.

The implementation of A-TRCF may be different in different access networks due to different access transport technologies and their QoS mechanisms in the data plane.

7.2.3.3.2 Core Transport Resource Control Functional entity (C-TRCF)

In addition to the basis TRCF functions, the C-TRCF entity has the following specific functions:

- Technology Dependent Decision Point (TDDP):
  - Receives and responds the QoS resource availability check requests from PDF via the Rq reference point.
  - Receives and responds the QoS resource availability check request relayed from the upstream C-TRCF entity along a media flow path via the Rp reference point, if there are multiple C-TRCF entities for different sub-networks in a large scale core network.
  - Computes the requested QoS resource availability based on the network topology and resource status information database within its purview.
  - Position the downstream C-TRCF entity along a media flow path based on the inter-sub-network routing information that is technology-dependent, and relay the QoS resource availability check request to the downstream C-TRCF entity via the Rp reference point if there are multiple C-TRCF entities for different sub-networks in a large scale core network.
  - Interact with each other via the Rp reference point to check the edge-to-edge resource availability for a QoS resource request, if there are multiple C-TRCF entities in a network.

Editor's note: Further study is needed if Re should be added to C-TRCF.

The implementation of C-TRCF may be different in different core networks due to different core transport technologies and their QoS mechanisms in the data plane.

The C-TRCF entities in different operators' domains generally interact indirectly through PDF.

Editor's Note: The following paragraphs are about the internal implementation of TRCF entities. It's proposed to remove them into an Appendix.

With the accounting-based method, the TRCF checks if there are sufficient resources available in the Transport Function by comparing Transport Function capacity and the knowledge of how much bandwidth (or how many sessions) has already been assigned for. If there is, the TRCF updates the resource status information to include the new application request, and responds to the PDF with a positive answer (e.g., resources are available). If the Transport Function does not have the required resources, the TRCF responds with a negative answer (e.g., resources not available).

With the out-of-band measurement-based method, the TRCF admits service requests based on measured network resource availability through periodic polling of routers or switches. To handle high-volume service requests, the TRCF can compute admission rules based on most recent resource measurements, and apply these rules when the PDF requests a resource availability check. An example of the TRCF admission rules is to block a certain fraction of service requests between a pair of Border Gateway Functions (BGFs). The TRCF admission rules are updated based on resource utilization in the Transport Function through measurements. Note that in the out-of-band measurement-based method, there is no need to reserve

resources per service request. Furthermore, the TRCF admission rules can be uploaded to the PDF so that the PDF can apply the rules locally without consulting the TRCF per service request. The rules cached in the PDF are updated by the TRCF to reflect the changes in the resource usage in the Transport Function.

With the in-band measurement-based method, the TRCF admits service requests based on the measured network performance through active probes or other in-band performance measurement mechanisms. The probing can be done when PDF requests a resource availability check or can be done periodically independent of the PDF requests. With the latter, TRCF can compute admission rules similar to those suggested for the out-of-band measurement-based method. These rules can be cached in the PDF, and be updated to reflect the rule changes. Note that with the in-band measurement-based method, there is no need to reserve resources per service request. Note that such caching is a challenge to PDF, because there are many TRCF entities in access networks and core networks with different transport technologies.

With the reservation-based method, the TRCF explicitly requests bandwidth reservation from the Transport Functions. To handle high-volume service requests, the TRCF can compute admission rules based on per-aggregation resource reservation, and apply these rules when the PDF requests a resource availability check. Note that per-session resource reservation is inefficient, so per-aggregation resource reservation is applied in a pre-configuration way and can be adjusted based on the resource usage.

7.2.4 Transport Functions

The functions described in the following sections pertain only to those concerned RACF.

7.2.4.1 Access Node Functional entity (ANF)

The Access Node Function (ANF) in IP access network directly connects to CPN and terminates the first/last mile link signals at the network side. Generally, it is a Layer 2 device that may be IP capable.

The ANF performs QoS mechanisms dealing with the user traffic directly, including buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing, shaping, and forwarding.

As one key injection node for support of dynamic QoS control, the ANF may perform packet filtering, traffic classification, marking, policing and shaping at flow level or user level under the control of the A-TRCF via the Re reference point.

7.2.4.2 Edge Node Functional entity (ENF)

The Edge Node Function in IP access network acts as the upstream traffic egress that connects IP access network to the external networks and terminates the Layer 2 access session with the CPE. It shall be a Layer 3 device with IP routing capabilities.

The ENF performs QoS mechanisms dealing with the user traffic directly, including buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing, shaping, and forwarding.

As one key injection node for support of dynamic QoS control, the ENF performs packet filtering, traffic classification, marking, policing and shaping at flow level or user level under the control of the A-TRCF via the Re reference point.

Editor's note: The further study is needed for the descriptions and functionality of ANF and ENF.

7.2.4.3 Access Border Gateway Functional entity (A-BGF)

The Access - Border Gateway Function (A-BGF) is a packet gateway function between an access network and a core network used to mask a service provider's network from access networks, through which CPE accessing packet-based services (e.g. IMS, Internet).

The functions of the A-BGF may include:

Editor's note: contributions are invited to further clarify packet filtering and the different variants; where the policy rules are from; what is the role of the PDF in pushing the rules; if activation of policy rules provisioned via the management plane is another option; and whether gating is a distinct function.

- Opening and closing gate: enabling or disenabling packet filtering for a specific media flow based on flow classifier (e.g. IPv4 5-tuple) and flow direction to enforce policy control decision from PDF.

  A gate is unidirectional, associated with a media flow in either the upstream or downstream direction. When a gate is open, all of the packets associated the flow are allowed to pass through; when a gate is closed, all of the packets associated with the flow are blocked and dropped.
- Packet filtering based firewall: inspecting and dropping packets based on security policy rules defined by operators and gates installed by PDF.

  Four packet inspection modes for packet-filtering-based firewall:
  - Static packet filtering: inspecting packet header information and dropping packets based on static security policy rules. This is the default packet inspection mode applied for all flows.
  - Dynamic packet filtering: inspecting packet header information and dropping packets based on static security policy rules and dynamic gate status.
  - Stateful inspection: inspecting packet header information as well as TCP/UDP connection state information and dropping packets based on static security policy rules and dynamic gate status.
  - Deep packet inspection: inspecting packet header information, TCP/UDP connection state information and the content of payload together, and dropping packets based on static security policy rules and dynamic gate status.
- Traffic classification and marking
- Traffic policing and shaping
- Network address and port translation
- Media Relay (i.e. media latching) for NAT traversal
- Collecting and reporting resource Usage information (e.g. start-time, end-time, octets of sent data)

As one key injection node for support of dynamic QoS control, NAPT/FW control and NAT traversal, the A-BGF performs the above functions at flow level under the control of the PDF via the Go' reference point.

7.2.4.4 Interconnection Border Gateway Functional entity (I-BGF)

The Interconnection - Border Gateway Function (I-BGF) is a packet gateway function used to interconnect an operator's core network with another operator's core network supporting the packet-based services. There may be one or multiple I-BGF in a core network.

The functions of the I-BGF may be the same as that of the A-BGF.

As one key injection node for support of dynamic QoS control, NAPT/FW control and NAT traversal, the I-BGF performs the above functions at flow level under the control of the PDF via the Go' reference point.

8 Mechanisms

8.1 Selection Mechanisms

In order for transferring the QoS request between relevant functional entities (such as communications between SCFs-PDF, PDF-TRCF, PDF-BGF, TRCF-TRCF, or PDF-PDF), a functional entity first needs to select the communicating party based on the information provided by static mechanism or dynamic mechanism:

– Static Mechanism: A functional entity may identify the target communicating party (e.g. SCFs to PDF, PDF to TRCF) through statically (manually) configured location information, which includes either the IP address or the fully qualified domain name (FQDN). This information would be used to resolve through, for example, the DNS.
– Dynamic Mechanism: A functional entity may identify the target communicating party and determine its network address automatically through information such as the type of service and a set of service attributes, or the query of, for example, the DNS using the end user's identity for the target communicating party in a particular address realm.

In this specification, the static mechanism is mandatory and the dynamic mechanism is optional. The application identifier, address realm, user identity and source/destination address information is required by pertinent reference points (such as Gq', Go', Rq', Iq, Rd and Rp) in support of selection mechanism.

8.2 Binding Mechanisms

The RACF shall allow the use of the following information for binding the media flow QoS request with the policy decision information in support of policy enforcement in the BGF when a transport signalling is applied to pull the policy decision information from the PDF:

1) Authorization token: The PDF generates an authorization token for each application session on request from the SCFs. The Authorization token contains the fully qualified domain name of the PDF and a session ID in the PDF, which allows the PDF to uniquely identify the application session.
2) Source address of media flow: When neither near-end NAPT nor far-end NAPT is deployed between the CPE and SCFs, the end user network address is used for the binding. Otherwise, the source address of media flow received by BGF shall be used for the binding. The fully qualified domain name of the PDF and the session ID are derived based on the source address of media flow.
3) Source address of media flow + other filters (e.g. media flow classifier): When the multiple simultaneous media flows are provisioned in a session, the source address may not be adequate to identify a unique binding, other filters such as the port number of source address, destination address and port number and protocol number may be used with the source address for the binding. The fully qualified domain name of the PDF and the session ID are derived based on the source address of media flow and other applied filter information.
4) CPE identifier: When the transport subscription information is needed by the RACF for policy decision and resource control, e.g. A-TRCF in access networks, the CPE identifier may be used for accessing to the subscription profile in NACF directly.

9 Reference points

Editor's Note: In order to avoid the iteration on the description of reference points, suggest consolidating the common part of reference points. The edited Gq' and Go' can be used as the baseline for the consolidation.

9.1 Reference Point Gq'

The Gq' reference point allows QoS resource request information needed for QoS resource authorization and reservation to be exchanged between PDF and Service Control Functions. Either the push or pull mode may be used. The Gq' reference point should be compatible with the Gq interface as defined by 3GPP Release 6 in 3GPP TS 29.209 [8], and should support the NAPT/firewall control and NAT traversal at A-BGF/I-BGF as needed.

9.1.1 Functional requirements

9.1.1.1 Resource control functional requirements:

The Gq' reference point provides the ability for the SCF to make requests:

- For resource authorization and reservation for a media flow,
- For QoS handling,
- For priority handling,
- For gate control of a media flow,
- To insert a NAPT function and request address mapping information.
- For dynamic firewall working mode selection
- For resource usage information
- In addition, the SCF can request notification of events.

9.1.1.2 Resource control processing functional requirements:

To help assure the reliability and performance of resource control operations across the Gq' reference point, the following capabilities are required:

Overload Control: The PDF shall be able to support overload control for preventing the overflow of the information messages exchanged between SCFs s and PDF in support of reliability requirement.

Synchronization and Monitoring: The PDF shall be able to keep tracking and synchronize the resource control session status through Gq' in support of recovery and operational information statistics and auditing.

Session State Maintenance: When the stateful PDF is used, it shall be able to maintain the session state using either soft-state or hard-state approaches. The Reservation Holding Time specifies the time limitation in support of abnormal recovery. When the stateless PDF is used, the Resource Control Session Information passed by SCFs s or BGF can be used to derive the session state and relevant information.

9.1.2 Protocol Requirements

This section provides a brief description of the protocol requirements for the Gq' reference point.

Request-Response Transactions: The protocol must allow the SCF to request a transaction to be performed by the PDF and get a response (that can be correlated with the request) in return.

Notifications: The protocol must allow the notification of asynchronous events (from the PDF to the SCF).

Reliable Delivery: The protocol should provide reliable delivery of messages.

Extension Mechanisms: The protocol should including extension mechanisms such as versioning or other means to allow changes while ensuring backwards compatibility.

Capabilities: The SCF must be able to determine capabilities when requesting resources and other transport plane functions via the PDF.

Security: All messages between SCF and PDF must be authenticated such that requests to the PDF from unauthenticated sources will not be performed and such that notifications sent from the PDF to SCF can be ensured to come from the authenticated PDF source.

One to Many: Multiple Service Control Functions must be able to make requests to a given PDF. An SCF may also communicate with multiple PDFs. However, only a single SCF will make a request to a given PDF for a particular session.

9.1.3 Information elements

The Gq' reference point supports the exchange of the following information:

Authorisation tokens (optional): In the policy pull mode, the PDF may generate one or more authorisation tokens on request from the SCFs. Authorization tokens contain an identifier that identifies the PDF and a Resource Control Session Identifier that allows the PDF to uniquely identify the application session.

Charging correlation information: The SCFs and PDF may exchange charging correlation information, including resource usage information.

Gate control commands: The SCFs shall be able to enable the gate (open the gate) or disable the gate (close the gate) for a given media flow during the application session. Note that closing the gate does not release bandwidth resources.

- Gate Control Policy: Indication of whether the gate should be automatically and immediately opened (i.e. media enabled or resource committed) when the resources are reserved or whether the SCF will supply a separate "enable" message.
- Revoke Policy: An indication as to whether or not the PDF has the authority to revoke the authorization and modify or release the reserved resources at some future point in time (e.g. pre-emption).

Resource Demand Information: This is an upper limit on the amount of resource (e.g. bandwidth, Class of Service) that may be authorized, reserved and committed. This value is specified whether the Push or Pull mode is used. A value of 0 indicates that no bandwidth is authorized.

In the Push mode, the resource request for reservation and commitment should not be greater than the resource for authorization. In the Pull mode, after the resource request is authorized, a path-coupled reservation request that remains within the authorized limits will be accepted as long as resources are available.

Available Resource Information: This is an optional capability that allows PDF to provide the maximum available resource information to SCFs (e.g. bandwidth, Class of Service) if the requested resource cannot be permitted.

Request to Modify: The SCFs shall be able to request the PDF to modify the resource authorization and allocation for a media flow.

Request to Release: The SCFs shall be able to request the PDF to release the resource authorization and allocation for a media flow. It is to release all resources associated with that media flow.

Notifications: The PDF shall be able to notify the required information to the SCFs that do not have to be requested by the SCFs. Notifications Required:

- A persistent notification is provided to the SCF in the case that the PDF determines that the bearer is lost or resources released for some reason.
- Notifications associated with path-coupled mechanisms (e.g. RSVP): when resources are reserved, modified and released.
- Resource Usage information when resource reservation for the media flow is released..

Responses: The PDF shall be able to respond to a request or confirm a command from the SCFs .

NAPT Indication: The PDF shall be able to indicate the deployment of near-end NAT to SCFs for modifying application signaling message body Optional.

Address Binding Information Request: The SCFs shall be able to notify and request the address mapping for far-end NAT Optional.

The information elements exchanged across Gq' reference point are categorized as follows:

9.1.3.1 Resource Control Processing information elements

The information elements for request processing are described, which provide the information used for discovery, binding, flow control (overload control), state maintenance etc:

Application Identifier	Globally unique identifier for different instances of service control functions
Resource Control Session Identifier	An identifier for the session that may be composed of multiple media flows requesting the resource reservation to RACF.
Transport Subscriber Identifier	A globally unique identifier for the subscriber requesting the transport resource. This identifier can be used for locating the transport subscription information for the subscriber.
Global IP Address Information	A set of IP address information for identifying the associated network to which the subscriber is attached. It can be used for locating the access network to which the subscriber is requesting the transport resource.
– Unique IP address	The IP address for identifying the subscriber.
– Address Realm	The addressing domain of the IP address (e.g. Subnet prefix or VPN ID).
Resource Request Client Information	A set of information sub-elements for the client of resource control service (i.e. the owner of service subsystem (e.g. a Service Provider).
– Client Name	A local identifier for the client requesting the resource control.
– Request Class	The priority level of resource control request
– Resource Control Session Information (Optional)	The record of the resource control session information. This is used for deriving the session state and other information (e.g. association of SCFs, PDF, TRCF and BGF) only when a stateless PDF is deployed and only has a local significance between the PDF and pertinent parties.
Reservation Holding Time	The value of time interval for which the resource are reserved, requested by SCF or granted by PDF per the information message.

Editor's note: how SCFs obtain the information of transport subscriber ID is an issue for service stratum functionality.

9.1.3.2 QoS resource information elements

The components for media session and media flows are described, which provides the information for media session profile:

Media Profile	A set of information sub-elements for a media session, which may be composed of data flows and control flows (e.g. RTP and RTCP flows for a VoIP call).
– Media Number	An identifier for a media session (e.g. ordinal number of the position of the "m=" line in the SDP).
– Type of Service	Indication of service type for the media data flow (e.g. voice bearer, video telephony, and streaming video).
– Class of Service (Optional)???	The application service class for the media, which is of local significance between the resource request client and PDF (e.g. multimedia – first class) and is to be converted to the network service class???.
– Media Priority (Optional)	Information for priority handling (e.g., TDR/ETS).
– Media Flow Description	A set of parameters for the individual media flow within a media session.

Media Flow Description information sub-element defines the break-down components for a media flow:

Media Flow Description	A set of parameters for the individual media flow within a media session
– Flow direction (in->out, out->in, bi-directional)	Direction of the media flow, where "in" refers to inside the core network so that "out->in" refers to the direction towards the core network.
– Flow Number	An identifier for the individual media flow within a media session
– Flow Status	Indication of enabled or disabled status for a media flow
– Protocol Version	The Version of Source and destination unicast network address protocol (e.g. IPv4 and IPv6).
– IP Addresses	The source and destination network addresses.
– Ports	The source and destination port numbers. Port ranges shall be supported (e.g. two consecutive ports for RTP, RTCP).
– Protocol Number	The protocol ID (e.g. UDP, TCP etc.)
– Bandwidth	The requested maximum bandwidth. The upstream and downstream BW should be provided separately.

9.1.3.3 Authorization Token information element

The authorization token is used for binding purpose in the pull mode:

Authorization token	A unique identifier used for locating the PDF in policy pull mode, which is used for the request of the authorization token by SCFs and the response of the authorization token generated by PDF.

9.1.3.4 Charging correlation information element

The charging related component is described, which provides the resource usage information:

Charging correlation information	Charging correlation information, such as charging ID of SCFs and networks, and resource usage information.

9.1.3.5 Resource Control Action information elements

A variety of indicators are described, which is used to request a specific resource control action per network event/condition:

Resource Reservation Mode (for further study)	Indication of resource reservation mode (e.g. non-reservation, reservation only or reservation + commitment).
Dynamic firewall working mode (Optional)	Service information for dynamic firewall working mode selection (e.g., security level.)
Resource Request Result	Indication of the result for a resource request (initiation, modification, release).
Timestamp	The time when the resources were lost.
Reason	Information of the cause for an event (e.g. Abort event)
Event Notification Information	A set of information sub-elements specifying the notification of a transport layer event.
– Service Information Request (for further study)	This value shall be used when the PDF requests the service information from the SCFs for the bearer event, or indicates that the SCFs requests the PDF to demand service information at each bearer authorization.

– Bearer Loss Indicator	SCFs' subscription for the notification of the bearer loss events or notification of a bearer loss event to SCFs
– Bearer Recovery Indicator	SCFs' subscription for the bearer recovery events or notification of a bearer recovery event
– Bearer Release Indicator	SCFs' subscription for the bearer release events or notification of a bearer release event to SCFs
NAPT Control and NAT Traversal Indication (Conditional)	The events of NAPT control and NAT traversal are not mutual exclusive. They can be used in the same information message.
– Address Translation Command	The PDF may perform the NAPT control, obtain the address binding information, and request the SCFs to modify signalling messages accordingly based on network address hiding policy decision.
– Address Binding Information Request	The SCFs may request the RACF for the network address and port translation information in support of far-end NAT Traversal
– Address Binding Information Response:	The PDF shall obtain the NAPT information, generate the address binding information and send it to the relevant SCFs. The SCFs shall modify the relevant message body of application signalling packet.

9.1.4 Information messages exchanged over Gq'

This section describes the messages (namely requests and responses) exchanged over Gq'.

9.1.4.1 Resource Initiation Request

This message is sent by SCFs to initiate a resource control session to PDF. Depending on the resource reservation mode desired, a single resource initiation request may be used for Authorization only or Reservation only or Commitment only or some combination of the above. It consists of:

- Application Identifier
- Resource Control Session Identifier
- Global IP Address Information (optional, see note 1)
  - Unique IP address
  - Address Realm
- Transport Subscriber Identifier (Optional, see note 1)
- Resource Request Client Information
  - Client Name
  - Request Class
- Reservation Holding Time
- Resource Control Session Information (Optional)
- Dynamic firewall working mode (Optional)
- Media Profile
  - Media Number
  - Type of Service
  - Class of Service (Optional)
  - Media Priority (Optional)
  - Media Flow Description
    - Flow direction
    - Flow Number
    - Flow Status

  - Protocol Version
  - IP Addresses
  - Ports
  - Protocol Number
  - Bandwidth
- Resource Reservation Mode
- Bearer Event Notification Information (Optional)
  - Service Information Indicator
  - Bearer Loss Indicator
  - Bearer Recovery Indicator
  - Bearer Release Indicator
- NAPT Control and NAT Traversal (Conditional)
  - Address Binding Information Request

Note 1: one of them shall be present.

9.1.4.2 Resource Initiation Response

This message is sent by PDF to confirm the resource initiation request from SCFs. It consists of:

- Application Identifier
- Resource Control Session Identifier
- Reservation Holding Time (Optional)
- Resource Control Session Information (Optional)
- Resource Request Result
- Authorization token (Optional)
- Media Profile (Optional)
  - Media Number
  - Type of Service
  - Class of Service (Optional)
  - Media Priority (Optional)
  - Media Flow Description
    - Flow direction
    - Flow Number
    - Flow Status
    - Protocol Version
    - IP Addresses
    - Ports
    - Protocol Number
    - Bandwidth
- NAPT Control and NAT Traversal (Optional)
  - Address Translation Command
  - Address Binding Information Response

9.1.4.3 Resource Modification Request

This message is sent by SCFs to request the resource modification of an established session to PDF. The session state can be retrieved with the Resource Control Session Information provided by SCFs if a stateless PDF is used. It consists of:

- Application Identifier
- Resource Control Session Identifier
- Resource Request Client Information
  - Client Name
  - Request Class
- Reservation Holding Time
- Resource Control Session Information (Optional)
- Dynamic firewall working mode (Optional)
- Media Profile
  - Media Number
  - Type of Service
  - Class of Service (Optional)
  - Media Priority (Optional)
  - Media Flow Description
    - Flow direction
    - Flow Number
    - Flow Status
    - Protocol Version
    - IP Addresses
    - Ports
    - Protocol Number
    - Bandwidth
- Resource Reservation Mode
- Bearer Event Notification Information (Optional)
  - Service Information Indicator
  - Bearer Loss Indicator
  - Bearer Recovery Indicator
  - Bearer Release Indicator
- NAPT Control and NAT Traversal (Conditional)
  - Address Binding Information Request

9.1.4.4 Resource Modification Response

This message is sent by PDF to confirm the resource modification request from SCFs. The information elements are same as Resource Initiation Response.

9.1.4.5 Resource Action Request

This message is sent by PDF to request a specific resource control action (e.g. retrieving the service information) for an established session to SCFs as needed. It consists of:

- Application Identifier
- Resource Control Session Identifier
- Resource Control Session Information (Optional)
- Dynamic firewall working mode (Optional)
- Media Profile
  - Media Number
  - Type of Service
  - Class of Service (Optional)
  - Media Priority (Optional)
  - Media Flow Description
    - Flow direction
    - Flow Number
    - Flow Status
    - Protocol Version
    - IP Addresses
    - Ports
    - Protocol Number
    - Bandwidth
- Bearer Event Notification Information (Optional)
  - Service Information Indicator
  - Bearer Loss Indicator
  - Bearer Recovery Indicator
  - Bearer Release Indicator

9.1.4.6 Resource Action Response

This message is sent by SCFs to confirm the request of the specific action and provide the service information to PDF as needed. It consists of:

- Application Identifier
- Resource Control Session Identifier
- Resource Control Session Information (Optional)
- Dynamic firewall working mode (Optional)
- Media Profile (Optional)
  - Media Number
  - Type of Service
  - Class of Service (Optional)
  - Media Priority (Optional)
  - Media Flow Description
    - Flow direction

  - Flow Number
  - Flow Status
  - Protocol Version
  - IP Addresses
  - Ports
  - Protocol Number
  - Bandwidth
- Bearer Event Notification Information (Optional)
  - Service Information Indicator
  - Bearer Loss Indicator
  - Bearer Recovery Indicator
  - Bearer Release Indicator
- NAPT Control and NAT Traversal (Conditional)
  - Address Binding Information Request

9.1.4.7 Resource Notification

This message is sent by PDF to notify SCFs of the bearer resource events. It consists of:

- Application Identifier
- Resource Control Session Identifier
- Resource Control Session Information (Optional)
- Dynamic firewall working mode (Optional)
- Media Profile
  - Media Number
  - Type of Service
  - Class of Service (Optional)
  - Media Priority (Optional)
  - Media Flow Description
    - Flow direction
    - Flow Number
    - Flow Status
    - Protocol Version
    - IP Addresses
    - Ports
    - Protocol Number
    - Bandwidth
- Bearer Event Notification Information (Optional)
  - Service Information Indicator
  - Bearer Loss Indicator
  - Bearer Recovery Indicator
  - Bearer Release Indicator

Editor's Note: the notification of usage information is for further study.

9.1.4.8 Resource Release Request

This message is sent by SCFs to request the resource release for an established session or individual media flow to PDF. The resource release can be session based, flow-based, and a wildcard is used to indicate the release of all of sessions related to this client. When a request is received, all of relevant resource is released including the bearer event notification settings. It consists of:

- Application Identifier
- Resource Control Session Identifier
- Resource Request Client Information (Optional)
  - Client Name
  - Request Class
- Resource Control Session Information (Optional)
- Dynamic firewall working mode (Optional)
- Media Profile
  - Media Number
  - Type of Service
  - Class of Service (Optional)
  - Media Priority (Optional)
  - Media Flow Description
    - Flow direction
    - Flow Number
    - Flow Status
    - Protocol Version
    - IP Addresses
    - Ports
    - Protocol Number
    - Bandwidth

9.1.4.9 Resource Release Response

This message is sent by PDF to confirm the resource release request from SCFs. It consists of:

- Application Identifier
- Resource Control Session Identifier
- Resource Request Client Information (Optional)
  - Client Name
  - Request Class
- Resource Control Session Information (Optional)
- Resource Request Result

9.1.4.10 Abort Resource Request

This message is sent by PDF to indicate the loss of all resources for established sessions to SCFs. One Abort request may carry the indication of multiple sessions. It consists of:

- Application Identifier

- Resource Control Session Identifier
- Resource Control Session Information (Optional)
- Timestamp
- Reason

9.1.4.10 Abort Resource Response

This message is sent by SCFs to confirm the resource abort request. It consists of:

- Application Identifier
- Resource Control Session Identifier
- Resource Control Session Information (Optional)

9.2 Reference Point Go'

The Go' reference point allows the final admission decisions to be installed ("pushed" or "pulled") to A-BGF/I-BGF from PDF. This reference point should be compatible as defined by 3GPP Release 6 in 3GPP TS 29.207 [7], and should support the NAPT/Firewall Control and NAT traversal at A-BGF/I-BGF as needed.

9.2.1 Functional Requirements

The Go' reference point allows the PDF to push the final admission decisions to the A-BGF/I-BGF and also allows for path-coupled resource reservation mechanisms where the reservation and admission decisions are requested from the A-BGF/I-BGF using the "pull" mode. The PDF may specify:

- Resources to be reserved and/or committed for a media flow,
- QoS handling such as packet marking and policing to use,
- Gate control (opening/closing) for a media flow,
- The insertion of a NAPT function, requesting the necessary address mapping information.
- Resource Usage information request and report for a media flow.
- Dynamic firewall working mode selection (e.g. selection of the working mode of packet-filtering-based firewall) for a media flow,
- Technology independent core network ingress path information for a media flow,

In addition, the PDF can request notification of events and may receive a request from the A-BGF/I-BGF to verify an authorization token that has been obtained via a path-coupled resource signalling mechanism.

Note that the NAPT function may be contained within the same or different component from the function providing bandwidth reservation. The Go' reference point should allow for this flexibility.

9.2.2 Protocol Requirements

This section provides a brief description of the protocol requirements for the Go' reference point.

Request-Response Transactions: The protocol must allow the PDF to request a transaction to be performed by the A-BGF/I-BGF and get a response (that can be correlated with the request) in return.

Notifications: The protocol must allow the notification of asynchronous events (from the A-BGF/I-BGF to the PDF).

Reliable Delivery: The protocol should provide reliable delivery of messages.

Extension Mechanisms: The protocol should including extension mechanisms such as versioning or other means to allow changes while ensuring backwards compatibility.

Capabilities: The PDF must be able to determine capabilities when requesting resources and other transport plane functions from the A-BGF/I-BGF.

Security: All messages between PDF and A-BGF/I-BGF must be authenticated such that requests to the A-BGF/I-BGF from unauthenticated sources will not be performed and such that notifications sent from the A-BGF/I-BGF to PDF can be ensured to come from an authenticated A-BGF/I-BGF source.

9.2.3 Information Exchanged

This section describes the information exchanged across the Go' reference point.

Request to reserve for a media flow: The PDF provides the following information to the A-BGF/I-BGF when requesting resource reservation and QoS handling for a given media flow. If success, the final admission decisions are installed in the A-BGF/I-BGF.

- Media Flow Identification Information:
  - Direction (in->out, out->in, bi-directional), where "in" refers to inside the core network so that "out->in" refers to the direction towards the core network.
  - IP protocol version: IPv4 or IPv6.
  - Media Flow Classifiers: either one or two classifiers depending on whether the media flow is unidirectional or bi-directional. The classifier consists of an IPv4/IPv6 5-tuple (source/destination address and port numbers, protocol Id) or an IPv6 3-tuple (source/destination address, flow label). Wild-cards may be provided for information that is not available. Note that a given media flow may require that two ports are specified for each direction (RTP and RTCP).
- QoS handling parameters: IPv4 DSCP values or IPv6 traffic classes to mark or remark.
- Bandwidth to be Reserved: This value is specified whether the "push" or "pull" mode is used. A value of 0 indicates that no bandwidth should be reserved.
- Bandwidth Authorized: This is an upper limit on the amount of bandwidth that may be reserved and committed. This value is specified whether the "push" or "pull" mode is used. A value of 0 indicates that no bandwidth is authorized. A later path-coupled reservation request that remains within the authorized limits will be accepted as long as resources are available.
- Notifications Required:
  - A persistent notification (one that does not have to be requested) is provided to the PDF in the case where the bearer is lost.
  - Notifications associated with path-coupled mechanisms (e.g. RSVP): reservation committed; reservation modified; reservation released.
  - Resource Usage information when resource reservation for the media flow is released.
- Gate Control Policy: Indication of whether the gate should be automatically and immediately opened (i.e. media enabled or resource committed) when the resources are reserved or whether the SCF will supply a separate "enable" message.
- Firewall Working Mode Selection Policy: Indication of the working mode of the firewall based on the related service information.

Authorisation tokens: In the case of a path-coupled mechanism, an authorization token for the media session may be passed from the A-BGF/I-BGF to the PDF for authentication check. The token may contain policy data that was previously authorized and authenticated by the PDF. Once the token is received by the PDF, the PDF may push additional policy to the A-/BGF/I-BGF beyond that specified in the authorization token.

Charging correlation information: The PDF and A-BGF/I-BGF may exchange charging correlation information, including resource usage information.

Gate control commands: The PDF must be able to enable the gate (open the gate) or disable the gate (close the gate) for a given media flow as the SCF requested. Closing the gate does not release the reserved bandwidth resources.

Request for NAPT binding information: In the case where network address and port translation is required, the PDF must be able to act as an intermediary and respond with the NAPT mapping information obtained from the A-BGF/I-BGF to the SCF. The SCF use the NAPT mapping information to modify the related application signalling message body.

Request to Modify: The PDF must be able to request the A-BGF/I-BGF to modify the resource reservation and flow handling for a media flow.

Request to Release: The PDF must be able to request the A-BGF/I-BGF to release the resource reservation and flow handling for a media flow. It is to release all resources associated with that media flow.

Notifications: The A-BGF/I-BGF must be able to notify the required information to the PDF that do not have to be requested by the PDF.

Responses: The A-BGF/I-BGF must be able to respond to a request or confirm a command from the PDF.

9.3 Reference Point Re

The Re reference point allows QoS admission decisions to be installed ("pushed") to ANF/ENF from A-TRCF for support of absolute QoS in an access network.

9.3.1 Functional Requirements

Editor's note: This section needs much further work. The current description is largely Layer 3.

The Re reference point provides the ability for A-TRCF to make requests to ANF/ENF for support of absolute QoS in the access network:

- Control the packet filtering of ANF/ENF at per-flow level;
- Control the packet marking of ANF/ENF at per-flow level;
- Control the traffic policing and shaping of ANF/ENF at per-flow level
- Control the shaping of L2 egress flows toward the UNI

9.3.2 Protocol Requirements

This section provides a brief description of the protocol requirements for the Re reference point.

Request-Response Transactions: The protocol must allow the A-TRCF to request a transaction to be performed by the ANF/ENF and get a response (that can be correlated with the request) in return.

Notifications: The protocol must allow the notification of asynchronous events (from the ANF/ENF to the A-TRCF).

Reliable Delivery: The protocol should provide reliable delivery of messages.

Extension Mechanisms: The protocol should including extension mechanisms such as versioning or other means to allow changes while ensuring backwards compatibility.

Capabilities: The A-TRCF must be able to determine capabilities when requesting resources and other transport plane functions from the ANF/ENF.

Security: All messages between A-TRCF and ANF/ENF must be authenticated such that requests to the ANF/ENF from unauthenticated sources will not be performed and such that notifications sent from the ANF/ENF to A-TRCF can be ensured to come from an authenticated A-TRCF source.

9.3.3 Information Exchanged

This section describes the information exchanged across the Re reference point.

Request to reserve for a media flow: The A-TRCF provides the following information to the ANF/ENF when requesting resource reservation and QoS handling for a given media flow:

- Media Flow Identification Information:
  - Direction (in->out, out->in, bi-directional), where "in" refers to inside the core network so that "out->in" refers to the direction towards the core network.
  - IP protocol version: IPv4 or IPv6.
  - Media Flow Classifiers: either one or two classifiers depending on whether the media flow is unidirectional or bi-directional. The classifier consists of an IPv4/IPv6 5-tuple (source/destination address and port numbers, protocol Id) or an IPv6 3-tuple (source/destination address, flow label). Wild-cards may be provided for information that is not available. Note that a given media flow may require that two ports are specified for each direction (RTP and RTCP).
- QoS handling parameters to mark or remark, which is transport technology specific.
- Bandwidth to be Reserved. A value of 0 indicates that no bandwidth should be reserved.

Request to Modify: The A-TRCF must be able to request the ANF/ENF to modify resource reservation and QoS handling for a given media flow.

Request to Release: The A-TRCF must be able to request the ANF/ENF to release resource reservation and QoS handling for a given media flow.

Responses: The ANF/ENF must be able to respond to a request or confirm a command from the A-TRCF.

9.4 Reference Point Rc

The Rc reference point allows A-TRCF/C-TRCF to collect the network topology and resource status information of an access or a core network. It is relevant to a transport functional entity at the network boundary or inside the network.

9.4.1 Functional requirements

The Rc reference point provides the ability for TRCF to make requests to all transport elements within its purview:

- Collect the network topology;
- Collect the resource status information;

In addition, the TRCF can request notification of events (e.g. link or port failure) from a transport element to update the resource status information.

9.4.2 Protocol requirements

This section provides a brief description of the protocol requirements for the Rc reference point.

Request-Response Transactions: The protocol must allow the TRCF to request a transaction to be performed by a transport element and get a response (that can be correlated with the request) in return.

Notifications: The protocol must allow the notification of asynchronous events (from a transport element to the TRCF).

Reliable Delivery: The protocol should provide reliable delivery of messages.

Extension Mechanisms: The protocol should including extension mechanisms such as versioning or other means to allow changes while ensuring backwards compatibility.

Capabilities: The TRCF must be able to determine capabilities when requesting resources and other transport plane functions from a transport element.

Security: All messages between TRCF and transport elements must be authenticated such that requests to the transport elements from unauthenticated sources will not be performed and such that notifications sent from the transport elements to TRCF can be ensured to come from an authenticated source.

9.4.3 Information exchanged

The resource status information should include reserved resources for applications and amount of actual traffic using the resources.

The resource status information is specific to the L2/L3 transport technologies of a network.

This information may be specific to each traffic class in the Transport Functions if different traffic classes are supported.

The resource status information may be specific to the resource-related admission control scheme being used by TRCF whether it is accounting, out-of-band measurements, in-band measurements, or reservation-based. Note that the TRCF can employ more than one resource-related admission control methods simultaneously and use the relevant information based on the applicable method.

9.5 Reference Point Ub

The Ub interface allows A-TRCF to interact with the NACF for checking on CPE configuration information and the binding information of the logical/physical port address to an assigned IP address.

9.6 Reference Point Rq'

The Rq' reference point allows PDF to interact with A-TRCF and C-TRCF for checking on the requested QoS resource availability in the involved access network and core network along a media flow path.

9.6.1 Functional requirements

The Rq' reference point provides the ability for PDF to make requests to one of the TRCF entities in an involved network for a given media flow if there is the required QoS resource available in the network.

9.6.2 Protocol requirements

This section provides a brief description of the protocol requirements for the Rq' reference point.

9.6.3 Information exchanged

This section describes the information exchanged across the Rq' reference point.

Request to Check Resource Availability for a Media Flow: The PDF provides the following information to the TRCF when requesting resource availability check for a media flow:

- Media Flow Identification Information:

  - Direction (in->out, out->in, bi-directional), where "in" refers to inside the core network so that "out->in" refers to the direction towards the core network.
  - IP protocol version: IPv4 or IPv6.
  - Media Flow Classifiers: either one or two classifiers depending on whether the media flow is unidirectional or bi-directional. The classifier consists of an IPv4/IPv6 5-tuple (source/destination address and port numbers, protocol Id) or an IPv6 3-tuple (source/destination address, flow label). Wild-cards may be provided for information that is not available. Note that a given media flow may require that two ports are specified for each direction (RTP and RTCP).
- Network Priority Information: Network information for priority handling (e.g. TDR/ETS), if available.
- Network QoS parameters: network QoS classes (e.g. as defined in Y.1541).
- Bandwidth to be Reserved: This is an upper limit on the amount of bandwidth that may be committed.
- Path to be selected: Ingress path information at the A-BGF/I-BGF for a media flow (e.g. VPN ID (VR/VRF)).
- Notifications Required:
  - A persistent notification (one that does not have to be requested) is provided to the PDF in the case where the bearer is lost.

Respond to Resource Availability Check: The TRCF must be able to respond the resource availability checking result for a given media flow to the PDF if requested. The checking result includes the following information:

- Media Flow Identification Information: same as in the request.
- Network Priority Information: Acceptable network priority information that may be lower than the requested.
- Network QoS parameters: Acceptable network QoS parameters that may be lower than the requested.
- Bandwidth to be Reserved: Acceptable bandwidth to be reserved that may be lower than the requested.
- Path to be selected: Acceptable ingress path information for a media flow that may be different from the requested.
- Resource availability checking result: a positive response (i.e. resources are available) or a negative response (i.e. resources are not available).

Resource Release Indication: The PDF must be able to provide an indication to the TRCF when resource reservation for a media flow is released for any reason. That results in the update of the network resource status database maintained by the TRCF.

Notifications: The TRCF must be able to notify the required information to the PDF that do not have to be requested by the PDF.

9.7 Reference Point Rp

An operator’s core network may have multiple sub-domains or sub-layers. For a large scale operator’s core network, it is required and necessary to deploy multiple C-TRCF instances to control the different sub-domains in the operator’s network. Some sub-domains only provide inter-city or inter-province transport functions without service support nodes. It means that not every sub-domain contains service support nodes where service subsystems are attached. In NGN, the signalling path between SCFs for a session isn’t always

along with the data path. For a session, commonly only the SCFs in the source and destination domains were involved into the session control signalling, whereas other domains along the data path were not. It's difficult and inefficient for the SCF in the source and destination domains to position and contact all of C-TRCF entities along the media flow path within the whole operator's network to check the resource availability, since SCF and PDF have no knowledge of the details of the media flow path and the transport-dependent network resource status information within the operator's network. The communication between C-TRCF entities enables the SCF to only contact a single C-TRCF entity through the PDF.

It's also allowed to deploy multiple C-TRCF instances to control the different areas in a large scale sub-domain of an operator's network. The checking of resource availability in the upstream sub-network and the downstream sub-network are closely relevant since the path of a media flow in the transport plane is hop-by-hop or segment-by-segment.

9.7.1 Functional requirements

The Rp reference point allows the C-TRCF instances communicate with each other to check the edge-to-edge availability of the requested QoS resource for a media flow within an operator's core network. Rp is applicable to C-TRCF instances under the control of the same PDF.

9.7.2 Protocol requirements

This section provides a brief description of the protocol requirements for the Rp reference point.

Request-Response Transactions: The protocol must allow a C-TRCF to request a transaction to be performed by another C-TRCF and get a response (that can be correlated with the request) in return.

Notifications: The protocol must allow the notification of asynchronous events (from a C-TRCF to another C-TRCF).

Reliable Delivery: The protocol should provide reliable delivery of messages.

Extension Mechanisms: The protocol should including extension mechanisms such as versioning or other means to allow changes while ensuring backwards compatibility.

Capabilities: A C-TRCF must be able to determine capabilities when requesting resources and other transport plane functions from another C-TRCF.

Security: All messages between C-TRCF entities must be authenticated such that requests to a C-TRCF from unauthenticated sources will not be performed and such that notifications sent from a C-TRCF to another C-TRCF can be ensured to come from an authenticated source.

9.7.3 Information exchanged

This section describes the information exchanged across the Rp reference point.

Resource reservation request: A C-TRCF may request another C-TRCF in the downstream sub-network to check the availability of the requested QoS resource, with the following information:

- Unique Identifier for the request;
- Media flow identifier (i.e. IPv4 5-tuple or IPv6 3/5-tuple);
- Requested QoS parameters (e.g. bandwidth or QoS class);
- Path information in the local sub-network (e.g. identifier of ingress and egress).

Resource modification request: A C-TRCF may request another C-TRCF in the downstream sub-network to check the availability of the modified requested QoS resource, with the following information:

- Unique Identifier for the request;

- Media flow identifier (i.e. IPv4 5-tuple or IPv6 3/5-tuple);
- Requested QoS parameters (e.g. bandwidth and QoS class);
- Path information in the local sub-network (e.g. identifier of ingress and egress).

Resource request acceptance: A C-TRCF may respond another C-TRCF in the upstream sub-network that the requested QoS resource is available, with the following information:

- Unique Identifier for the request;
- Media flow identifier (i.e. IPv4 5-tuple or IPv6 3/5-tuple);
- Accepted QoS parameters (e.g. bandwidth and QoS class);
- Path information in the local sub-network (e.g. identifier of ingress and egress).

Resource request rejection: A C-TRCF may respond another C-TRCF in the upstream sub-network that the requested QoS resource is unavailable, with the following information:

- Unique Identifier for the request;
- Rejection cause;

Resource unavailable indication: A C-TRCF may notify another C-TRCF in the upstream sub-network that the requested QoS resource is no longer available, with the following information:

- Unique Identifier for the request;
- Unavailable cause;

Resource release request: A C-TRCF may request another C-TRCF in the downstream sub-network to release the requested QoS resource, with the following information:

- Unique Identifier for the request;
- Release cause;

Resource release confirmation: A C-TRCF may respond another C-TRCF in the upstream sub-network that the requested QoS resource is released or not.

- Unique Identifier for the request;
- Execution result (i.e. Ok or Fail);

9.8 Reference point Iq

The Iq interface allows inter-operator-domain RACF communication between PDFs for end-to-end QoS control.

To be developed.

9.9 Reference point Rd

The Rd interface allows intra-operator-domain RACF communication between PDFs for end-to-end QoS control.

To be developed.

9.10 Summary

Reference Point	Inter-Domain	Intra-Domain
Gq’	X	
Go’		X
Iq	X	
Rc		X
Rd		X
Re		X
Rp		X
Rq’		?
Ub		X

In this specification, each reference point corresponds to an interface.

Editor’s note: The text still needs to be checked to make sure that the description of Rq’ is consistently intra-provider.

10 Procedures

This section defines basic procedures triggered by a single event (e.g. a session initiation request). These basic procedures could be further composed into any possible composite procedures triggered by a series of events.

10.1 Procedures for QoS control

Note: In the following figures, the interaction between A-TRCF and ENF/ANF in access network is omitted. It is similar with the interaction between PDF and BGF, but only the “push” model is used.

10.1.1 SCF-requested QoS control procedures

Scenario 1 described in Section 6.1 use the SCF-requested QoS resource reservation mechanism, i.e. the SCF (Service Control Functions) send the RACF a ‘resource request’ to invoke the QoS resource authorization and reservation for a given service flow. The RACF will push the admission control decisions into the network border nodes if the resource request is authorized and admitted.

10.1.1.1 Basic procedures

Editor’s note: Whether installation and allocation have the same meaning and can be replaced with commitment needs further checking.

10.1.1.1.1 QoS resource reservation procedure

The SCF-requested QoS resource reservation procedure is initiated by a ‘resource request’ from the SCF for a given service.

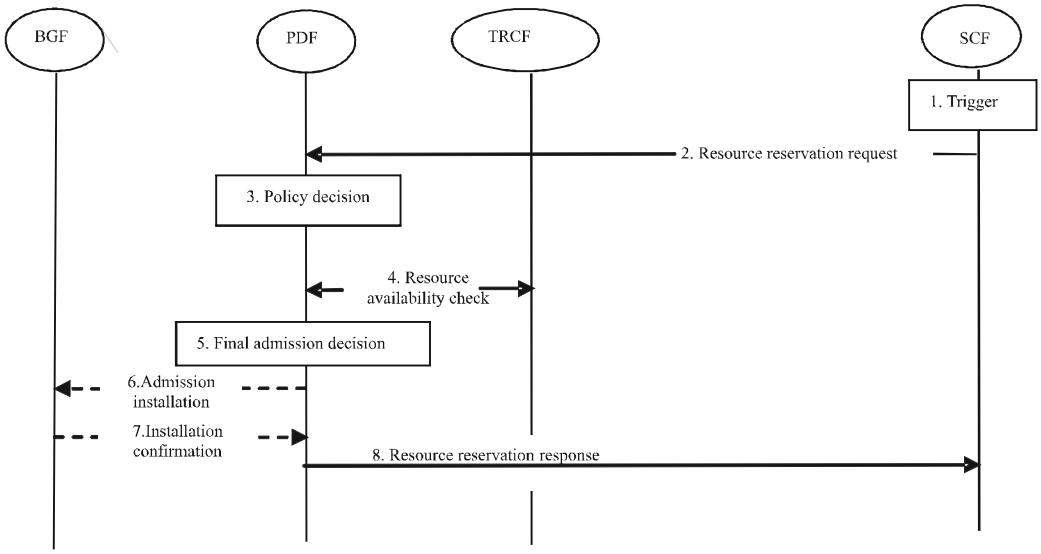


Figure 6 – SCF-requested QoS resource reservation procedure

(1) A 'resource reservation request' is usually triggered by a service establishment event or an internal action in the SCF (Service Control Functions). An example event is that a service signalling message is received at or generated by the SCF.

(2) The SCF determines or extracts the QoS requirement parameters (including bandwidth, delay, jitter, loss, etc.) for the media flow of a given service. It then sends a 'resource reservation request' with the flow description and its QoS parameters to the PDF across the Gq interface for QoS resource authorization and reservation.

(3) On receipt of the 'resource reservation request', the PDF shall authorize the required QoS resources for the media flow. The PDF checks if the flow description and the required QoS resources are consistent with the operator policy rules held in the PDF.

(4) The PDF positions and determines which access networks and core networks are involved for the media flow. If there are TRCF instances in an involved network, the PDF sends a 'Request to check resource availability' to one of the TRCF instances registered in the PDF for checking if the required QoS resource is available in the involved network. If there are multiple TRCF instances in the involved network, they communicate with each other to determine if the required QoS resource is available from edge to edge in the involved network. Then the TRCF instance which received the 'Request to check resource availability' shall send a 'Respond to resource availability check' back to the PDF.

(5) The PDF makes the final admission decisions to the 'resource reservation request' based on the checking results of Step 3 and 4. If the 'resource reservation request' from the SCF is not admitted, the PDF sends a 'resource reservation response' with the rejection reason back to the SCF.

(6) The PDF may send an 'admission installation' command to install the final admission decisions in the BGF.

(7) The BGF installs the final admission decisions sent from the PDF and sends an 'installation confirm' back to the PDF. Note that the installed admission decisions may be enforced automatically and immediately or may wait for an activation request for gates opening and resources commitment.

(8) The PDF sends the 'resource reservation response' back to SCF.

There are two cases. In case 1, which is the one-phase control scheme, when the final admission decisions are installed in the BGF, the gates are open and the reserved resources are committed automatically and

immediately so that there doesn't need any intervention from SCF to enforce gate control; and in case 2, which is the two-phase control scheme, after the final admission decisions are installed in the BGF and the 'resource reservation response' is sent back to SCF, the PDF opens the gates and activates the admission decisions installed in the BGF only after receiving the admission activation request from SCF. There are two alternative procedures for case 2, either one can be applied.

10.1.1.1.2 QoS resource modification procedure

The SCF-requested QoS resource modification procedure is invoked by a 'resource modification request' from the SCF for a given service. A 'resource modification request' is usually triggered by a media renegotiation event or an internal action in the SCF (Service Control Functions). An example event is that a service signalling message is received at or generated by the SCF.

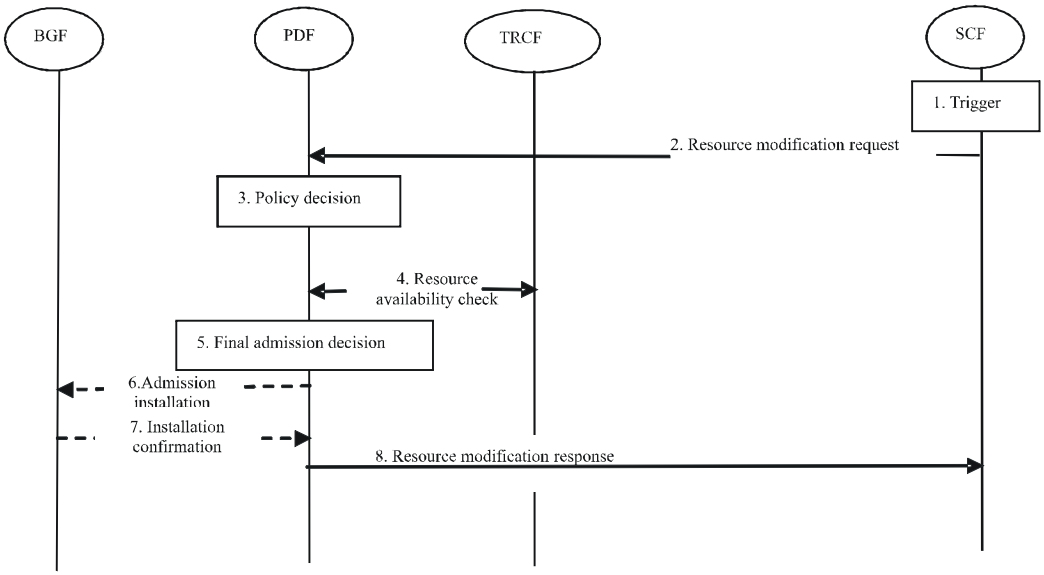


Figure 7 – SCF-requested QoS resource modification procedure

There are two cases. In case 1, which is the one-phase control scheme, when after the final admission decisions are installed in the BGF, the gates are open and the reserved resources are committed automatically and immediately so that there doesn't need any intervention from SCF to enforce gate control; and in case 2, which is the two-phase control scheme, after the final admission decisions are installed in the BGF and the 'resource reservation response' is sent back to SCF, the PDF opens the gates and activates the admission decisions installed in the BGF only after receiving the admission activation request from SCF. There are two alternative procedures for case 2, either one can be applied.

10.1.1.1.3 Admission decision activation procedure

In the two-phase control scheme, the PDF opens the gates and activates the admission decisions installed in the BGF only upon receiving the admission activation request from SCF. The admission decision activation procedure is only needed when the SCF ordered the PDF to wait for an "admission decision activation request'. The admission decision activation procedure is invoked by an 'activation request' from the SCF for a given service. In the case that the PDF has not installed the admission decisions in the BGF, the PDF sends the admission decisions to the BGF through this procedure.

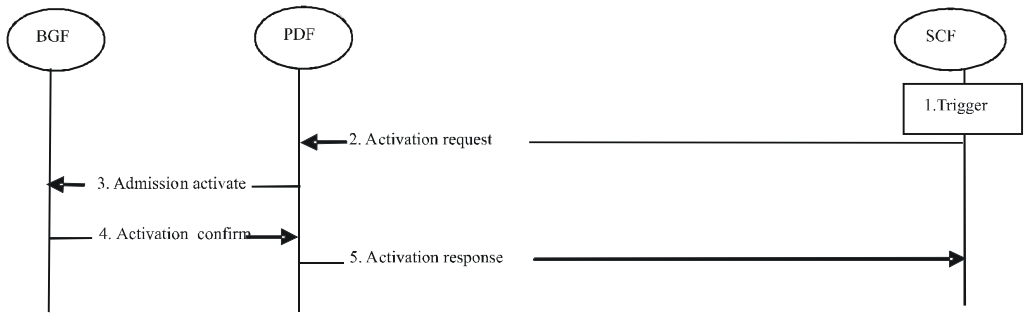


Figure 8 – Admission Decision Activation procedure

10.1.1.1.4 Admission decision de-activation procedure

The admission decision de-activation procedure is invoked by an 'de-activate request' from the SCF for a given service. It makes the BGF not to enforce an admission decisions previously installed for the media flow of the service any longer, but the admission decisions won't be deleted or removed from the BGF. The de-activation procedure is only needed when the media flow of a given service needs to be disabled.

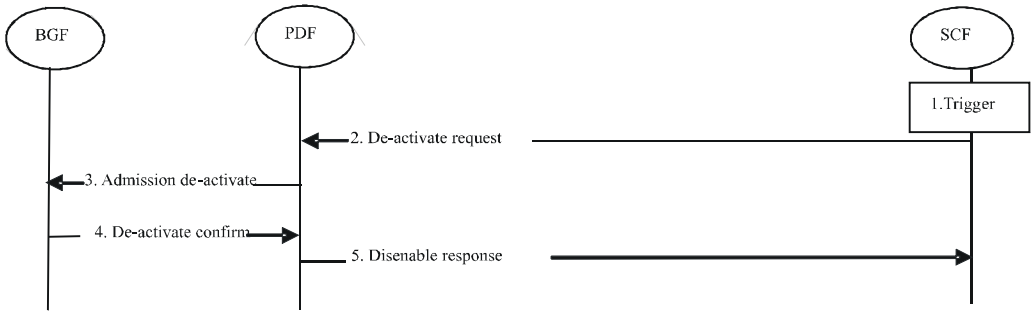


Figure 9 – Admission decision de-activation procedure

10.1.1.1.5 QoS resource release procedure

The SCF-requested QoS resource release procedure is invoked by a 'resource release request' from the SCF for a given service. A 'resource release request' is triggered usually by a service termination event, a media renegotiation event, or an internal action in the SCF (Service Control Functions). An example event is that a service signalling message is received at or generated by the SCF.

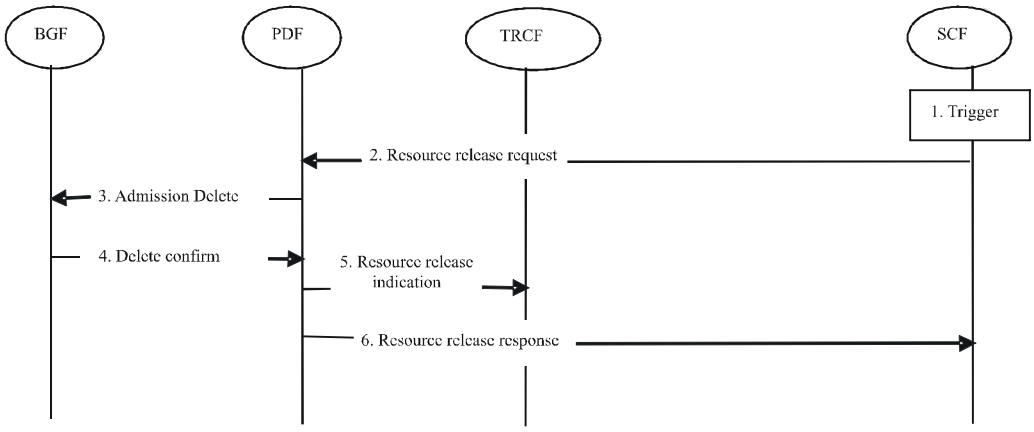


Figure 10 – SCF-requested QoS resource release procedure

10.1.1.2 Failure handling

Editor's note: The complexity of providing network failure indications to SCF needs further study.

10.1.1.2.1 BGF-indicated resource release procedure

During the running of a media flow, if the BGF cannot provide the reserved QoS resource any longer for the media flow due to its interface failure, the BGF shall send a 'resource unavailable indication' to the PDF on its initiative. If the reserved QoS resource is relevant with an SCF session, the PDF shall forward the 'resource unavailable indication' to the SCF.

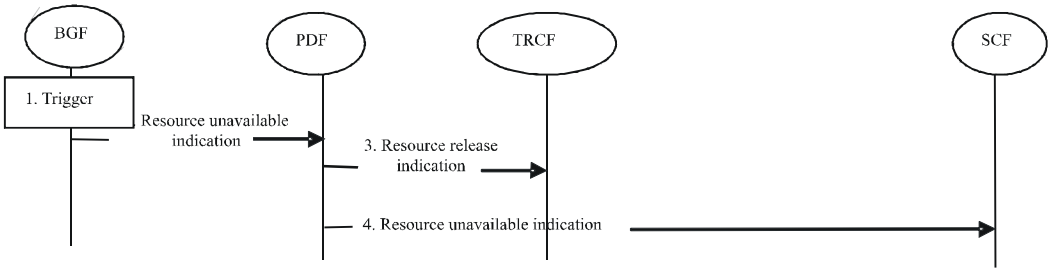


Figure 11 – BGF-indicated resource release procedure

10.1.1.2.2 TRCF-indicated resource release procedure

During the running of a media flow, if the TRCF inspects that the network cannot provide the reserved QoS resource any longer for the media flow due to the network failure, the TRCF shall send a 'resource unavailable indication' to the PDF on its initiative. If the reserved QoS resource is relevant with an SCF session, the PDF shall forward the 'resource unavailable indication' to the SCF.

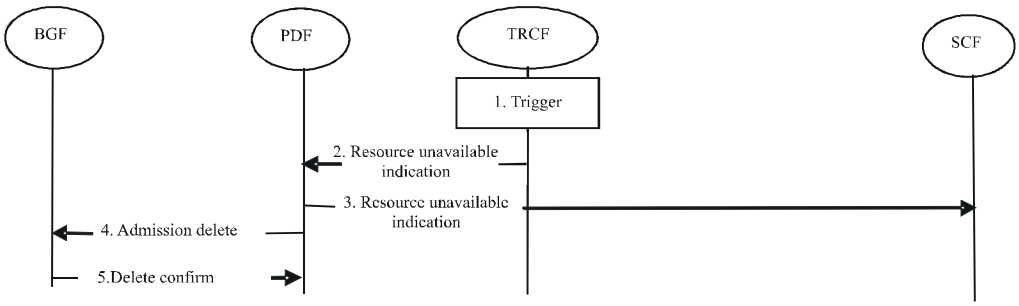


Figure 12 – TRCF-indicated resource release procedure

10.1.2 CPE-requested QoS control procedures

Scenario 2 described in Section 6.1 uses the CPE-requested QoS resource reservation mechanism, i.e. the CPE sends a 'QoS request' over a dedicated path-coupled QoS signalling to invoke the QoS resource reservation for a given flow. Based on the 'QoS request' from the CPE, the network border node is responsible for sending the RACF a 'resource request' to pull the admission control decisions from the RACF.

The following procedures are for support of CPE-requested QoS resource reservation mechanism.

10.1.2.1 Basic procedures

10.1.2.1.1 CPE-requested QoS resource reservation procedure

The CPE-requested QoS resource reservation procedure is invoked by a dedicated path-coupled QoS signalling message from the CPE for a given flow.

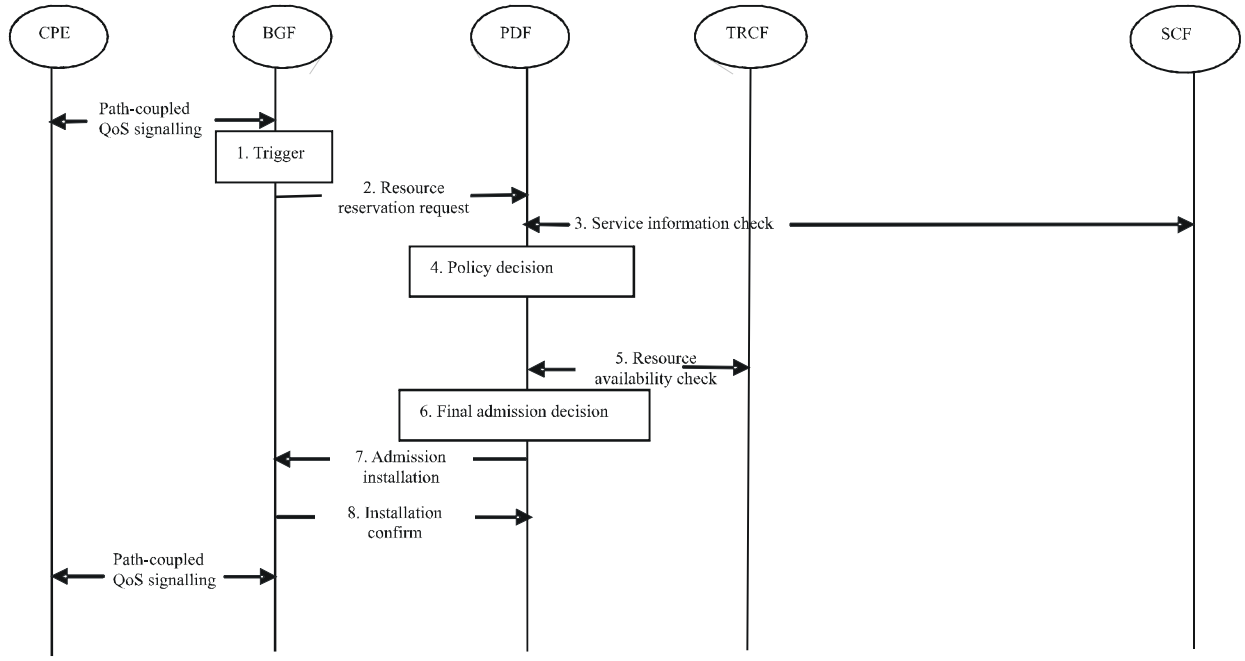


Figure 13 – CPE-requested QoS resource reservation procedure

(1) A 'resource reservation request' is usually triggered by a request indicated through the QoS signalling from the CPE to reserve the required QoS resource for a given flow. Other nodes in the access or core networks shall forward the QoS signalling messages transparently.

(2) Base on the 'QoS request' from the CPE, the BGF sends a 'resource reservation request' with the flow description and its QoS parameters to the PDF across the Go interface to pull the admission control decisions from the PDF. The BGF shall be able to filter the duplicated or evil QoS request messages, especially if the QoS signalling functions in a periodically refresh way.

(3) On receipt of the 'resource reservation request', the PDF shall authorize the required QoS resources for the flow. Firstly, if the flow is relevant to an SCF (i.e. the SCF interacted with the PDF for QoS pre-authorization during the service establishment signalling), the PDF shall send a request to the SCF for the service information of the flow.

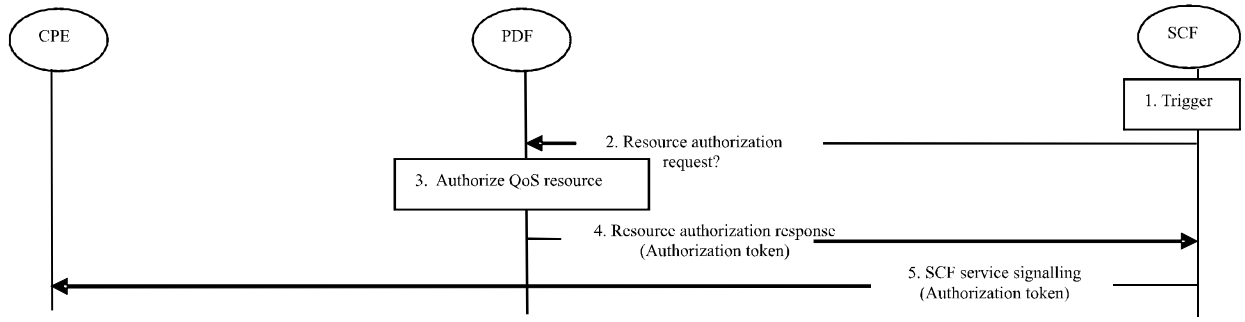


Figure 14 – SCF-requested QoS pre-authorization procedure

The SCF-requested QoS pre-authorization procedure is usually triggered by a service establishment signalling message. The PDF may generate an authorization token for a given service and send it to the SCF. The SCF may then indicate the authorization token in the service signalling message to the CPE.

(4) The PDF checks if the flow description, the required QoS resources and the service information are consistent with the operator policy rules held in the PDF.

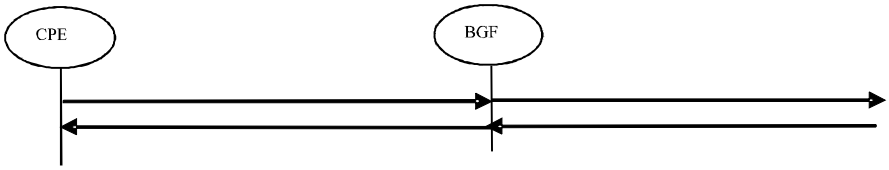
(5) The PDF positions and determines which access networks and core networks are involved for the media flow. If there are TRCF instances in an involved network, the PDF sends a 'Request to check resource availability' to one of the TRCF instances registered in the PDF for checking if the required QoS resource is available in the involved network. If there are multiple TRCF instances in the involved network, they communicate with each other to determine if the required QoS resource is available in the involved network. Then the TRCF instance which received the 'Request to check resource availability' shall send a 'Respond to check resource availability' back to the PDF.

(6) The PDF makes the final admission decision to the 'resource reservation request' based on the checking results of Step 4 and 5.

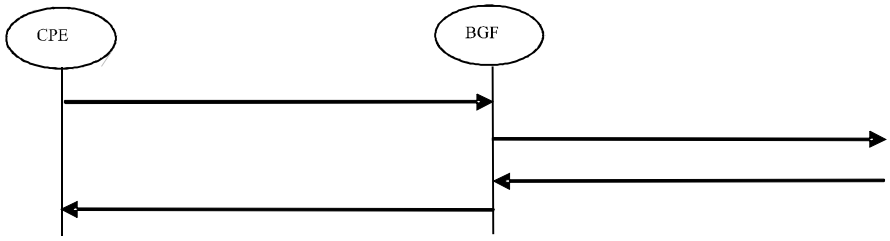
(7) If the 'resource reservation request' from the BGF is admitted, the PDF shall send an 'admission installation' command to install the final admission decisions in the BGF. If not, the PDF sends an 'admission rejection' back to the BGF.

(8) The BGF installs the final admission decisions from the PDF. It then sends an 'installation confirm' back to the PDF. Note that the installed admission decisions may be enforced automatically and immediately or may wait for an activation request for gates opening and resources commitment. The BGF may process the QoS signalling messages in a termination, snooping or proxy way. Refer to Figure 15 a), b) and c) respectively. If in a proxy way, the BGF may modify, aggregate and de-aggregate the QoS signalling messages.

a) The BGF processes the path-coupled QoS signalling in a termination way



b) The BGF processes the path-coupled QoS signalling in a snooping way



c) The BGF processes the path-coupled QoS signalling in a proxy way

Figure 15 – Three possible QoS signalling processing way at the BGF (not exhaustive)

10.1.2.1.2 CPE-requested QoS resource modification procedure

The CPE-requested QoS resource modification procedure is invoked by a 'resource modification request' from the BGF for a given flow. A 'resource modification request' is usually triggered by a request indicated through the QoS signalling from the CPE to modify the reserved resource for the flow.

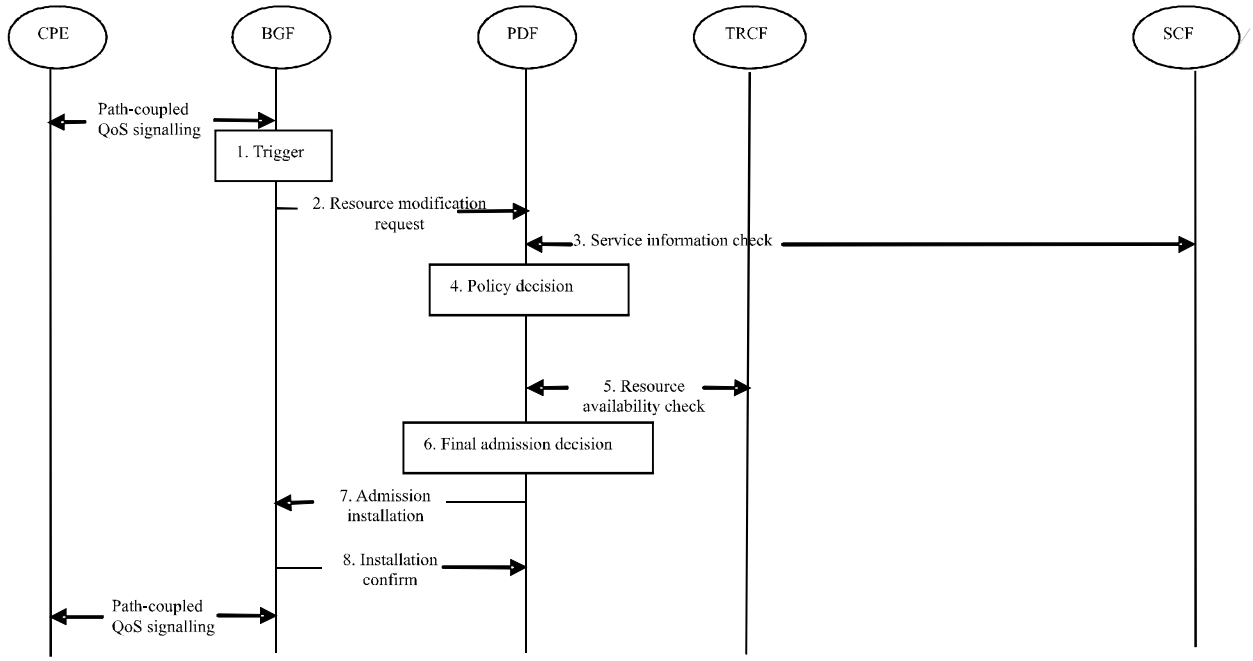


Figure 16 – CPE-requested QoS resource modification procedure

10.1.2.1.3 Admission Decision Activation procedure

In the two-phase or three-phase control scheme, the PDF opens the gates and activates the admission decisions installed in the BGF only upon receiving the admission activation request from SCF. The admission decision activation procedure is only needed when the SCF ordered the PDF to wait for an "admission decision activation request'. The admission decision activation procedure is invoked by an 'activation request' from the SCF for a given service.

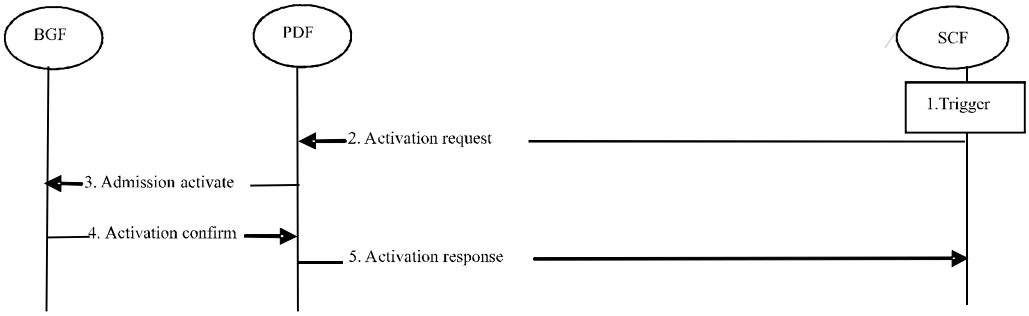


Figure 17 – Admission Decision Activation procedure

10.1.2.1.4 Admission decision de-activation procedure

The admission decision de-activation procedure is invoked by an 'de-activate request' from the SCF for a given service. It makes the BGF not to enforce an admission decision previously installed for the media flow of the service any longer, but the admission decision won't be deleted or removed from the BGF. The de-activation procedure is only needed when the media flow of a given service needs to be disabled.

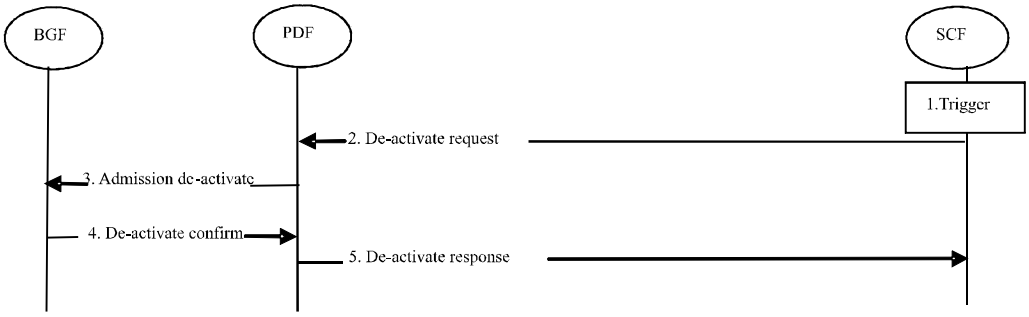


Figure 18 – Admission decision de-activation procedure

10.1.2.1.5 CPE-requested QoS resource release procedure

The CPE-requested QoS resource release procedure is invoked by a 'resource release indication' from the BGF for a given flow. A 'resource release indication' is usually triggered by a request indicated through the QoS signalling from the CPE to release the reserved resource for the flow.

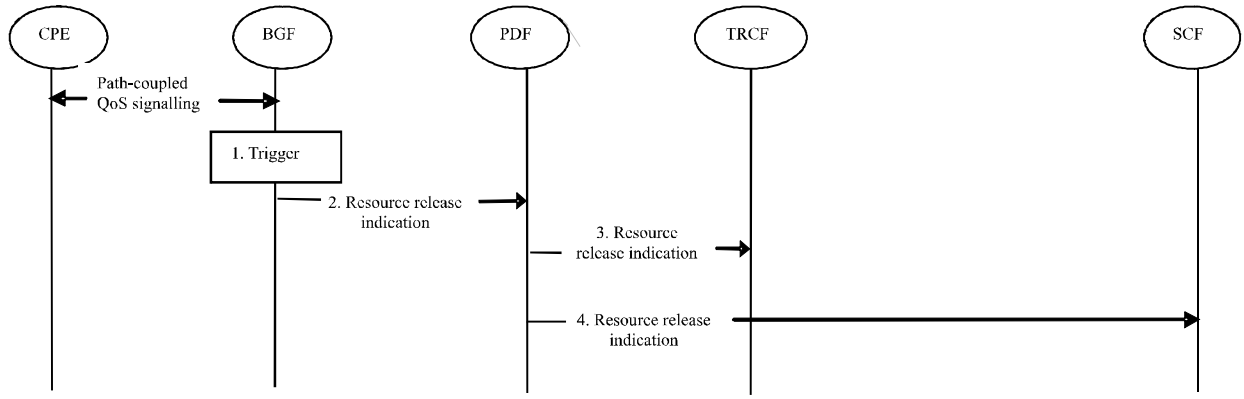


Figure 19 – CPE-requested QoS resource release procedure

10.1.2.1.6 SCF-requested QoS resource release procedure

The SCF-requested QoS resource release procedure is invoked by a 'resource release request' from the SCF for a given service. A 'resource release request' is triggered usually by a service termination event, a media renegotiation event, or an internal action in the SCF (Service Control Functions). An example event is that a service signalling message is received at or generated by the SCF.

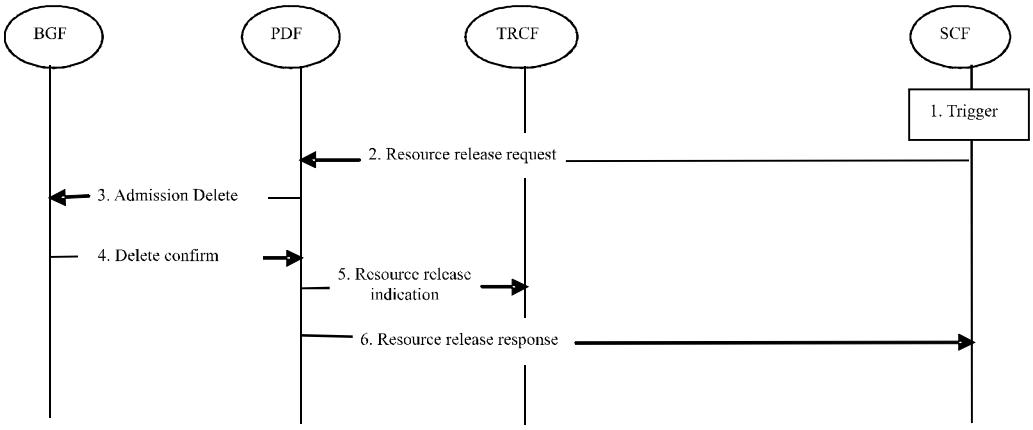


Figure 20 – SCF-requested QoS resource release procedure

10.1.2.2 Failure handling

Editor's note: The complexity of providing network failure indications to SCF needs further study.

10.1.2.2.1 BGF-indicated resource release procedure

During the running of a media flow, if the BGF cannot provide the reserved QoS resource any longer for the media flow due to its interface failure, the BGF shall send a 'resource unavailable indication' to the PDF on its initiative. If the reserved QoS resource is relevant with an SCF session, the PDF shall forward the 'resource unavailable indication' to the SCF.

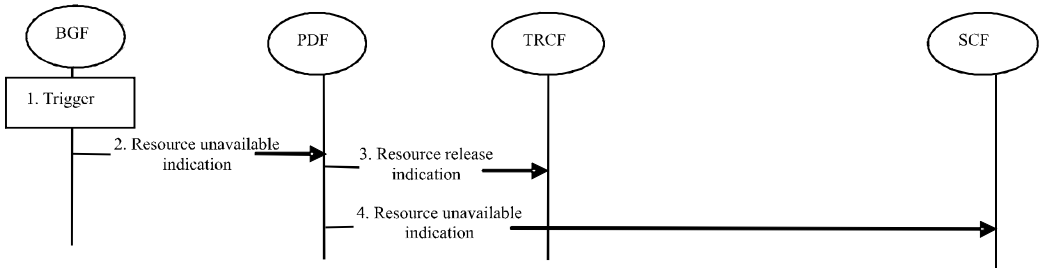


Figure 21 – BGF-indicated resource release procedure

10.1.2.2.12 TRCF-indicated resource release procedure

During the running of a media flow, if the TRCF inspects that the network cannot provide the reserved QoS resource any longer for the media flow due to the network failure, the TRGF shall send a 'resource unavailable indication' to the PDF on its initiative. If the reserved QoS resource is relevant with an SCF session, the PDF shall forward the 'resource unavailable indication' to the SCF.

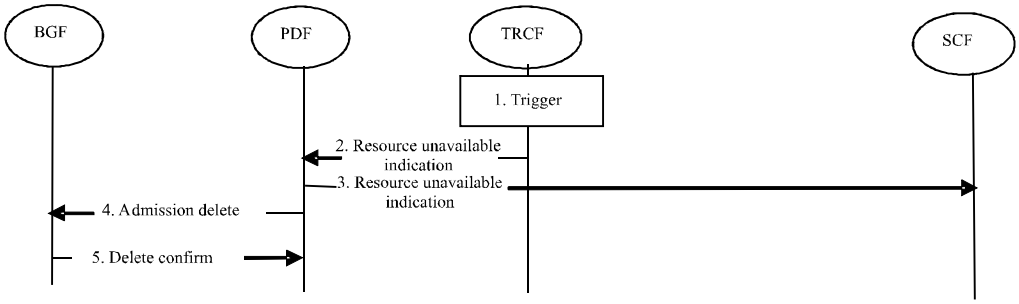


Figure 22 – TRCF-indicated resource release procedure

10.2 Procedures for NAPT Control and NAT Traversal

10.2.1 NAPT Control Procedures

This subclause describes the procedures of controlling an IP address and/or port translation in the media path at the border of the access and core network and of core networks. The SCFs (e.g. SCPF), PDF, TRCFs and BGFs are involved in performing the IP address and/or port translation.

The NAPT control procedure shall be invoked by RACF (e.g. PDF) based on the network security policies (e.g. Network Address Hiding rules). The SCFs shall be able to determine the NAPT control request upon the end-to-end call flow status when application signalling messages to request and respond the session establishment (e.g. SIP INVITE and 183 Session Progress) are received and the indication of NAPT Control provided by PDF. The PDF performs NAPT policy control, obtains the address binding information and

performs the gate control to open/close the "gate". The A-TRCF and C-TRCF may be involved in locating the A-BGF and I-BGF per PDF request; the A-TRCF may be involved in performing the NAPT control function for ANF and ENF per PDF request and NAPT policy.

10.2.1.1 Upon receipt of a session initiation request

1) The SCFs shall extract the source and destination network addresses and port numbers from the signalling message body received from the calling party endpoint and send to RACF (i.e. PDF), and shall request the address binding information if a far end NAT traversal is needed.

2) Upon the receipt of source/destination network address and port and related information from SCFs, the PDF shall check NAPT policy to decide the NAPT control procedure, e.g. whether Network Address Hiding is required or not (e.g. between access and core networks).

3) If the NAPT is required at the border of access and core networks, the PDF shall locate the BGF (i.e. A-BGF) based on the network address from SCFs and shall obtain local network address/port and public network address/port of selected BGF. If the destination endpoint is in the other operator's domain, the PDF shall obtain the public network address and port number from the public network address pool of operator network.

4) The PDF shall generate the address binding information of selected BGF for the requested media flows and may store the address binding information if the PDF is a stateful functional entity. The PDF shall return the network address binding information to SCF.

5) Upon receipt of the RACF response, the SCF shall modify the addresses and/or ports contained in the application signalling message body based on the public address information and NAPT policy decision provided by RACF, and may store the address binding information if the SCF uses a stateful proxy.

10.2.1.2 Upon the receipt of a session initiation response

1) The SCFs shall extract the source and destination network address and port number in the signalling message body received from the called party and send to RACF (i.e. PDF) and send to PDF.

2) When the PDF receives network address and port information from SCFs, the PDF shall check the NAPT policy to decide the NAPT control procedure, e.g. whether Network Address Hiding is required or not (e.g. between core networks).

3) If the NAPT is required at the border of core networks, the PDF shall locate the BGF (i.e. I-BGF) based on the network address information received from SCFs and obtain a local network address/port and a public network address/port of selected BGF.

4) The PDF shall generate the network address binding information of selected BGF for the requested media flows and may store the address binding information if the PDF is a stateful functional entity. The PDF shall return the network address binding information to SCF. In the originating network, the PDF shall return the public network address binding information of selected A-BGF to SCFs. In the terminating network, the PDF shall return the network address binding information of selected I-BGF to SCF.

5) Upon receipt of NAPT information from PDF, the SCFs shall modify the addresses and/or ports contained in the application signalling message body based on the address information and NAPT policy decision provided by RACF, and may store the address binding information if the SCF uses a stateful proxy.

10.2.1.3 Upon receipt of media connection change request for an established session

The SCFs shall decide the possible change of media connection based on the recorded network address binding information if SCF uses a stateful proxy, and/or request the PDF to make a decision and perform the appropriate NAPT control procedure. The possible scenarios include:

1) New network address(es) or/and port number(s) have been added: additional binding(s) shall be provided by SCFs/RACF as detailed for the aforementioned procedures;
2) Existing network address(es) or/and port number(s) have been eliminated: the relevant binding(s) shall be released by SCFs/RACF;
3) Network address(es) and port number(s) have been re-committed to the users: the binding(s) shall reflect the re-allocation;
4) No change has been made to the network address(es) and port number(s): no operation shall be conducted to the existing binding(s).

10.2.1.4 Upon receipt of a session release request:

1) The SCFs shall request the RACF to release the bindings established for the session.

10.2.2 NAT Traversal Procedure

This subclause describes the procedure for controlling the traversal of a far-end NAT for both signaling flows and media flows at the border of the access and core network. The SCFs (e.g. SCPF), PDF, TRCFs and BGFs are involved in performing the IP address and/or port translation in accordance with the procedure.

10.2.2.1 NAT Traversal Procedure for Signaling Flows

In order to support the NAT Traversal procedure for signalling flows, the SCFs shall return the application signalling packets to CPE on the same address and port number that the signaling packets are sent from.

The relevant operations shall be performed in the follow stages:

Registration:

1) When the first instanceService Control Functions (e.g. SCPF for a session based applicaton) receives a registration request, it shall store the network address and port number information of the calling CPE in the registration message (e.g. contact header in SIP registration).
2) The Service Control Functions may request a registration interval shorter than the keep alive time for the gate in the far-end NAT.

Session Setup Process:

1) When a session setup request signalling message is received, the pertinent instance of Service Control Functions shall request the RACF to obtain public network address and port number, and shall replace the network address and port number (e.g. contact header in SDP) of the originating endpoint with the requested network address and port number.
2) When a session setup response is received, the pertinent instance of Service Control Functions shall modify the network address and port number field of the calling CPE in the message body and replace it by CPE's original network address information, and forward the modified message to the CPE.

10.2.2.2 NAT Traversal Procedure for Media Flows

The NAT traversal procedure for media flows is similar to NAPT control procedure between access and core networks as described in subclause 9.2.1. However, the NAT traversal procedure shall be invoked by the SCFs based on access network and/or CPN configurations, rather than by the PDF based on network security policies. The A-BGF shall serve as an anchor point in support of the media relay function to forward the media flows behind the far-end NAT. For certain applications, both media packets and accompanying media control packets shall be controlled by the same procedure (e.g. RTP and RTCP for VoIP).

10.2.2.3 Correlation between QoS Control and NAT Traversal Procedures for Media Flows

When the far-end NAT is deployed in the CPN, the end user IP addresses shall not be used directly as the source and destination addresses in the QoS control procedure involving RACF-related entities (e.g., PDF, TRCF, SCFs, and BGF). Instead, the public source and destination addresses of the involved media flow received by the BGFs in the media path shall be used.

11 Inter-operator-domain communication for end-to-end QoS control

Two QoS resource control scenarios are identified in Section 6.1. There are two ways of passing the QoS requirements for a given service over end-to-end path. (1) In Scenario 1, the QoS requirements for a given service can be passed through application layer signalling over end-to-end path or through the Iq reference point. (2) In Scenario 2, the QoS requirements for a given service can be passed through path-coupled QoS signalling (e.g. RSVP or the like) over end-to-end path.

In both scenarios, if the media flow isn't transferred through the transit transport network owned by the third operator, inter-operator-domain RACF communication may not be needed. No information needs to be exchanged directly between different operators' RACF systems. Because application layer signalling or path-coupled QoS signalling can pass the QoS requirements information between different operator's domains, the RACF system in each operator's domain can work independently domain by domain without any inter-operator-domain RACF communication. In the case that the operator can evaluate the validity of the request from the other operator, the RACF may exchange information between different operators' RACF systems.

In Scenario 2, if the media flow is transferred through the transit transport network owned by the third operator, inter-operator-domain RACF communication also wouldn't be needed. So in this case, no information needs to be exchanged between different operators' RACF systems. Because path-coupled QoS signalling can pass the QoS requirements information to the transit transport network, the RACF system in each operator's domain can work independently domain by domain without any inter-operator-domain RACF communication.

However in Scenario 1, if the media flow is transferred through the transit transport network owned by the third operator, the QoS requirements for a given service cannot be passed through application layer signalling to the RACF in the transit transport network. The RACF in the transit transport network is required for the end-to-end QoS, but generally no application functions exist in the transit transport networks. In this case, inter-operator-domain RACF communication might be needed for invoking the RACF in the transit transport network with resource requests.

12 Security considerations and requirements for RACF

12.1 Security Considerations

These involve the threat and potential attack overview, as well as the proposal for employing existing NGN protocols as presented in *Guidelines for NGN Security Release 1*. These items are reflected in sections below.

These considerations are relevant only insofar as the communications protocols are concerned; the internal security of each RACF system is defined by the implementation of the security policies set forth by the owner of a specific network.

12.2 Overview of threats and attacks

The major security requirements for RACF are

1) Protection of the signalling exchange in support of resource requests
2) Protection of the information contained in all RACF entities involved in this exchange
3) Ensuring the availability and overall expected performance of the RACF system
4) Prevention illegitimate access to RACF

The taxonomy of the related generic threats (according to *Guidelines for NGN Security Release 1*) and their applicability are as follows:

Destruction of information*:* In terms of the RACF, it means deletion of the information pertaining to the operations of RACF, such as transaction state information, resource usage information, accounting information, topology information, or policy rules. An example of potential consequences is when the information about the existence (or availability) of a particular resource has been destroyed, the resource effectively becomes unavailable. (This is one aspect of the interruption or denial of services described below.)

Corruption or modification of information: In terms of the RACF, there are three aspects to it, as follows:

1) Corruption of the recorded resource information (or policy rules) so that such data are rendered meaningless or unusable. This can result in a total loss of resource information or policy rules, which is in itself a threat to the reliability of the system.
2) Undetected modification of the recorded resource information or policy rules so that such data appear to be meaningful. This can result in theft of services, degradation of services, loss of services, or fraudulent accounting or all four of the above.
3) Corruption or modification of a signalling message with the same results as the above.

Theft, removal, or loss of information: In terms of the RACF, it means theft or loss of the recorded resource information that may result in 1) violation of a subscriber's privacy (in case of theft of subscriber information), 2) theft of services and 3) degradation, interruption, and, ultimately, unavailability of services (in case of the loss of information).

The theft-of -services attacks can be achieved through *repudiation*, that is the denial that a certain transaction had taken place.

Disclosure of information: This can take place because of the interception of the signalling messages or because of granting access to an illegitimate user. The consequence is the same as in the case of theft, removal, or loss of information.

Interruption of services: This can make the whole system partially or totally unavailable. Specifically, the resources (including the computing power of the systems involved) can be exhausted by forcing it to process too many requests, or by authorization of illegitimate requests. This threat is typically realized through a denial of service (DoS) attack. A few known DoS attacks can be achieved by

1. *Replaying* the resource request (or response) messages;
2. *Injection* or *modification* of the resource request (or response) messages; and
3. *Flooding* where an adversary sends a large number of resource requests. The processing of such requests may exhaust system's resources rendering them unavailable for QoS requests from the legitimate users.

There are a number of well-known security mechanisms that have been either proven or deemed appropriate for mutual authentication and provision of integrity and confidentiality.

Transport Layer Security (TLS) [16] and IPsec [17 - 30] protocols already employ such mechanisms for provision of the transport and network layer security, respectively. Various aspects of the use of these protocols are also described in [31]. In addition, networks can employ back-end Authentication, Authorization, and Accounting (AAA) servers, which keep the information necessary for these functions.

Denial of Service (DoS) attacks, however cannot be prevented. They can only be mitigated.

12.3 Security Requirements

- The RACF protocols must take the above threats into account and it must include the measures to counter relevant attacks.
- Specifically, mechanisms must be explicitly defined for mitigation of the flooding attack. Even in the presence of a DOS attack, RACF must retain its availability.
- Any two entities located in different trust environments (e.g., PDF and SCF) must authenticate each other before a security association has been established. This requirement requires special treatment in support of redundancy (which may be, in turn, necessitated to ensure reliability or performance or both). If the service of RACF or any of its components is replicated, an entity that communicates with any such replica must use the same authentication information. With that, an eavesdropper must be unable to repeat a recorded authentication handshake with another replica.
- During the association, all messages must be protected against insertion, deletion, or replay.
- Depending on a specific interface, the confidentiality protection of the messages may be left optional; however the integrity of all messages must be protected. The decisions should be made for specific protocols and they should leave open a choice of standard cryptographic algorithms to be used in support of confidentiality or integrity.
- Non-repudiation must be supported for all requests (unless specifically overridden by a PDF policy in effect)
- A protocol that needs to operate across an un-trusted domain should pass through commonly-used firewalls.
- Except for the DOS *flooding* attack, which is systemic, the above requirements must be implemented using the existing secure-channel protocols such as TLS or IPsec (or both) so that the well-tested security mechanisms be reused rather than re-invented.

Annex A

TRCF over different transport technologies

This section is to describe the implementation examples of TRCF over different transport technologies, including IP, MPLS, Ethernet and GMPLS.

Editor's note: If needed, the following description can go details to be as a guideline for industry.

A.1 TRCF over IP network

Editor's note: At the previous SG13 and JRG-NGN meetings, some contributions *and comments aim at this case.*

In an IP network without MPLS support, most nodes can only handle packets in the conventional IP routing way. Routing and forwarding of all traffic is under the control of conventional IP routing protocols and IP Diffserv. If TRCF is implemented, the admission control and resource allocation are dynamically applied with the link-by-link resource reservation.

One or multiple TRCF entities are deployed to directly manage all of the physical link resources within an administrative domain. The TRCF entity holds and maintains a network topology and resource database (NTRD). Based on the information in the NTRD, the TRCF entity handles route look-up, link-by-link resource allocation and admission control for each flow that requires QoS guarantee. If a flow is admitted with high priority, it will not interfere with other traffic flows. If there are more than one TRCF entities deployed in a domain, they interact with each other through a protocol.

A.2 TRCF over MPLS network

Editor's note: Section10 of the previous Y.e2eqos.2 version mainly aim at this case.

In a packet network with MPLS support, most nodes can handle packets in the label switching way. MPLS LSP technology is used to pre-provision a logical bearer network (LBN) for each service type over the underlying packet network infrastructure manually or automatically through RSVP-TE or CR-LDP protocol. (Diffserv-aware) MPLS TE can be applied for optimizing network performance. The topology planning and bandwidth reservation of each LBN depends on the traffic metering and forecasting, operator policies and SLAs. For purpose of LSP protection, capacity changes and network performance optimization, LBN can be adjusted automatically or manually in accordance with traffic engineering constraints. If TRCF is implemented, the admission control, route selection, resource allocation and label forwarding for the service flows belonging to a service type are dealt within the same one LBN.

One or multiple TRCF entities are deployed to manage the bandwidth resources of each LBN or all LBN within an administrative domain. The TRCF entity records and maintains a network topology and resource database (NTRD) separately for each LBN. Based on the NTRDs and policies, the TRCF entity makes intra-domain route selection, resource allocation and admission control for a service flow within its corresponding LBN. If there are more than one TRCF entities deployed for one LBN in a domain, they interact with each other through a protocol.

The QoS route for a flow specified by the TRCF entity is a label stack that represents a concated LSP set. The edge router encapsulates the packets with this label stack, which in turn makes the intermediate transit routers forward the packets of a flow along the specified route with the specified priority.

A.3 TRCF over Ethe1) rnet network

Editor's note: The ARCF in TR-123.qos aims at the Ethernet aggregation network.

In an Ethernet network, most nodes handle packets in the Ethernet MAC bridging or virtual bridged way. Generally, only edge nodes are IP-capable. If TRCF is implemented, the admission control and resource allocation are dynamically applied with the Ethernet link-by-link resource reservation.

One or multiple TRCF entities are deployed to directly manage all of the physical link resources within an Ethernet network. The TRCF entity holds and maintains a link layer network topology and resource attributes database of the whole network. Based on the information database, the TRCF entity makes admission control and resource allocation to ensure that sufficient resources are available within the network for the happening flows. If there are more than one TRCF entities deployed in a domain, they interact with each other through a protocol.

……

A.4 TRCF over GMPLS network

For further study.

A.5 TRCF over Broadband wireless network

(Editor's note) In this description, The QoS classes in broadband wireless network are defined in IEEE 802.16. It needs to align with ITU-T recommendation Y.1541.

In broadband wireless network, mobile nodes handle packets through the wireless MAC protocol. Broadband wireless MAC protocol provides QoS signaling mechanisms such as the connection setup, bandwidth request, uplink information. The QoS classes for the QoS signaling define four QoS services: Unsolicited Grant Service (UGS) used for CBR-like service flows, Real-Time Polling Service (rtPS) used for rt-VBR-like service flows, Non-real-Time Polling Service (nrtPS) used for non-real-time service flows, and Best Effort Service (BE). Efficient queuing policies for such different QoS classes can support priority scheduling and dynamic bandwidth allocation. However, broadband wireless network does not define the resource control and admission control mechanisms to demand different QoS requirements.

Therefore, functions using the TRCF are required for the resource control to provide priority scheduling and dynamic bandwidth allocation. If TRCF is implemented, TRCF manages the access transport resource based on the resourece status information databse. As a result, the admission control and resource allocation are dynamically applied according to each service flow with different QoS reqirements.

One or multiple TRCF entities are deployed to directly manage the bandwidth resources within a administrative domain. The TRCF entity records and maintains a network topology and resource database (NTRD) for the whole network. Based on the information in NTRDs, the TRCF entity realizes admission control and resource allocation to maintain QoS levels and fairness for different applications, thus achieving high system utilization. If there are more than one TRCF entities deployed in a domain, they interact with each other through a protocol.

Appendix I

Intra-network RACF interaction approaches

This section is to describe the implementation examples of the intra-network RACF interaction approaches.

From the viewpoint of the end-to-end association between functional entities of RACF, there are two approaches for the QoS control from one end to another end. One is the approach in which the RACF performs the QoS control in parts and achieves the entire end-to-end control with the intermediation of the service stratum functions (Approach A). Another is the approach in which the RACF performs the QoS control within the transport stratum without the intermediation of the service stratum functions (Approach B).

Note: This consideration is about the QoS control. Approach B is not applied to NAPT control, NAT traversal and FW control.

The typical cases for the application of Approach A are, for example;

– The case that there is a part, in which the admission control is not required per flow, through the entire end-to-end route of the media,

– The case that the approach meets the requirement of the network control.

The typical cases for the application of Approach B are, for example;

– The case that there is a single SCPF related the service requesting QoS control (e.g. non-session based services)

– The case that it is required for the interaction between functional entities in RACF to be independent from the intermediation of functional entities in the service stratum. This may be required for the consideration on the business model, the immediacy of the coordination between functional entities of the transport stratum, etc.

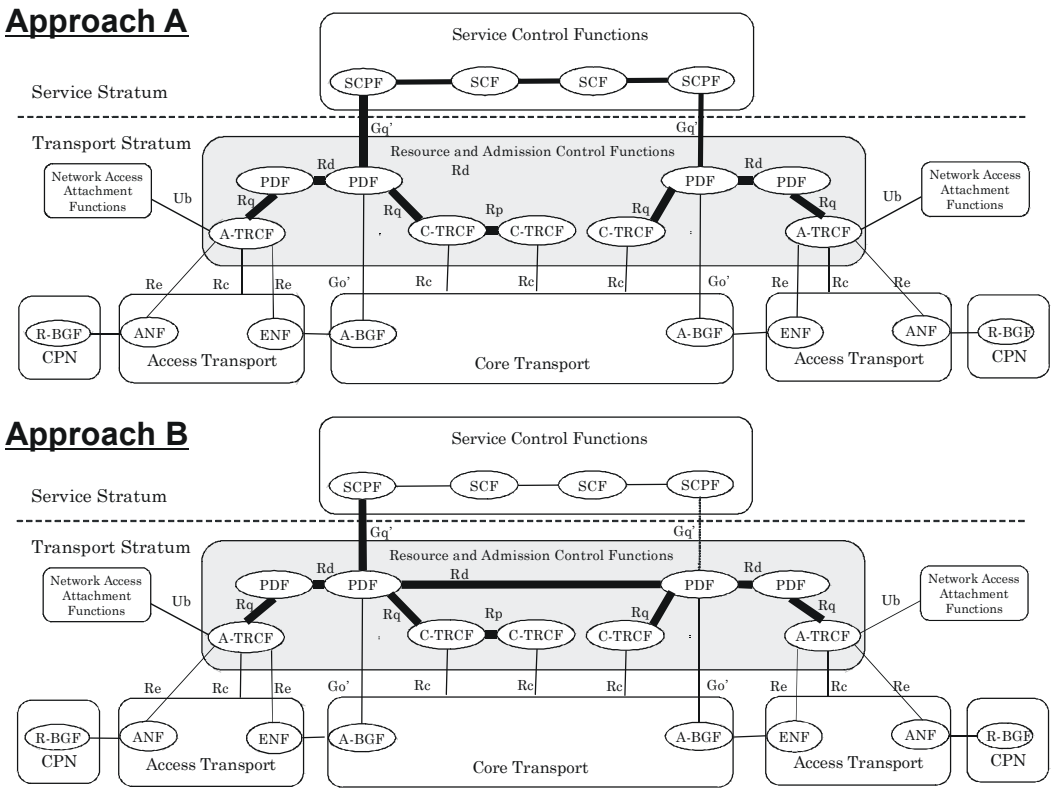


Figure I-1 – Approaches for intra-network RACF interaction

Note:

– These figures describe the case that the leftmost PDF is invoked initially by SCPF.

– The bold lines show the route of the end-to-end QoS control.

– The PDF interacting with A-TRCF may be the same as the neighbouring PDF interacting with C-TRCF.

Appendix II

Inter-network RACF interaction approaches

In the general case that the data stream is transferred through the transit transport network(s), the resource and admission control in the transit network(s) as well as the both end networks is required for the end-to-end QoS. The RACF in the transit network should communicate with both ends for the control of the end-to-end resource control. For the inter-working of the transit RACF with the RACF invoked with resource request, there are two example approaches as followed;

Approach 1: The direct communication between RACSs other than the communication between the last RACF and the previous RACF

Approach 2: The direct communication through all the RACF along the data transmission route (without the interaction between the rightmost SCF and the rightmost RACF as the resource and admission control) Approach 2 is not applied to NAPT control, NAT traversal and FW control.

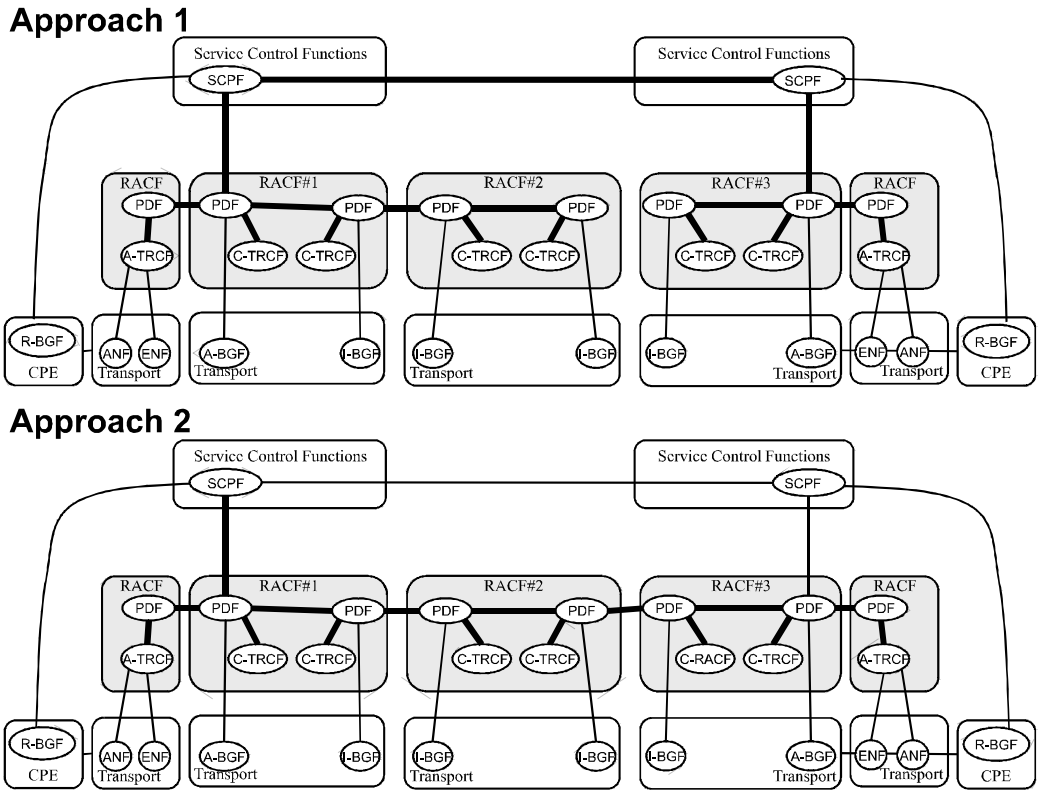


Figure II-1 – Approaches for the inter-network RACF interaction

Notes:

– This figure describes the case that the left PDF in RACF#1 is invoked initially by SCPF.

– The policy decision on the interworking across the network boundary is assumed to be performed by PDF. I-BCF is omitted for simplicity.

– The bold lines show the route of the end-to-end QoS control.

In the case of approach 1, there is discontinuity of the inter-RACF communication. In the case with such the indirect interaction (i.e. the intermediation of SCPFs), it should be examined whether the information/notification for the resource and admission control can be performed, whether the allocated routes is continuous across the discontinuity point, and so on.

There may be a problem in an immediacy of the interaction from one end through another end in the case that the route changes due to the link failure. The link failure may result in the route change without the termination of active data streams and this may cause the route change in the succeeding domain or network. In such the cases, in preparation to the succeeding resource requests, it is necessary for RACFs to immediately notify the change of the resource assignment with each other due to this route change. In approach 1, the interaction for the notification between RACF#2 and RACF#3 is performed through the SCPF-SCPF interaction and this results in the procedural delay. From the viewpoint of the immediate notification through end-to-end RACFs, approach 2 is applied.

Approach 2 means not only that the inter-RACF communication is performed from one end to another end without discontinuity but also RACFs receive the QoS request at a single point.

2.12 – A QoS framework for IP-based access networks*

Introduction

The purpose of this draft is to provide a general framework for QoS support for IP-based access networks, which share many commonalities, integrates it into the NGN.

General features will be that access networks are based on broadband access techniques (i.e., radio, cable, copper, etc.) and IP technologies are dominant. From the services point of view many voice and data services are envisioned. QoS support and delivery and compliance mechanisms are the distinguishing new aspects of NGN services.

Table of Contents

* Status D: The FGNGN considers that this deliverable is not yet mature, requiring discussion and technical input to complete development.

2.12 – A QoS framework for IP-based access networks

1 Scope

The Scope of the new draft is to provide a general QoS framework for IP-based access networks. A reference architecture for IP access networks for QoS support will be provided as well as detailed QoS requirements and validation procedures. The reference model will be part of the overall NGN framework with the service and transport layers, functional entities in each layer, and interfaces between the functional entities. In particular the functional entities are to facilitate interworking with the QoS functionality in the core network as well as that specific to each type of access networks.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Draft. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Draft are therefore encouraged to investigate the possibility of applying the most recent edition of the Drafts and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Draft does not give it, as a stand-alone document, the status of a Recommendation

ITU-T Y.1291

FGNGN TR-e2eqos.1

ITU-T H.610

FGNGN TR-123.qos

DSLF TR-059

DSLF WT-101

DSLF PD022

DSLF PD021

[Y.1231] ITU-T Recommendation Y.1231 (2000), *IP access network architecture*

[Y.1540] ITU-T Recommendation Y.1540 (1999), *Internet protocol data communication service – IP packet transfer and availability performance parameters*

[Y.1541] ITU-T Recommendation Y.1541 (2002), *Network Performance Objectives for IP-based services*

[Y.1291] ITU-T Recommendation Y.1291 (2004), *An architectural framework for support of Quality of Service (QoS) in packet networks*

TBD

3 Definitions

TBD

Access Node (Aggregation Node) (AN): A network element that provides aggregation capability between the drop network and the aggregation network.

Customer Premise Gateway (CPGW): A customer premises functional element that provides IP routing and QoS capabilities.

Service Node (SN): FFS.

Service Node Interface (SNI): FFS.

Drop Segment (medium): Refers to the network used to transport services in a common format from the Remote Node to the Network Termination.

Aggregation Network: A regional network providing traffic aggregation between the drop segment and the Service Node.

4 Abbreviations

TBD

5 Conventions

TBD

6 QoS Requirements

General service requirements for Access Networks

- All attributes have to have unambiguous meaning;
- Allow independent evolution of Access networks(i.e., eliminate or minimise the impact of evolution of Access networks);
- The QoS of Access networks negotiation mechanisms should accord with end-to-end QoS negotiation mechanisms;
- The QoS of Access networks mechanisms shall provide a mapping between application requirements and Access services;
- The QoS of Access networks control mechanisms shall be able to efficiently interwork with current QoS schemes. Further, the QoS concept should be capable of providing different levels of QoS by using Access networks specific control mechanisms;
- The overhead and additional complexity caused by the QoS of Access networks scheme should be kept reasonably low, as well as the amount of state information transmitted and stored in the network;
- QoS of Access networks shall support efficient Access networks resource utilisation;
- The attributes of Access networks QoS are needed to support asymmetric bearers;
- Applications should be able to indicate values of Access networks QoS for their data transmissions;
- The behaviour of Access networks QoS should be dynamic , i.e., it shall be possible to modify QoS attributes during an active session;

- Number of attributes should be kept reasonably low (increasing number of attributes, increase system complexity).

7 IP access technologies

Ed. Note. The current status of various documents in different standards bodies will be investigated.

7.1 QoS mechanisms over Copper/ xDSL

Ed. Note. Extensive partnership with DSLForum is needed

7.2 QoS mechanisms over Cable

Ed. Note. Extensive partnership with other standards groups and SG 9 is needed

7.3 QoS mechanisms over UTRAN

Ed. Note Extensive partnership with 3GPP Radio Access Network working group is needed

7.4 QoS mechanisms over Ethernet (including PON)

Ed. Note Extensive partnership with Y.123.qos is needed since the structures are very similar in all cases.

7.5 Other access technologies

8 Reference architecture

8.1 General QoS architecture for IP based access network

Fig.1 depicts a QoS architecture for IP based access network. This figure is consistent with the principles of Y.1231 and G.902 of ITU recommendations.

The figure shows two types of functional nodes comprising an access network and a CPGW node that is intimately part of the QoS architecture of Access Networks in NGN.

CPGW node represents customer premise equipment with user interfaces and can use wired and wireless drop segments to access the AN.

AN is the aggregation node that provide point to point connection to CPN. AN provides aggregation functions as well as termination of data link and physical connections.

AN examples are DSLAM (xDSL), CMTS (Cable systems), OLT (Passive Optical Networks), BS (Fixed Radio), RNC (UTRAN), Ethernet switch (Ethernet), BAA (Metro Ethernet) etc.

SN is the multi service node that provide connections to network and application providers. Depending on the configuration several nodes of each type can exist with multiple interfaces in an Access network.

SN examples are BRAS (ATM and Ethernet), ER with BRAS functionality, GGSN/GMSC (UMTS) etc.

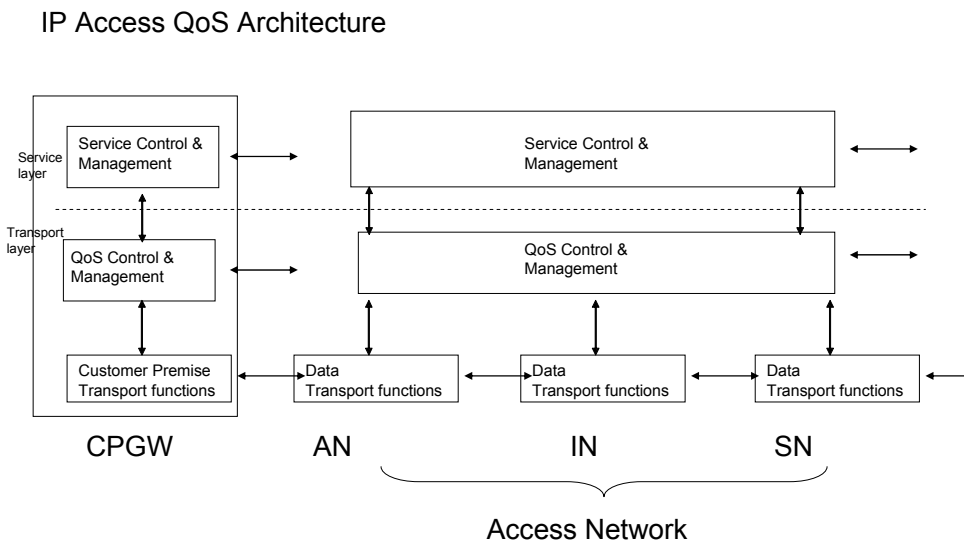


Figure 1 – General QoS architecture for IP based Access network

Service management functions include management of access provisioning and registration, AAA, service-specific OAM, etc.

Service control functions consists of the control of data, voice and video service, the control of VPN and other existing and future value added services.

QoS Control functions are resource control and reservations, admission control, various tuning functions as well as QoS routing and other traffic control functions. QoS management functions include SLA and Policy management, Capacity management, Reliability and Monitoring functions among others. CPN, AN and SN also performs other QoS mechanisms in data plane, which includes traffic conditioning (marking, shaping, policing), classification, queuing & scheduling, buffer management andcongestion avoidance.

8.2 Categorisation of various QoS solutions

According to the distribution of the resource control function, there could be different scenarios.

One is the solution based on centralized resource control. In this scenarios the resource control is physically centralized in a function element and independent of the elements which fulfil the data transport function in access network.

Also the resource control can be distributed in every network element. All the resource control function block in these network elements interact with each other to fulfil the unified access resource control.

When the above two scenarios are integrated in one access QoS solution, we could call it hybrid resource control.

According to the technology of access aggregation used in the access network, there could be several implementation schemes which have been discussed or completed in DSLF, MEF, 3GPP, and etc.

Note: The TR59 and WT101 from DSLF provide a solution for ATM based IP access network and a solution for Ethernet based IP access network. The TR.123.qos is also a good starting.

8.3 Requirements for functional elements in access networks

8.3.1 Requirements for AN Functionality

AN supports a variety of technologies and provides a concentration point for logical connections to CPN.

The following are some of the supported requirements for AN:

- Support multi-user, multi-destination, multi-service differentiation on CPN side
- Ability to segregate data flows for QoS support towards SN
- Support QoS control functions in cooperation with SN
- Switching/Routing functionality for various technologies
- Classification, queuing, scheduling and shaping of IP flows
- Marking/Re-marking capabilities
- Congestion avoidance
- Management control interfaces
- QoS mapping between CPN and aggragation network
- QoS mechanisms specific to particular physical access

8.3.2 Requirements for Intermediate Devices Functionality

Similar to AN, TBD.

8.3.3 Requirements for SN Functionality

- Support multi-user, multi-destination, multi-service differentiation
- Ability to segregate data flows for QoS support
- Support QoS control functions in cooperation with AN and ER (if there is a separate ER)
- Switching/Routing functionality for various technologies
- Classification, queuing, scheduling and shaping of IP flows
- Marking/Re-marking capabilities
- Congestion avoidance
- Management control interfaces
- QoS mapping between CPN and aggragation network
- QoS mechanisms specific to particular physical access
- Support Protection and restoration mechanisms
- Support multiple Service Provider Interfaces

8.3.4 Requirements for CPN Gateway Functionality

- Multi-user, multi-destination support
- QoS mechanisms such Diffserv, RSVP and TE
- Dynamic MTU negotiation
- Packet segmentation based on traffic/queue type
- Classification, queuing, scheduling and shaping of IP flows
- Marking/Re-marking capabilities
- Congestion avoidance

- Management interface
- Capability for resource/service request
- QoS mapping between CPN and access network
- OAM
- … …

… …

Ed. Note Relevant new sections will be added as necessitated by the general architecture.

Control and Management

9 Interface Requirements

10 Architectural Scenarios

The following scenarios are not exhaustive.

Scenario 1: A separate resource controller connected to CPGW, AN and SN.

In this scenario, a separate resource controller is responsible for the admission control and resource allocation in the access network. It is connected to CPGW, AN and SN. COPS or other protocols may be used to download the configurations info to and also get the capability info from end user's device, L2 aggregation's device and L3 aggregation's device. There is also possibility that multiple SNs, such as BRAS, media gateway and CDN edge device etc., share the same AN. In this case, RC will control the resource utilization between different SNs.

Scenario 2: A separate resource controller only connected to SN(s)

In this scenario, a separate resource controller is in charge of admission control and resource allocation in access networks and it is only connected to the SN (s). The resource controller will communicate with SN(s) by COPS or other protocols, and the SN could get the resource information by using an extended layer 2 protocol.

Scenario 3: Distributed and embedded implementation.

In this scenario, resource control function in access network is separated and embedded in the SN, AN and CPGW. There is no separate resource control device. CPGW is responsible for end user's resource control. AN is responsible for resource control of Layer 2 aggregation. SN is responsible for resource control Layer 3 aggregation. There exits an internal interaction between them for resource information exchange.

11 Other considerations

2.13 – Performance measurements and management for NGN*

Abstract

Network performance expectations must be set and monitored among Users and Service Providers to raise confidence in network delivery. Existing standards specify several metrics and measurement methods for point to point performance. However, many options and parameters are left unspecified, as are concatenation of performance over multiple network segments, accuracy, and data handling. Each of these topics must be specified in order to support QoS across multiple heterogeneous Service Providers.

Note that all values are Strawman values and may change

Table of Contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

2.13 – Performance measurements and management for NGN

1 Introduction

Network performance expectations must be set and monitored among Users and Service Providers to raise confidence in network delivery. Users typically only see the end-to-end performance, i.e., the concatenation of performance over multiple network segments and/or across multiple heterogeneous Service Providers. Thus, meaningful discussions of QoS between Users and Service Providers can only be end-to-end.

Existing standards specify several metrics and measurement methods for point to point performance. Notable are the ITU-T Y.1540 and Y.1541 standards and the IETF IP Performance Metrics (IPPM) Working Group standards. However, many options and parameters are left unspecified, as are concatenation of performance over multiple network segments, allocation of impairment budgets, mapping between IP and non-IP metrics, accuracy, and data handling. Each of these topics must be specified in order to support QoS across multiple heterogeneous Service Providers.

Recommendations for future work:

a) Complete the specifications of the information transfers, data model and protocol requirements

b) Develop the framework for the use of passive measurements, possibly in conjunction with active measurements.

c) Develop accuracy requirements and implications

2 Scope

This document describes measurements and their management which are applicable for:

1) Providers' delivery assurance of customers' network performance

2) Providers to supply performance information for prospective customers

3) Providers' troubleshooting among their networks along defined paths

4) Provider's internal indication of performance impact of changes within their networks

5) Provider's monitoring of each others network performance

6) Provides information to other NGN components e.g., RACF, Bandwidth Broker, OSS/BSS, etc.

It reviews requirements for performance measurements including performance attributes, and timescales. Building upon existing standards it extends current specifications in these areas. Comparisons to existing standards are included. Defining the probe packet format is beyond the scope of this document.

It reviews requirements for a scalable monitoring system, and describes a network model which will meet those requirements. It categorizes various measurements and shows how they may be applied to the network model. It reviews time synchronization and sets targets for equipment which is located at various points in the network model.

It reviews management architectures, considers different approaches and picks one, giving a detailed example. The aspects of management covered include: – discovery, inter-provider communication regarding the life cycle of measurements and reports. Defining the management packet format is beyond the scope of this document.

Security requirements of the measurement and management traffic transfers are analyzed, approaches are considered, then a set of approaches are picked. Security of BGP, synchronization systems, and customer equipment are beyond the scope of this document.

Customer interactions with their service provider are discussed at a high level. Details of information transfers are beyond the scope of this document.

The target network of this document is IP networks, pure L2 and other non-native IP networks are out of its scope.

This document describes how to measure, aggregate and disseminate basic required information performance metrics. Specification of advanced analysis and its dissemination of measurement data are beyond the scope of this document.

Impairment allocation and translation among IP and Non-IP networks are beyond the scope of this document."

3 References

3.1 ITU-T

- Y.1540 (2002) IP packet transfer and availability performance parameters
- Y.1541 (10/05) Network performance objectives for IP-based services
- G.107 (03/05) The E-model, a computational model for use in transmission planning
- P.800 (08/96) Methods for objective and subjective assessment of quality
- X.805 (10/03) Security architecture for systems providing end-to-end communications

3.2 IETF

- RFC1889 RTP: A Transport Protocol for Real-Time Applications
- RFC2330 Framework for IP Performance Metrics
- RFC2679 A One-way Delay Metric for IPPM
- RFC2680 A One-way Packet Loss Metric for IPPM
- RFC3357 One-way Loss Pattern Sample Metrics
- RFC3393 IP Packet Delay Variation Metric for IP Performance Metrics (IPPM
- RFC3432 Network performance measurement with periodic streams
- RFC3871 Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure
- RFC3550 RTP: A Transport Protocol for Real-Time Applications
- RFC3917 Requirements for IP Flow Information Export (IPFIX)
- "IPFIX: Information Model", (work in progress), Internet Draft, draft-ietf-ipfix-info-11.txt, September 2005.
- "IPFIX:Protocol", (work in progress), Internet Draft, draft-ietf-ipfix-protocol-19.txt, September 2005.
- "IPFIX: Applicability", (work in progress), Internet Draft, draft-ietf-ipfix-as-06.txt, July 2005.
- "IPFIX: Protocol", (work in progress), Internet Draft, draft-ietf-ipfix-architecture-09, August 2005

4 Terms and Definitions

Aggregate Loss Ratio – The loss aggregated along a path across multiple provider's networks.

Demarcation Point – Generally a point which separates two domains, here the separation between the access and transit networks.

Fraction Lost – The fraction of RTP data packets from source SSRC_n lost since the previous SR or RR packet was sent (RFC1889)

Interarrival Jitter – An estimate of the statistical variance of the RTP data packet interarrival time. The interarrival jitter J is defined to be the mean deviation (smoothed absolute value) of the difference D in packet spacing at the receiver compared to the sender for a pair of packets (RFC1889)

Landmark system – A proxy system for customer premise terminal equipment.

Measurement point – A point in the network containing functionality that may initiate or respond to measurements with other measurement points. (located at peering points, demarcation points, PEs, CEs and Landmark customer premise equipment)

Path Unavailability – The period of time from when losses exceed a threshold until they drop below another threshold, a measure of bursty loss.

Period Path Unavailability – The total period of unavailability during a customer reporting period (typically 1 month).

5 Abbreviations and Acronyms

ALR	Aggregate Loss Ratio
ATM	Asynchronous Transfer Mode
CE	Customer Edge
CoS	Class of Service
DoS	Denial of Service
DP	Demarcation Point
DSCP	DiffServ Code Point
DSL	Digital Subscriber Line
ECMP	Equal Cost Multi Path
FEC	Forwarding Equivalency Classes (multi-protocol label switching)
FSD	Flow Summary Data
GLONASS	Global Navigation Satellite System
GPS	Global Positioning System
IANA	Internet Assigned Numbers Authority
IDQ	Inter Domain QoS
IPDV	Internet Protocol Packet Delay Variation
IPFIX	IP Flow Information eXport

IPLR	Internet Protocol Packet Loss Ratio
IPPM	Internet Protocol Packet Performance Metrics
IPSLBR	IP packet Severe Loss Block Ratio
IPTD	IP Packet Transfer Delay
IPUA	Internet Protocol UnAvailability
LAN	Local Area Network
LSP	Label Switched Path
MOS	Mean Opinion Score
MP	Measurement Point
MPLS	Multi-Protocol Label Switching
MSNG	Number of MiSsiNG probes
NDETL	Number of probes exceeding DETL
NE	Network Element
NMS	Network Management System
NTP	Network Time Protocol
OAM	Operations Administration and Maintenance
PE	Provider Edge
PES	Performance Evaluation System
PL	Packets Lost
PLE	Threshold number of Probes Lost to End unavailability period
PLR	Packet Loss Ration
PLS	Threshold number of Probes Lost to Start unavailability period
POP	Point of Presence
PTP	Probe Transmission Period
PW	Policing Window
QoS	Quality of Service
RP	Rollup Period
RTP	Real-time Transport Protocol
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
SNMP	System Network Management Protocol.
SONET	Synchronous Optical Network
SP	Service Provider

SPW	Sliding Probe Window
TBD	To Be Determined
TCP	Transmission Control Protocol
TE	Terminal Endpoint
TMF	Traffic Measurement Function
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VPN	Virtual Private Network

6 Overview

The remainder of this document is partitioned into two major sections, one for measurements (section 7), and the other for the management of those measurements (section 8). Section 9 considers the security requirements that need to be addressed for the content of these two previous sections. Section 10 is an Annex which considers the use of passive measurements. Section 11 contains Annex B which summarizes all the measurement associated parameters discussed in this document into a single table.

7 Measurement Requirements

7.1 Traffic Performance Attributes

Inter Domain QoS (IDQ) requires consistent service descriptions and similar service levels across a large number of interconnected Service Providers. To support this, there must also be consistency in the measurement of performance attributes. The key elements of consistency of performance measurement are:

- Objectives – which attributes are measured?
- Timescales – what timescales are attributes measured over?
- Techniques – how are the attributes measured?

This section deals with measurement objectives and timescales while section 7.2 deals with measurement techniques. Both sections use examples of Network QoS Classes and values as aids for understanding. However, the actual Network QoS Classes and values are described in Annex B.

It is important to recognize that the model of Inter Domain QoS is an extension of the Internet which supports a connectionless IP service that delivers user payloads in the form of packets/bytes in each direction. Since outbound and inbound traffic routes may differ, the targets and measurements for all performance attributes in IDQ are one-way and reflect the connectionless nature of the service.

The performance attributes that are used to characterize a QoS class are:

- Mean Delay
- Delay Variation
- Packet Loss
- Path Unavailability

Application throughput depends upon many factors including packet loss and transit delay, and others not under the control of the SP. Application throughput is not an independent IDQ performance attribute in its own right

The offered traffic rate is also an important as part of service descriptions and inter-SP contracts, but this is not considered a performance attribute.

Other performance metrics such as "delay equivalent to loss" and "packet disorder" are known to have value. However, their incremental value over the metrics selected above are currently believed not to be worth the additional complexity they would require to specify, implement, and deploy. Time may prove otherwise and other basic network metrics may be added in the future.

Other attributes, such as application-level metrics, may be added in the future. An example of which is the Mean Opinion Score. The Mean Opinion Score (MOS) is defined in Methods for Subjective Determination of Voice Quality (ITU-T P.800). In P-800, an expert panel of listeners rated pre-selected voice samples of voice encoding and compression algorithms under controlled conditions. An MOS score can range from 1 (bad) to 5 (excellent), a MOS of 4 is considered toll quality.

7.1.1 Measurement Timescales

Before looking at performance attributes, we consider a common reference, namely timescales. Inter Domain QoS requires that all performance metrics are measured over the same timescales. This greatly simplifies analysis of inter-domain performance.

The selected timescales for performance measurement support the following criteria:

- The measurement overhead traffic must be kept at a low level
- The basic timescale must be large enough to contain the start and end of a large number of traffic flows
- The basic timescale must be common and synchronized globally among SPs
- The timescale must be meaningful to network users and capture any productivity or service quality issues they perceive in the network.
- The timescales should not unduly emphasize momentary glitches such as link outages or rerouting events where they do not significantly impact network user experience.

Given these criteria, the default timescales selected are:

- Measurement: timescale unit is 5 minutes. This is synchronized via GPS or similar service, and aligned with UTC. This allows all SPs to synchronize their measurement periods and correlate measurements. The targets and measurements for Mean Delay, Delay Variation and Packet Loss apply to 5 minute periods. Measurement samples are aggregated over this period of time which is referred to as the Rollup Period
- Customer reporting: timescale unit is 1 "month" with start and end hour/day defined by the SP offering the IDQ service. The start and end monthly definitions may not be aligned between SPs. To be able to correlate measurements from one time zone to another and one SP's "month" to another, all timestamps are referenced to UTC as well as any local time references. The actual timescale of customer reporting needs be determined by agreement between the network provider and each customer

7.1.1.1 Relationship to existing standards

RFC3423 refers to the Rollup Time as defined above as "Tcons, a time interval for consolidating parameters collected at the measurement points."

Y.1541 refers to the "Rollup Period" as the "Evaluation Interval" and suggests an evaluation time of 1 minute for IPTD, IPDV, and IPLR.

7.1.2 Mean Delay

Delay is important to the support of many applications including telephony, multimedia conferencing, financial transactions and online gaming. In addition, delay is indirectly related to throughput and impacts file transfer speeds and email delays

The Delay attributes of a QoS class are characterized by a mean delay and a specific set of upper percentile delay variations. The percentile approach is used in preference to a standard deviation or variance model due to the frequent occurrence of bi-modal or multi-modal delay distributions. Thus delay is characterized through mean delay and delay variation.

The mean delay is defined as the mean delay of all successfully delivered packets during periods of network availability within the specified timescale.

Since delay is distance sensitive due to the finite signal propagation delay, distance is taken into account when setting targets. Mean delay may vary between QoS classes due to priority queuing which is taken into account when setting targets.

7.1.2.1 Relationship to existing standards

The Mean Delay of IDQ is identical to the Mean IP Packet Transfer Delay (IPTD) of ITU-T Recommendation Y.1540 and Y1541.

The Mean Delay of IDQ would correspond to "Type-P-Finite-One-way-Delay-Mean" if extrapolated from IETF RFC2679.

7.1.3 Delay Variation

In addition to the mean delay, delay variation is important to many applications including telephony, gaming and transactions.

Delay variation is a measure of how much variation is observed over a period of time as contrasted to jitter which is a measure of variation between successive packets. Jitter measurements are dependent on the frequency with which packets are sent and focus exclusively on short-term effects. Delay variation is insensitive to the frequency of packets and measures both short term and long term variation. For these reasons, the IDQ model measures delay variation.

Delay variation in IDQ is the difference between a delay percentile and minimum delay. The actual delay percentiles can be estimated by summing the minimum delay and the delay variation percentiles.

The delay variation percentiles that can be measured are:

- 90^{th} percentile – DV90
- 99^{th} percentile – DV99
- 99.9^{th} percentile – DV99.9

Conceptually, percentiles are measured by stack-ranking all measurements of successfully delivered packets, discarding a top percentage e.g. 0.1% in the case of 99.9^{th} percentile, then selecting the remaining highest value. In reality, we measure a subset of packets… the active probes, see section 7.2. All lost packets or packets delivered while the network is considered unavailable are ignored from other metrics.

By taking multiple percentile readings and a mean percentile, the distribution of delays can be better understood. This information is more useful than a simple standard deviation metric which can be easily used only when assuming a mathematically friendly underlying probability distribution function. In reality,

network delay characteristics are multi-modal and have many peaks and valleys. There is a cost associated with both engineering a network to more closely match a particular delay distribution and in closely measuring that distribution. Therefore only QoS Classes that require multiple percentiles will have them specified and measured.

Delay variation is loosely correlated to distance, (since distance is loosely correlated to number of hops) and allows targets to be set independently of site locations. Delay variation is very sensitive to bandwidth and utilization and will vary significantly with access bandwidth.

7.1.3.1 Relationship to existing standards

ITU-T recommendation Y.1540 discusses IP packet delay variation (IPDV), including multiple calculation options. IDQ is aligned with Y.1541 and a Y.1540 proposal selecting the use of 99.9 percentile minus minimum as the exclusive IPDV method. IDQ suggests additional percentiles be specified and used in the future beyond the 99.9 percentile

IDQ delay variation is based upon bulk delay measurements rather than on the difference between two successive measurements and therefore differs from IETF RFC3393.

7.1.4 Packet Loss

Packet loss is important to most applications. It significantly impacts either perceived quality or perceived throughput of the network.

A packet is considered lost in IDQ if the packet never reaches the destination.

The Packet Loss Ratio (PLR) is determined for a period by only looking at the packets transmitted while the network was considered available. The packet loss ratio is the number of lost packets divided by the number of transmitted packets.

Packet Loss is largely insensitive to distance and targets can be set independently of the end site locations. Packet loss ratios are sensitive to access technologies, bandwidth and utilizations, and number of hops, and targets must be set accordingly.

7.1.4.1 Relationship to existing standards

The Packet Loss Ratio of IDQ is identical to the IP Packet Loss Ratio (IPLR) of ITU-T recommendation Y.1540 and Y1541.

IDQ packet loss is identical as described in IETF RFC2680 as Type-P-One-way-Packet-Loss.

7.1.5 Path Unavailability

Path unavailability is significant when a human observer detects a business impacting application failure due to network loss. For a typical application such as telephony, a network path is considered unavailable by the user if there is an inability to connect, or a connection is lost. The measurement of unavailability attempts to approximate this view by detecting periods during which network path unavailability would have noticeable impacts on applications and individual or business productivity.

Unlike delay and loss attributes, the unavailability attribute is not statistically simple to define and an approximation is required.

In IDQ, unavailability is calculated from the distribution of loss measurements over time; see section 7.2 for loss measurement details. A period is considered unavailable if there is an excessive packet loss ratio (PLR) (e.g. >20%) over a specific interval. The interval may be set independently for each QoS class. The unavailability period is defined as follows:

1) The starting point for a period of network unavailability is when a packet is lost and during a subsequent interval, the PLR is beyond the defined threshold. The period of the interval is hence counted as unavailable.

2) The ending point of a period of network unavailability is when during an interval, the packet loss ratio is below a specific threshold (e.g. < 1%). The interval is counted as available and hence the unavailability ends at the start of this interval.

This definition is intended to capture any periods of very poor performance and require the network performance to return to normal levels before the unavailability is ended. During a period of unavailability, none of the delay or loss statistics are impacted.

Path Period Unavailability (IPUA) is measured by summing the periods of unavailability and dividing by the total period being covered. The period being covered to be used is the default "reporting to customer" period. It should be noted that the IDQ system keeps track of each individual period of unavailability for reporting to customers.

Unavailability is largely insensitive to distance, but is sensitive to single points of failure in a network architecture. It will vary significantly with access technologies and configurations. To achieve a low level of unavailability, diverse transmission paths are required.

7.1.5.1 Relationship to existing standard

The Availability metric of IDQ is derived from ITU-T recommendation Y.1540 which discusses IP packet Severe Loss Block Ratio (IPSLBR). "An IP packet severe loss block outcome occurs for a block of packets observed during time interval T_s at ingress MP_0 when the ratio of lost packets at egress MP_i to total packets in the block exceeds s1". IPSLBR was identified as a candidate additional IP packet transfer performance parameter for further study. IDQ uses two thresholds, (which may have the same value,) one to enter a period of Unavailability plus another to exit a period of Unavailability.

ITU-T Recommendation Y.1540 defines a Service Availability Function based on packet loss ratio threshold evaluation in a fixed time window. The current values suggested are >75% packet loss ratio and window time of 5 minutes.

The IETF's RFC3357 builds statistics on definitions of Type-P-One-Way-Loss-Distance-Stream and The Type-P-One-Way-Loss-Period-Stream which measure loss blocks in a different way to IDQ availability.

7.2 Performance Measurements

Inter Domain QoS is intended to increase the level of confidence in the expected service characteristics of the NGN. Increased confidence will enable new applications, services and revenue streams. An integral part of achieving this confidence is the continuous measurement of service performance. The purpose of taking measurements is to provide information for customers, potential customers and Service Providers, and includes:

1) For Customers and potential customers
   a) Reports to customers of what service has been delivered
   b) Reports to potential customers to support marketing claims on service characteristics

1) For Service Providers and third party delivery assurance entities
   a) Reports to design service offerings
   b) Reports for Troubleshooting
   c) Data for Marketing collateral
   d) Reports to enable capacity planning and service development.

The IDQ measurement system and the statistics that it produces must:

a) be easily understood by SPs and customers

b) be well defined (non-ambiguous)

c) be relevant to customers' applications

d) enable Service Providers to diagnose issues and anticipate capacity requirements

e) be independently repeatable (multiple SP measurers over the same time get the same result)

f) be independently verifiable by customers (customer measurements should be close to SP estimates)

g) be widely applicable (traffic type, link size, load independent, any IP network)

h) be appropriately sensitive to distance and path

i) not significantly impact the forwarding of other data

j) be sufficiently scalable to support millions of customer sites

k) be sufficiently reliable to enable SLAs with financial penalties to be administered

l) be sufficiently accurate to enable SLAs with financial penalties to be administered

Since outbound and inbound traffic routes may differ, all measurements will be "one-way". Customers or Service Providers may aggregate the statistics of two directions to estimate the round-trip performance.

Measurements will be taken from each of the segments of the Measurement Network model (described in section 7.3) and may be combined to form multi-segment, site-to-site, edge-to-edge or IPTerminal-to-IPTerminal metrics. A subset of these metrics will be used for reports for the offered services.

Quantitative requirements for end-to-end and segment accuracy have not yet been developed. The following incomplete list of measurement aspects should be considered when requirements are set, and when systems and components are designed:

- Number of segments (due to concatenation errors)
- Impact of measurement equipment not being directly in user data path
- Measurement equipment processor load
- Time synchronization errors
- ECMP related errors
- Measurement granularity (unit)
- Number of measurement samples per evaluation period to support required statistical accuracy
- Active probe frequency
- Active probe size

7.2.1 Active Probing

The performance of active probes will be used as a predictor of the performance of Users' data. Time-stamped Delay and Loss measurements will be collected. Probes will be injected into the network at certain devices and sent to extracting devices which will return the measured information to the injection device.

The probes will be

a) UDP-echo based

b) Usable for the measurement of both delay and loss, preferably in both directions between two devices

c) Marked with the appropriate DiffServ QoS class preferably both in the header and body for each direction

d) Preferably transmitted at pseudo-random intervals (Poisson)

e) Time-stamped at injection and extraction devices

f) Preferably marked with source and destination addresses from address pools (to minimize impact of load-balancing)

g) Able to indicate a loss in confidence of local clock sync back to initiating device

h) Probe packets should be able to be marked with the appropriate MPLS labels if the underlying network uses MPLS technology.

A separate set of probes will be used for each of the IDQ network QoS classes. Probe packet size is selected to represent the majority of users' packets in each QoS class. The current recommendation is as follows:

Table 1

Network QoS Class	Description	Probe Payload Size (octets)
Class 0	Telephony	20
Class 2	Low latency data	256

Probe packet sizes for other QoS classes are given in Annex B. The use of a set of different sized probes may provide a better representation than the use of a single sized probe. For example, a repeating sequence of probes sized 128, 256, 256, 384, and 512.

Consideration of the pattern of inter-probe timing is important. The current recommendation is to use continuous probing with equal inter-probe timing varied by poisson distribution

The following segment metrics are derived from the probe delay, probe loss and probe timestamp measurements:

a) Mean delay

b) Minimum delay

c) Delay variation (90, 99 and 99.9 percentiles)

e) Unavailability

f) Loss Ratio

The mean inter-probe transmission period about which time the pseudo random offset varies, is determined by the number of measurement samples required for sufficient accuracy of delay percentiles. This will be referred to as the Probe Transmission Period (PTP). The PTP may be different for each QoS class and by default is 200 ms.

Measurement samples are aggregated over a period of time to be referred to as the Rollup Period (RP). The Rollup Period for all measurements will be 5 minutes.

The start of RP is synchronized among all participating SPs to Coordinated Universal Time and is based on the beginning of each UTC hour. Accuracy is derived from the Global Positioning System (GPS).

An estimated average probe rate of 1,500 probes per 5 minute rollup period is to be used for all percentiles and QoS classes. This includes an allowance of 1% for lost probes. The estimated probe rate will be validated before deployment since too low a choice impacts accuracy and too high a choice wastes resources.

Looking at the bandwidth consumption that each-way probing consumes, assume

- An average of 5 probe packets per second
- Measurements of 3 network QoS classes
- Using 64 byte probe packets

Each probe stream consumes 2,560bps, so for 3 QoS classes the total probe stream is 7,680bps. This is 0.015% of the total traffic of an OC-12/STM-4 link, 5 % of a T1 link or 4% of an E1 link

A typical CE having IDQ service would use two-way probing. Total probe stream traffic on the CE-PE link would be 15,360bps.

The bandwidth consumption within a backbone is dependent upon the number of probe streams. Purposes of different probes streams are described in section 7.3. Once a probing scheme has been designed, the evaluation of bandwidth consumption may occur.

7.2.1.1 Relationship to existing standards

The set of probes that are included in the calculations should only include those with correct headers. This differs from Y.1540 which includes probes with damaged headers (errored IP packet outcome). The reason for exclusion is due to the expectation that the DSCP fields will be used to indicate which set of measurements that probe should be included in. If for example, the DSCP field is corrupted but indicates a different valid QoS class, then the measurements generated by that probe would erroneously be included in the wrong calculation.

IDQ probe sampling preferably complies with IETF's RFC2330 suggestion of Poisson sampling intervals.

RFC 3432 suggests that rather than each sequential probe being varied around UTC time by a random time, that a sequence is started with a variation around UTC time and subsequent probes each keep the same offset from UTC.

7.2.2 Mean Delay

The Delay attributes of a network QoS class over a network segment are characterized by minimum delay, mean delay and a specific set of upper percentile delays. The percentile approach is used in preference to a standard deviation or variance model due to the frequent occurrence of bi-modal or multi-modal delay distributions.

In real networks, there are occasional events such as rerouting and momentary link outages that cause significant additional delays over and above the normal propagation and queuing delays. Packets that are delayed excessively are of little or no value to the application being supported and could be treated as lost packets, however the incremental value that doing so is not considered to be worth the additional complexity, therefore delay outliers will be included in the delay statistics.

The segment one-way mean delay is calculated as follows:

1) Collect measurements from N probes generated every probe transmission period PTP for Rollup Period RP
2) Discard all measurements from periods of unavailability
3) Mean delay = Sum(1..M) Measurements / M

Multi-segment mean delay is calculated by aggregating the mean delays of each segment mean delays through a simple summation.

Measurement samples from unavailability periods are not included in statistics

7.2.3 Delay Variation

Segment (one-way) Delay Variation (DV) is derived from the minimum delay and percentile. It is derived on a Rollup Period basis. For each segment,

DV = Percentile – Minimum

For specific percentiles,

DV99.9 = 99.9Percentile – Minimum

DV99 = 99Percentile – Minimum

DV90 = 90Percentile – Minimum

Multiple segment delay variations are used per network QoS class as follows:

Table 2

DV	Most stringent QoS Class	Mid-level stringency QoS Class	Least stringent QoS Class
DV99.9	x		
DV99	x	x	
DV90	x	x	x

Segment one-way delay percentiles are calculated as follows:

1) Collect measurements from N probes generated every probe transmission period PTP for Rollup Period RP
2) Discard all measurements from periods of unavailability leaving M samples
3) Stack rank the measurement set
4) Discard the top D measurements (D = Round((100 – Percentile) x M))
5) Percentile = delay value of top remaining sample

Multi-segment delay variation is calculated by aggregating the delay variations of each segment through a provisional method defined in Y.1541. It is also derived on a Rollup Period basis

Since minimum delay and percentiles from unavailability periods are not included in statistics, derived DVs are also not included from unavailability periods.

7.2.4 Packet Loss

Segment (one-way) Packet Loss (PL) is measured over the same period as delay. It is derived on a Rollup Period basis. Segment Packet Loss is the number of probes whose measured one way delay was >= DETL (NDETL) and those that never made it to their destination, or missing (MSNG)

PL = (NDETL + MSNG)

Packet Loss Ratio (PLR) is Packet Loss divided by the number of Transmitted Packets (N)

PLR = PL / N = (NDETL + MSNG) / N

Measurements from unavailability periods are not included in packet loss statistics. Both the number of lost packets and the number of transmitted packets are reduced accordingly. This process avoids the packet loss ratios being unduly impacted by network unavailability.

To combine these to produce a multi-segment packet loss ratio, called the Aggregate Loss Ratio (ALR), the following method is used.

ALR = 1 – (1 – PLR for segment 1) x (1 – PLR for segment 2) x (1 – PLR for segment 3)

ALR is derived for each Rollup Period.

7.2.5 Path Unavailability

Unavailability is significant when a human observer detects a business impacting application failure due to network loss. For a typical application such as telephony and a network is considered unavailable by the user if there is an inability to connect, or a connection is lost. The measurement of unavailability attempts to approximate this view by detecting periods during which would have noticeable impacts on applications.

Unavailability is derived on a per QoS class, per direction basis, from one-way packet loss measurements. See the previous section where packet loss is defined. The period of Unavailability is defined as follows:

1) The starting point for a period of network unavailability is when a packet is lost and during a subsequent sliding probe window of SPW probes, a total of at least PLS probes are lost. The period of the sliding probe window is hence counted as unavailable.

2) The ending point of a period of path unavailability is when the total number of packets lost during SPW successive probes falls below PLE. The period of these probes is counted as available and hence the unavailability ends with the first of these successfully delivered packets.

where the starting and ending criteria described are measured by transmit probe timestamps

The sliding probe window size (SPW) and number of probes lost (PL) to start or end the period of unavailability may vary per class. The current default recommendation is as follows:

Table 3

Path Unavailability Parameter	Default values
Probes lost to Start (PLS)	25
Probes lost to End (PLE)	5
Window size (SPW)	50

Note that since the sliding window crosses Rollup Period boundaries, there are cases when inter-provider reports at the end of each Rollup Period may indicate no periods of unavailability for that Rollup Period, but the next Rollup Period report will retroactively report that the previous period included unavailability."

As an example, using the above definition and values, Figure 1 shows how unavailability is derived from packet loss results of outbound active probes.

In order to calculate one-way unavailability, the absence of a one-way delay measurement must be understood to be due to an outbound loss rather than an inbound loss.

In the figure above, the time indicated is the initiating device's probe transmission time. Assuming that no delay result indicates an outbound loss, we determine that the segment was unavailable for 4.79 seconds between 14:10:30.755 and 14:10:35.545

Delay and loss measurements and their derived metrics are ignored for a segment for the duration of its unavailability.

For each segment, unavailability is calculated by summing the periods of unavailability during all Rollup Periods.

Multi-segment unavailability is calculated by summing the periods of each segment's unavailability. (This will overestimate the actual unavailability when unavailability occurs simultaneously in different segments).

Time in hours and minutes	Time in seconds	One-way delay (mS)
14:10	30.755	**Lost probe 1**
14:10	30.955	**Lost probe 2**
14:10	31.155	**Lost probe 3**
14:10	31.355	**Lost probe 4**
14:10	31.555	**Lost probe 5**
14:10	31.755	**Lost probe 6**
14:10	31.950	**Lost probe 7**
14:10	32.165	**Lost probe 8**
14:10	32.345	**Lost probe 9**
14:10	32.550	**Lost probe 10**
14:10	32.745	**Lost probe 11**
14:10	32.965	**Lost probe 12**
14:10	33.155	**Lost probe 13**
14:10	33.355	**Lost probe 14**
14:10	33.525	**Lost probe 15**
14:10	33.735	**Lost probe 16**
14:10	33.955	**Lost probe 17**
14:10	34.145	**Lost probe 18**
14:10	34.350	**Lost probe 19**
14:10	34.555	**Lost probe 20**
14:10	34.755	**Lost probe 21**
14:10	34.925	**Lost probe 22**
14:10	35.135	**Lost probe 23**
14:10	35.355	**Lost probe 24**
14:10	35.545	**Lost probe 25**
14:10	35.750	**Lost probe 26**
14:10	35.955	**Lost probe 27**
14:10	36.155	**Lost probe 28**
14:10	36.355	**Lost probe 29**
14:10	36.555	290
14:10	36.755	300
14:10	36.955	290
14:10	37.155	290
14:10	37.350	290
14:10	37.565	290
14:10	37.745	310
14:10	37.950	301
14:10	38.145	301
14:10	38.365	310
14:10	38.555	305
14:10	38.755	305
14:10	38.925	310
14:10	39.135	305
14:10	39.355	302
14:10	39.545	301
14:10	39.750	310
14:10	39.955	301
14:10	40.155	310
14:10	40.325	305
14:10	40.535	305
14:10	40.755	310
14:10	40.945	305
14:10	41.150	302
14:10	41.335	301
14:10	41.555	310
14:10	41.745	305
14:10	41.950	302
14:10	42.155	304
14:10	42.355	320
14:10	42.525	309
14:10	42.735	300
14:10	42.955	310
14:10	43.145	305
14:10	43.353	302
14:10	43.555	310
14:10	43.745	305
14:10	43.953	302
14:10	44.135	301
14:10	44.355	310
14:10	44.545	305
14:10	44.750	302
14:10	44.955	304
14:10	45.155	320
14:10	45.325	309
14:10	45.535	300
14:10	45.755	310
14:10	45.945	305

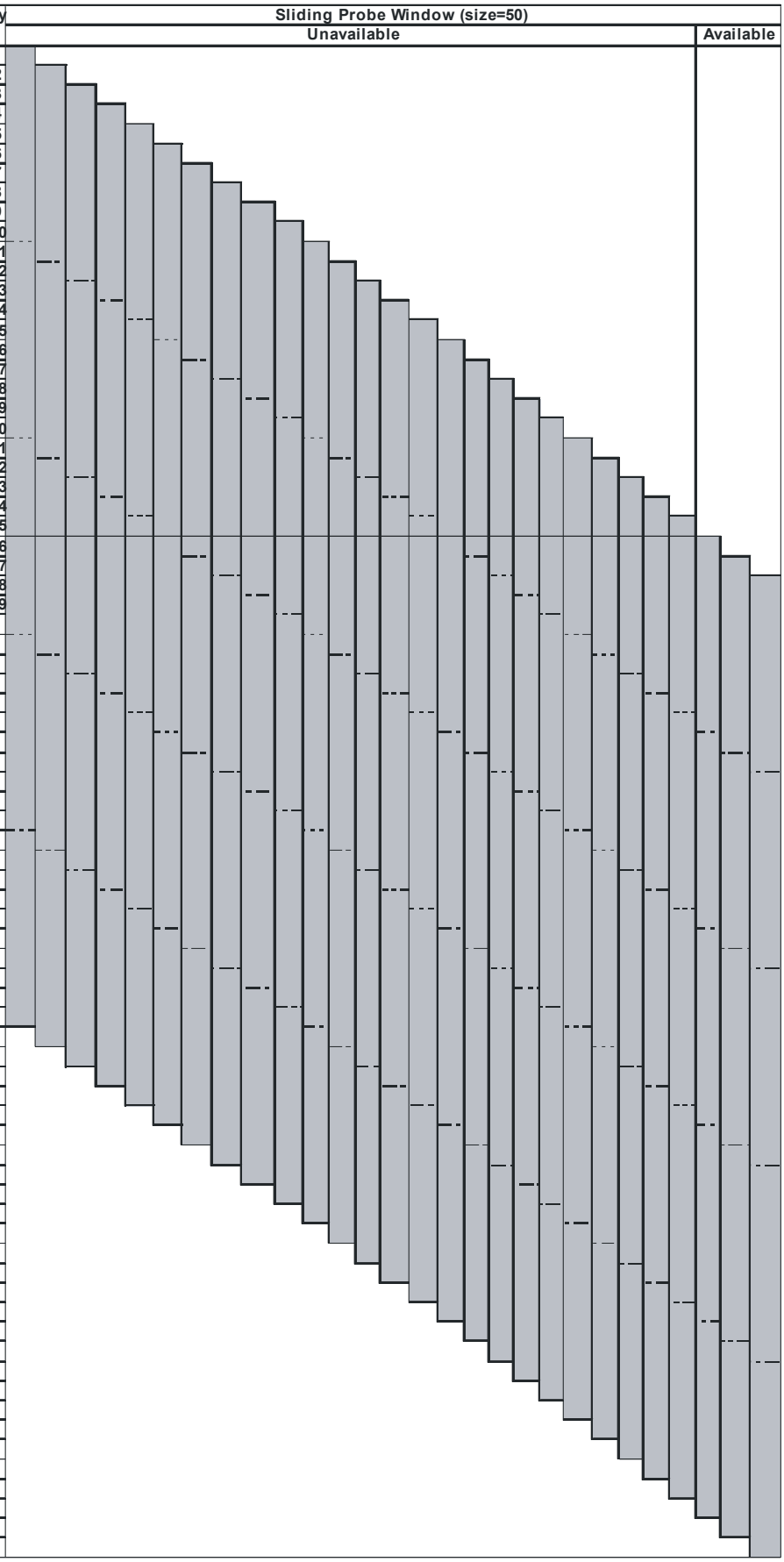


Figure 1 – Unavailability Derived From Packet Loss Results of Active Probes.

7.2.6 Measurement System Unavailability

If parts of the measurement system itself are unavailable, that will inhibit the ability of the provider to demonstrate that his QoS targets have been met during the period of unavailability. However, it is almost certainly not as serious for the measurement system to be unavailable as for the IDQ service itself to be unavailable as defined above. We therefore suggest that while unavailability of the measurement system should be tracked, it should not be automatically treated as equivalent to unavailability of the service. In the event that a customer claims that an SLA target was violated during some measurement interval, the provider would normally have measurement data to show how his segment of the network was performing at that time. If the provider cannot produce data to show that SLA targets were being met because his measurement system was not operational during that interval, he may have no choice but to assume that he did in fact violate the SLA. Thus providers will be highly motivated to keep their measurement systems operational all the time but will not automatically be penalized for measurement system outages.

7.2.7 Interaction of Policing and Performance Measurement

Ingress and egress segment performance is sensitive to the level of customer traffic. The performance levels of each IDQ network QoS class can only be delivered assuming that the traffic is within the subscription bounds for that QoS class.

In the event that traffic does exceed its subscription bounds, packets may be delayed, discarded or have their DSCP remarked. These actions will potentially change the delay and loss characteristics of the data streams as well as any UDP echo probes that traverse the policing point. There is no failsafe mechanism to detect which UDP echo probes are impacted by a policing event.

To handle the interaction between policing and performance measurement, Inter Domain QoS discounts measurements taken during a period when there is a policing-detected violation for that QoS class.

The determination of when policing-detected violations occur for a network QoS class is made through SNMP polling of the DIFFSERV-MIB. The DIFFSERV-MIB keeps a counter of any policing-detected violation in each QoS class and by comparing the counters at the start and end of the Policing Window (PW); the determination is made whether any policing-detected violations occurred.

The Policing Window (PW) is the periodic rate at which SNMP polling takes place and by default is 5 minutes for each QoS class.

If a policing-detected violation occurs for a QoS class during a policing window, the delay, loss and availability statistics for that rollup period are not used. Instead the list of these rollup periods, and the associated number of packets that exceeded the agreement for each QoS class is kept. These details and an aggregate of the total time and total exceeding packet count are reported to customers.

This method encourages the customers to subscribe to the appropriate level of bandwidth in order to ensure that their QoS class characteristics are maintained at all times.

Policing-detected violations between SPs **will similarly be detected and reported each rollup period**

7.3 Measurement Network Model

Ideally measurements to assure performance of customer traffic would be taken between the same endpoints as each customer's traffic. Whether these endpoints are the customer's terminal (TE), customer edge router (CE) or provider edge router (PE), the number of measurements would be so great as to make this impracticable. Therefore we look to a practical solution and find one by segmenting the network into a measurement network model.

Segmenting a network is a trade-off between the following requirements.

- Minimize cost
- Support service flexibility
- Accurate end-to-end measurements
- Support measurement comparison to each provider's impairment target

Costs associated with each segment include (assuming one-way active probing):

- Clock synchronization at each segment end
- Initiation and response of probes at respective segment ends.
- Associated measurement data which needs retrieval, storage and distribution
- Contribution to concatenation error

The greater the leverage of a single measurement produced by a segment probe, the fewer probes will be needed. If fewer segment measurements may be used in the calculations of thousands of concatenated estimates, then there will be lower total probe overhead.

Providers offer assured delivery services between different endpoints. We use the shorthand terminology.

1) "Edge-Edge" for services that extend to the edge of a provider's network
2) "Site-Site" for services that extend to the edge of a customer's premises. (This is sometimes called end-to-end)
3) "TE-TE" for a managed customer network service, we will consider this as extending to a customer's terminal

All three services must be supported by the models. There is no requirement that both endpoints have similar services (i.e. demarcation points). This terminology is used to emphasize the distinction in endpoints. Network segmentation provides service differentiation opportunities to providers, who may offer assured delivery and reporting for a subset of segments.

The models must support measurements which will enable comparison of measured performance to impairment targets. Measurement points located at CE or PE locations may use capabilities of the CE or PE routers themselves or separate co-located measurement equipment.

7.3.1 Network Partitioning

The network is partitioned into segments, each is monitored independently. This partitioning enables the scaling of the network with sub-linear growth in the amount of monitoring traffic and equipment relative to the number of customer sites involved.

Typically, the network is considered to consist of ingress and egress access segments, and a transit segment. It is assumed that one regional Service Provider will provide an access network that supports both ingress and egress segments for a specific site. There may be backbone Service Provider(s) providing transit services between the regional Service Providers.

A specific Service Provider may act as either or both an access provider for some traffic and as a transit provider for some traffic. A demarcation point between access and transit segments is named a "Demarcation POP" (DP).

Demarcation points at the customer end of the ingress and egress segments are dependent upon the service.

- For "Edge-Edge" services, demarcation points are typically PEs.
- For "Site-Site" services, demarcation points are typically managed CEs.
- For "TE-TE" services, demarcation points are typically customer's terminals.

These demarcation points are illustrated in the following figures 2, 3 and 4, where the models are named "Edge-Edge", "Site-Site" and "TE-TE".

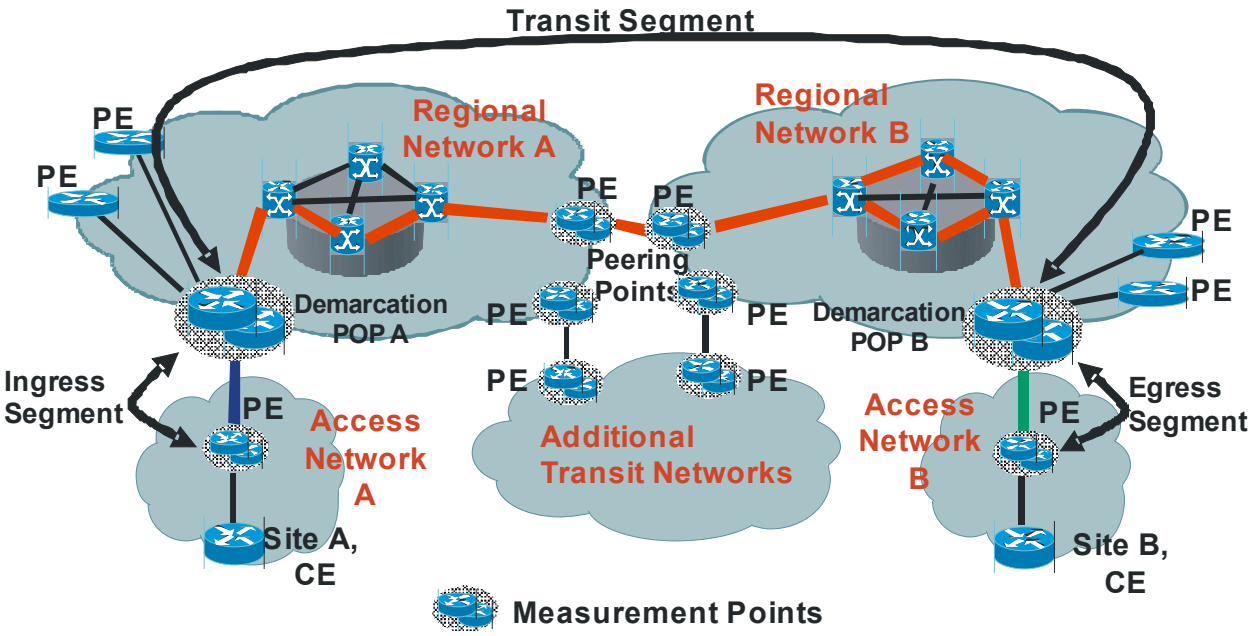


Figure 2 – Edge-Edge Model

In the Edge-Edge model, delivery is assured to a PE nearest a customer, service between customer terminals or CE to the PE is not assured. The assured performance characteristics of the network are comprised of the aggregate of the performance characteristics of the ingress, transit and egress segments.

The ingress and egress segments do not include the CE-PE link, but do include the Provider Edge router as well as regional switching and transport.

The Transit segment is measured from Demarcation POP of the ingress Regional Service Provider to the Demarcation POP of the egress Regional Service Provider. This segment may or may not include separate Backbone Service Providers. The transit segment may span a city, country/state, continent or multiple continents.

The transit segment may include parts of the ingress and egress Regional networks, interconnects between the regional and backbone providers, and transit service across any Backbone networks. The transit service of the Backbone network is a sub-segment of the entire transit service.

The models support multiple peering connections between providers. Only one is shown for simplicity. The models support Equal Cost MultiPath (ECMP) as indicated by the multiple paths shown within providers. In many instances, there may be multiple paths over which traffic may traverse. By having probes follow a plurality of paths, performance contributions from each path will be included in the reported statistics. Covering this path diversity as part of the measurement is achieved by using a range of addresses for each Demarcation POP. Each of which will be configured to respond to probes sent to any of 16 addresses and will be able to send probes sourced from any of 16 addresses. This will support a total of 256 flows which increases the likelihood that in the case of load balancing, active probes will follow all the paths that Customer's data follows between 2 sites.

Since there is limited load balancing expected between CE or PE and the Demarcation POP, the CE/PE need only have one address, which in combination with the 16 addresses of the DP's measurement device will

provide sufficient route diversity to include measurement contributions from all load balanced paths. If the CE/PE is configured to probe across the transit segment then 16 addresses would be preferable.

This approach to ECMP emphasizes coverage of all the paths that can be seen. A future approach may be able to conduct measurements on a subset of paths which match particular users' traffic.

The ingress, transit and egress segments are monitored from Demarcation POPs that are specifically located for the role. Demarcation POP selection is an SP choice. Each customer site is assigned to a Demarcation POP within its Regional Provider's network. The POP is selected on the basis that the majority of the traffic from that site to others, goes through this specific POP, which is within the same geographic region as the customer site. There is a minimum number based on the location of customer sites. SPs may increase the number of measurement POPs as they see fit and some SPs may elect to make every PE POP a measurement POP.

The Demarcation POP will have one or more measurement systems. It will monitor the backbone network and initiate tests with PE and CE devices. Thus it will be capable of measuring Ingress, Egress and Transit segment performance. It will also collect and collate all necessary statistics.

Inter Domain QoS relies on the ability to collect inter-Service Provider statistics on a continuous basis and for Service Providers to be able to resolve the causes of performance targets not being met. To support this monitoring and troubleshooting requirement there are a set of requirements that must be met by Service Providers:

- Each provider must provide Measurement Points that act as performance characteristic test points for their use, and for restricted use by other SPs.
- Measurement Points must be located at any major Service Provider interconnection peering POP
- There must be a Measurement Point (Demarcation POP) nominated by Regional Providers for each customer site.
- A service dependent measurement point at PE, CE and/or Customer TE.

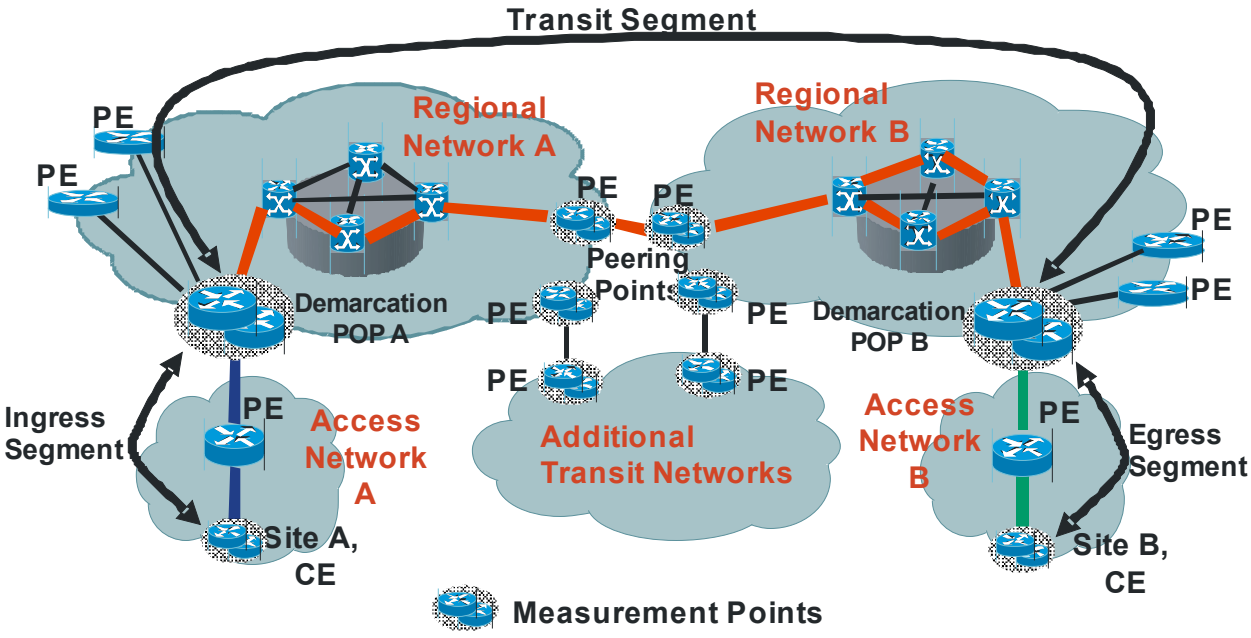


Figure 3 – Site-Site Model

In the Site-Site model, delivery is assured to customer CE, service between customer terminals to the CE is not assured by the Service Provider. It is the responsibility of the customer. The assured performance characteristics of the network are comprised of the aggregate of the performance characteristics of the ingress, transit and egress segments.

The ingress and egress segments include an access segment (DSL, Cable, SONET/SDH, and Ethernet etc) including the Customers Edge (CE) router as well as regional switching and transport.

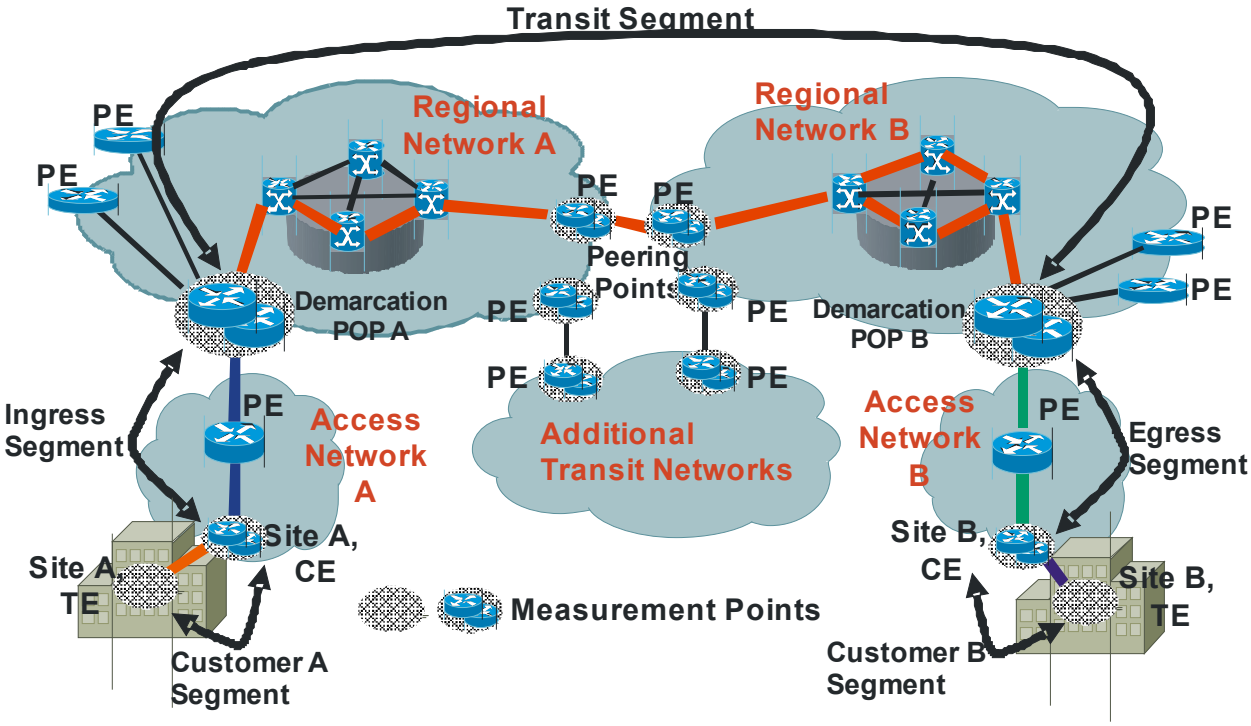


Figure 4 – TE-TE Model

In the TE-TE model, the assured performance characteristics of the network are comprised of the aggregate of the performance characteristics of the ingress, transit, egress and Customer segments.

The Customer segment includes the network between a CE and a Customer's TE. This may include home networking arrangements to company LANs, computers and appliances.

Selection of the customer's TEs to be used for measurements include considerations of

1) Stability
   a) Static address or directory lookup
   b) Stationary rather than mobile
   c) Always online
2) Performance
   a) Probe response not impacted by other programs
3) Clock Synchronization
   a) Required for one way delay and delay percentile measurements
4) Representativeness of many other TEs

a) Analysis or measurement may show that measurements between a CE and a particular TE is representative of many other TEs. Call these "Landmark" TEs.

5) Number of TEs probed

a) To minimize the number of probes, a minimum number of Landmark TEs should be used.

b) To minimize the complexity of data handling and reporting, a minimum number of Landmark TEs should be used.

Communication from a CE to a TE may require NAT traversal. Depending upon the administration of these devices pre-provisioning or NAT traversal protocols may need to be used. Alternatively, the NAT device may be used as a measurement point as a proxy for TEs.

It is expected that there will be cases when there will be very little performance variation in the Customer's network. In these cases, instead of the use of operating measurements, fixed impairment values may be agreed to.

7.3.2 Applied Measurements

Measurement purposes fall into three broad categories, **Operating**, **Supporting** and **Testing**.

- **Operating** measurements are those which are made on an ongoing basis between Measurement Points, to monitor normal operation of the assured segments along customers' data paths. E.g. measurements of Ingress, Transit and Egress segments
- **Supporting** measurements which may be taken continuously are used to provide information for SPs. These measurements occur in addition to Operating measurements and can be between various Measurement Points. E.g. measurements of each SPs' contribution to the Transit segment.
- **Testing** measurements are made on an exception basis following the detection of abnormal operating measurements for troubleshooting or to test a new path. These measurements occur in addition to Operating or Supporting measurements and are between Measurement Points which do not have Operating or Supporting measurements being taken. E.g. measurement of a particular CE to CE path for a prospective customer.

Some measurements may fall into multiple classes. For example, a CE-CE measurement may be used for a prospective customer (testing), as a sanity check for providers (supporting), or as a premium (un-scalable) customer service (operating).

Different views of the same measurement data may be useful for different purposes. For example, a provider that collects and analyses ongoing measurements at sub-intervals of RP may evaluate the impact of remedial action upon network performance more quickly, than had they waited for the RP before doing so.

The following scenarios show how the performance measurement techniques from section 7.2 may be applied to the measurement network models. The flexibility of the models support more applied measurements than those described here.

In the following scenarios, the measurement information exchanged among providers every rollup period includes the following:

1) Minimum delay
2) Mean delay
3) High delay percentiles
4) Loss Ratio
5) Unavailability period info
6) Miscellaneous info

7.3.2.1 Operating Measurements Scenario

The Site-Site Operating Measurement scenario is shown below in Figure 5, where the endpoints are CEs.

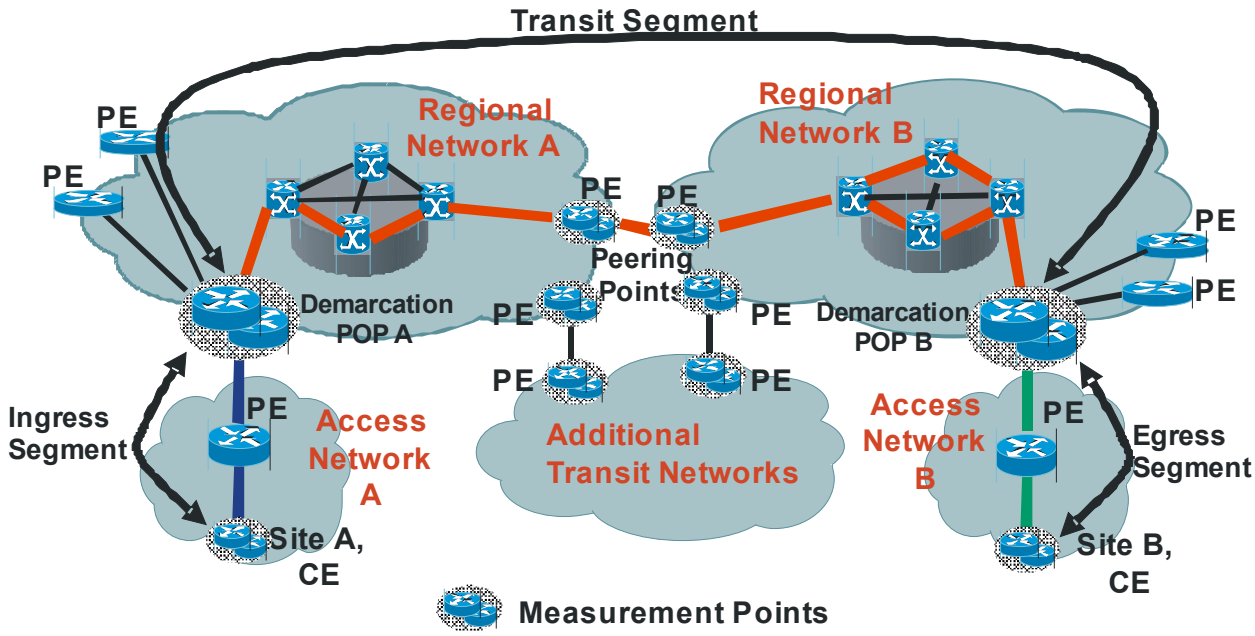


Figure 5 – Site-Site Operating Measurement

Figure 5 represents two connected Service Providers, A and B, each having regional and access networks to which end Customers have managed CEs. The following operating measurements are required to estimate the site-to-site performance being delivered for customer site A.

1) SP A initiates measurements between
   a) DP A and Site A CE, and
   b) DP A and DP B
2) SP B initiates measurements between
   a) DP B and Site B CE
3) SP A retrieves results of measurements between
   a) DP B and Site B CE from SP B.
4) SP A compares the aggregated metric of the 3 segments to the guarantee and provides a report to Site A customer

The supporting measurements for the above service are detailed in Figure 8.

The Edge-Edge Operating Measurement scenario is shown below in Figure 6, where the endpoints are PEs.

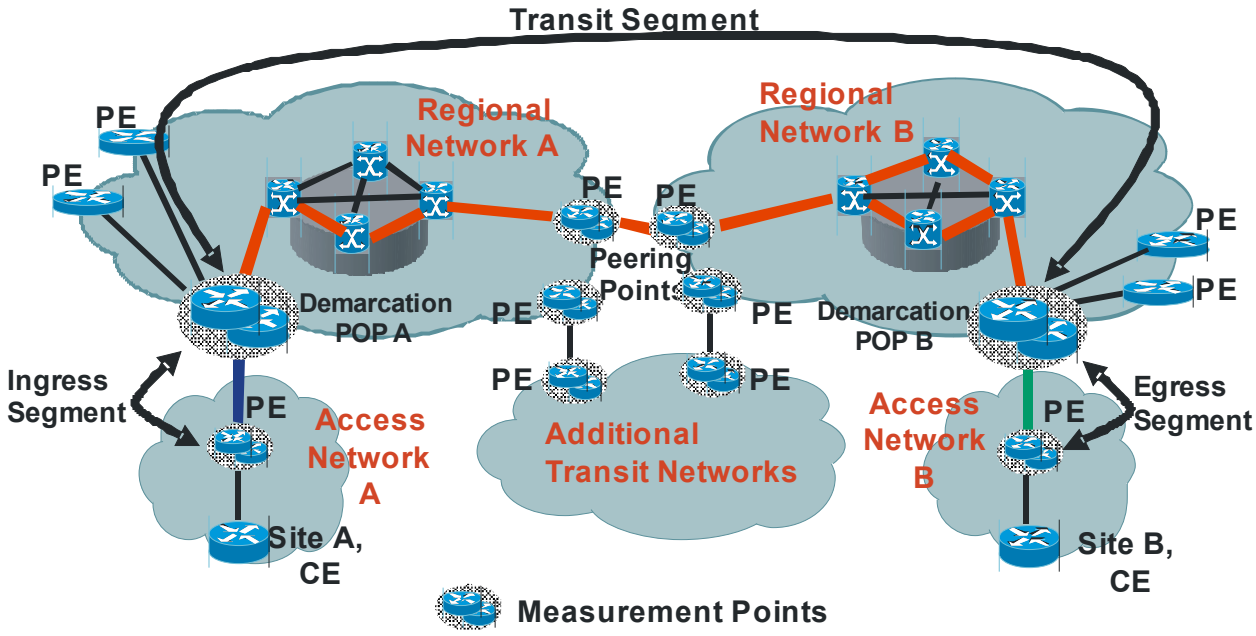


Figure 6 – Edge-Edge Operating Measurement

Similarly to Figure 5, the following operating measurements are required to estimate the edge-to-edge performance being delivered for customer site A. Note that the only difference to Figure 5 is the use of PEs versus the use of CEs.

1) SP A initiates measurements between
   a) DP A and Site A PE, and
   b) DP A and DP B
2) SP B initiates measurements between
   a) DP B and Site B PE
3) SP A retrieves results of measurements between
   a) DP B and Site B PE from SP B.
4) SP A compares the aggregated metric of the 3 segments to the guarantee and provides a report to Site A customer

The supporting measurements are similar to those shown in Figure 8.

The TE-TE Operating Measurement scenario is shown below in Figure 7, where the endpoints are TEs

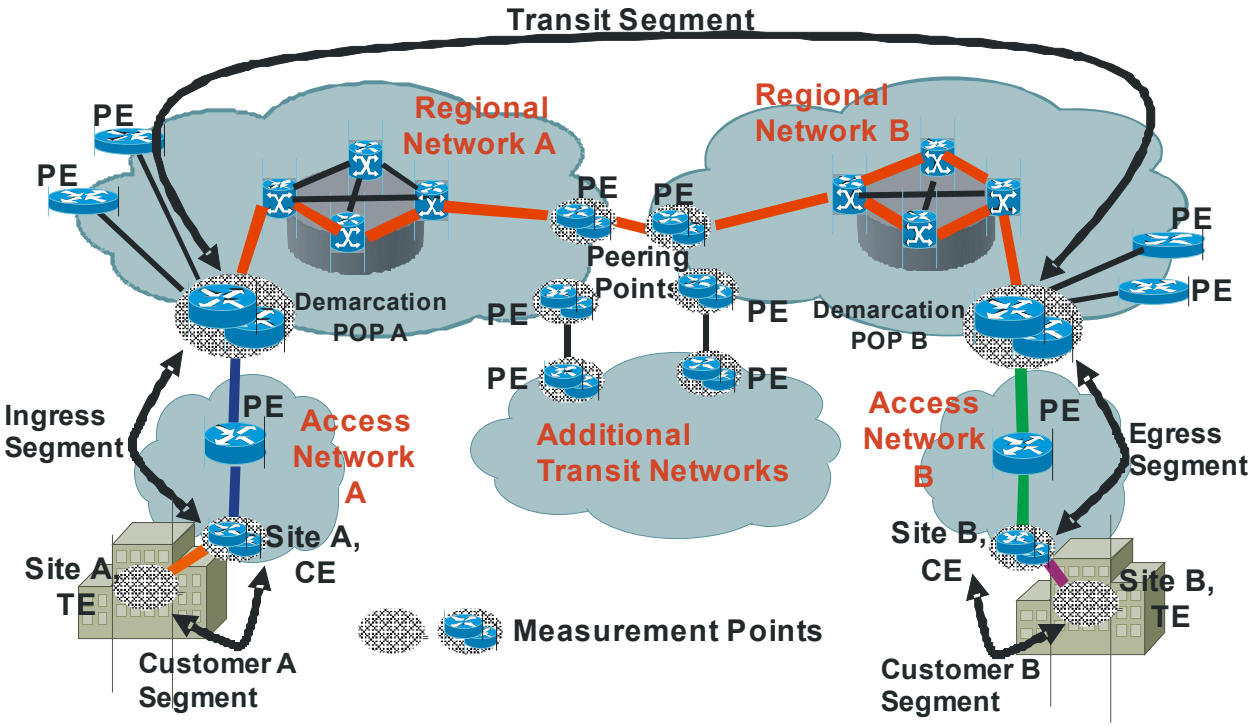


Figure 7 – TE-TE Operating Measurement

Similarly to Figure 5, the following operating measurements are required to estimate the TE-to-TE performance being delivered for customer A. Note that the only difference to Figure 5 is the addition of CE-TE measurements and the retrieval of those measurements from SP B.

1) SP A initiates measurements between
   a) DP A and Site A CE
   b) Site A CE and Site A TE
   c) DP A and DP B
2) SP B initiates measurements between
   a) DP B and Site B CE
   b) Site B CE and Site B TE
3) SP A retrieves results of measurements from SP B for measurements between
   a) DP B and Site B CE
   b) Site B CE and Site B TE
4) SP A compares the aggregated metric of the 5 segments to the guarantee and provides a report to Site A customer

This scenario assumes a single TE, measurements with multiple TEs may be supported.

7.3.2.2 Supporting Measurements Scenario

To provide measurements for purposes in the support category, SPs may choose to perform measurement across their network to key Measurement Points in other cities/regions of their networks. SPs may choose the

mechanism used for internal support measurements, which may be the same as used for operating measurements. It is recommended, however, that each SP implement sufficient support tools to enable resolution of performance issues within their networks.

In many cases, the sending and receiving customer sites will be connected to the same regional Service Provider. To support these cases, the regional Service Provider is fully responsible for the transit segment of the network and should perform the appropriate measurement functions.

The transit segment of the network will often comprise of two Regional SPs and one Backbone SP and their interconnections. Each of these Service Providers should enable resolution of performance issues that may occur. This resolution process will include monitoring of specific sections of the transit segment. The collection of these statistics is part of the support process.

An SP should measure performance to each neighboring POP of the other directly connected Regional SPs and Backbone SPs. This enables issue resolution of the interconnect performance and dimensioning as opposed to the network performance of the neighboring SPs. In some cases, the interconnects may be through Peering Points with more complex performance characteristics and in other cases, high speed SONET/SDH interconnect may be used. The interconnect egress performance and dimensioning is the responsibility of the Regional SP that the customer connects to. In the case of a Regional SP interconnect to a backbone SP, the performance and dimensioning of both directions through the interconnect is the responsibility of the Regional SP. The backbone SP may supply services that simplify this process and ensure performance targets are met.

In Figure 8 below, SP A and B each measure their own contribution to the transit segment, and may allow other interconnected SPs to retrieve those measurements. In this case, SP A and SP B each includes in their measurements, one direction through the interconnect. SP A may retrieve the measurements of SP B's contribution to the transit segment.

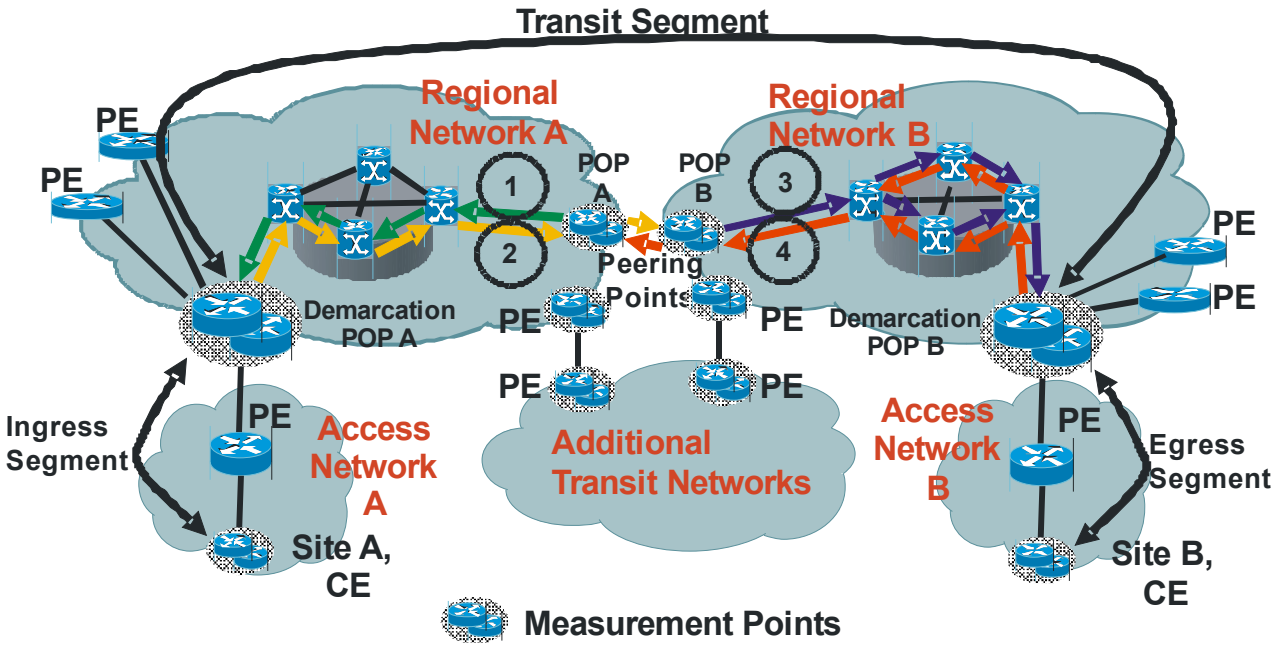


Figure 8 – Site-Site Supporting Measurements

In this scenario, assume that each SP is responsible for performance assurance of their egress traffic over peering point links.

In order to obtain supporting measurements for the customer service indicated in Figures 5 and 6, the following activities would be performed as indicated above in Figure 8:

1) SP A initiates measurements between DP A and its Peering Point POP A, for the direction from Peering Point POP A to DP A.
2) SP A initiates measurements between DP A and Network B Peering Point POP, for the direction DP A to Peering Point POP B.
3) SP B initiates measurements between DP B and its Peering Point POP B, for the direction from Peering Point POP B to DP B.
4) SP B initiates measurements between DP B and Network A Peering Point POP, for the direction from DP B to Peering Point POP A.

In addition to this data being used for a SP to confirm its own transit performance, if these measurements are concatenatable:

- If aggregated with DP-CE measurements it is an estimator of a SP's total CE-Peering point performance.
- This data may be exchanged with partner SPs to provide assurance, and if aggregated with other supporting measurements, may be used as a sanity check for operating measurements.

Note that in Figure 8, four additional supporting measurements are required, 2 for each SP's part of the transit segment. Further addition of IDQ services across this network would not require additional transit segment measurements but would re-use the results of these measurements. Extension of the model in Figure 8 to include more SPs would require additional supporting measurement of that SPs' transit segment.

The description for supporting measurements above is for the case where each SP is responsible for its egress traffic over a single peering link. Similar scenarios may be used in the case of:

1) Dual links (in parallel) where each provider pays for one of the links, and both links are actively used
2) 3rd party Internet Exchange Point

7.3.2.3 Test Measurements Scenario

Information useful for troubleshooting or prospective customers may require additional measurements.

In Figure 9, SP A or SP B initiates measurements between major global POPs named Metropolis POP and BoomTown POP and publishes them in a report. This report indicates whether the transit performance targets are being met for a significant set of destinations and approximates the expected performance for nearby POPs. This is useful for SP A and SP B as a basis for offering prospective service to customers who connect through or close to the Metropolis and BoomTown POPs.

SP A may wish to initiate measurement between DP A and the Metropolis measurement POP. This may be useful for SP A as a basis for offering prospective service to customers who connect both source and destination CEs to SP A's network.

Measurements from each Demarcation POP to a significant set of high profile, global Measurement POPs of multiple SPs may occur for similar purposes. This set of measurements characterizes the transit segment of the network for a representative set of customer traffic flows. The selected Global POPs should cover all major cities and continents and include many other Service Providers. It is expected that a minimum of 50 Global POPs would be monitored from each Demarcation POP.

In some cases, a customer may not be satisfied that any of the chosen set of Global Measurement POPs is sufficient to characterize a specific transit segment. At a customer's request, an SP may initiate measurements between the customer's DP and a set of selected POPs. This would normally be viewed as a custom service. Along with custom end-points, additional statistics and reports could be provided.

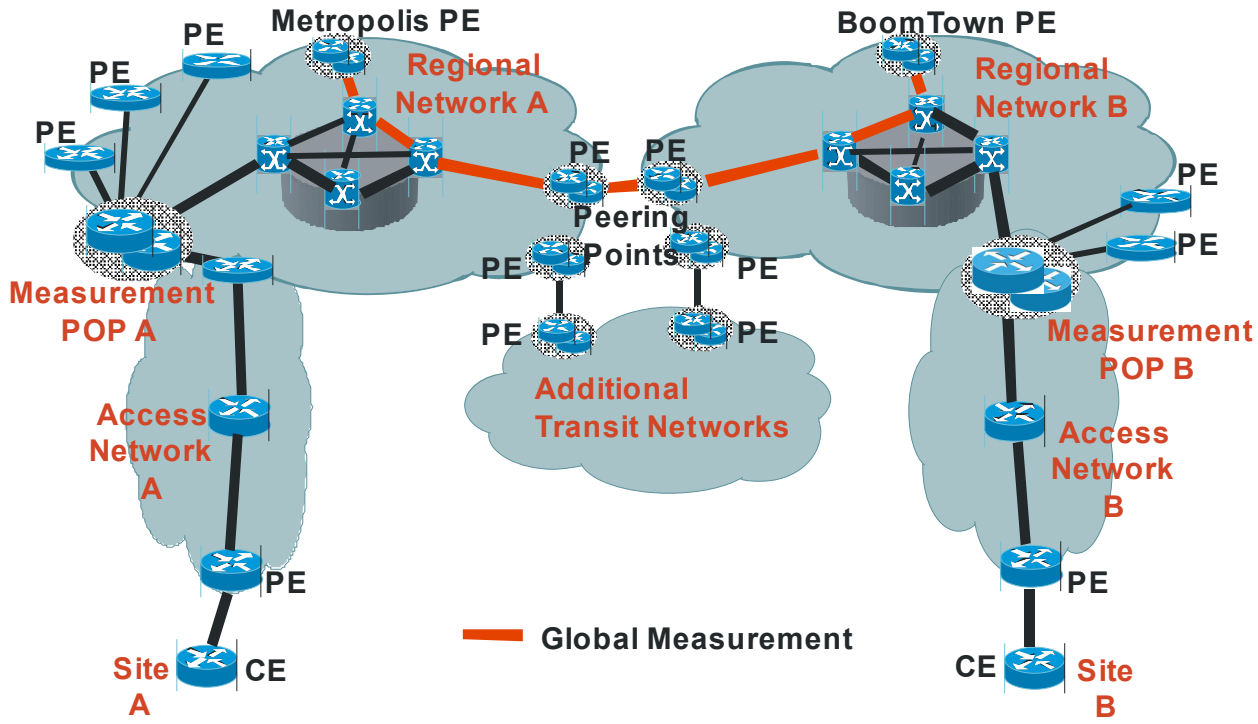


Figure 9 – Global-Global Measurements

7.4 Clock Synchronization

Clock synchronization, specifies the extent to which multiple clocks agree on the time.

It impacts

1) Common understanding of when a measurement or event occurred or is planned to occur.

2) The accuracy of certain network performance measurements

The magnitude of time offset between measurement points is critical to the accuracy of the one way measurement attributes of Minimum delay, Mean delay and Delay Percentile. The attributes of Delay Variation and Loss are unaffected by offset magnitude. Unavailability is unaffected although there may be minor inaccuracies in the reported time of occurrence.

The measurement points per the network models can be grouped into three categories

1) Demarcation and Peering measurement points

2) CE and PE measurement points

3) Customer host measurement points

We allocate a maximum offset to each category:

1) The clock of Demarcation and Peering measurement points can have an offset from GPS of no more than 100uS magnitude

2) The clock of the CE router, PE router or co-located non-router measurement device can have an offset from its paired Demarcation measurement point of no more than 1mS magnitude

3) The clock of certain customer host measurement points can have an offset from its paired CE router of no more than 1mS magnitude

If a PE is also a Demarcation Point then the tighter offset is to be applied.

Providing clock synchronization at these points supports the measurements described in section 7.3

Figure 10 shows these three categories and where the specified offsets apply.

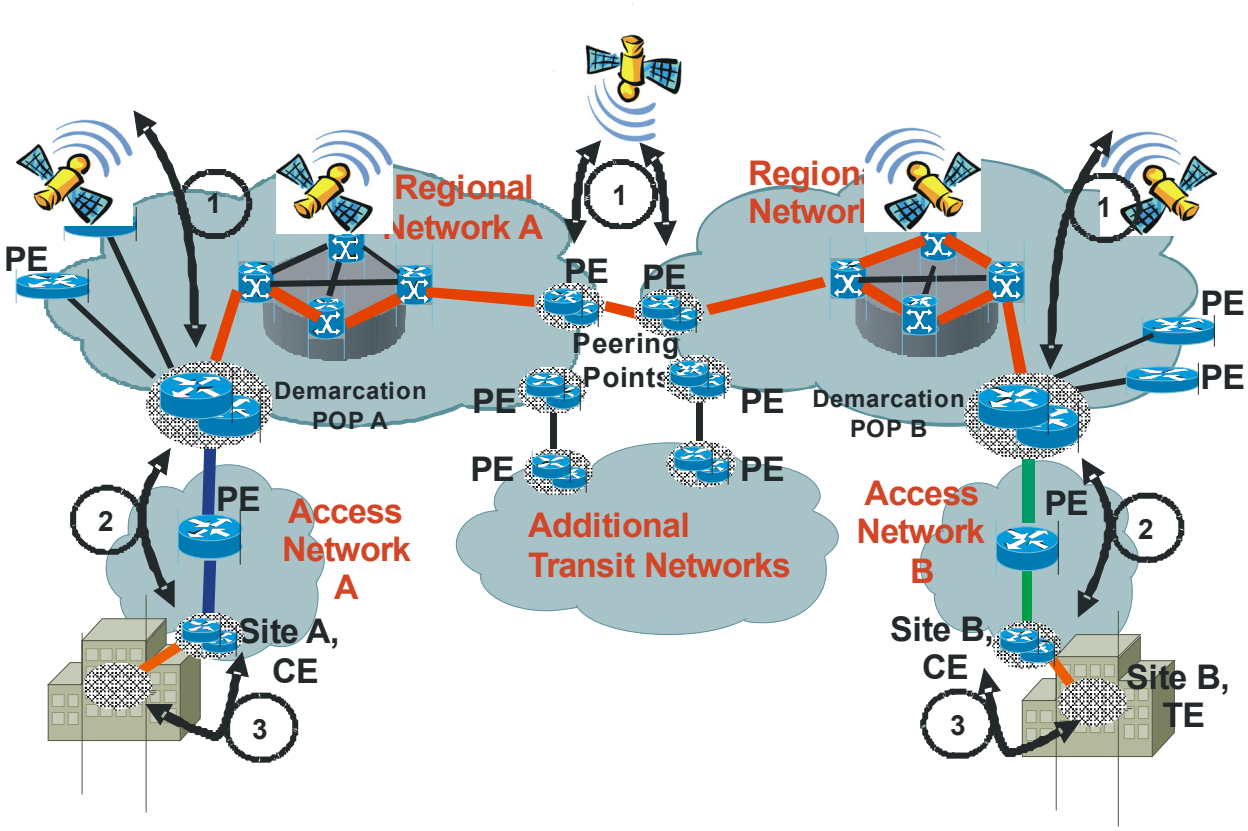


Figure 10 – Three Categories of Equipment Which Offset Maximums Apply To

7.4.1 Relationship to existing standards

Informational RFC2330 describes clock terminology and wire time.

We use the term “Synchronization” per RFC 2679. Synchronization measures the extent to which two clocks agree on what time it is. RFC2679 loosely maps the IPPM group’s terminology to ITU-T’s terminology (e.g. G.810, "Definitions and terminology for synchronization networks" and I.356, "B-ISDN ATM layer cell transfer performance"). It analyzes measurement errors.

RFC3393 discusses the minimal impact of clock synchronization on differential measurements, of which Delay Variation is an example.

7.4.2 Implementation methods

GPS is used as a reference; however other implementation methods (e.g. Galileo, GLONASS) may be used to synchronize Demarcation and Peering points as long as the offset to GPS requirements are met. In cases of inadequate reception the use of pseudolites or other techniques to provide accurate clock derived from GPS may be required.

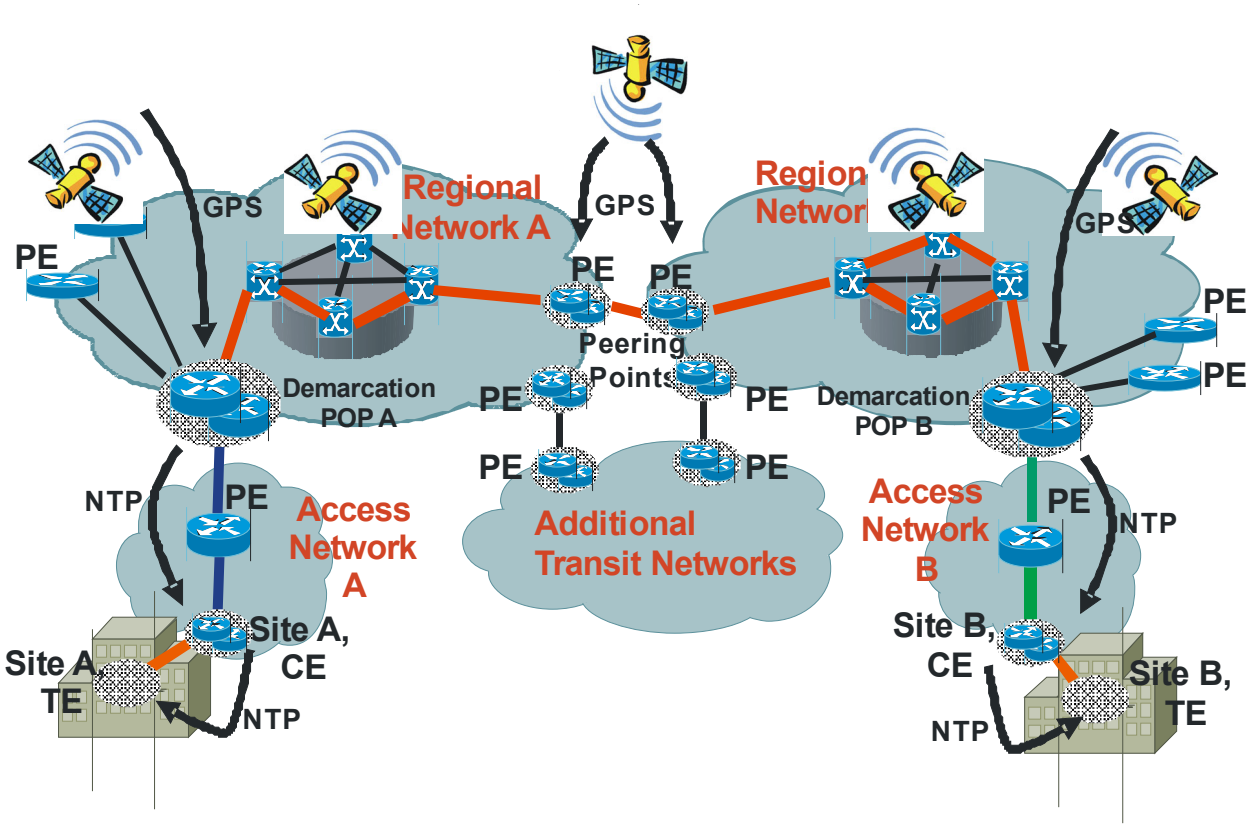


Figure 11 – Example of Clock Synchronization Implementation

Figure 11 shows an example clock synchronization configuration for a TE-TE scenario, where

1) GPS receivers are used to set the time of shadow routers at both Demarcation POPs

2) NTP is used to set the time at the CEs which are NTP clients using a Demarcation POP's shadow router as an NTP server.

3) NTP is used to set the time at selected customer hosts which are NTP clients using the CE as an NTP server.

CE clock synchronization should be via NTP to the SP's closest GPS system as client. This may not be their associated Demarcation POP. Since NTP offset from client to server is a function of delay asymmetry between client and server, using NTP in some cases may not meet the clock synchronization offset requirements, in which case alternatives must be found.

CE routers may be used to provide multi-homed IDQ service from single or multiple SPs. In any case, clock synchronization should be set using "prefer" via NTP from the closest Measurement POP. It will automatically switch upon loss of synchronization.

This document does not address how SPs may set up GPS and NTP to meet these requirements, nor how to validate the offsets of their systems relative to a GPS derived time. These topics will be the subjects of other documents.

7.4.3 Loss of synchronization

Measurement points should be able to detect when they have low confidence of being adequately synchronized e.g. NTP server becomes unreachable, measurement points should

1) Notify a management station

2) Inform other measurement points whose probes they are responding to

During periods of low confidence in the synchronization of measurement systems, there may still be value in measurements of packet loss.

7.5 Inter-domain Performance Measurement Data Information Model and Protocol

For the successful end-to-end inter-domain performance measurement, it is essential to define a common performance metric data model. Although the performance attributes are agreed, it is necessary to define a common template to describe them for interoperability purpose. Once the common data model is defined, a standard protocol to carry such information between different domains is needed. The exchange protocol can be used directly between different domains in distributed manner or indirectly through NMSs which are responsible for their own domains.

The following lists requirements for the information model and protocol.

- The information model should be exchange protocol neutral
- The information model shall cover all five performance attributes, namely, minimum delay, mean delay, delay variation, packet loss, and unavailability
- The information model should be extensible for future use
- The information model should be flexible to include different set of performance attributes
- The exchange protocol should be efficient, reliable and secure
- The exchange protocol should be congestion aware

7.6 Measurement Granularity

QoS in NGN can be provided in various levels depending on service requirements. Its granularity can be as fine as a flow-level or as coarse as CoS (class of service) level. More specifically, the granularity levels consist of a flow, various layer 2 tunnels (e.g., L2TP, L2VPN, etc.), an MPLS LSP, Layer 3 tunnels (e.g., GRE, IPsec, L3VPN, etc.), any other class-based logical paths (e.g., an IP path associated with DiffServ class), and an application session. Various mappings are possible among them. For example, a number of flows can be aggregated to form a tunnel. Several tunnels or logical paths may represent an application session.

There are several definitions of the term “flow” being used. This document adopts the definition in RFC3917 as follows:

A flow is defined as a set of IP packets passing an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties. Each property is defined as the result of applying a function to the values of:

1) One or more packet header field (e.g., destination IP address), transport header field (e.g., destination port number), or application header field (e.g., RTP header fields [RFC3550])
2) One or more characteristics of the packet itself (e.g., number of MPLS labels, etc.)
3) One or more of fields derived from packet treatment (e.g., next hop IP address, the output interface, etc.)

A packet is defined to belong to a flow if it completely satisfies all the defined properties of the flow.

Flow-level performance measurement may be needed for a high quality user service which needs special care or billing purpose. Due to the performance complexity, it may not be practical to have continuous real-time flow-level measurement for all the service flows. However, it is necessary to define such functional capabilities to meet a special service requirement. Fortunately it may be possible to meet both flow level measurement and scalability requirements. If we measure entire flows at a particular measurement point of

interest, it is not scalable. Typically meaningful flows which take most traffic volume (e.g., over 95% of a particular link bandwidth) comprise of small portion of the entire number of flows. Thus if we can identify these meaningful flows, we can measure them in real-time continuously and avoid measuring unnecessary flows. Measurement on tunnel and other higher level paths introduce much less stringent performance burdens and thus scalability is not an issue.

Tunnel level, logical-path level, as well as application-session level measurement also need to be supported to meet various measurement requirements such as tunnel statistics, per-class statistics, and per-application statistics. These measurements are meaningful for an entire end-to-end path whether it is a tunnel, a logical path, or an application-session. Flow, tunnel, and logical path level measurement is relatively clear on how to measure them since each one has a unique way of identification. However, an application-session level measurement requires mapping or aggregation of lower-level measurement results. For instance, a Video Telephony session can be composed up with a voice and a video flows. Each flow can be class-based logical path or a part of L2VPN paths.

The selected granularity for performance measurement shall support the following criteria:

- The measurement overhead must be kept at a low level as much as possible
- The measurement may support all levels of granularity as described above
- Both active and passive measurement methods can be used as applicable
- The flow-level and other fine-grained (e.g., LSP-level) measurement shall be supported on demand basis
- The flow-level measurement should have an end-to-end context. Concatenation of segment-based flow measurement may not reflect the original flow characteristics.
- The measurement may support relevant levels of granularity for multicast traffic.

8 Management Requirements

8.1 Architectural Considerations

The inter-domain performance measurement requires close collaboration between different administration domains. Performance measurement in each domain can be relatively easily achievable. However, when it crosses a domain boundary, the complexity increases dramatically. The main issues involved are the following:

- Who will measure what and how?
- What are the common data model to store the measured data?
- How to exchange the measured data?
- Are Network Management Systems (NMSs) involved in the measurement collaboration?

Depending on the answers to these questions, we can classify architecture as follows:

- Architecture that NMS is not involved
  - Manual Model

    In this model, performance measurement data is stored in a standardized common information object and exchanged among service providers through a standard protocol. Management of measurement processes such as configuration of active/passive probes, collection of performance attributes, convert them to common information object, and triggering exchange protocols is performed in proprietary way in each domain. This model doesn't assume that there exists a representative performance measurement management system which coordinates all such processes. The advantage of this model is simplicity and cost effectiveness. However, configuration in each

domain requires manual intervention, thus it has limitation in automation. This model may raise security issues if the exchange protocol is not secure.

- Architectures that NMSs are involved

  In this case, one or more NMSs exist in each domain and NMS is responsible for both internal and inter-domain performance measurement management and collaboration.

  – Centralized Model

    A single NMS is responsible for the management of all the active and passive measurement over each domain. It is simple to manage but has scalability limitation. Also it is not easy to have one centralized NMS controls entire domains which may fall under different administration responsibility. Scalability issues may arise since all performance measurement data should be reported to one centralized NMS.

  – Distributed Models

  – Federated Model

    The NMSs of the domains are structured into a freely federated process group for the management of active and passive measurement. This model distributes the responsibility of the centralized NMS into a number of NMSs across domains. Thus it enhances the scalability greatly. NMSs can be freely grouped and exchange information to solve a common problem, in this case, inter-domain performance measurement. Figure 12 illustrates one example model. NMS1, NMS2, and NMS3 are responsible for regional network A, regional network B, and a transit network. Each NMS measures performance data for its associated regional/transit network, and exchanges it with other NMSs to collaborate with each other for the end-to-end performance data.

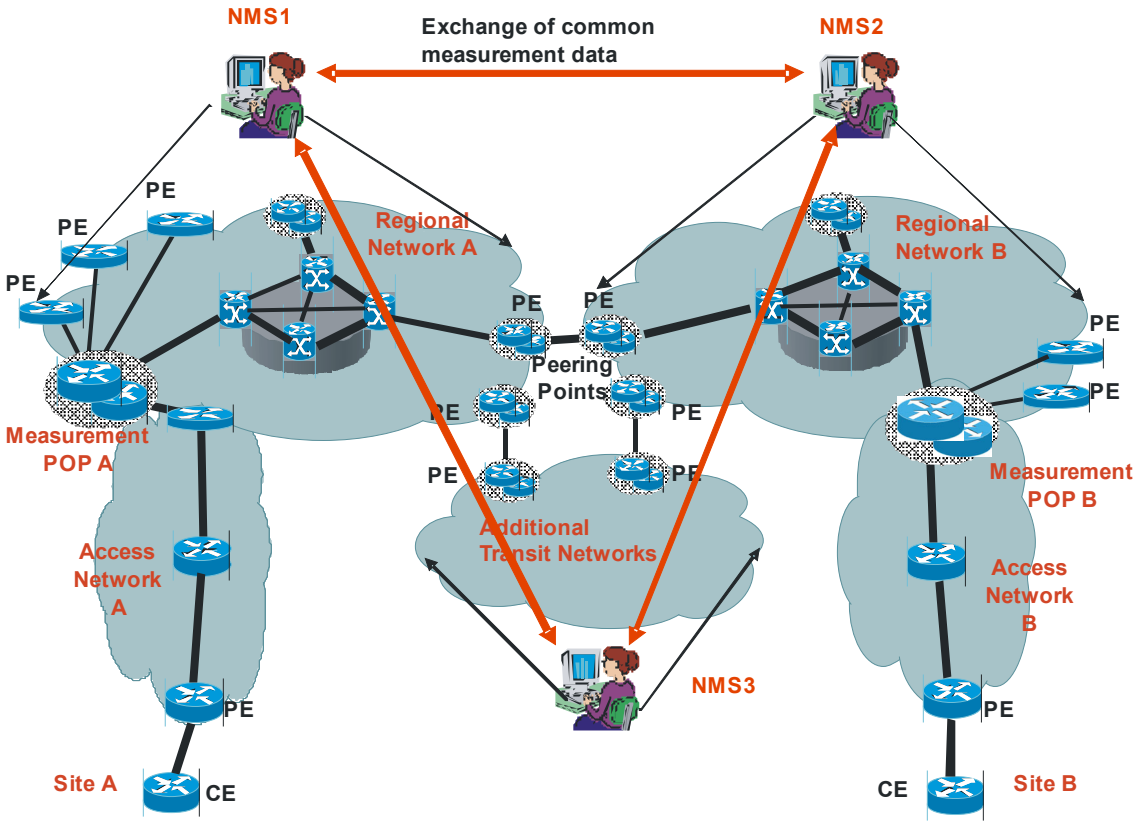


Figure 12 – An example of Federated Inter-domain Measurement Model

– Hierarchical Model

The NMSs of the domains are hierarchically stratified into a process group of well-defined structure for the management of active and passive measurement. It is similar model with federated one. However, the main difference is the rigid relationship and structure among NMSs. NMS in a certain level can perform specifically defined functions only. Lower level NMSs perform detailed functions and upper level NMSs perform overall functions. For example, lower-layer NMSs perform: one NMS measures access network segment, another does it for backbone segment, and the other does it for transit or peering segment. Upper-layer NMS then correlates the results from lower layers NMSs and exchange them with its peer in other domains. Figure 13 shows an example hierarchical model. NMS1 manages two NMSs which perform measurement of access and core networks. Similarly NMS2 manages two NMSs. NMS is the highest level NMS which sits on top of NMS1, 2, and 3.

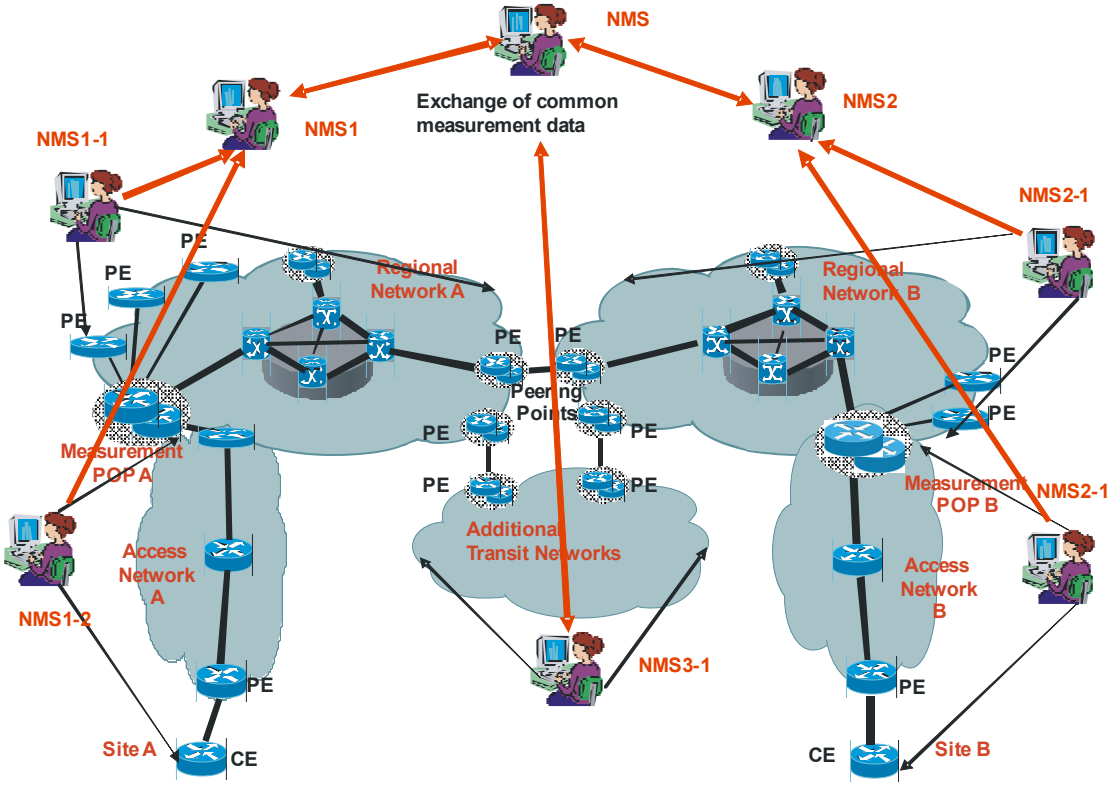


Figure 13 – An Example of Hierarchical Inter-domain Measurement Model

– Cascading Neighbor Model

The NMS of each domain is interconnected only with those of neighbouring domains to create a process of well-defined structure for the management of active and passive measurement. Figure 14 provides pictorial view of a cascading neighbor inter-domain measurement model. As shown in the picture, each NMS exchanges measurement data with neighbouring NMS only. There aren't any direct interactions among other NMS besides its neighbours.

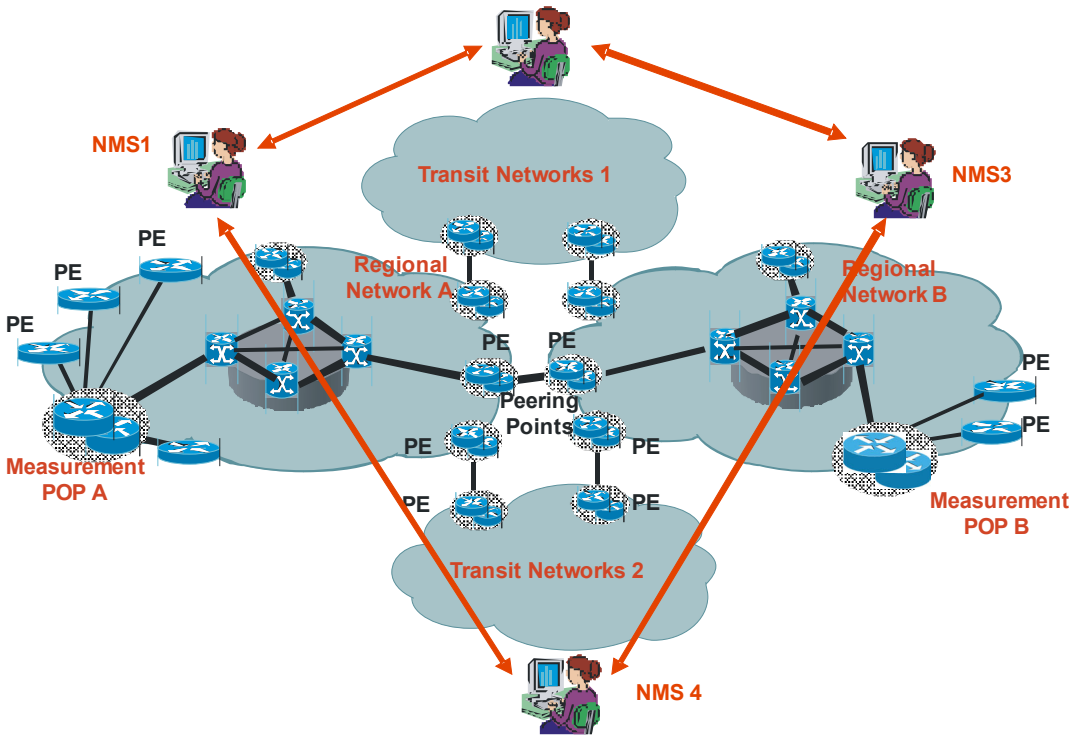


Figure 14 – An Example of Cascading Neighbor Inter-domain Measurement Model

Depending on the requirements, hybrids of these basic models may also be considered.

8.1.1 Discovery Considerations

The NMS of each domain have to exchange performance data for end-to-end "aggregation" of data. Before they can exchange data, they have to discover each other. It is obvious that, in a multi-provider environment, a standard mechanism for discovery and performance data exchange will be required. It will be preferable to use a widely deployed mechanism for discovery and data exchange. A possible candidate is a Web/XML or Web Services based mechanism, because of its wide acceptance and deployment in the industry and SP environment. The NMS function of a SP can be provided as a web service with limited access and appropriate security. The discovery process then consists of learning the web service address of the NMS. Three possible options of discovery are as follows:

1) Manual: When two neighboring NMSs negotiate for collaboration, they exchange *manually* (via agreement document or other manual means) the web service addresses (URL, for example) of the NMSs.

   a) Propagate: The addresses can be further propagated to other NMSs. For example, in figure 15, NMS B and NMS C manually exchange their addresses. When NMS Z exchanges initial (*capability*) messages with NMS C, information about more distant NMSs (NMSs A and B) may be passed to NMS Z.

2) Registry: The providers can agree upon a global NMS web service registry. The service can be based on UDDI or other mechanism. When an NMS is commissioned, information about it, including its *capabilities* is registered in the registry service. NMSs discover about each other via the registry service.

3) A combination of 1 and 2.

The details of standard XML messages and format need to be defined.

When considering the choice of discovery mechanisms. A factor of key importance is security, since the exposure of information may have adverse impacts. The adverse impacts may be categorized as:

1) Competitive Exposure – where a competitor could take business advantage of the information exposed

2) Attack Exposure – where an attacker could better target a provider's network and its customers

Therefore it is highly preferable to limit or hide the information made available about providers' networks, especially when kept in centralized locations such as registries.

The dynamic nature of the network (adds, deletes and moves) should be taken into account when considering the methods to provide new data as timely as possible.

8.1.2 Messaging Considerations

The NMSs can exchange following "*control*" messages:

1) Capability: Metrics supported, data distribution and aggregation capabilities supported

2) Collect: request to start collecting requested set of metrics.

3) Pull: request to get data that has been or being collected based on "Collect" request. Bulk get should be supported.

4) Push: Push data based on "Collect" request, for example, when the specified (by the "Collect" request) size or time interval has been reached.

5) Metrics to collect.

The details of standard XML messages and format need to be defined.

8.1.3 Data Handling Considerations

8.1.3.1 Distribution

An NMS may request data from multiple segments for end-to-end performance data "aggregation". Following are the potential options for data collection and distribution requests:

1) Mesh: The requesting NMS requests all the NMSs towards the destination. For example, in figure 15, if NMS Z collects delay data towards NMS A, it will send requests to NMS C, NMS B and NMS A. Data will be sent directly to NMS Z from each NMS (A, B and C).

2) Cascade: The requesting NMS requests its immediate neighbor, which propagates the requests to the destination. The requested data may be transferred in a cascaded fashion (not further aggregated).

3) Combination of the above.

The capability of an NMS may be exchanged during capability negotiation. For example, NMS B can indicate to NMS Z that it will not cascade.

Following are the reasons for the cascading support:

1) When collecting data end-to-end, an intermediate NMS may need to retain and analyze data. For example, while Z collects delay data towards A, NMS B may want to retain and aggregate data to find out NMS B to NMS A delay.

2) When there is a need (or desire) to mask individual components of performance values of a set of segments from another set of segments. For example, SPA and SP B may want (negotiate) to mask their individual components of performance values from Z.

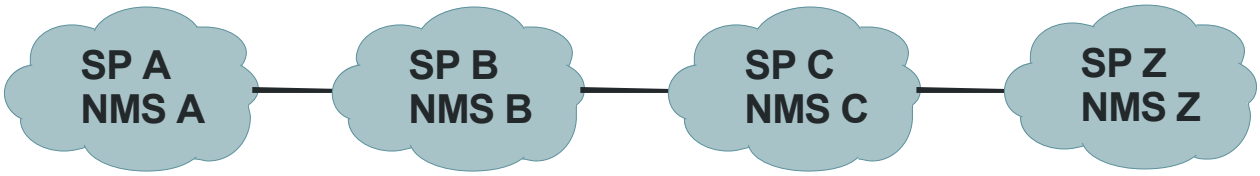


Figure 15 – Inter provider NMS Network

8.1.3.2 Aggregation

Performance data can be aggregated at various points in the network depending on distribution architecture described above. For example, in the case of Z to A delay data collection, data may be aggregated as follows:

- NMS A aggregates its own data and data from any more distant NMSs. NMS B aggregates data received from NMS A with its own, NMS C aggregates data received from NMS B with its own, and sends to NMS Z, or
- NMSs A, B and C send their own data to NMS Z.

8.1.3.3 Internal Architecture Considerations

The internal architecture of an NMS should not have any bearing on the overall (global) NMS network. Within a single SP any combination of the following protocol/mechanisms could be used:

1) SNMP
2) XML/http based
3) IPFIX
4) Proprietary

Except the XML based one, these protocols/mechanisms may not be suitable for multi-provider environment. For example, one of the disadvantages of SNMP or IPFIX is that these protocols are (mostly) UDP based, where has issue when firewall or SP boundaries have to be crossed.

The primary internal functions of a measurement NMS include the following:

- Discovery of other NMSs and their measurement components
- Communications with other NMSs to request and receive measurements
- Comparison of measured and expected results
- Collection, aggregation and storage of measurements
- Initiation of and response to measurement probes
- Configuration and monitoring the health of the measurement components
- Monitor Policing
- Time synchronization
- Reporting

The IPFIX protocol provides network administrators with access to IP flow information. The architecture for the export of measured IP flow information out of an IPFIX exporting process to a collecting process is defined in [IPFIX-Protocol], per the requirements defined in [RFC3917]. The IPFIX protocol specifies how IPFIX data record and templates are carried via a congestion-aware transport protocol from IPFIX exporting processes to IPFIX collecting process. IPFIX has a formal description of IPFIX information elements, their name, type and additional semantic information, as specified in [IPFIX:Information model]. Finally [IPFIX-Applicability] describes what type of applications can use the IPFIX protocol and how they can use the

information provided. It furthermore shows how the IPFIX framework relates to other architectures and frameworks.

8.2 Management Hierarchy

Given the considerations of the previous section, the following architecture is presented. Other internal architectures may achieve the same functionality; however communications among providers must be standardized. In order to distinguish the NMS measurement functions from other NMS functions. We will name the NMS as "Performance Reporting System" or PRS.

Configuration, measurement and reporting are accomplished by a group of devices having different functions which are arranged in a hierarchy. There are four functional components: the Performance Reporting System, Collection Platform, Measurement Platform, and PE/CEs. (Terminal Equipment is not included here).The hierarchy and the communications among components are shown in figure 16 below.

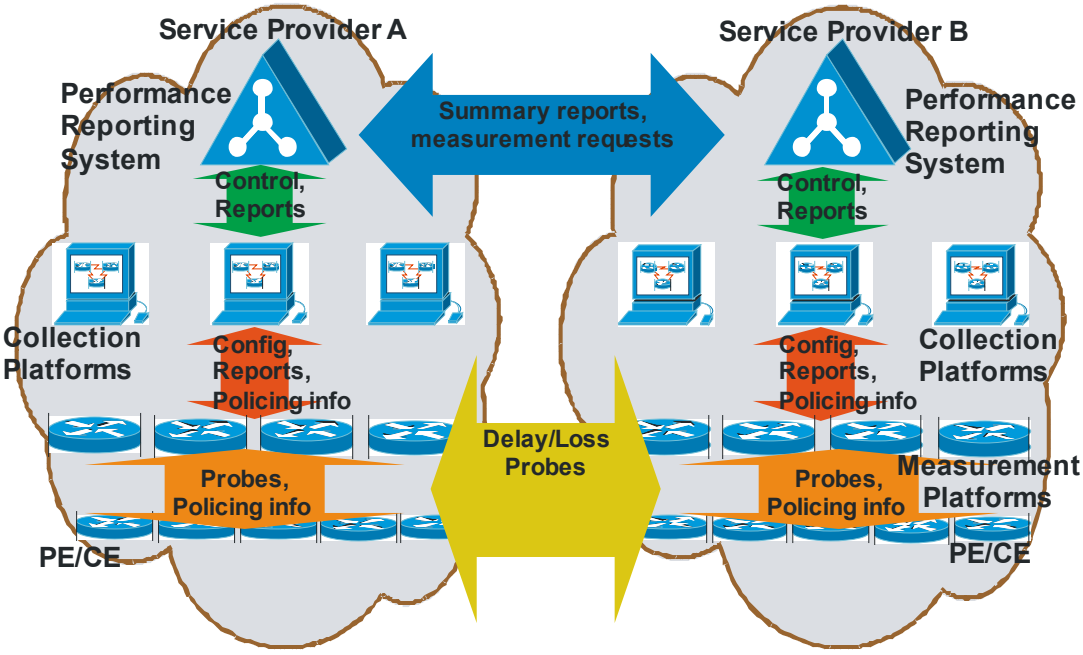


Figure 16 – A Hierarchical Internal Architecture

8.2.1 Performance Reporting Systems

At the top of the hierarchy is the Performance Reporting System (PRS). While this may be implemented using multiple computers, it will appear as a single system to other SPs. The PRS is the primary configuration tool. The PRS pushes probe initiation commands to a Collection platform which is associated with the initiating Measurement Platform, PE or CE which is to initiate probing. That Collection Platform then configures the Measurement Platform, PE or CE.

The Performance Reporting System will simultaneously perform the following functions:

1 Control of Collection Platforms

1.1 Probes required

1.1.1 Source (MP, PE or CE)

1.1.2 Destination (MP, PE or CE)

1.1.3 Class(es)

1.1.4 Frequency

2 Retrieval of rollup period reports from Collection Platforms

3 Storage and analysis of rollup period reports

3.1 Measurement Data will be stored for a minimum of 12 months

4 Locate probing destinations (MPs, PEs or CEs)

5 Communication with other SPs' PRS

5.1 Respond to rollup period report retrieval requests from other SPs depending upon their customers' permissions

5.2 Retrieval of rollup period reports from other SPs' PRS for specifically designated customer sites (managed service)

6 Reporting

6.1 To other SPs' PRS as required

6.2 Real-time network status to SP operations

6.3 To customers

8.2.2 Collection Platforms

At the second level of the hierarchy are the Collection Platforms.

Collection Platforms communicate "up" to the PRS and "down" to the Measurement Platforms, CEs and PEs.

The Collection Platform will simultaneously perform the following functions:

1 Configuration of Measurement Platforms

1.1 Probes required

1.1.1 Destination (MP, PE or CE)

1.1.2 Class(es)

1.1.3 Frequency

2 Configuration of CEs and PEs

2.1 Probes required

2.1.1 Destination (PE or CE)

2.1.2 Class(es)

2.1.3 Frequency

3 Retrieval and storage of probe results from Measurement Platforms

3.1 Probe results will be stored for a minimum of 24 hours

4 Monitor Policing at PEs and CEs

5 Monitor Policing at Peering Points

6 Analysis of probe results

6.1 Network unavailability determination

6.2 Identification of performance issues

6.3 Determination of rollup period metrics

7 Reporting to PRS

7.1 Create rollup period reports

7.2 Generate critical event reports

7.2.1 Clock synchronization loss

8.2.3 POP Measurement Platforms

At the third level of the hierarchy are the Measurement Platforms which are geographically distributed at POPs.

Measurement Platforms communicate "up" with associated Collection Platform(s), and "horizontally" with other Measurement Platforms which may belong to other SPs.

The Measurement Platform (MP) will simultaneously perform the following functions:

1 Take configuration from Collection Platform

1.1 Probes required

1.1.1 Destination MPs, CEs and PEs

1.1.2 Class(es)

1.1.3 Probe frequency

2 Implement performance measurements, by initiating "per-class" active probes to measure delay and loss to many other MPs, PEs and CEs

3 Provide "per-class" response to other MPs

4 Store measurements which it initiated for 2 hours

5 Control, Retrieve and store measurements (30 minutes) initiated by associated CEs to support CE to CE/PE probing

6 Control, Retrieve and store measurements (30 minutes) initiated by associated PEs to support PE to CE/PE probing

7 Clock synchronization

7.1 Synchronize itself with GPS

7.2 Synchronize associated CEs and PEs

8 Suspend initiating probes while they are not meeting time offset requirements, and reinitiate when they meet time offset requirements.

9 Indicate in their response to probes to other MPs, their state of compliance with the time offset requirements.

10 Report to Collection Platform

10.1 When its time offset goes out of spec and back into spec, as defined in section 7.4.

10.2 When it detects in probe responses from the responding destination device that its time offset is out of spec.

8.2.4 Customer and Provider Edge Routers

The IDQ functions that may be supported at either CE or PE are almost identical. The differences being in their:

1 Ownership

2 Management

3 Required scale (A PE may have to support multiple CEs.)

The CE or PE will simultaneously perform the following functions:

1 Respond to Policing queries from Collection Platform

2 Take configuration from Measurement Platform

2.1 Probes required to be initiated for CE to CE or PE to PE measurements

2.1.1 Destination CEs and PEs

2.1.2 Class(es)

2.1.3 Probe frequency

3 Run Remarking and Forwarding

4 Clock Synchronization to Measurement Platform using NTP

5 Implement performance measurements, by initiating "per-class" active probes to measure delay and loss to other PEs and CEs

6 Indicate in their response to probes to MPs, PEs and CEs, their state of compliance with the time offset requirements.

8.2.5 Customer Terminal Equipment

The functions of customers "Landmark" terminal equipment is TBD. When TEs are included in a measurement scheme, the functionality of CEs is likely to be expanded.

8.3 Discovery

SPs need to be able to locate the following entities belonging to other SPs.

1) Performance Reporting Systems

2) Measurement Platforms at Peering and Demarcation POPs

3) PEs and CEs

8.3.1 Locating Performance Reporting Systems

The IP address of Performance Reporting Systems should be listed in a registry, linked to AS numbers, Provider Name, contact info and freshness indicator.

Existing tools may be used to relate customer prefixes to AS numbers and hence to a related PRS. A PRS may be requested to confirm whether an IP address belonging to it is a subscriber. (This seems preferential to listing subscribers in the registry)

PRS addresses are not expected to change frequently, however there should be a mechanism, which is used prior to PRS address change, to inform other PRSs that it has contact with, what the new address will be and when. The registry is updated when the change is made.

8.3.2 Locating Measurement Platforms

The measurement platforms of other providers whose IP addresses must be located are:

1) The measurement platform in the POP associated with the destination site (e.g. Demarcation POP B in figure 17)

   a) This may be used to measure the total transit segment by the source access network provider

   b) It is located by asking the PRS associated with the destination site for its IP address. (This seems preferential to listing demarcation POPs in the registry)

2) The measurement platform on the far side of a peering link (e.g. Provider C needs to know about PE 3 in figure 17)

   a) This is needed for each provider to measure its own performance (assuming that it is responsible for the performance of egress traffic over a peering link) by measuring from an

ingress peering measurement point to the measurement platform on the far side of a peering link.

b) Since there may be multiple peering links among providers, the determination of which pair of measurement points should be monitored is important. The pair should be identified by the destination address. The method of doing this is left to the provider doing the measurement.

Measurement POP addresses are not expected to change frequently, however there should be a mechanism, which is used prior to measurement POP address change, to inform other PRSs that it has contact with, what the new address will be and when.

8.3.3 Locating CE/PEs

SPs need to be able to find the location of CE/PEs of other providers so that occasional measurements may be taken between measurement points, CEs or PEs of one provider to CEs or PEs of the destination provider. The IP address of a CE/PE associated with a destination prefix is located by asking the PRS associated with the destination site. (This seems preferential to listing CEs/PEs in the registry)

CE/PE addresses are not expected to change frequently, however there should be a mechanism, which is used prior to CE/PE address change, to inform other PRSs that it has contact with, what the new address will be and when.

8.4 Initiation of Measurements

While the segmentation of the network enables scalability through re-use of probes for many purposes, initiating a full mesh of measurements among measurement points globally is unlikely to become possible. Therefore the initiation of measurements must be such that most of the measurements taken are actually required. Requests for the initiation of inter-provider measurements may be issued by any provider; these authenticated requests should be granted according to each provider's policy.

Measurements may be initiated independently of a customers' traffic, for example when they sign up for service to other particular sites; and/or dynamically when an "Access" Provider sees customer traffic going to a subscribing 3rd party across other IDQ supporting providers' networks.

Before describing the procedure, we review the 9 measurements required for the scenario in the figure 17 below.

As described in section 7.3.2, measurements are made for operating, supporting purposes. The procedures for the initiation of each are as follows.

To initiate operating measurements between site A CE and site B CE, measurements are needed between

1) Site A CE and Demarcation POP A, bidirectionally (Access segment)
2) Demarcation POP A and Demarcation POP B, bidirectionally (Total transit segment)
3) Demarcation POP B and Site B CE, bidirectionally (Access segment)

For troubleshooting purposes, measurements are required from

4) Demarcation POP A to PE2 (egress transit traffic across provider A)
5 PE1 to demarcation POP A (ingress transit traffic across provider A)
6) PE2 to PE3 (egress transit traffic across provider C)
7) PE4 to PE1 (ingress transit traffic across provider C)
8) Demarcation POP B to PE4 (egress transit traffic across provider B)
9) PE3 to demarcation POP B (ingress transit traffic across provider B)

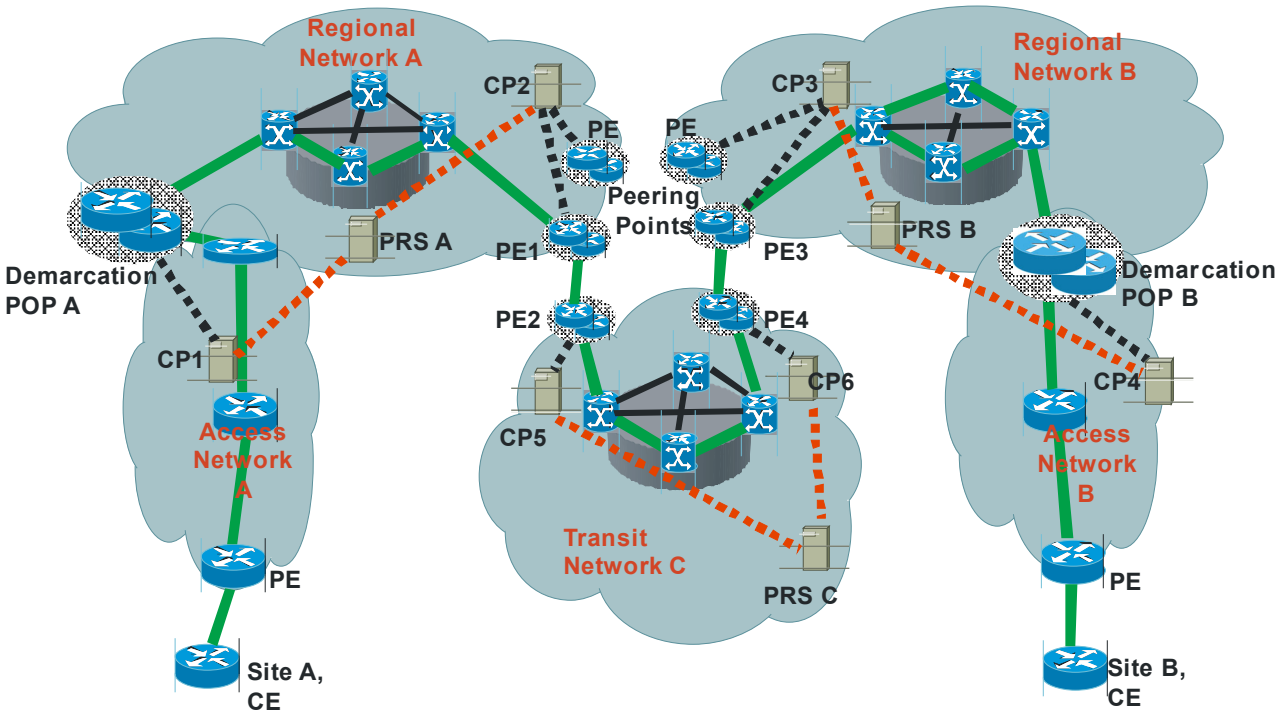


Figure 17 – Collection Platforms communicating to PRS and Measurement POPs

For a dynamic initiation of measurements the following hi-level procedure is applied, referring to the measurements as numbered above figure 17.

1) PRS A sees a new destination prefix for which measurements should be initiated. (Method left up to provider A)

2) PRS A determines which other providers' networks the traffic will cross (Method left up to provider A)

3) PRS A learns the PRS addresses of the other providers' networks the traffic will cross (from registry)

4) PRS A contacts PRS B and

   a) Provides PRS A address

   b) Provides PRS C address

   c) Provides destination address, and requests whether it is a subscriber to this service, if not then requests PRS A aborts the setup sequence.

   d) Requests the IP address of measurement point associated with destination prefix.

   e) Requests that the above operating measurements be sent to PRS A periodically

   f) Requests that the above non-compliant supporting measurements be sent to PRS A

   g) Requests that any non-compliant customer use be sent to PRS A

   h) Requests that any health issues relating to these measurements be sent to PRS A.

5) PRS A initiates measurements #1, 2, 4 and 5

6) PRS B initiates measurements #3, 8 and 9

7) PRS A contacts PRS C and

   a) Provides PRS A address

b) Provides PRS B address

c) Provides destination address

d) Requests that non-compliant supporting measurements be sent to PRS A

e) Requests that any health issues relating to these measurements be sent to PRS A.

8) PRS C initiates measurements #6, 7

Note that it is assumed the routing used assures that only service providers which support the requested service are considered in the above.

Once a measurement has been initiated due to a request, the question of how long to keep measuring for, and how frequently a refresh request should be sent. Following a request, measurements should be continued for 2 months. Refresh requests should be monthly for as long as the requesting provider wants the measurements. Note that a PRS needs to keep track of which other PRS asked for which measurements and when.

8.5 Communication between Performance Reporting Systems (PRSs)

This section names and describes the messages among the Registry and the PRSs, and how they are used. Following "Registration", three phases are defined which are named "Initiation", "Measurement", and "Shutdown".

8.5.1 Registration Procedures

Each PRS is responsible for initially registering or updating its own IP address in the registry. The registry is responsible for responding to authenticated PRS requests to administer their IP addresses, and to provide those IP addresses to other PRSs.

The 5 messages involved in Registration include:

Registry_IP_update_Rq – Request from a PRS to Registry to set its IP address (or related info)

Registry_IP_update_Rs – Response from Registry to Request from a PRS to Registry to set its IP address (or related info)

Registry_IP_access_Rq – Request from PRS A to Registry for the IP address of PRS B (or related info)

Registry_IP_access_Rs – Response from Registry to request from PRS A to Registry for the IP address of PRS B (or related info)

Registry_Update – Following a PRS A update of its IP address (or related info), this response update is sent from Registry to PRSs (functionally a broadcast) that have previously sent requests to registry for the IP address of PRS A.

Successful registration must be completed by all PRSs along a path prior to measurements along that path being initiated.

The Initiation, Measurement and Shutdown phases occur following a provider's determination of

1) A new destination prefix for which measurements might be initiated

2) Which other providers' networks the traffic will cross to that destination

3) Location of addresses of intermediate and destination PRSs using the registry

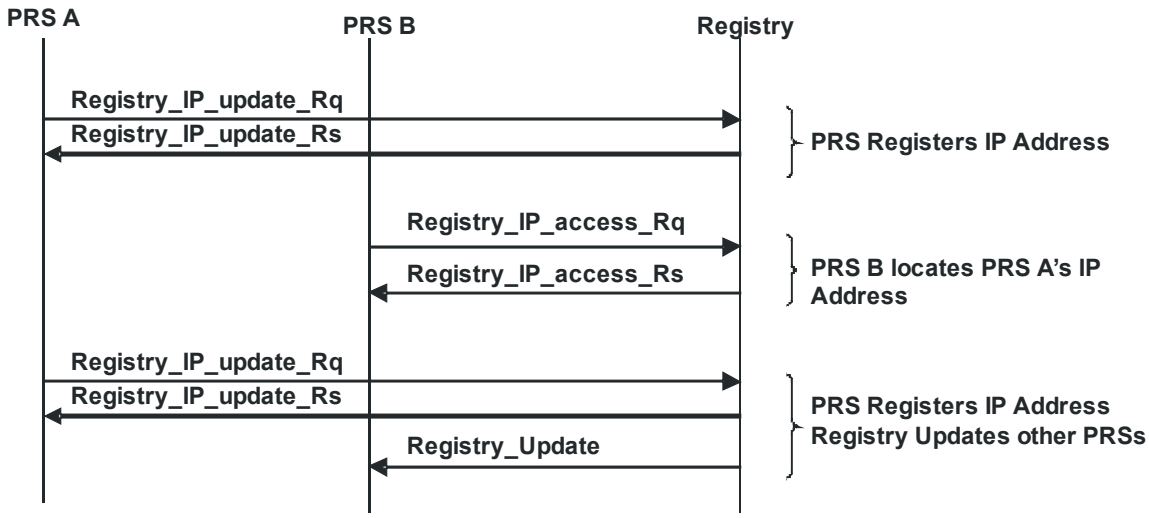


Figure 18 – Example Registration Information Flows

8.5.2 Initiation Phase Procedures

Before measurements are started, the PRS that is the source of the measurement request (source PRS) must first:

1) Confirm that the destination IP is a subscriber to IDQ of the destination PRS
2) Provide details of the measurement request to intermediate and destination PRSs.
3) Receive responses indicating successful initiation.

The 6 messages involved in Initiation include 4 to determine further information and 2 to initiate measurements:

Query_CustomerIP_Request – Query the destination PRS to see if the customer is an IDQ subscriber

Query_CustomerIP_Response – Destination PRS response to **Query_CustomerIP_Request**

Query_DestinationIP_Request – Ask destination PRS what the IP address of their appropriate measurement point is.

Query_DestinationIP_Response – Destination PRS response to **Query_DestinationIP_Request**

Start_Performance_Measurement_Request – Ask a PRS along the path to initiate or allow measurements for a measurement segment.

Start_Performance_Measurement_Response – PRS response to **Start_Performance_Measurement_Request**

8.5.3 Measurement Phase Procedures

Following successful completion of the Initiation phase, the Measurement phase occurs which includes:

1) Occurrence of measurements over the requested network segments
2) Distribution of reports to the source PRS by the intermediate and destination PRSs.
3) Maintenance due to changes in measurement elements or customer subscriptions.

The 4 messages involved in Measurement include:

Performance_Metric_Report – Periodic report of performance metric values or response to Query_Performance_Metric_Request.

Query_Performance_Metric_Request – Ad hoc request for a performance report

There are some cases when measurement point IP should be changed, or the customer no longer subscribes to the IDQ service. The messages handling maintenance during the Measurement phase include:

DestinationIP_Change_Notification – Destination PRS sends notification to source PRS which relays to transit PRSs.

DestinationIP_Change_Confirmation – Response to DestinationIP_Change_Notification

8.5.4 Shutdown Phase Procedures

The Shutdown phase may occur following:

1) Timeout of Refresh Requests from source PRS no longer being received
2) Source PRS no longer requires measurement
3) Destination customer no longer subscribes to IDQ
4) Any provider on selected path no longer subscribes to IDQ

The 2 messages involved in Shutdown include:

Stop_Performance_Measurement_Request – Source PRS's request message to all PRSs engaged in the measurement to stop measurement.

Stop_Performance_Measurement_Response – Response to Stop_Performance_Measurement_Request

8.5.5 Message Description

Identification of measurements among PRSs is based upon defining particular measurement segments and network service class. A measurement flow can be identified by source IP address, destination IP address, and network QoS class.

There are nine measurement segments in figure 17 of section 8.4. The source network has 4 for which it is responsible, wheras a transit network has 2, and a destination network has 3.

In the messages below, Flow_Identification and Measurement_SegmentID are defined as follows:

Flow_Identification consists of {SourceIP, DestinationIP, Class}.

Measurement_SegmentID can be abstracted as

a) Upstream PE to Downstream peer PE (uni-directional measurement)
b) Downstream PE to Upstream peer PE (uni-directional measurement)
c) Upstream PE to Downstream PE (uni-directional measurement)
d) Downstream PE to Upstream PE (uni-directional measurement)
e) Access (bidirectional measurements)
f) Far PE To Downstream (bidirectional measurements from a specified address to a downstream PE)

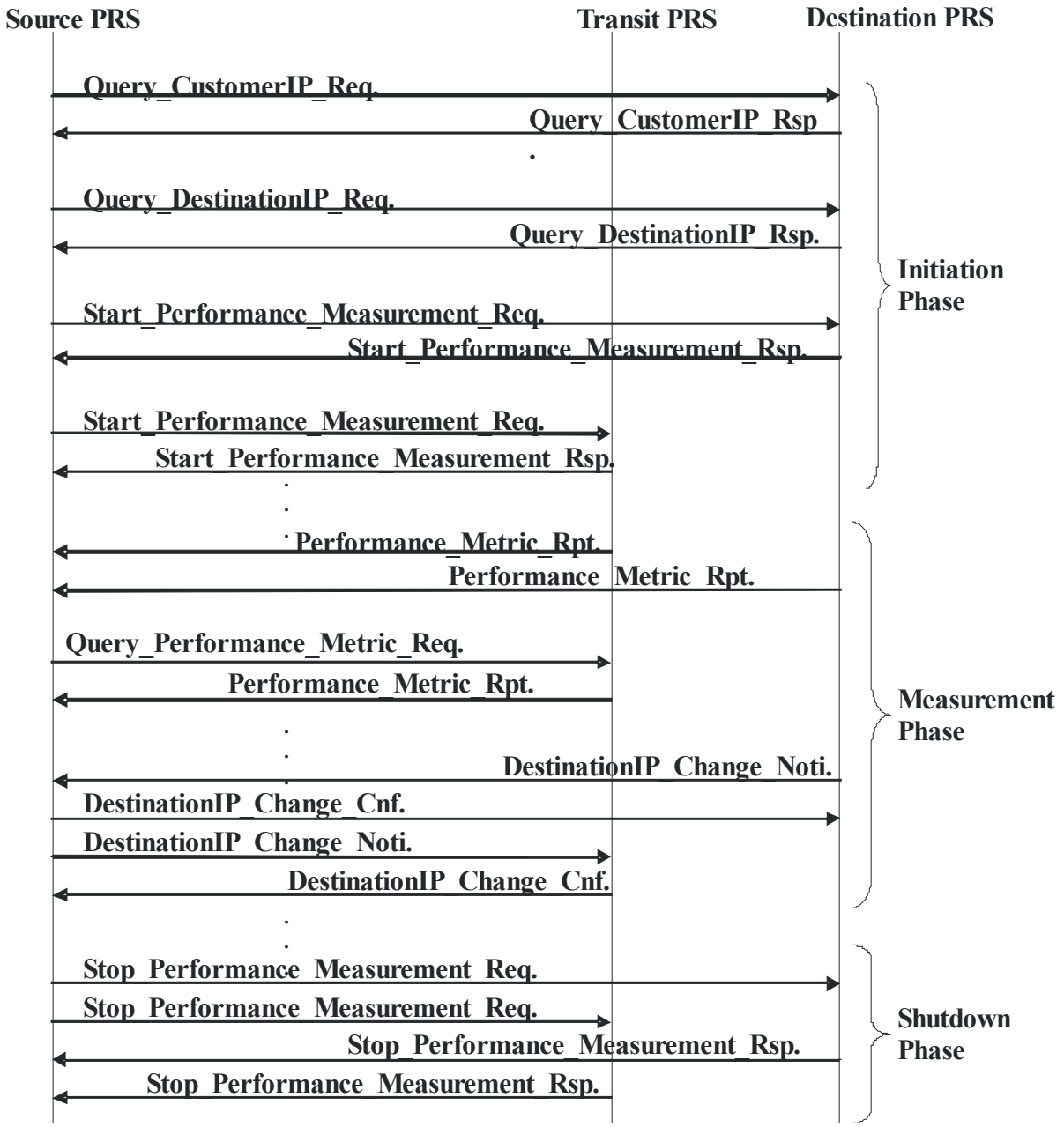


Figure 19 – Example Information Flows

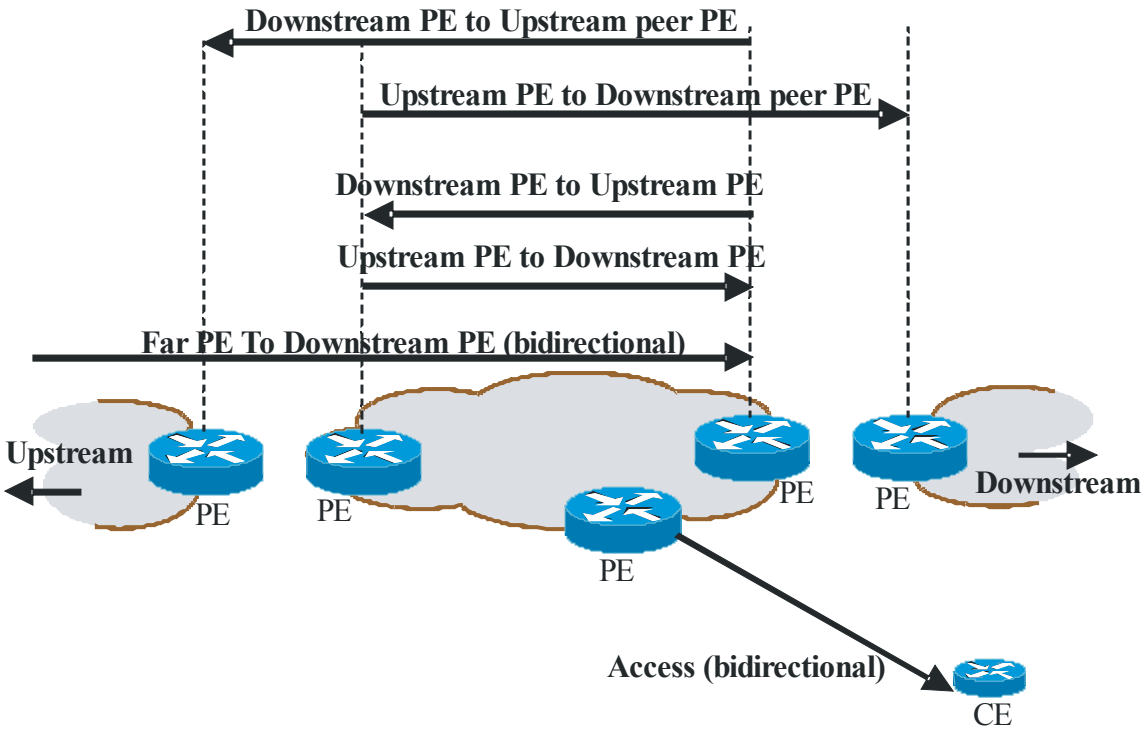


Figure 20 – Abstracted Measurement Segments

The above abstraction relates to the measurements identified in figure 17 in section 8.4 as follows:

1) Site A CE and POP A = Access (bidirectional measurements)
2) POP A to POP B = Far To Downstream (bidirectional measurements)
3) POP B and site B CE = Access (bidirectional measurements)
4) POP A to PE2 = Upstream to Downstream peer (unidirectional measurements)
5) PE1 to POP A = Downstream to Upstream (unidirectional measurements)
6) PE2 to PE3 = Upstream to Downstream peer (unidirectional measurements)
7) PE4 to PE1 =Downstream to Upstream peer (unidirectional measurements)
8) POP B to PE4 = Downstream to Upstream peer (unidirectional measurements)
9) PE3 to POP B = Upstream to Downstream (unidirectional measurements)

Note that communications with other PRSs are only required regarding measurements within a source network when those measurements are asked for by other PRSs. So in the case of the above 9 measurements, no inter-PRS communication is required for measurements 1 and 5. Note that measurement 4 requires inter-PRS communications to obtain permission and the IP address of PE2 from PRS C.

There are 3 elements which are common to all messages.

InvokeID : Uniquely identifies the message or message pair. The InvokeID of Request-Response and Notification-Confirmation message pairs should be identical.

Invoking_PRS/Reg : PRS or Registry IP address that sends this message.

Invoked_PRS/Reg : PRS or Registry IP address that receives this message.

8.5.5.1 Registry_IP_update_Rq

– Description : Request to set the IP address associated with a PRS

– Direction : From PRS to Registry

– Elements :

A. PRS Unique ID#

B. AS numbers

C. Contact information

D. Period during which this IP address is valid

8.5.5.2 Registry_IP_update_Rs

1) Description : Response message to Registry_IP_update_Rq

2) Direction : From Registry to PRS

3) Elements :

a) OK_NOK

b) NOK reason code

8.5.5.3 Registry_IP_access_Rq

1) Description : Request for IP address associated with PRS B

2) Direction : From PRS A to Registry

3) Elements : AS number

8.5.5.4 Registry_IP_access_Rs

1) Description : Response message to Registry_IP_access_Rq

2) Direction : From Registry to PRS A

3) Elements :

a) IP address of requested PRS

b) Period during which this IP address is valid

c) Contact information

8.5.5.5 Registry_IP_update

1) Description: Following an update by a PRS of its IP address (or other info) in the registry, this is a message in response to previously received Registry_IP_access_Rq messages for that PRS's IP address (functionally this is a broadcast).

2) Direction : From Registry to PRSs

3) Elements :

a) List of which elements have been updated

b) Old IP address of requested PRS

c) New IP address of requested PRS

d) Old Period during which this IP address is valid

e) New Period during which this IP address is valid

f) Old Contact information

g) New Contact information

8.5.5.6 Query_CustomerIP_Request

1) Description : Query whether the customer IP prefix belongs to a subscriber of the destination network
2) Direction : From source PRS to destination PRS
3) Elements :
   a) Customer_IP_Prefix
   b) Set of queried network QoS classes

8.5.5.7 Query_CustomerIP_Response

1) Description: Response to Query_CustomerIP_Request.
2) Direction : From destination PRS to source PRS
3) Elements : Set of OK_NOK for requested network QoS classes.

8.5.5.8 Query_DestinationIP_Request

1) Description : Query for the IP address of the measurement point at either the demarcation POP, PE, or CE of the destination network
2) Direction : From source PRS to destination PRS
3) Elements
   a) Customer_IP_Prefix
   b) System_Type : Demarcation POP / PE / CE

8.5.5.9 Query_DestinationIP_Response

1) Description: Response to Query_DestinationIP_Request.
2) Direction : From destination PRS to source PRS
3) Elements
   a) OK_NOK
   b) DestinationIP

8.5.5.10 Start_Performance_Measurement_Request

1) Description : Request for PRS to start or allow performance measurements
2) Direction : From source PRS to destination or transit PRS
3) Elements
   a) Flow_Identification : Uniquely identifies the target measurement flow (SourceIP, DestIP, Class)
   b) Measurement_SegmentID: Indicates which Measurement-segment should be performed (upstream->downstream, upstream->downstream peer, downstream->upstream, downstream->upstream peer, access or far to downstream)
   c) MetricID list: Lists the requested metrics that are to be measured and reported.
   d) Destination_Or_Transit_Flag : Indicates whether the network the target PRS belongs to is destination or transit.
   e) UpstreamPeer_PRS_Address : PRS address of the adjacent upstream network
   f) DownstreamPeer_PRS_Address : PRS address of the adjacent downstream network. Null For destination PRS.

g) Report_Frequency : Desired report frequency. Right to decide the report frequency is up to target PRS.

h) Probe_Injection_Frequency

i) Backward_Injection_Flag : Setting this flag to 1 means to request backward measurement. For unidirectional test, this flag should be 0.

j) Start_Time : Null Start-Time means 'right now'.

k) Allow_Inform: Indicates that the target PRS is being asked to allow the probe to enter the target provider's domain and be responded to by a measurement point, plus to inform the source PRS of any IPaddress change of that measurement point.

l) Non-compliant customer report: Indicates if a report of times when the customer exceeds their SLA agreed bandwidth should be sent

m) Health issue request: Indicates is a report of times when the health of the PRS measurement system was below expected performance levels.

8.5.5.11 Start_Performance_Measurement_Response

1) Description: Response to Start_Performance_Measurement_Request.

2) Direction : From destination or transit PRS to source PRS

3) Elements

a) OK_NOK

b) Reason_For_NOK (ex : capability not supported, no such flow in transit network)

c) Backward_Injection_Flag : From destination PRS. Indicates whether backward injection is possible or not.

d) List of {MetricID, OK_NOK} : For each performance metric, indicate whether the measurement of that metric is supportable or not.

e) Report_Frequency : May be different from that of Start_Performance_Measurement_Request.

f) Duration: Period of time for which the responding PRS agrees to measure, notify and provide reports

8.5.5.12 Query_Performance_Metric_Request

l) Description : Query performance values measured between From_Time and To_Time. This message is not used in normal condition. Report of performance value is initiated by destination or transit PRSs periodically.

2) Direction : From source PRS to destination or transit PRS

3) Elements

a) Request_Mode (either bulk mode or single mode)

i) Bulk_Mode : Request for report for all measurements made by the target PRS for the source PRS.

ii) Single_Mode : Request for report for a particular flow and Measurement-segment.

b) Flow_Identification : Only if the Request_Mode is Single_Mode.

c) Measurement_SegmentID: : Only if the Request_Mode is Single_Mode.

d) From_Time, To_Time

8.5.5.13 Performance_Metric_Report

1) Description: Periodic report of performance metric values or reponse to Query_Performance_Metric_Request. InvokeID is NULL for periodic report.
2) Direction : From destination or transit PRS to source PRS
3) Elements
   a) List of { Flow_Identification, Start_Time, Stop_Time,
      1) List of { Measurement_SegmentID, Problem_Code,
         i) List of {MetricID, Metric_Value}}} : If this Problem_Code is not 0, it indicates that there was some problem, for example, reroute_occurred or MP_failure, thus the metric values are not trustworthy.

8.5.5.14 DestinationIP_Change_Notification

1) Description: Notify that the destination IP of a measurement point is changed by some reason.. This means that source and transit PRS should re-target the route of this flow. Upon receiving this message, source PRS should relay this message to transit PRSs. This message must be re-sent periodically (every 3 seconds) to the source PRS until a confirmation message is received
2) Direction: From destination PRS to source PRS or from source PRS to transit PRS.
3) Elements:
   a) Flow_Identification
   b) New_DestinationIP
   c) Date and time, when the address change will or did occur

8.5.5.15 DestinationIP_Change_Confirmation

1) Description: Confirmation to DestinationIP_Change_Notification.
2) Direction: From source PRS to destination to PRS or from transit PRS to source PRS.
3) Elements : New_Flow_Identification

8.5.5.16 Stop_Performance_Measurement_Request

1) Description: Request to stop performance measurement. No response message is needed.
2) Direction: From source PRS to destination and transit PRS.
3) Elements:
   a) Flow_Identification : Uniquely identifies the target flow
   b) Measurement_SegmentID: On which Measurement-segment, measurements should stop.
   c) Stop_IPaddress_Updates: Relieves the destination PRS of notifying the source PRS of subsequent IP address changes of measurement equipment until the next Start_Performance_Measurement_Request is received from that source PRS.

8.5.5.17 Stop_Performance_Measurement_Response

1) Description: Response to Stop_Performance_Measurement_Request.
2) Direction: From destination or transit PRS to source PRS.
3) Elements:
   a) Flow_Identification : Uniquely identifies the target flow
   b) Measurement_SegmentID: On which Measurement-segment, measurements have stopped.

8.6 Performance of Measurement Management Systems

The following table specifies the message timing required between providers, and between providers and the registry.

Table 4 – Performance of Management Messages

Parameter	Action	Requirement	Comment
RP_latency	Latency time following Rollup period to distribute Rollup Period report to other providers	10 minutes max	Where exchange is previously agreed
IP_setup	Lead time to update Registry with new address info prior to changing address	1 hour min	Applies to PRS and measurement points
Sync_out_latency	Latency time following detection of loss of sync until indicated in response to probes to other providers	1 second max	
InterP-Probe_request_latency	Latency time following Inter provider request to allow probe until a response is sent	1 second max	
Misc_request latency	Latency time following Provider request for miscellaneous info until a response is sent	1 second max	
InfraP-Probe_request_latency	Latency time following Inter provider request for provider's internal measurement until a response is sent	1 second max	
Cust_compliance_latency	Latency time following Inter provider request for customer non-compliance report until a response is sent	1 second max	
Provider_compliance latency	Latency time following Inter provider request for provider non-compliance report until a response is sent	1 second max	
Registry_IP_access_latency	Latency time for registry to respond to IP address request	1 second max	
Registry_IP_update_latency	Latency time for registry to respond to update IP address request	1 second max	
Registry_update_latency	Latency time for registry to send update response to prior requesters following IP address update	10 seconds max	
Misc_update_setup	Lead time to update prior inter provider requesters with new information prior to change in information	1 second max	

9 Security Requirements

9.1 Introduction

Security is based on the protocol and surrounding environment defined in this document to support the measurements and their management. The security architecture defined in X.805 is used to create a framework to discuss the security requirements of measurements and their management. X.805 uses the concept of protecting the network by using an architecture that can be applied to create end to end security. The security dimensions are applied across the security layers described in X.805 and then again across the security planes. This section will further discuss security planes, layers and dimensions and the applicability for this document. Figure 20 summarizes the X.805 architecture.

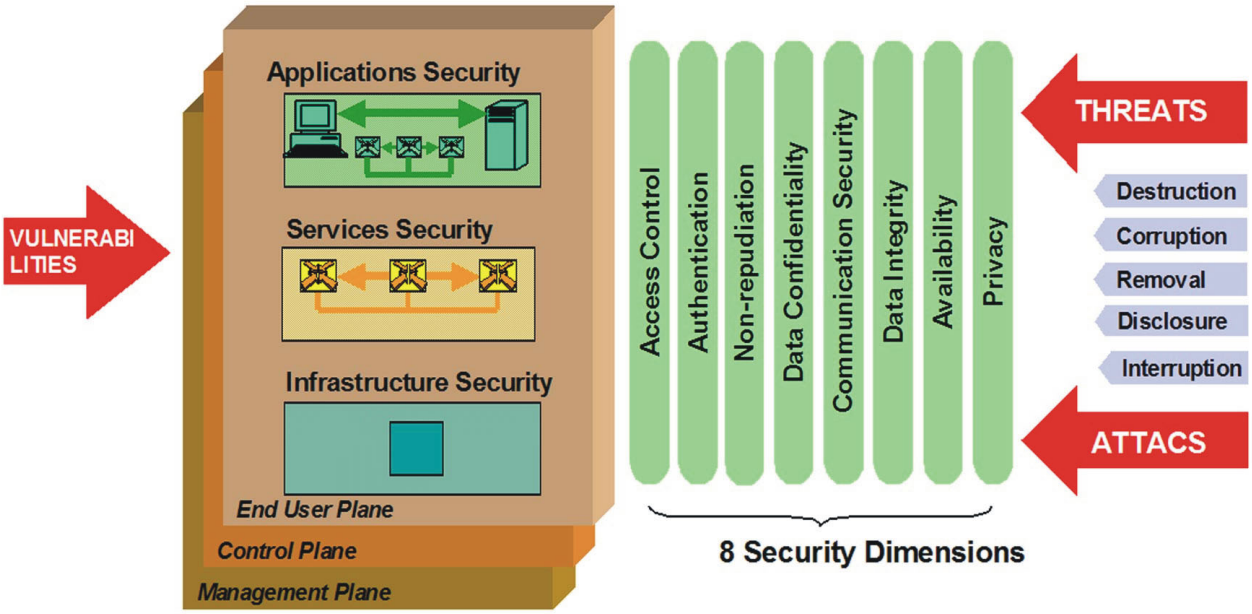


Figure 21 – Architecture of X.805

This document uses X.805 as the architecture to base the security solutions for Measurement and Management with the Inter Provider Information Transfers as the points to be secured.

The Inter Provider Information Transfers have dependencies upon systems whose security methods are not covered here.

1) Distributed time is important to being able to have accurate information in measurements and logging. However the security of the time sub-system is considered to be beyond the scope of this document.

2) Inter Provider measurements and management are dependent upon the availability of providers' measurement and management systems. The impact of their non-availability is discussed in 7.2.5.1. Methods to secure the host aspects of these systems are considered to be beyond the scope of this document.

3) Inter Provider measurements and management are dependent upon the underlying transport network whose security aspects are considered to be beyond the scope of this document. See informational RFC 3871.

9.2 Inter Provider Information Transfers

The following list is a summary of the inter provider information transfers used for Measurements and Management, where provider A has a PRS A, and provider B has a PRS B.

1) Active measurement probes (per section 7.2.1)
   a) Measurement Probe (UDP) between measurement points belonging to provider A and provider B
   b) Measurement Probe Response (UDP) between measurement points belonging to provider A and provider B
2) Measurement initiation and reports (per sections 7.3.2 and 8.4)
   a) Request from PRS A to PRS B to for permission to initiate measurements by PRS A to PRS B
   b) Response from PRS B to PRS A to request for permission to initiate measurement by PRS A to PRS B
   c) Request from PRS A to PRS B for measurement report from PRS B of measurements within provider B
   d) Response from PRS B to PRS A to request for measurement report from PRS B of measurements within provider B
   e) Request from PRS A to PRS B for customer non-compliance reports from PRS B of measurements within provider B to a customer of provider B
   f) Response from PRS B to PRS A to request for customer non-compliance reports from PRS B of measurements within provider B to a customer of provider B
   g) Request from PRS A to PRS B for provider non-compliance reports from PRS B of measurements within provider B
   h) Response from PRS B to PRS A to Request for provider non-compliance reports from PRS B of measurements within provider B
3) Locating PRS' IP address (per section 8.3.1)
   a) Web services request from PRS A to a registry for PRS B's IP address
   b) Response to PRS A's web services request to a registry for PRS B's IP address
   c) Request from provider's PRS to registry to update its own IP address
   d) Response from registry to request from provider's PRS to registry to update its own IP address
   e) Update response from registry to PRS A's web services request to a registry for PRS B's IP address
4) Additional information e.g. IP addresses of measurement points, confirmation of customer subscriptions, etc. (per sections 8.3.2, 8.3.3, and 8.4)
   a) PRS A request to PRS B for additional information
   b) Response from PRS B to PRS A's request to PRS B for additional information
   c) Update response from PRS B to PRS A's request to PRS B for additional information

9.3 Security Assessment

In this section, X.805 is applied to measurements and their management.

9.3.1 Security Planes and Layers

9.3.1.1 End-User Plane, Control Plane, Infrastructure Layer, and Services Layer

For the purposes of this section, it is assumed that the End-user plane, Control plane, Infrastructure layer, and Services layer is secure per the policies of the Providers. It is considered outside the scope of this document to address End-user plane, Control plane, Infrastructure layer, or Services layer security.

9.3.1.2 Management Plane

The management security plane is concerned with the protection of OAM&P functions of the network elements, transmission facilities, back-office systems (operations support systems, business support systems, customer care systems, etc.), and data centers. The management plane supports the fault, capacity, administration, provisioning, and security (FCAPS) functions. It should be noted that the network carrying the traffic for these activities may be in-band or out-of-band with respect to the service provider's user traffic.[X.805]

The management plane is considered to be the appropriate location for where the information transfers would take place. Thus for purposes of this document the management plane is the only applicable security plane.

9.3.1.3 Application Security Layer

The applications security layer focuses on security of the network-based applications accessed by service provider customers. These applications are enabled by network services and include basic file transport (e.g., FTP) and web browsing applications, fundamental applications such as directory assistance, network-based voice messaging and email, as well as high-end applications such as customer relationship management, electronic/mobile-commerce, network-based training, video collaboration, etc. Network-based applications may be provided by third-party Application Service Providers (ASPs), service providers acting also as ASPs, or by enterprises hosting them in their own (or leased) data centres. At this layer there are four potential targets for security attacks: the application user, the application provider, the middleware provided by third-party integrators (e.g., web-hosting services), and the service provider. [X.805]

For the purposes of this section it is considered that all measurement and management reports and information to fall under the Application Security Layer. The information transfers fall in to the Application Security Layer.

9.3.2 Security Dimensions

This section considers the 8 security dimensions and maps them to the Information Transfers listed in section 9.2. In this way the security requirements for each Information Transfer are established, allowing for consideration of effective solutions for meeting those requirements. The security dimensions are:

1) Access Control
2) Authentication
3) Non-repudiation
4) Data Confidentiality
5) Communication Security
6) Data Integrity
7) Availability
8) Privacy

Table 5 illustrates the mapping between the security dimensions and the Information Transfers. The Information Transfers are referred to by number and letter as referenced in section 9.2. The mappings take on

what is the level of importance for the security dimension in relation to the Information Transfer being referenced. The numbers 1, 2, and 3 are used to reference the level of importance. 1 is considered to be of very important, 2 is considered to be important and security should really be implemented, 3 is considered of little importance and thus security can be present, but the impact of it not being there is minimal. Following the table, is a description of how each of the security dimensions relates to context of the information transfers.

Table 5 – Security Dimensions per Information Transfer

Information Transfers	Security Dimensions							
	Access Control	Authentication	Non-repudiation	Data Confidentiality	Communication Security	Data Integrity	Availability	Privacy
1a	1	1	3	3	1	1	2	3
1b	1	1	3	2	1	1	2	3
2a	1	1	1	3	3	1	3	3
2b	1	1	1	1	3	2	3	3
2c	1	1	1	1	3	2	3	3
2d	1	1	1	1	3	1	3	3
2e	1	1	1	1	3	2	3	3
2f	1	1	1	1	3	1	3	3
2g	1	1	1	1	3	2	3	3
2h	1	1	1	1	3	1	3	3
3a	1	1	3	3	3	2	3	3
3b	1	1	3	1[A]	3	1	1	3
3c	1	1	1	1[A]	3	1	1	3
3d	1	1	1	1[B]	3	1[B]	1	3
3e	1	1	1	1	3	1	3	3
4a	1	1	1	1	3	2	3	3
4b	1	1	1	1	3	1	3	3
4c	1	1	1	1	3	1	3	3

NOTE A –Data Confidentiality High is to protect the registry IP information from unauthorized access or viewing.

NOTE B – Depending on what data is actually being passed here (response to registry update) will vary the level that Data Confidentiality and Data Integrity should be set to. If it is simply an acknowledgement that it received the information then the Data Confidentiality/Data Integrity would be Low or Medium. If it is sending back "I got your information and this is what I got" then the Data Confidentiality/Data Integrity is going to be High. For the purposes of this section it is assumed that the latter is the case.

9.3.2.1 Access Control

The access control security dimension protects against unauthorized use of network resources. Access control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. In addition, Role-Based Access Control (RBAC) provides different access levels to guarantee that individuals and devices can only gain access to, and perform operations on, network elements, stored information, and information flows that they are authorized for. [X.805]

Access Control here refers to authorization. The following should be ensured:

- Only authorized probes have access to measurement points.
- Only authorized provider PRSs are able to request measurement information, query the registry or request additional information from another provider's PRS.
- Limit the ability of unauthorized systems or users from requesting potentially sensitive information that could be used to expose vulnerability.
- Only accept information from authorized systems.
- Protect against spoofing.

9.3.2.2 Authentication

The authentication security dimension serves to confirm the identities of communicating entities. Authentication ensures the validity of the claimed identities of the entities participating in communication (e.g., person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication. [X.805]

- Only trusted systems have access to measurements, reports and additional information
- Identity of system requesting information is verified
- Registry access limited to trusted resources
- Verify identity for measurement probes to sent or received
- Verification of measurement probes may cause an overhead that could impact the performance of the system. It may not be optimal to authenticate each probe, but a caching of authentication could be allowed. However considerations for caching would include how often to update, when are the updates done, and how and when to clear the cache.

9.3.2.3 Non-repudiation

The non-repudiation security dimension provides means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). It ensures the availability of evidence that can be presented to a third party and used to prove that some kind of event or action has taken place. [X.805]

- Tracking of requests for measurement, reports, or additional information
- Record of request origination for updates to registry

The reason non-repudiation is important is because Providers may chose to charge a fee for these services. In this case, the provider requesting and receiving information should not be able to falsely claim they neither made the request, nor received the requested data.

9.3.2.4 Data Confidentiality

The data confidentiality security dimension protects data from unauthorized disclosure. Data confidentiality ensures that the data content cannot be understood by unauthorized entities. Encryption, access control lists and file permissions are methods often used to provide data confidentiality [X.805]

- Protection of non-authorized users from viewing information in measurement reports, or additional information provided by a Provider's PRS system to another Providers PRS system
- Protection of unauthorized access or viewing of measurement reports and additional information stored on a Provider's PRS system
- Protection of unauthorized access or viewing of information stored in the repository

9.3.2.5 Communication Security

The communication security dimension ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points). [X.805]

- Measurement information to be accurate must follow a precise path. Ensuring a constant data flow that is not intercepted or diverted is critical to accurate information.

For the purpose of this document it is assumed that the provider is already managing the traffic path as part of the provider policies.

9.3.2.6 Data Integrity

The data integrity security dimension ensures the correctness or accuracy of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities. [X.805]

- Protection from unauthorized modification of measurement information
- Protection from unauthorized modification of reports or additional information requested from one provider's PRS to another provider's PRS
- Protection from unauthorized modification of updates to the registry

9.3.2.7 Availability

The availability security dimension ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions are included in this category. [X.805]

- Ensure Measurement and Management devices are not impacted by information requests or probes

It is assumed that device protection against DoS attacks has been addressed in standard operations.

9.3.2.8 Privacy

The privacy security dimension provides for the protection of information that might be derived from the observation of network activities. Examples of this information include web-sites that a user has visited, a user's geographic location, and the IP addresses and DNS names of devices in a service provider network. [X.805]

With the nature of measurement and monitoring privacy is not a high priority.

9.3.3 Security Threats

Examination of the 5 threat categories, destruction, corruption, removal, disclosure and interruption as they relate to measurement and management, yields the following:

9.3.3.1 Destruction of information and/or other resources

Destruction of information is defined to be the erasure of data stored on the PRS or Registry. This threat is focused on the host and is secured with proper host security.

For the puroses of this document it is assumed that the host security will be maintained by the provider per existing security policies.

9.3.3.2 Corruption or modification of information

Some examples of the form that this threat could take are:

- Undetectable changes in contents such as the timestamp or clock sync monitor
- Acceptance of unauthorized requests for measurement reports
- Acceptance of unauthorized requests for customer subscriptions information
- Acceptance of unauthorized reports
- Loss of registry data integrity
- Different routing of probes versus regular traffic in the same QoS class
- Delaying/accelerating probes versus regular traffic in the same QoS class

9.3.3.3 Theft, removal or loss of information and/or other resources

For the purposes of this document it is assumed that the host security will be maintained by the provider per existing security policies.

9.3.3.4 Disclosure of information

Some examples of the form that this threat could take are:

- Unauthorized disclosure of customer subscriptions information
- Unauthorized disclosure of measurement report information
- Unauthorized disclosure of PRS's or measurement point's IP address

9.3.3.5 Interruption of services

Some examples of the form that this threat could take are:

- Acceptance and processing of misdirected probes
- An unexpectedly huge number of probes impinging a measurement point
- An unexpectedly huge number of requests impinging a PRS
- An unexpectedly huge number of response updates
- Acceptance of unauthorized requests for initiation of measurements
- Registry unavailability
- PRS unavailability
- Measurement point unavailability
- Disruption of the distributed "time"
- Disruption of the measurement system.
- Huge sustained packet loss
- An unexpectedly huge number of BGP updates

9.4 Security Solutions

This section considers solutions to the security dimensions: Access Control, Authentication, Data Integrity, and Availability.

Table 5 illustrates the mapping between the security dimensions and the Information Transfers which are grouped into 4 types, active measurement probes, measurement initiation and reports, locating PRS' IP addresses, and additional information. To further group similar functions the Information Transfers have

been grouped into either Measurement or Management Solutions. Measurement Solutions include active measurement probes. Management Solutions include inter-PRS (initiation of measurements, the requesting of reports and requesting additional information) and PRS-Registry communications (location PRS's IP addresses).

9.4.1 Measurement Solution

From table 5, probes need to have strong Access Control, Authentication, and Data Integrity.

- Access Control for any measurement probes should verify that probes only come from known or authorized addresses. To limit access to probes from only the known addresses a firewall or Access Control Lists should be used for protection.
- Authentication of the probes will be done using certificates to be sure that the probes are coming from the known locations. Since the availability of measurement points is important for the monitoring operation rate-limiting should be used to protect against authorized but errant probes.
- Data Integrity is required to protect from unauthorized modification of measurement information. Data Integrity must be achieved using signed message authentication code (such as MD5 or stronger) supported by appropriate digital certificates.

9.4.2 Management Solution

From table 5, management information transfers need to have strong Access Control, and Authentication. Regarding inter-PRS information transfers:

- Access control of both requesting and receiving reports is of high importance. To limit access to known providers a firewall or access control lists should be used for protection. Considering how to scale the ability to manage the various security aspects, more centrally managed solutions are recommended.
- Authentication needs to be controlled via a central system to be sure that only authorized providers have access to the reports. Authentication has two potential methods that could be used, first is the use of certificates (which imply PKI) to confirm user identity and then a centralized data backend that approves the authorization of that user to request particular reports or initiate measurements. If a certificate system can not be used to perform authentication then pre-shared symmetrical keys should be used. However there would still need to be a centralized data backend that authorizes access. The use of the certificate can provide the additional requirement of non-repudiation because only the specified provider would have the certificate. In addition certificates can be used in the security solution for data integrity, non-reputation and data confidentiality as well. Because of the multiple functions that certificates can provide, the solution that will be used is based on certificates for authentication. A common Certificate Authority structure will need to be created (or an existing one leveraged) and maintained. This could be co-located with Registry functionality.

Regarding PRS-Registry information flows:

- Access control to limit who can access the registry would be done via a Firewall or Access Control Lists.
- Authentication will be achieved via certificates with a backend data system that determines authorization to the particular data being requested. This limits who has the authorization to make changes to a provider's information and differentiate that from the providers that may have read only access. The usage of certificates also supports the ability to do non-repudiation and data integrity. Since the availability of the registry is key for many providers' operation rate-limiting could be used to protect against authorized but errant requests.

9.5 Measurement Performance Impact of Security

The strength of security measures used in a solution can burden systems, and/or cause extra security-related traffic. Since a heavily burdened router or firewall, or waiting for security related traffic to return may delay measurements, some risks versus benefits need to be considered.

To meet the high level of security requirements listed above by implementing Authentication and Data Integrity into the probes would require additional overhead on the measurement devices to do the authentication and data integrity. Depending on the number of probes this could impact the measurement devices with the overhead cause by this operation.

To handle the performance of doing authentication, this could be done on the measurement device itself or off-loaded to another system. The recommendation is to do the authentication on the measurement device itself since it would likely allow for faster response than off-loading to another device requiring security-related network traffic.

Annex A

Passive Measurement

A.1 Purpose

Passive measurements are a method of observing user data packets on a network link without the need to generate test packets like those required to implement active measurements. Thus it quantifies the performance that the users actually experience more precisely. Additional active probe traffic is not necessary however movement of large amounts of measurement data for correlation is typically required. Passive measurement traces can be used for a number of purposes, including the monitoring of application and network performance, the characterization of various traffic types being used, the accounting of traffic being used, the diagnoses of faults in the network, the traffic engineering, anomaly detection and the trends in network behavior over time.

Before passive measurement can be made it is necessary to define a mechanism to capture the packets. This potentially can be achieved with the use of 2 or more devices connected to the network area that passive measurements are to be made for. The device can be the network elements themselves or standalone dedicated measurement equipment. The use of network elements to capture packet information is efficient because it directly uses the existing measurement data associated with the network elements. However, the principal function of elements such as routers and switches is to forward packets and for this reason they commonly do not contain enough storage or processing capability to enable packet capture to be implemented on a large-scale. They typically provide packet and byte counter on each incoming and outgoing interface and flow data in a limited scope (use sampling if the interface is very high speed). Another form of network element based measurement is OAM-based traffic management. OAM is defined mainly for fault management but efforts to support performance monitoring are also under way. If this capability is in place, passive measurement can utilize OAM for fine-grain traffic measurement and analysis without adding additional cost for probe deployment.

The deployment of dedicated measurement devices enables a more comprehensive packet capturing functionality. The commercially available products typically insert measurement devices on to the network links where analysis is required. These measurement devices operate passively and do not affect the characteristics of the packet flows that pass through them. The key benefit that the measurement devices have is their ability to aggregate comprehensive statistical information on their associated packet flows at very high data rates with little or no loss and with accurate time synchronization. The measurement devices generally have large storages that enable the archiving of such statistical data and the subsequent identification of long-term trends in packet flows is possible.

The implementation of performance measurement using passive techniques is challenging because it is necessary to construct a comprehensive view of the network performance from a series of statistical cuts that represent the operational state of the network elements or deployed measurement devices. Fortunately, the relevant technology in this field is advancing fast such a way that it should be possible to construct a comprehensive view of the network and application performance as a set of end-to-end paths. Passive measurement along with active one can be used harmoniously to compensate each other's disadvantages and will eventually provide solutions to achieve the required objectives.

A.2 Passive Measurement Mechanisms

Packet-based passive measurement method relies on full packet capture from the network area of interest. Typically, it is used for lower speed interfaces or links due to the performance overhead involved. Fully captured packet traces can provide the most detailed information for the analysis but it also exposes a limitation of real-time analysis. Storage requirement is also another issue for storing large amount of captured packet traces. Thus, this method is used mainly for off-line non-realtime analysis of network and application traffic characteristics. Embedding this capability in the network element itself is not a trivial thing and, thus, a dedicated measurement device is usually used. Recent research copes with performance and storage limitations by introducing sampling, filtering, and other techniques by compromising the accuracy of the measurement and analysis. Various public and commercial hardware and software tools in this category have been developed such as CAIDA's OCxmon, Tcpdump, and Ethereal, and SPRINT's IPMon, and NDACE's DAG cards.

Flow-based passive measurement method was introduced to resolve the limitations shown by the packet-based method. Instead of dealing with each packet for the analysis, this method constructs a flow record from a series of packets which have a certain common characteristic (e.g., the same source and destination addresses, port number, and protocol ID). This aggregation significantly reduces the amount of storage and packet processing overhead. Each flow record only keeps track of summary information of packets of the common characteristics and discards packets themselves. Flow records can be measured either in the network element itself or by a dedicated flow measurement device. If the interface or link to be measured is low speed, both methods can perform their job without performance degradation. However, if it is high speed, either sampling in the embedded elements or standalone device is required since large memory is required to hold flow cache and fast flow records generation negatively influences system forwarding performance. This method can be utilized for various applications such as traffic profiling, traffic engineering, attack/intrusion detection, QoS monitoring and usage-based accounting. Many tools in this area have also been developed. Some of the notable ones are Cisco's Netflow, CAIDA's CoralReef, Flowscan, and NetraMet. Recently, IETF IPFIX(IP Flow Information eXport) working group has been defining a standard way of exporting flow information.

Content-based passive measurement method has been emerged recently due to highly dynamic nature of the development and the use of the current Internet applications. Traditionally, Internet traffic was dominated mostly by the client-server type of applications such as WWW, FTP, TELNET, etc. However, this characteristic has been changed significantly when new applications such as peer-to-peer, multimedia and network game applications were introduced. These applications use a range of port numbers or dynamically allocated ones for their sub-transactions. (e.g., EDONKEY uses 4661, 4662, 4665, 6667 and RTSP streaming

application allocates a port number dynamically for a stream data transfer) Internet Assigned Numbers Authority (IANA) recommends the usage of application port numbers: 0 ~ 1023 for well-known ports, 1024 ~ 49151 for registered ports, and 49152 ~ 65535 for dynamic and/or private ports. However, the application developers do not strictly follow this recommendation. Several Internet applications can use the same port number and some do this for malicious purposes, e.g., port number 80 for firewall bypass or security attack. This means that distinguishing flows based on a port number and other header properties is not safe and accurate enough. Thus, application header information and application signature matching in a packet payload are needed for the precise measurement. This method can be considered as an enhancement of flow-based method if flow characteristics include application header and application signature information. However its use is limited to un-encrypted traffic. This method may cause more performance overhead for deep packet inspections but it enables precise application traffic measurement and analysis. Most tools available in this area are still limited in the research stage. There are few commercial solutions.

OAM-based passive measurement method is the one which relies on OAM performance data. Currently, OAM standardization efforts are underway in the area of MPLS and Ethernet. OAM-based fault management work is quite mature but OAM-based performance monitoring work is at the beginning stage. OAM-based method has a number of advantages. Its capability is purely embedded in the network elements and, thus, it supports wire-speed domain-wide performance monitoring. Path level (e.g., an MPLS LSP in a managed domain) end-to-end real user's traffic performance monitoring is possible. A number of commercial solutions are under development.

Four representative passive measurement mechanisms have been described in this section. Each method has its own pros and cons and they are not mutually exclusive. In fact, one or a combination of several methods can be used appropriately to serve particular measurement objectives.

The following table summarizes the above mechanisms and possible measurement device types used in each case. It also identifies their characteristics in terms of scalability, cost, real-time support, and supported metrics.

Table A.1 – Measurement Device Types and Characteristics

Measurement Methods	Measurement device Type	Scalability	Cost	Real-time	Metrics
Packet-based	Embedded in Network Element	Low	Low	Yes	IPLR, Packet, Byte count per interface
	S/W Probe in User Terminal	Low	High	Yes	Packet, Byte, other terminal specific metrics (e.g., MOS, etc.)
	Dedicated Standalone Measurement device	High	Medium	No	IPTD, IPDV, IPLR, Packet, Byte count per interface
Flow-based	Embedded in Network Element	Low	Low	Yes	IPTD, IPDV, IPLR per flow
	S/W Probe in User Terminal	Low	High	Yes	IPTD, IPDV, IPLR per flow
	Dedicated Standalone Measurement device	High	Medium	Yes	IPTD, IPDV, IPLR per flow

Table A.1 – Measurement Device Types and Characteristics

Measurement Methods	Measurement device Type	Scalability	Cost	Real-time	Metrics
Content-based	Embedded in Network Element	Low	Low	Yes	IPTD, IPDV, IPLR per flow and applications
	Dedicated Standalone Measurement device	High	High	Yes	IPTD, IPDV, IPLR per flow and applications
OAM-based	OAM based	High	Low	Yes	IPTD, IPDV, IPLR per path

More detailed description of each mechanism is provided in the following sub-sections.

A.2.1 OAM-based Passive Measurement

OAM-based performance measurement could be classified as either active or passive depending on how it is used. If generation of additional OAM packets by a performance reporting system is controllable, it can be considered as OAM-based active measurement. Whereas, if OAM packet generation is not controlled by the PRS, and OEM packets are also used by passive measurement systems then it is considered as OAM-based passive measurement. In this section, OAM-based passive measurement only is described.

A.2.1.1 Requirements for OAM-based Passive Measurement

Some application level protocols such as RTP include the sequence-number and time-stamp fields in the packet header. They can be used for performance measurement but there are some limitations:

1) Only real-time applications use RTP protocols;

2) RTP packets only occur within the duration of an application session;

3) Performance measurement can not be performed at anytime.

If an OAM packet has the sequence-number and time-stamp fields in its header, OAM-based passive measurements can be performed without the limitations mentioned above and can be embedded into the transport devices. The cost is very low and can be applied independent of applications.

To perform OAM-based passive measurement, there are some requirements as follows for any packet-based transport technology:

- OAM packet has the sequence-number and time-stamp fields in its header;
- Clock synchronization at each measurement point;
- The devices on measurement points must support OAM packet. It is optional if the network devices along the transit path support OAM packet or not. (If the devices along the path support OAM packet, we can locate the failure point in the case of packet loss.)
- In case of use of load spreading techniques such as ECMP, any individual measurement is only representative of the measurement for a FEC.

At least four types of OAM packet formats as well as the related OAM-based passive measurement methods deserve study for NGN. These include IPv4, IPv6 , MPLS, and Ethernet OAM packet formats and their corresponding passive measurement methods.

MPLS and Ethernet OAM packet formats can be specified for link-by-link network performance measurement. As far as end-to-end network performance measurement, IP OAM packets can be specified.

A.2.1.2 OAM Packet Format Examples for Support of Passive Measurement

We provide several examples of possible OAM packet formats which meet the requirements for OAM-based passive measurements. The examples are shown in this section strictly to clarify the usage of OAM for passive measurement. The standardization of the OAM packet formats and their semantics are out of scope of this document.

- Example of MPLS OAM packet format

Table A.2 – Example of MPLS OAM Packet Format to Support Passive Measurements

Function type (04)	Reserve (all 00Hex)	Sequence Number	LSP Trail Termination Source Identifier	Timestamp Sent	Timestamp Received	Padding (all 00Hex)	BIP16
1 octet	1 octet	2 octets	20 octets	4 octets	4 octets	10 octets	2 octets

– Function type: Identify OAM packet function. Referring to Y.1771, there is a function type field in the MPLS OAM packet structure. “04” is reserved for Performance measurement.

– Sequence Number: Identify a packet. It can be used to determine if packet loss occurs.

– Timestamp Sent: the timestamp applied when a packet is sent.

– Timestamp Received: the timestamp applied when a packet is received.

- Ethernet OAM packet format

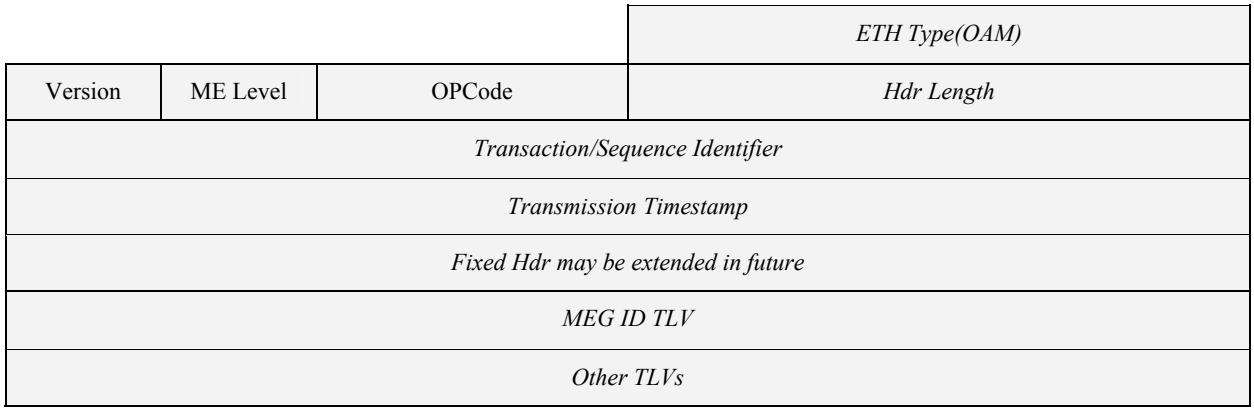


Figure A.1 – Ethernet OAM Packet Format to Support Passive Measurements

The Ethernet OAM format conforms to the definition of Y.17ethoam as follows:

– OAM Ethernet Type: This is a unique Ethernet Type that identifies OAM frames.

– Version: The Version field identifies the OAM protocol version. Value for current version is 0x00

– ME Level: ME Level identifies the administrative domain of the OAM frame.

– OpCode: The OpCode defines the type of OAM frame.

– Hdr Length: The number of bytes in the fixed-length header, starting with the Version field.

– Transmission/Sequence Identifier: Supplied by the originator of OAM request and copied in the OAM reply. Semantics of this field are dependent on the OpCode.

– Transmission Timestamp: Time at which the OAM frame was transmitted from originating MEP.

– MEG ID: The first TLV that identifies the MEG.

– Other TLVs: These TLVs correspond to OAM frame type.

- Example of an IP OAM packet format

Version	IHL	TOS	Total Length	
Identification			Flags	Fragment Offset
TTL		Protocol ID (255)	Header Checksum	
Source Address				
Destination Address				
OAM Type		Detection ID	Sequence Number	
Timestamp Sent				
Timestamp Received				
Extension Field				

Figure A.2 – Example of an IP OAM Packet Format to Support Passive Measurements

– Protocol ID: Referring to RFC 791, there is a protocol field in IP header.
"255" is a reserved value for this field and here can be used to identify the IP OAM packets.

– OAM Type: An 8-bit OAM Type field defines as follows:
0: Reserved;
1: Performance Measurement Information;
2: Performance Measurement Request;
3: Performance Measurement Reply;
Others are reserved for latter use.

– Detection ID: The ID is used for identifying the detection. For instance, multiple detections may be carried out at the same node simultaneously. The Detection ID could uniquely identify on which link the delay detection is operated.

– Sequence Number: Identify a packet. It can be used to determine if packet loss occurs.

– Timestamp Sent: the timestamp applied when a packet is sent.

– Timestamp Received: the timestamp applied when a packet is received.

– Extension Field: reserved for further standardization

The structure of IPv6 OAM packet can be similar to that of the IPv4 OAM packet. The IPv6 OAM packet can also be identified by a special protocol ID.

A.3 Comparison between Active and Passive Measurement

The following table briefly highlights main properties of the active and passive measurement methods. It identifies differences between the two in terms of configuration, direction, data size, network overhead, CPU requirement, scalability, blocking, and major purpose.

Active method requires multiple probes in the close proximity of source and destination of the measurement area, whereas passive method usually requires less number of measurement devices and its locations can also be independent from the source and destination of measurement area. Both active and passive measurements can be made both one-way and two-way . Test data generated by active measurement is relatively small amount compared to what passive measurement can collect. Both passive and active measurements may impact the performance of user traffic. Passive measurement CPU resource consumption is much higher than that of active method. Making measurement at the level of granularity necessary for a per-customer basis in an end-to-end context is very challenging for both active and passive methods. In case of the active method, many probes have to be deployed at the closest proximity of the end-users. In case of the passive method,

many measurement devices have to be deployed at the necessary links of measurement. Passive measurement of appropriate capability can measure end-to-end performance of many real end-users paths or flows which are not possible by the active method. Active method test packets can be blocked by service providers when it crosses administrative domain boundaries, however, the passive method doesn't have such a concept. Accuracy in terms of reflecting real end-users traffic performance is much higher in the case of passive method.

Table A.3 – Comparison of Active Probing and Passive Measurement methods

	Active	**Passive**
Configuration	Multipoint	Single or Multi
Direction	One-way/Round-trip	One-way/Round-trip
Data Size	Small	Large
Network Overhead	Additional probeTraffic plus some measurement data traffic	Large amount of measurement data traffic
CPU requirement	Low to moderate	High
Scalability	High	Low to High
Blockable	Likely to be blocked or rate-limited if probes look like DoS attack.	Less likely, but possible for undesirable traffic e.g. peer-to-peer
Major Purpose	SLA compliance	Traffic Engineering, Usage-based Accounting, Traffic Profiling, QoS Monitoring, and Anomaly Detection
Accuracy relative to users data	Varies	High
Impact of user traffic encryption	None	Limits capabilities depending upon where the encryption occurs relative to the measurement points.

IETF IPPM metrics are defined for active method while ITU-T Y.1540 metrics are intended for passive method. However, active probes can be deployed at the Measurement Points defined by Y.1540 and metrics 4 ~ 10 below also can be used for active measurement. However, the difference is that IPTD in active method is for test traffic whereas IPTD in passive method is for real user traffic.

Table A.4 – Metrics supportable by Active Probing and Passive Measurement Methods

	Metric	**Active**	**Passive**
1	Type-P-*-One way Delay	X	
2	Type-P-*-Delay Variation	X	
3	Type-P-One way-Packet Loss	X	
4	IP Packet Transfer Delay	X	X
5	Variation in IP Packet Delay	X	X
6	IP Packet Error Ratio		X
7	IP Packet Loss Ratio	X	X
8	Spurious IP Packet Rate		X
9	IP Packet Throughput	X	X
10	IP Service Availability	X	
12	R-Value	X	X
13	Succeeded/Failed Call Attempt		X
14	Frames per second		X

The two methods can be used to compensate each other's limitations.

A.4 Architectural Considerations for Passive Measurements

One-way or two-way passive measurement requires the deployment of measurement devices to monitor traffic on network links or collection of data from the network elements. The passive definition of performance-based metrics on a per-customer basis in an end-to-end path context would require the monitoring of significant number of network links between customers' points-of-presence and the end points of paths. The simplest solution is the deployment of a monitoring measurement device on every one of these links but the associated cost is very high. The extreme case of this solution is to deploy the measurement devices in the core of a transport network. The assumption that the measurement device can identify the necessary packets and the timing information given in the packets is required in this case. Metrics can be measured from the customer to the measurement devices and between measurement devices. The concatenation of them can result in the end-to-end metrics. And other combinations between these two extreme solutions can be possible depending on the scalability and costs involved.

A.5 Passive Measurement Requirements

The passive measurement general requirements are:

- Should be able to contain one or more measurement entities: network element resident measurement entity, standalone measurement device, or OAM performance monitor
- Measurement should have a source and destination addresses, an associated QoS metric, and accurate starting and ending time
- Timestamps should be based upon UTC
- Should be able to capture a copy of the traffic without introducing modifications in the original traffic
- Should be able to classify a packet based on both IPv4 and IPv6 properties
- Should be able to classify tunneled traffic
- Should be able to perform measurement operation at wire-speed
- Should be able to timestamp at the arrival of the packets in micro-second level
- Should be able to perform time-stamping operation at wire-speed
- Should be able to synchronize clocks from a single source
- Should be able to support various sampling methods such as random, probabilistic, hash, flow-based, etc.
- Should be able to perform sampling operation at wire-speed
- Should be able to support sampling before classification and vice versa
- Should be able to perform flow accounting including packet and byte accounting
- Should be able to classify flows according to their types
- Should be able to handle fragmented packets
- Should be able to measure various packet sizes including full packet
- Should be able to derive various performance metrics such as delay, jitter, packet loss, unavailability, R-value, MOS, succeeded call attempt, failed call attempt, Frames per second, etc.
- Should be able to support various levels of measurement and analysis granularity ranging from subnet matrix to flow

The passive measurement configuration related requirements are:

- A measurement point should be able to be accessible by the management system to enable setting up, removing and stopping the measurement when requested

- Should be able to configure classification processes with configuration parameters
- Should be able to configure time-stamping source and its characteristics (e.g., resolution)
- Should be able to configure sampling process with sampling parameters
- Should be able to configure measurement devices remotely

The measurement device related requirements are:

- Should be as light as a software module which can reside in an end-user terminal or as complex as a separate large scale measurement system which can handle multi gigabit or higher traffic speed and volumes
- Should be able to export or respond to the polling request of the measurement results (RFC 3917 defines requirements for the export of measured IP flow information out of routers, traffic measurement probes, and middleboxes.)
- Should support a single interface for configuration and measurement operations
- Should be able to support a protocol for export and configuration operations and it has to be efficient, reliable, scalable, and secure
- Should be able to support multiple requests in parallel
- Should be able to notify the faults of the measurement device

A.6 Passive Measurement Metrics

This section defines performance metrics which can be measured by passive method.

a) One-way Delay – Passive one-way delay measurements require the collection of data at two measurement points. It is necessary to recognize packets at the second measurement point to correlate packet arrival events from both points. This can be done by defining a unique packet ID. Typically it can be done by capturing packet header and parts of the packet that can be used to recognize the same packet at the subsequent measurement point. Other variations are also possible. If OAM performance monitoring capability is supported, one-way delay measurement is one of the intrinsic capabilities. Also if application header inspection is possible, application provided timing information can be used to measure one-way delay. Passive one-way delay measurement assumes clocks at measurement points are synchronized by a single timing source.

b) IP Delay variation – IP Delay variation is defined as the difference of one-way-delay values for selected packets. Therefore, this metric can be calculated by performing passive measurement of one-way delay for subsequent packets of a flow and then calculating the differences.

c) One-way packet Loss – Passive loss measurements for single flows can be performed at one measurement point by using sequence numbers that are present in protocols such as IP identification and TCP sequence numbers. This requires the capturing of the sequence numbers of subsequent packets of the observed flow. An alternative is to perform a two-point measurement as described in one-way delay method and consider packets as lost that do not arrive at the second measurement point in a given time frame. This approach assumes that a packet observed at the first point should be also observed at the second observation point.

d) Unavailability

e) R-value

f) Succeeded call attempt, Failed call attempt

g) Frames per second

Passive measurement of d) ~ g) can be performed from the TE if appropriate passive measurement capability is provided in the TE.

h) Application-aware Traffic Usage Measurement

Another important but interesting applicability is measurement of traffic usage per application in very detail level if network elements or passive measurement devices have such capabilities. For example, when an NE or a measurement device can recognize applications based on application signatures which only can be detected by inspecting payload of packets, (if not encrypted) then accurate application performance monitoring and accounting measurement are possible. This is important especially because many Internet applications and even future NGN applications cannot be accurately recognized only by looking at the port numbers. Many applications use a range of port numbers or dynamically assigned ones. It is no longer assured that IANA assigned port numbers represent the intended applications. The only way to ensure the identity of the application is via a deep packet inspection.

A.7 Passive Measurement Scenarios

A.7.1 Two-point measurement

A.7.1.1 Architecture

Fig. A.3 shows the proposed hierarchical architecture of two-point measurement. In Fig. A.3, PRS of network A has the control of the measurement action. Under the condition of clock synchronization mentioned in section 7.4, we assume that PRSs can find out the current route of target flow.

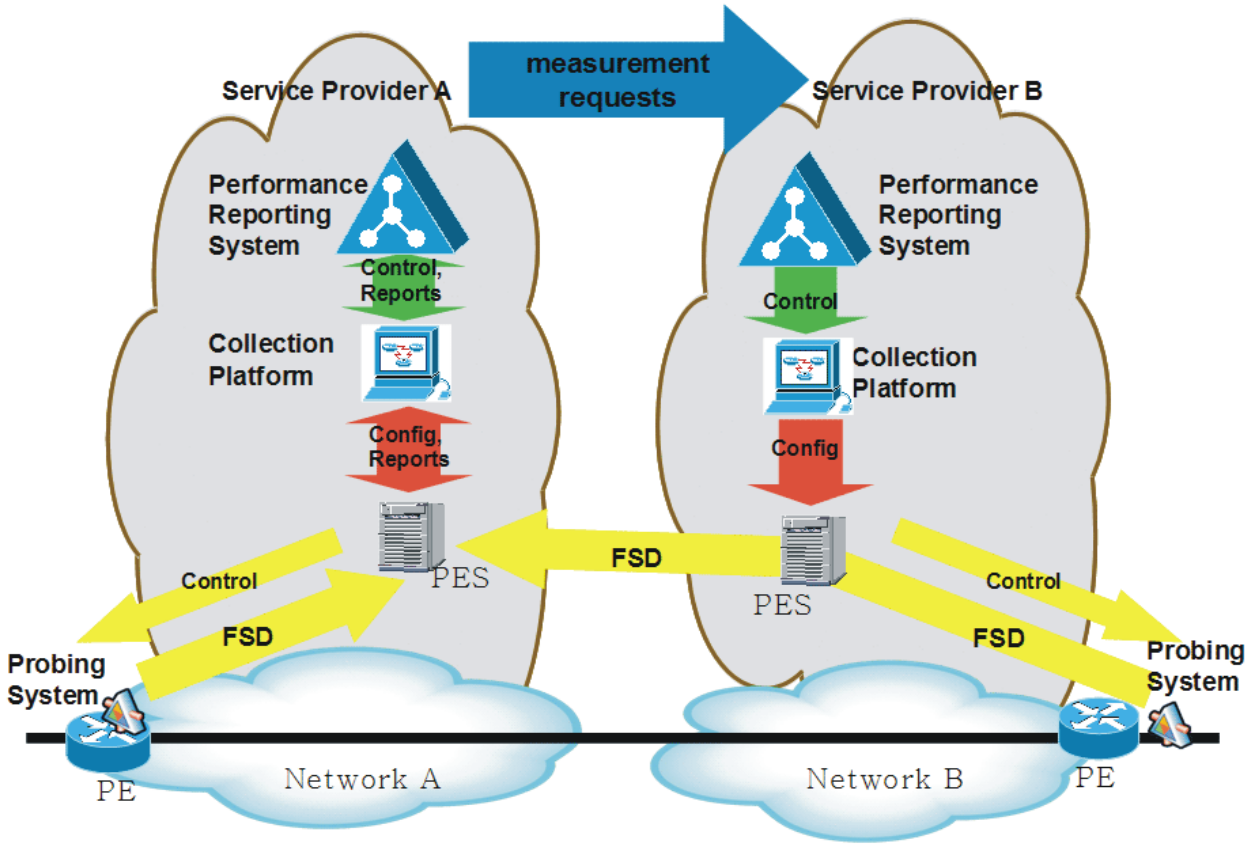


Figure A.3 – A Hierarchical Architecture of Passive Performance Measurement

Two Probing Systems extract some information (let's call this Flow Summary Data : FSD) from the packets of target flow and attach time-stamps. Probing System may be a dedicated H/W equipment tapping the optical signal from the transmission link, or may be a S/W or H/W module installed in a network element. FSDs from the two Probing Systems are reported at some gathering system (let's call this Performance

Evaluation System : PES). The PES in network A derives performance metric values by comparing the FSDs. Note that PES in network B just relays the FSD report to PES in network A. The performance metric values are stored in Collection Platform of network A.

If the routing path happens to change, one or both of the two Probing Systems may not be able to extract the packets. This may be perceived by PES. PES should report this to PRS. PRS will stop or restart the measurement procedure then.

Before starting measurement action, PRSs should exchange the address of their PESs to be involved.

Fig. A.3 shows only two networks and two Probing Systems. But there may be transit networks and intermediate Probing Systems.

A.7.1.2 Flow Summary Data

Contents of the FSD report from the Probing System should have the following information at the minimum:

- Flow-identification (FlowID) : The target flow which the packet belongs to. To identify a flow, source IP and port, destination IP and port, protocol ID, service class information are needed. These can be derived from IP and TCP/UDP headers.
- Time-stamp : The exact time when the packet passes the Probing System.
- Packet-identification (PacketID) : To identify each packet in the flow. It's from Identification and Fragment-offset field for IPv4 and Flow-label field from IPv6

PES can evaluate the packet transit delay and delay-variation between the two Probing System of each packet from the difference between Time-stamps. And PES can detect the loss of packet by comparing the two list of PacketIDs.

The volume of FSD report, from Probing System to PES, from PES to PES, must be reasonable. Thus, care must be given when the format of the FSD report is designed. Trade-off between accuracy and volume of report should be well managed.

- FSD report should be done collectively. In other words, it should not be done for each packet. And, naturally, the FlowID should be one of the heading fields of the FSD report.
- Reporting only for sampled packets will drastically reduce the volume of the FSD report. The reasonable rule of sampling is to use PacketID of a packet :
  - IPv4 : Sample the packet whose Identification is multiple of a number N.
  - IPv6 : Sample the packet whose Flow-label is multiple of a number M.

  The number N or M above should be properly decided according to the average bandwidth of the target flow, and should be given to Probing Systems during the initiation of measurement action.
- Reporting the inter-arrival time between the sampled packets rather than reporting the absolute arrival time of each sampled packets will also reduce the volume for reporting Time-stamp information. Only the absolute arrival time of the first packet in the report needed to be recorded in the heading field of the FSD report. How many bytes should be used to report inter-arrival time and the precision of this value also should be properly decided according to the average bandwidth of the target flow, and should be given to Probing Systems during the initiation of measurement action.

A.7.1.3 Shortcomings of Two-Point Measurement

Although the two-point measurement method can derive the accurate performance metrics of the real customer flow, it has some shortcomings below :

- If the Probing System is a specialized H/W equipment, scalability and coverage is the problem as the active performance measurement.

- Traffic volume of FSD report is not negligible, especially for inter-domain measurement action.
- Not trivial to measure the performance between PE-CE or PE-TE.

A.7.2 One-Point Measurement Using Real Time Protocol.

As mentioned above, the packet header of customer's usual traffic at transport layer and below does not have time stamp for delay and delay variation calculation.

Delay and delay-variation are important to real-time applications such as VoIP and Video-streaming. RTP (Real Time Protocol, RFC3550) is an additional transport layer protocol for real-time applications. RTP is designed to be independent of transport or network layer protocols. A RTP packet has Time-stamp and Sequence-number fields in its header. A Probing System can evaluate packet loss from the Sequence-number field. And, from the Time-stamp field, although its content and resolution depends on the category of application, the Probing System can evaluate the delay and delay-variation performance of the target flow if it has some knowledge, for example, encoding sampling rate, about the application of each target flow.

Though the accuracy of this method is not as high as the two-point one, its benefit in scalability and coverage deserves much consideration.

A.7.3 Passive Measurement at TE

It is possible to evaluate performance metrics by installing additional S/W and/or H/W modules in TEs. Some application specific metrics (e.g., MOS and R-value) and network level metrics (e.g., delay, jitter, and loss) can be evaluated by this method without using additional active probing systems in the network.

For example, RTCP is an optional control protocol for RTP mentioned above. Participating TEs exchange RTCP packets. In a RTCP packet, some performance related parameters like Fraction-lost and Inter-arrival-jitters are reported. TEs also are able to evaluate rough round-trip delay with these packets. By installing a light-weight agent S/W in TEs based on RTCP, network providers can collect the performance parameters without any active probing systems.

In the case that TE has a passive measurement agent, the agent can initiate end-to-end application and network level measurement when a new application session is started and report the measurement result when this session is terminated. For the scalability purpose, a proper number of measurement result collection systems can be deployed to cover a certain number of TEs. These numbers and coverage range can be decided empirically by the operational experiences. A decision of the exact number is out of scope of this document.

A.7.4 Active and Passive Hybrid Measurement

Section 7.3.2 defined various active measurement scenarios based on the three purposes: operating, supporting, and testing. Also several passive measurement scenarios have been defined. Active and passive measurements mechanisms can be used independently to meet a specific purpose. However, there may be a situation where passive measurements can take advantage of active probes enabling both methods to be used cooperatively. For example, TE-to-TE operating active measurement scenario requires separate measurement of several segments and each segment requires a pair of active measurement points. The measurement results from each segment are compared and aggregated to make an end-to-end metrics. Another possible solution is to have a single TE-TE active measurement and a number of passive measurement devices deployed at strategic locations such as demarcation PoP points, PEs, and CEs. Each passive device can recognize the sent active probe packets and measure network level metrics such as delay and jitter from the TE to the passive measurement point. For this method to be possible, we need an assumption. That is, each active probe packet has a unique identifier in the packet header that identifies whether it is an active probe packet and each packet has a timestamp when the packet is generated in the payload of the packet. The detailed format of such fields is out of scope of this document. If this method is possible, the main advantage is to reduce a

large number of active probes in the middle of the managed networks since one passive measurement device can handle a large number of active measurement sessions. Figure A.4 below shows one possible measurement scenario.

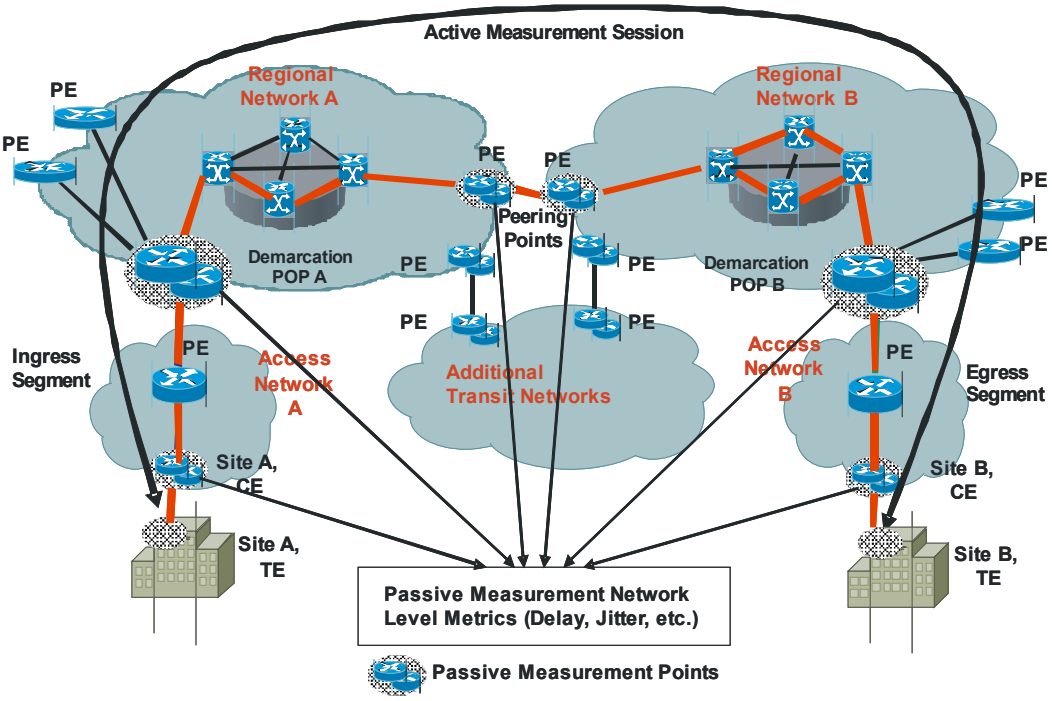


Figure A.4 – Example of Active and Passive Hybrid Measurement Scenario

In Figure A.4, one active probing session between a site A TE to a site B TE is shown and multiple passive measurement devices at CE, PE, and PoPs are deployed. The passive measurement result at each passive measurement devices is delivered to the collection system. Although only one active probing session is shown in the figure but passive measurement devices can handle numerous active probing sessions. Note that firewall and NAT traversal may need to be considered in this scenario.

Besides the network level metrics, this hybrid approach can be utilized to identify network measurement anomalies in routine operations due to erroneous data from active measurement probes.

A.7.5 OAM-based Passive Performance Measurement

Using the OAM packet formats described in the section 10.2.1.2, we can provide a general OAM-based performance measurement scenaro which can be applied in the similar way for any packet-based transport technology. The following is an example in IP network.

Figure A.5 – An example OAM-based Passive Measurement Scenario in an IP network

As shown in Figure A.5, an IP OAM packet is sent from A to D. Sequence number and timestamp (Timestamp sent) are added in the packet when IP OAM packet is sent from A. Sequence number is initiated from 1 and increased by one thereafter. When D receives the OAM packet, timestamp (Timestamp Received) is recorded in the packet. D can check sequence number and determine if packet loss or disorder occurs.

Here, packet disorder is considered as packet loss. IPTD can be figured out according to 2 timestamps and Mean IPTD can also be derived from all IPTD data in a measurement period. IPLR can be derived from all packets sent by A and received by D. Unavailability is determined if IPLR performance exceeds the predefined threshold. For the measurement of two-way performance metrics, D can send an OAM packet back to A after exchanging source and destination IP addresses. When A receives the OAM packet, timestamp (Timestamp Received) is recorded in the packet. Performance metrics including IPTD, IPDV, IPLR and IPUA can be derived from Sequence Number, Timestamp Sent, and Timestamp Received by A.

Annex B

Summary of Performance Objectives and Measurements

Table B.1 refers to Y.1541 revision in progress per Jan'05 (T05-SG12-050118-TD-WP3-0014!!MSW-E)

This table refers to draft Y.1541 proposals which may change prior to submission for October SG12 meeting. Note that classes 6 and 7 are proposed to become provisional classes.

U means Unspecified (Unbounded)

Regarding the Y.1541 network QoS classes, note that certain pairs of classes collapse into Node Mechanisms/Per Hop Behaviours/Queues. These are classes 0 and 1, 2 and 3, and 6 and 7. Therefore to probe all classes would require 4 measurement flows. Measurement results for these pairs would be used in comparison to objectives for each class.

Table B.1 – Summary of Performance Objectives and Measurements

Network Parameter Acronym	Parameter Description	Performance Objective	Units	Y.1541 Network QoS Classes								Relative to Y.1541	Covered in section(s)
				Class 0	Class 1	Class 2	Class 3	Class 4	Class 5	Class 6	Class 7		
IPTD	Mean IP packet transfer delay.	Upper bound over RP	ms	100	400	100	400	1,000	U	100	400	Per Y.1541. Classes 1 and 3 are for less contrained distance than 0 and 2 respectively.	7.1.2.1
DV90	IP Packet Delay Variation 90th percentile - minimum IPTD	Upper bound on delay variation over RP	ms	future	future	future	future	future	future	future	future	Not covered in Y.1541	7.1.3
DV99	IP Packet Delay Variation 99th percentile - minimum IPTD	Upper bound on delay variation over RP	ms	future	future	future	future	future	future	future	future	Not covered in Y.1541	7.1.3
IPDV, DV99.9	IP Packet Delay Variation 99.9th percentile - minimum IPTD	Upper bound on delay variation over RP	ms	50	50	U	U	U	U	50	50	Per Y.1541	7.1.3, 7.2.3
IPLR, ALR	IP packet loss ratio, Aggregate loss ratio	Upper bound on the packet loss probability over RP	%	0.1	0.1	0.1	0.1	0.1	U	0.001	0.001	Per Y.1541	7.1.4.1, 7.2.4
IPUA	Total period of excessive short term loss during which the network is considered unavailable	Upper bound on the percentage over month	%	0	0	0	0	0	1	0	0	Not covered in Y.1541	7.1.5, 7.2.5
SPW	Sliding Probe Window for unavailability	Corollary	Number of probes	50	50	50	50	50	50	50	50	Not covered in Y.1541	7.2.5
PLS	Threshold number of Probes Lost to Start unavailability period	Threshold	Number of probes	25	25	25	25	25	25	25	25	Not covered in Y.1541	7.2.6
PLE	Threshold number of Probes Lost to End unavailability period	Threshold	Number of probes	5	5	5	5	5	5	5	5	Not covered in Y.1541	7.2.5
PW	Policing Window	Corollary	Minutes	5	5	5	5	5	5	5	5	Not covered in Y.1541	7.2.6
PPS	Probe Payload Size(s)	Corollary	Octets	20	20	256	256	256	256	20	20	Y.1541 suggests 160 or 1500 octets. Per Y.1541 proposal.	7.2.1
RP	Rollup Period	Corollary	Minutes	5	5	5	5	5	5	5	5	Y.1541 suggests 1 minute. Per Y.1541 proposal.	7.1.1, 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.2.5
PTP	Probe Transmission Period (continuous)	Corollary	ms	200	200	200	200	200	200	200	200	Y.1541 suggests 10 to 20 ms for telephony. Y.1541 proposal suggests 20 ms for classes 0,1 or 50ms for classes 2,3,4 for 1 minute sampled out of 5 minutes	7.2.1, 7.2.2

2.14 – Algorithms for achieving end-to-end performance objectives (TR-apo)*

Abstract

This document considers several approaches and algorithms to achieve end to end performance objectives. This document is proposed to be submitted to SG12 at their meeting 17-21 October 2005 for progress by SG12.

Table of Contents

* Status P: This deliverable has already been passed to ITU-T Study Group 13.

2.14 Algorithms for achieving end-to-end performance objectives (TR-apo)

1 Introduction

Compared to networks and systems that are circuit-based, those based on IP pose distinctly different challenges for planning and achieving the end-to-end performance levels necessary to adequately support the wide array of user applications (voice, data, fax, video, etc). The fundamental quality requirements for these applications are well understood and have not changed as perceived by the user; what has changed is the technology (and associated impairments) in the layers below these applications. The very nature of IP-based routers and terminals, with their queuing methods and de-jitter buffers, respectively, makes realizing good end-to-end performance across multiple network operators a very major challenge for applications with stringent performance requirements.

Fortunately ITU-T Recommendations Y.1540 and Y.1541 together provide the parameters needed to capture the performance of IP networks, and specify a set of "network QoS" classes with end-to-end objectives specified. It is widely accepted (i.e., beyond the ITU-T) that the network QoS classes of Y.1541 should be supported by Next Generation Networks, and thus by networks evolving into NGNs.

Thus, while there is general agreement that the IP network QoS classes of Y.1541 are what should be achieved, what is missing is the methodology for satisfying the end-to-end objectives over paths involving multiple network operators, and in some cases, unusual topologies and distances. The guidance provided here is intended to accelerate the planning, deployment and management of networks and systems that can interoperate with a clear goal of supporting the end-to-end performance objectives detailed in Y.1541.

2 Scope

The scope of this document includes:

1) Broad consideration of approaches toward achieving end-to-end performance the Apportionment of End-to-End Performance Impairments including detailed examples.
2) Evaluation of the pros and cons of each approach.
3) A detailed recommendation for an approach or approaches including specific algorithms.
4) Detailed analysis of the recommended approach(es) including the aspects of
   a) scalability
   b) performance
   c) security, resistance to "gaming", and
   d) how SPs handle cases where the aggregated impairments exceed those specified for a service class.

3 References

1. Y.1540 IP packet transfer and availability performance parameters (under revision)
2. Y.1541 Network performance objectives for IP-based services (under revision)
3. ITU-T NGN FG WG3 TR-pmm doc (work in process)

4 Terms and Definitions

Apportionment Method of portioning a performance impairment objective among segments.

Allocation Formulaic division or assignment of a performance impairment objective among segments.

Access segment The network segment from the interface on the customer's side of the CE to the interface on the customer side of the first Gateway Router [NOTE: this definition needs to be aligned with the NGN FRA definition finally settled on].

Core Network segment A core network segment is between Gateway routers, including the gateway routers themselves. The network segment may include some number of interior routers with various roles (as shown in the reference path in Y1541 Figure 1.).

5 Abbreviations and Acronyms

AS Autonomous System

BGP Border Gateway Protocol

CE Customer Edge

DST Destination

GW GateWay router

IPDV Internet Protocol Packet Delay Variation

IPLR Internet Protocol Packet Loss Ratio

IPTD IP Packet Transfer Delay

LAN Local Area Network

MD Mean Delay

NP Network Performance

NSIS Next Steps In Signaling

PE Provider Edge

PL Packet Loss

RSVP ReSerVation Protocol

SP Service Provider

SRC Source

TBD To Be Determined

TE Terminal Equipment

UNI User Network Interface

6 Document Overview

Generally the approaches that could be taken in allocating total impairment targets among network segments can be characterized by the amount of information shared among segments. Each approach has their pros and cons, we describe them here with simple examples. (Detailed examples of various approaches may be included in Appendix A). The next section contains a detailed recommendation for an approach or approaches including specific algorithms. Following which is a detailed analysis section of the recommended approach(es) including the aspects of

a) scalability

b) performance

c) security, resistance to "gaming", and

d) how SPs handle cases where the aggregated impairments exceed those specified for a service class

7 Consideration of Approaches

For all approaches, a "top-down" or "bottoms-up" method could be applied. That is, percentages of the aggregated target (top-down) or fixed/negotiated values for impairments (bottoms-up) may be allocated for each segment. A hybrid of these methods, with percentages for some segments and fixed/negotiated values for others could also be used.

For some approaches, transit segment distances are required to estimate distance dependence metrics such as mean delay. Ground level distance between any two (User) points may be readily estimated despite the traffic's signal being carried over varying altitude, the non-spherical shape of the earth, etc. Distance-inefficient routing over multiple segments may result in traffic traveling over a significantly longer distance than expected between two User points. The approaches to accounting for these inefficiencies can also be characterized by the amount of information shared among segments. Selection of the quantization of distance e.g. kilometers, metro, regional, continental and international is independent in approaches where awareness of distance is required.

Regardless of the approach, there is no guarantee that the end-to-end objectives will be met.

The long term objective is expected to be a signaled approach, however, near-term, some simpler approach evolving to a more capable signaled approach may be recommended. In which case the recommendation should include an evolution path.

Table 1 – Summary of performance impairment apportionment approaches

Approach	Description	Information required at each segment	Pros	Cons
Static (simplest/least flexible) - no information is required to be shared among segments	A fixed number of segments is assumed Impairment allocation is formulaic among User, Access, Transit, and Peering segments	Information required is a) type of link, b) traffic service class and, c) transit distance	No information is required to be shared among segments. Access providers may re-allocate among their User, Access and Transit segments	May be over-engineered when number of segments is less that the number assumed Paths having more that the assumed number of segments are not covered Negotiation not supported.
Pseudo-static - some information is required to be shared among segments	The exact number of transit providers is determined Impairment allocation is formulaic among User, Access, Transit, and Peering segments	Information required is a) type of link, b) traffic service class and, c) transit distance d) destination address e) BGP tables	Impairment allocation may be efficient and scalable.	Signaling among providers is required to determine the number of transit providers in each traffic path e.g. from BGP number of AS's Negotiation not supported
Signaled (least simple/most flexible) - some information is required to be shared among segments and possibly with Users	The exact number and sub-type of all segments may be known e.g. if User segment is wireless or wireline Impairment apportionment may be negotiated among segments and with Users	Information required is a) type of link, b) traffic service class c) destination address d) BGP tables, or other means to determine path or paths at the operator-level, e) Network edge-edge performance information Additional information that may be required includes f) transit distance	Negotiation is supported allowing highly flexible apportionment among segments. No predefined allocations are required. Transit distance may not be required Able to address cases where the objective can not be met by consulting user for relaxed objective Consistent with proposed direction of methods automated by QoS Signaling (e.g. RSVP/NSIS).	Signaling among providers is required to negotiate the impairment apportionment for each segment. Signaling may be required to negotiate with User when the requested objective cannot be met Performance and routing information must be exchanged among providers to determine the identities of transit providers in each traffic path (e.g. from BGP number of AS's) and their performance. However, there are alternative ways to determine path, and many providers publish performance info in real-time.

A fourth approach which does not start the apportionment process with target impairments per provider as a basis is called here the "Accumulation" approach, it is summarized in Table 2 below:

Table 2 – Approach to Impairment Apportionment based on Accumulation

Approach	Description	Information required at each segment	Pros	Cons
Accumulation - some information is required to be shared among segments	The path through various network operator domains is determined. Impairment levels and other parameters may be solicited for various network segments or their proxy, combined and compared with Desired Objectives. If not met, then Path or User negotiation takes place, or the request is rejected.	Information required is a) traffic service class, b) destination address (always known), c) BGP tables, or other means to determine path at the operator-level, d) Network edge-edge performance	No allocations required, so no process to achieve agreements Impairment accumulation is simple and scalable. No distance and route-to-air conversion factors required. Negotiation is supported. Consistent with future methods automated by QoS Signalling (RSVP/NSIS).	Performance and routing information must be exchanged among providers to determine the identities of transit providers in each traffic path (e.g. from BGP number of AS's) and their performance. However, there are alternative ways to determine path, and many providers publish performance info in real-time. Cannot guarantee that objectives will be met (true for all approaches to some extent).

Brief examples using the above approaches as applied to the figure below are provided here as background for the specified allocation scheme. Note that it is assumed that the provider which sends traffic over a peering connection is assumed to be responsible for its performance and impairments.

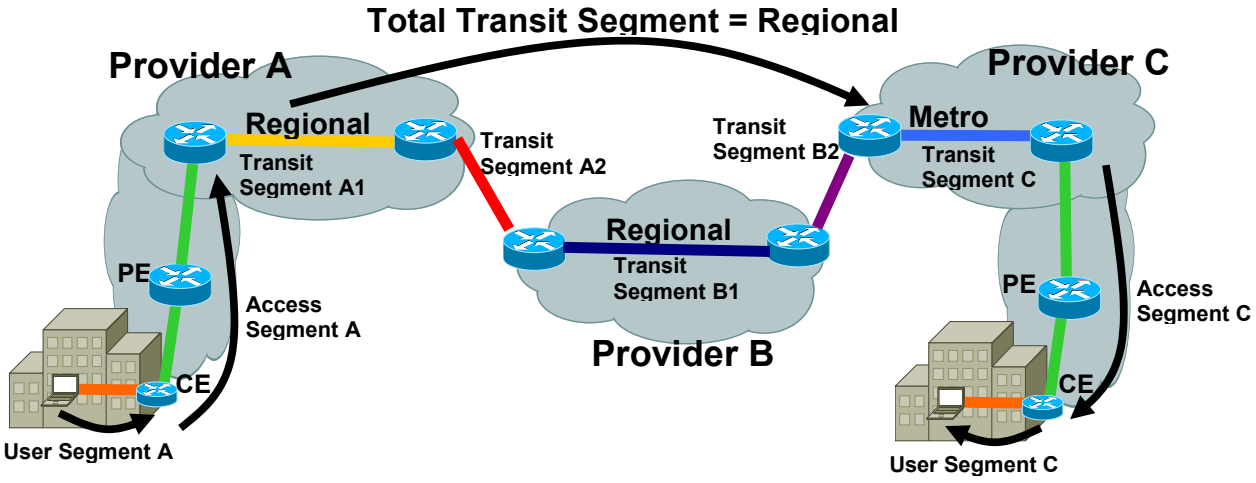


Figure 1 – Example topology for impairment allocation

7.1 Static Approach Examples

7.1.1 Static Divisor Approach

This approach requires that individual segments have knowledge of the distance between the edges of their domains. Regarding distance quantization, assume that "Metro" < 100km for which 4mS mean delay is budgeted, and "Regional" < 1,000km for which 16mS mean delay is budgeted.

For a "static divisor" approach, the following example assumes that

1) A hybrid method is used for mean delay
   a) The maximum number of providers is 3, therefore dividing the total transit budget by 3 yields an allowance of 16/3 = 5.3ms for transit segments A1 and B1. While transit segment C1 is allocated 4/3 = 1.3ms.
   b) The User, Access and Peering segments have allocated fixed delays of 2ms, 30ms and nominally zero delay respectively.
2) A bottoms up method is used for loss
   a) The User, Access and Peering and Transit segments are allocated 0.01%, 0.02%, 0% and 0.01% respectively.
3) A hybrid method is used for Delay Variation
   a) The User, Access, and Total Transit segments are allocated 10%, 40%, and 30% of the total Delay Variance budget
   b) If the Peering link DV is 0. Using the DV concatenation rule (tbd), allocate the Total Transit segment DV allowance 30%, equally to the three transit segments.

If above, the maximum number of providers is agreed to be 4 instead of 3. Then instead of allocating among 3, we would have allocated among 4 segments in 1a and 3b above. This would be an over-engineered scenario since the actual number of providers is less than the maximum design.

The Access providers may re-allocate their impairment target among the segments under their control.

7.1.2 Static Reference Allocation Approach

This approach requires that individual segments have knowledge of the distance between the edges of their domains. In this approach the Y.1541 reference model is used, which includes major components of each provider. Combining distance together with Y.1541 impairment values for each of these components, this method calculates the delay margin and allocates a proportion of that margin to each provider. As follows:

Step 1: Calculate transit delay for each provider

Step 2: Calculate the inherent delay of each provider using the Y.1541 reference model and values

Step 3: Calculate the delay margin by subtracting the total of the providers' inherent delays from the Y.1541 network QoS class objectives.

Step 4: Calculate the proportion of inherent delay of each provider to the total inherent delay of all providers

Step 5: For each provider, the allocated delay is equal to their transit delay plus that provider's proportion of the delay margin.

See Appendix A-2 for reference model, values and detailed examples.

Note that the scope this approach reaches between UNIs, and excludes the User segments.

7.1.3 Weighted Segment Approach

This approach allocates a significant proportion of the impairment budget to each access segment, with each core segment having a lesser fixed budget. This approach also allocates a fixed budget for core network segments, irrespective of the number of core network segments in any resulting services. This core network segment budget can be concatenated within bounds to create end to end services that have a high probability of still being within the overall end to end class targets.

An additional allowance for propagation delay for long network segments is also provided. With this approach core segments only need to have knowledge of the distance between their edges when the total distance between the edges of any core network segment exceeds an air path distance of 1200km.

For each access segment a fixed budget value for IPTD, IPDV and IPLR would be allocated for a given class.

For each core network segment, a combined budget would be allocated for the numerical sum of IPTD and IPDV. This allocation would be the same for Network QoS Classes 0 to 3 and Unspecified for Class 4.

In core network segments, the IPTD is largely determined by propagation times whereas IPDV is typically incurred as a result of network element processing and packet forwarding delays. The operator of any core network segment would be at liberty to allocate the total budget to either IPDV or IPTD or any mix of both, provided the numerical sum of IPTD and IPDV did not exceed the allocated budget value. This poses some risk that the overall outcome may exceed targets if the entire budget is allocated to one metric, but real core network segments will almost always result in a mix of IPTD and IPDV.

The recommended allocations are given in the table below.

Table 3 – Weighted Segment Recommended Allocations

	Access segment			**Core network segment (<1200km)**	
ITU-T 1541 class	IPTD (Note)	IPDV (99.9 percentile - minimum)	IPLR	IPTD + IPDV (99.9 percentile – minimum)	IPLR
Class 0 and 1	<25ms	<15ms	<4x 10-4	<10ms	<1x10-5
Class 2 and 3	<25ms	U	<4 x 10-4	<10ms	<1x10-5
Class 4	<500ms	U	<4 x 10-4	U	<1x10-5

Note: These transfer delay figures primarily take serialization delay on access links into account.

For any single core network segment that is greater 1200km from edge to edge, an additional allowance for propagation delay is allocated. For this the following formula would apply;

Additional IPTD (ms) = (total segment air path distance in km -1200) x 1.25 x 0.005

The additional IPTD budget should be rounded up to the nearest integer number of milliseconds.

This approach requires Class 0 services to have no more than three core network segment providers. Typically no more than this would be used in any “national” or regional connection to achieve Class 0 performance. Inter continental services could only be provided in Class 1 under this approach unless network segment providers negotiated lower budgets for a service. For Class 1 services, the number of core network segment operators can be greater than three.

Particular Pros and Cons of this approach are:

Pros

- Flexibility to trade off delay and delay variation impairments within each core network segment
- No need to have prior knowledge of other potential providers involved in services to be able to design the segment
- Maximum practical allocation of impairments to the access segment that is most cost performance sensitive
- No explicit knowledge of distance required for segments whose edges are less than 1200km apart.
- Operators who always provide both an access and one core network segment combined can also trade off impairments between these segments within their networks.
- On demand connections (eg public network calling) have a high probability of achieving end to end service class targets.
- Applicable to any number of core segments, Where less than 3 network segments are used for a service, operators are at liberty to negotiate the consumption of a greater proportion of the budget in any segment for any service but the underlying segments would not be planned to rely on this.

Cons

- If all segment providers use their maximum budget then end to end class targets may not be met.
- Some Wireless access technologies could only be supported in class 1.
- User's segment impairments are not taken into account.
- Explicit knowledge of distance is required for segments whose edges are greater than 1200km apart.

See Appendix A5 for detailed examples.

7.2 Pseudo-Static Example

If a "pseudo-static" approach had been taken then each provider would have knowledge of how many providers are present in the traffic path and allocate among 3 without wasting part of the impairment budget.

The Access providers may re-allocate their impairment target among the segments under their control.

7.3 Signaled Examples

Given the flexibility of a signaled approach, multiple examples are given to investigate its flexibility.

For a "signaled" approach, the use of resource management and signaling for the purposes of impairment apportionment is assumed.

7.3.1 Negotiated Allocation Example

In some situations, for the "Static and Pseudo-Static" approaches, certain segments will not be able to meet their formulaic targets, while others will easily meet their targets and have an "impairment budget" excess.

Access providers which require less than the normal allocation of impairments may be able to have the un-needed part of their allocation allocated instead to a transit or user link. They may re-allocate their impairment allocation within their control or negotiate the un-needed part to other segments.

A transit provider may negotiate the un-needed part to other segments.

Similarly, in a managed User segment scenario, the User may require a greater or lesser impairment allocation based upon access sub-type, e.g. by broad category (enterprise, home, wireless) or specific capability (802.11g, 100mb Ethernet) and negotiate with their access provider.

Starting with initial segment impairments targets, based possibly upon the static and pseudo-static allocations in this document; the distributed use of negotiation among providers provides the opportunity to negotiate for any "impairment budget" excesses, and to advertise to multiple interested parties if they can provide a network service that is within their collective impairment budget.

First, assume that an extension to BGP can provide for multiple advertisements to a prefix, depending upon whether particular network classes are supported along a path. Then starting with the provider closest to the destination prefix, the advertisement is conditionally transitive depending upon whether a collaborative impairment target for the network class is met.

Referring to figure 1, provider C advertises a real-time network class to provider B indicating that provider C can meet their impairment budget for that class. If provider B can meet their impairment budget then they will advertise the path to provider A.

However, if provider B cannot meet the impairment target that has been set for them, they may negotiate with provider C for the right to use any excess available impairment of provider C. Similarly, provider A may in a cascade fashion negotiate with provider B.

Pairwise negotiations between segment owners may occur either by signaling or manually, and are assumed to change infrequently.

This approach appears to support multiple connections among providers, where provider's BGP advertising policies and aggregation would influence the solution.

7.4 Accumulation Methods

Accumulation methods are defined here as those that include solicitation of what service each provider can offer or "bid", followed by decisions made following receipt of those bids. The solicitor may be the customer facing provider only (hub and spoke) or include all the providers along a path (cascade). The responder may be a provider or their proxy.

7.4.1 Impairment Accumulation Example

In this method:

1) The customer facing provider
   a) Determines the path that packets will follow (e.g., based on inter-domain routing information),
   b) Solicits from each provider the impairment that they will commit to for each segment of the path for packets identified by with source/destination pair.
2) Receives a commitment or "bid" from each provider which is good for the session (unless modified)
3) The customer facing provider
   a) Combines the segment impairment levels (according to rules that are approaching completion in Question 17/12) and
   b) Compares the estimated performance with the desired UNI-to-UNI QoS Class/Objectives.

If the path does not meet the requested objectives, there are two opportunities for negotiation:

- Path Negotiation: an alternative path might be sought, requiring a routing change based upon parallel or subsequent solicitation of other providers.

- User Negotiation: an alternative Service Class or relaxed objectives could be offered to the user. (Note that in many cases, the concatenation of parameter will result in a total that is slightly beyond a particular classes objectives but considerably better than the target parameter of a different service class).

Particular Pros and Cons of this approach are

Pros:

- No formulaic impairment allocation agreements are required to use this method.
- No explicit knowledge of distance is required.
- It is completely consistent with the vision of achieving UNI-UNI performance objectives (Y.1541 Network QoS Classes) with signaling protocols that automate the process of reserving bandwidth and accumulating impairment levels. SG 11 Supplement 51 on IP QoS Signaling codifies one set of requirements for this task, but clear parallels may be found in Integrated Services/RSVP and in the Next Steps in Signaling (NSIS) Qspec template.

Cons:

- Users segment impairments are not taken into account.
- Potentially multiple passes of request/bid cycles are required.
- Requires customer or customer proxy (rules driven agent or equivalent) involvement.
- Bids for each PE-PE pair must be pre-calculated taking distance into account.
- Bids for "all time" may need to be over-conservative for low-utilization circumstances.

A detailed example of the Impairment Accumulation approach is given in Appendix A4.

7.4.2 Costed Bids Example

This approach recognizes that economic factors may be included in the selection of providers' transport services. It suggests that multiple bids be submitted per service provider to a customer-facing provider which may select a transport service from each provider based upon both impairments and cost. For example, consider Providers A, B, C and D along a path, where A is a customer-facing Provider.

1) Provider A requests available services from Providers B, C and D for the bandwidth required.
2) Providers B, C and D submit multiple bids, where each bid includes impairments and cost that a Provider will commit to.
3) Provider A, having subtracted their own impairments from the UNI-UNI target, selects the bid services from each other Provider where
    a) The aggregated impairments fall within the remaining impairment budget
    b) The total cost is minimized.

Particular Pros and Cons of this approach are

Pros:

- Takes cost into account
- Provides incentives for network optimization

Cons:

- Adds complexity

See Appendix A-3 for a detailed example.

7.4.3 Bid Discovery Using a Global Registry Example

The use of a global registry could provide similar information as a real-time signaled approach without signaling among providers. A registry acts as a proxy for the management systems of many providers.

It assumes that updates to the registries stored bids by providers occur infrequently.

Providers would each post information to the registry for transit across their network including:

- Demarcation endpoint information (PE-PE, PE-CE or CE-CE).
- Network Classes carried
- Impairments for each class
- Period of validity information
- Read access rights

The information should support scheduled and un-scheduled changes to bids.

The registry would be globally distributed and fulfill functions including:

1) Provide secure access to authenticated entities
2) Store providers' information
3) Disseminate providers' information
4) Keep track of providers that were given what information
5) Send updated bid information to a filtered set of providers in 4

Particular Pros and Cons of this approach are

Pros:

- It is more centralized than a many-to-many signaled approach and is expected to be a distributed database. Less knowledge may be required of other providers' management systems' addresses. Less likelihood of a provider needing to talk in multiple protocols.
- It provides the opportunity to offload storage and communications from providers that need to communicate a change in bid to many other interested providers.
- It provides the opportunity to discover impairments from many providers in a single session.

Cons:

- Scalability, security and performance requirements may be greater than for a many-to-many provider signaled approach.

This approach may be combined with signaling negotiations between providers and their customers, resource reservations, and possibly leverage other proposed global registries.

8 Recommended Algorithms for Achieving End to End Performance Objectives

To be determined by SG12.

Appendix A

Further Examples

The following examples investigate the concepts summarized in section 7 in more detail.

A.1 Detailed Example of a Static Divisor Approach

To gain an appreciation of how a static allocation scheme may look, here is example A-1. Assuming a maximum of three transit providers in a path. This scheme supports user-to-user (TE-TE), edge-to-edge (PE-PE) and site-to-site (CE-CE) models. Note that terminology in this section is derived from an FGNGN WG3 Performance Monitoring and Management document (work in progress).

A.1-1 User Segments

User segment impairment budgets are dependent upon the nature and size of the enterprise, home etc between the User (TE) and the demarcation to the access segment (CE). As a simplifying approximation, a static allocation is made to user segments as follows for each service class.

The following impairment allocations apply for the user-to-user model. The percentages are of total user-to-user impairment targets for each service class.

Table A.1-1 – User segment impairment allocations

	Telephony	Low latency Data	Multimedia streaming
Packet Loss	1%	1%	1%
Delay Variation	1%	1%	1%
Availability	1%	1%	1%
Mean Delay	2mS	2mS	2mS

The impairment allocation for other service classes is TBD.

A.1-2 Access Segments

The following impairment allocations apply to the user-to-user, site-to-site and edge-to-edge models. The percentages are of total site-to-site impairment targets for each service class.

Table A.1-2 – Access segment impairment allocations

	Telephony	Low latency Data	Multimedia streaming
Packet Loss	47.5%	47.5%	47.5%
Delay Variation	40%	40%	40%
Availability	47.5%	47.5%	47.5%
Mean Delay	<30mS	<30mS	<30mS

The mean delay budget for the ingress segment is a fixed delay based on access speed/technology. A specific value shall be assigned to each site and shall not exceed 30ms.

In situations where the access segment cannot support these metrics, the access provider should use the edge-to-edge model for their service offerings and provide demarcation at the PE router.

A.1-3 Total Transit Segment

The following impairment allocations for the total transit segment apply to the user-to-user, site-to-site and edge-to-edge models.

The Total Transit Segment per figure 1 includes up to three providers' segments and two peering connections.

Table A.1-3 – Total transit segment impairment allocation

	Telephony	Low latency Data	Multimedia streaming
Packet Loss	5%	5%	5%
Delay Variation	40%	40%	40%
Availability	5%	5%	5%

The impairment allocation for other service classes is TBD.

Distances between transit segment demarcation points are quantized into 4 categories. Distance between any two points is measured by TBD.

Total Transit Delay = Shortest path propagation delay + Allowance for inefficient topology + Allowance for queuing delays

Note that differences in queuing delays due to per hop behavior of service classes are not made.

Table A.1-4 – Total transit delay by distance

Categories	Distance (km)	Shortest path propagation delay (ms)	Total Transit Delay (ms)
Metro	< 100	0.56	5
Regional	< 1,000	5.6	15
Continental	< 5,000	27.8	45
International	< 20,000	111.2	140

A.1-4 Individual Transit Segments

A budget will be allocated to each of the multiple Providers' networks which comprise the total transit segment as follows. The impairments of the peering connection are included in the impairment allocation of the responsible Provider's transit segment. The percentages are of the total transit allocation.

Table A.1-5 – Individual transit segment impairment allocation

	Telephony	Low latency Data	Multimedia streaming
Packet Loss	33%	33%	33%
Delay Variation	40%	40%	40%
Availability	33%	33%	33%

- The mean delay budget for each Provider is based on the distance between geographic locations bounding their part of the transit network. Each service provider is allowed to contribute up to 33%

of the appropriate transit delay listed in table 7, depending on whether their demarcation POPs are in the same metro area, same region, same continent, or in different continents.

- The maximum delay budget above which delay a packet will be treated as loss for each Provider is proportional to their allocated mean delay budget. The sum of each SPs maximum delay budgets will be greater than the total transit segment allocation since maximum delay is not strictly additive. The maximum delay budget for each SP is y (y is TBD) times their mean delay budget.

A.1-5 Relationship to existing standards

Y.1541 discusses route length calculation in the following manner.

If the distance-based component is proportional to the actual terrestrial distance, plus a proportional allowance for a typical physical-route-to-actual-distance ratio. The route length calculation used here is based on ITU-T Rec. G.826, and only for the long distances considered here. If D_{km} is the air-route distance between the two MPs that bound the portion, then the route length calculation is:

- if $D_{km} > 1200$, $R_{km} = 1.25 \times D_{km}$

A.2 Detailed Examples of the Static Reference Allocation Approach

A.2-1 Static reference allocation method

This method uses the following steps in the static reference allocation example method for determining IP delay time.

i) Establish inter-connection network section model (cf. Figure 2).

ii) Establish network element model for each network section (cf. Figure 3).

iii) Calculate transmission delay time of each network section distance (use G. 826).

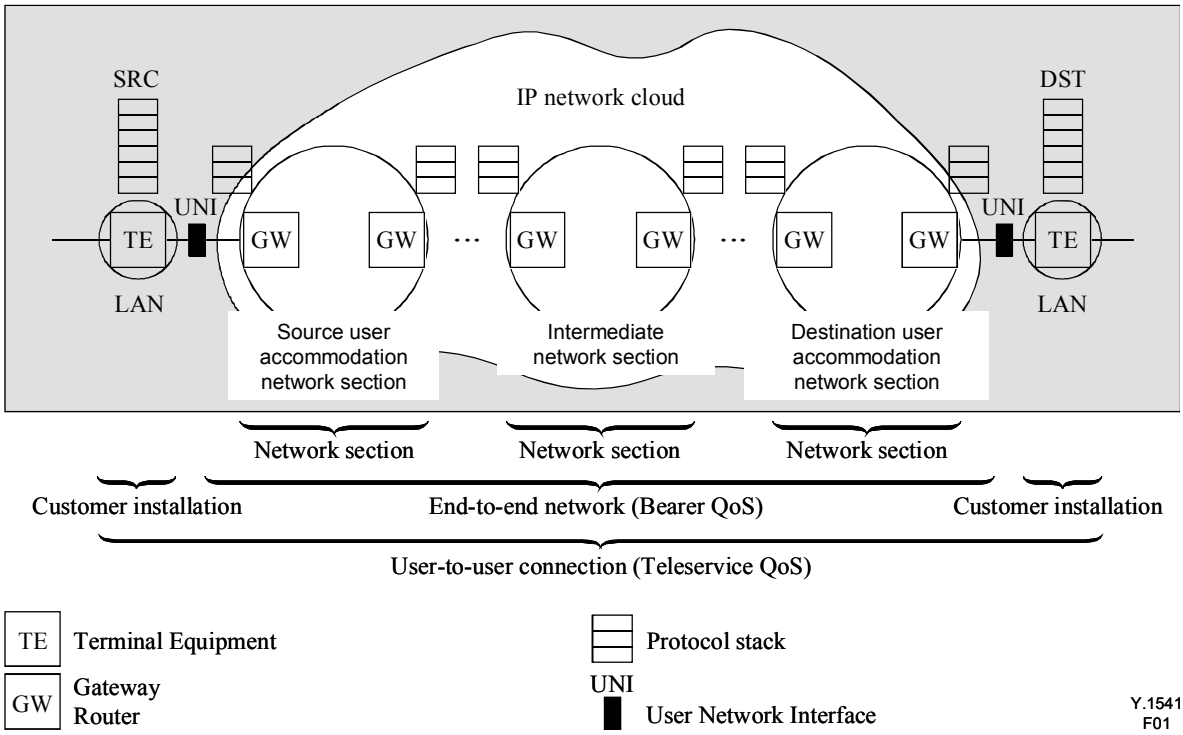
iv) Calculate each network section basic delay time.
Network section basic delay time is calculated using network element models and each element delay time. Table 1/Y.1541 Appendix III gives this calculation.

v) Subtract end-to-end transmission delay in item (iii) above from delay time of performance objective class. This value is the delay time accumulation resource.

vi) Divide the delay time resource in item (v) above by the sum of all network section basic delay times (iv).

vii) The allocated delay time of each network section is the sum of the transmission delay (iii) and the divided delay time resource (vi).

Figure A.2-1 is a inter connection network section model which refer to Y.1541 UNI-to-UNI reference path for network.



NOTE – Customer installation equipment (shaded area) is shown for illustrative purposes only.

Figure A.2-1/Y.1541 – UNI-to-UNI reference path for network QoS objectives

Figure A.2-2 is example of each network element model, and Table A.2-1 is example of typical delay contribution by router role. These model and values should refer from Y.1541, and when we have to change model or value, we should change Y.1541's models and values.

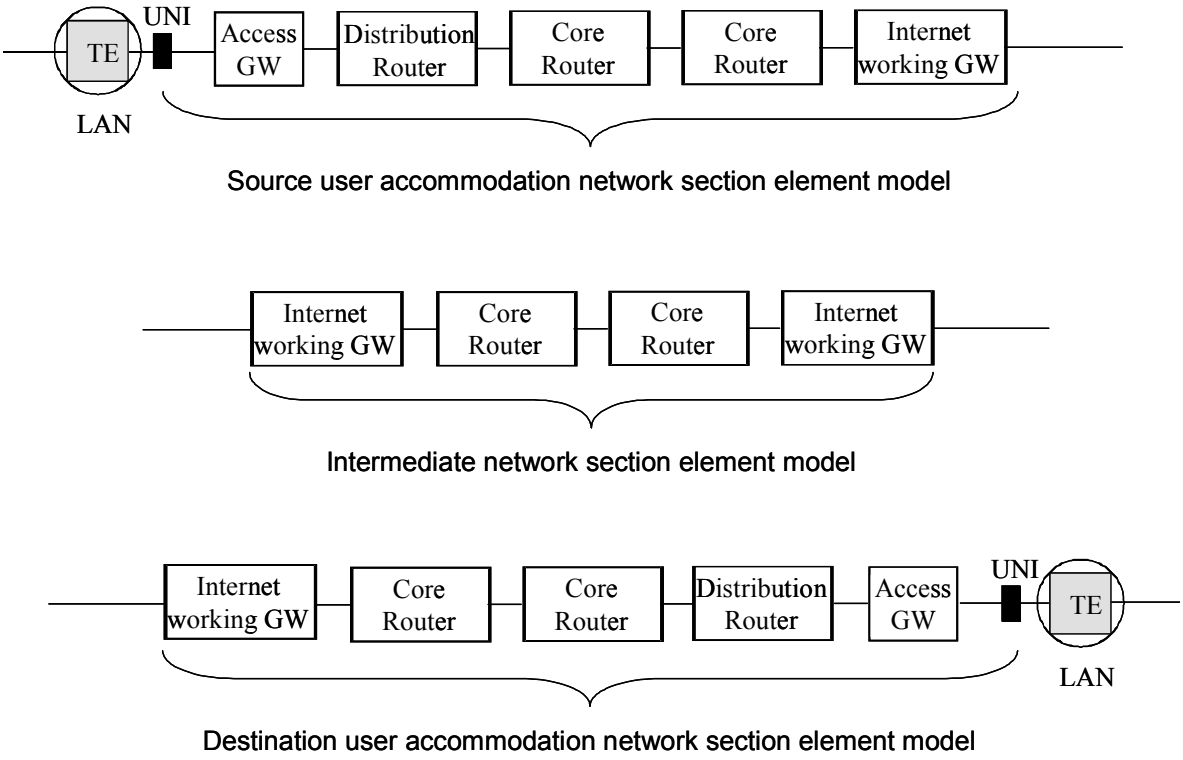


Figure A.2-2 – Example of network element model for each network section

Table A.2-1 – Example of typical delay contribution by router role (Table III.1/Y.1541)

Role	Average total delay (sum of queuing and processing)	Delay variation
Access gateway	10 ms	16 ms
Internetworking gateway	3 ms	3 ms
Distribution	3 ms	3 ms
Core	2 ms	3ms

A.2-2 Detailed Example 1

In this example, two network providers interconnect.

Assumptions:

A) Two network providers are interconnected. (Provider A and B)

B) Both network providers have access network which admit user direct.

C) Distance between provider A UNI and inter gateway with provider B is 3000Km, and provider B UNI and inter gateway with provider A is 2000Km.

D) Non IP networks are not needed in UNI to UNI.

E) End to end delay time limit is 100 ms (class 0, 1 delay time of Y.1541).

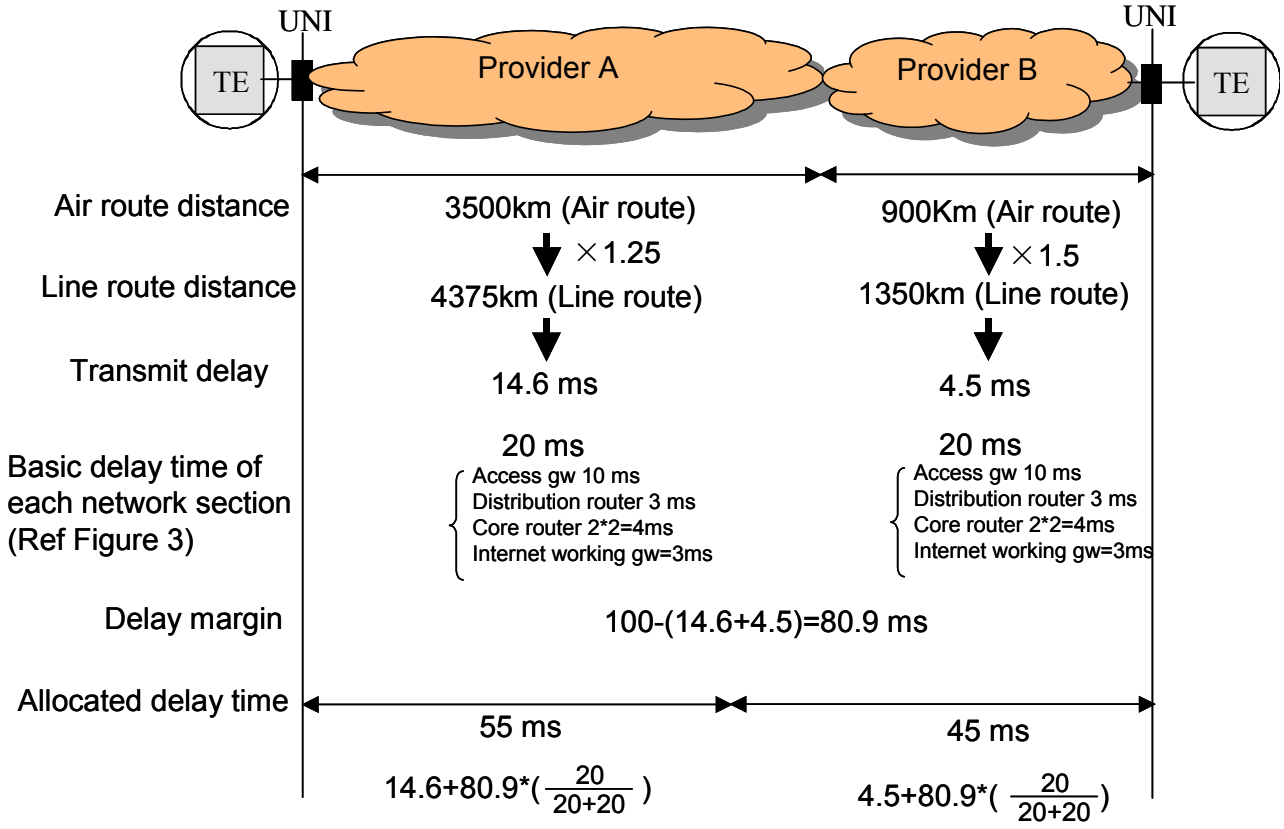


Figure A.2-3 – Static Reference Allocation Example 1

A.2-3 Detailed Example 2

In this example, three network providers interconnect.

Assumptions:

A) Three network providers are interconnected. (Providers A, B and C)

B) Network provider A and C have access network which admit user direct.

C) Distance between provider A UNI and inter gateway with provider C is 1500Km, and provider B UNI and inter gateway with provider C is 4000Km, and distance between provider C UNI and inter gateway with provider B is 500Km.

D) Non IP networks are not needed in UNI to UNI.

E) End to end delay time limit is 100 ms (class 0, 1 delay time of Y.1541).

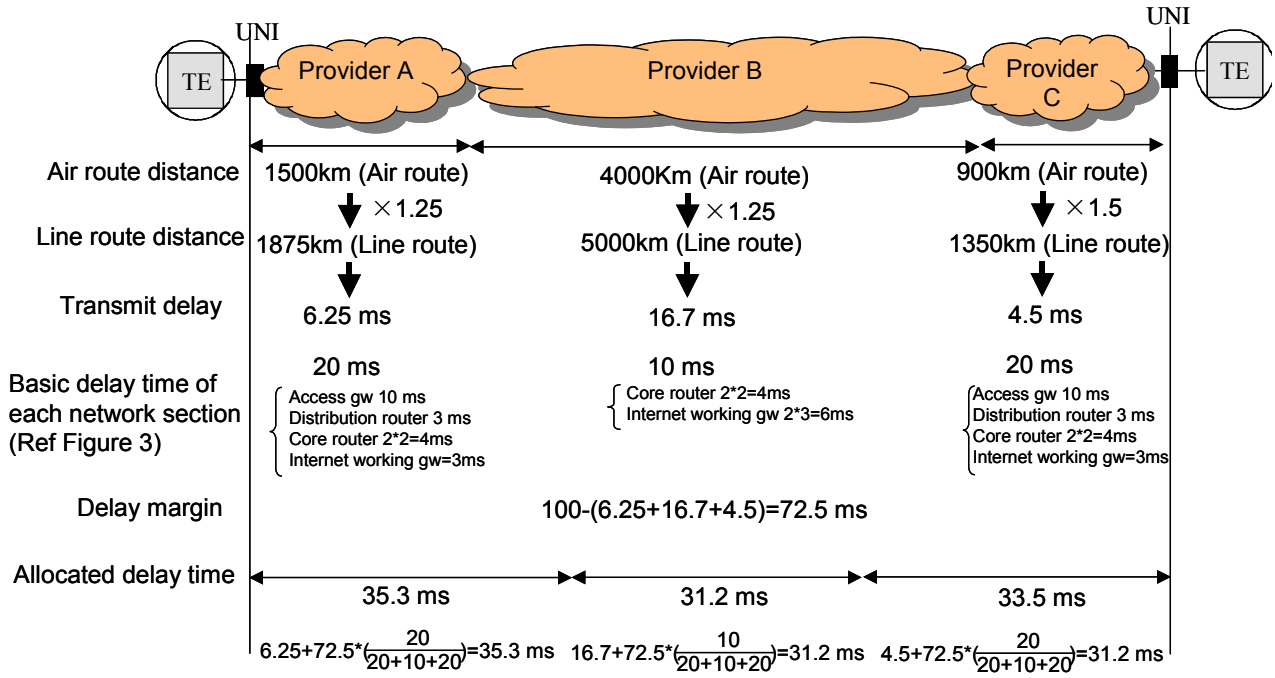


Figure A.2-4 – Static Reference Allocation Example 2

A.3 Detailed Example of the Costed Bids Approach

The end-to-end routing path always covers multiple sub-networks, so the total end-to-end impairment targets need to be allocated among these sub-networks. Different sub-networks may have different network technologies and the associated different QoS abilities, and this appendix presents a method to optimize impairment budgets.

Instead of arbitrarily allocating the impairments according to the specific network characteristics, each sub-network can pre-determine its own local QoS ability, group individual QoS parameters and associated impairment targets into sets of services, which can be called as local network performance (NP) services, (note that these local NP services are network dependent and based on the specific network technology), then the impairments allocation are based on local QoS abilities of the local NP services of every sub-network.

A simple example is presented to illustrate the scheme; two QoS parameters are selected, mean delay (MD) and Packet Loss (PL). The local NP services are listed in table A.3-1. In figure A.3-1, the routing path is A-B-C-D-E, A and E are end hosts and B, C, D are sub-networks. B supports the local QoS abilities of the local NP services C1, C2, C supports the local NP services C2, C3 and D supports the local NP services C3, C4. Here the impairments of the inter-link are included in the impairments allocation of the upstream sub-network. The possibility of local NP service selection, impairment allocation and the total end-to-end impairment aggregation are listed in table A.3-2.

Table A.3-1 – Local NP services

	Service C1	**Service C2**	**Service C3**	**Service C4**
MD(ms)	5	10	16	24
PL	0.03	0.06	0.20	0.30

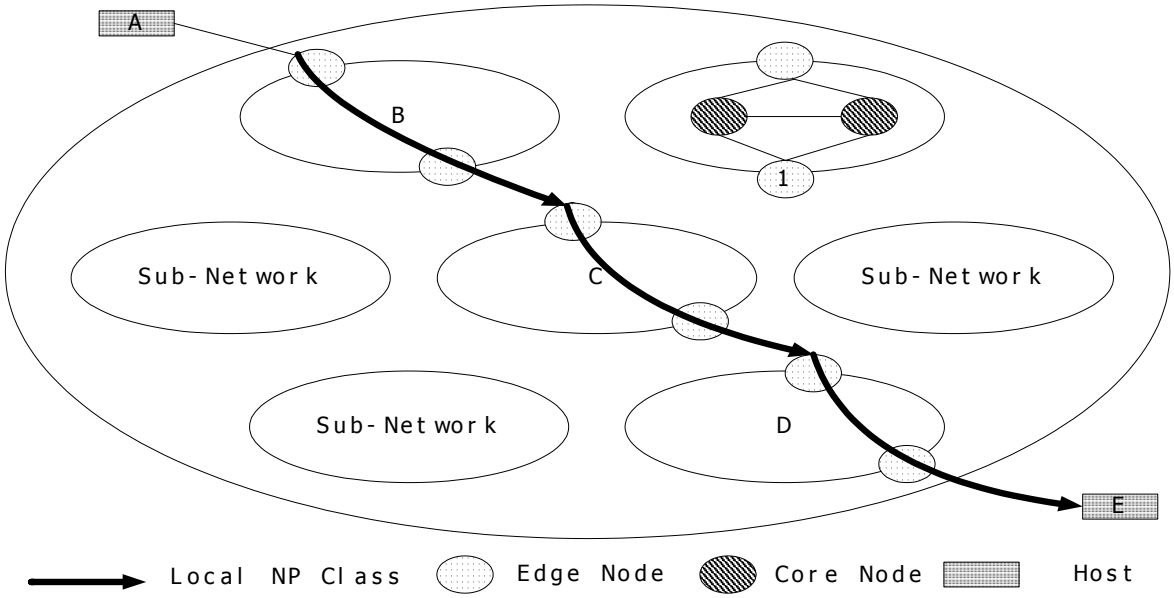


Figure A.3-1 – Network Topology for the Example

Table A.3-2 – Local NP Services Selection

Service B	MD B(ms)	PL B	Service C	MD C(ms)	PL C	Service D	MD D(ms)	PL D	Total MD(ms)	Total PL
C1	5	0.03	C2	10	0.06	C3	16	0.20	31	0.271
C1	5	0.03	C2	10	0.06	C4	24	0.30	39	0.362
C1	5	0.03	C3	16	0.20	C3	16	0.20	37	0.379
C1	5	0.03	C3	16	0.20	C4	24	0.30	45	0.457
C2	10	0.06	C2	10	0.06	C3	16	0.20	36	0.293
C2	10	0.06	C2	10	0.06	C4	24	0.30	44	0.381
C2	10	0.06	C3	16	0.20	C3	16	0.20	42	0.398
C2	10	0.06	C3	16	0.20	C4	24	0.30	50	0.474

If the end-to-end MD requirement is < 43ms and the PL requirement is < 0.390, the feasible allocations of impairments are listed in Table A.3-3. Each feasible choice of impairment allocation will waste some impairment budgets, maybe consequently using more resources than actually needed, for this reason, it is reasonable to assign each local NP service a price. The higher price will indicate more valuable resources and a better network performance, thus the reasonable criterion for selection of impairments allocation is to choose the one with least total price.

Table A.3-3 – Feasible Impairments Allocation

Service B	MD B(ms)	PL B	Service C	MD C(ms)	PL C	Service D	MD D(ms)	PL D	Total MD(ms)	Total PL
C1	5	0.03	C2	10	0.06	C3	16	0.20	31	0.271
C1	5	0.03	C2	10	0.06	C4	24	0.30	39	0.362
C1	5	0.03	C3	16	0.20	C3	16	0.20	37	0.379
C2	10	0.06	C2	10	0.06	C3	16	0.20	36	0.293

Table A.3-4 – Prices of Local NP Services

	Service C1	Service C2	Service C3	Service C4
Price	90	70	40	30

Table A.3-5 – Total Price of each Impairments Allocation

Sub-network B	Sub-network C	Sub-network D	Total Price
C1	C2	C3	200
C1	C2	C4	190
C1	C3	C3	170
C2	C2	C3	180

In this example, the prices of the local NP services are listed in Table A.3-4 and the total price of each feasible choice of impairments allocation is listed in Table A.3-5, the least total price is 170, and the final impairments allocation will be:

Table A.3-6 – Final Allocation of Impairments

MD B	PL B	MD C	PL C	MD D	PL D	Total MD	Total PL	Total Price
5ms	0.03	16ms	0.20	16ms	0.20	37ms	0.379	170

Each QoS service or service class will also have a price, to indicate optimal resource consumption; the total price of the impairment allocation among the sub-networks across the path can't exceed the price of the service or service class. Moreover, each sub-network must have enough resource to achieve the allocated impairments budgets. Based on the local QoS abilities of all the sub-networks, and considering the price and resource factors, thus the path selection of end-to-end QoS routing can be determined.

A.4 Detailed Example of Impairment Accumulation Approach

This section describes a process to accumulate network performance levels along an end-to-end path and compare the combined performance estimate with specified objectives, consistent with procedures envisioned with Quality of Service signalling protocols such as those that meet the requirements of Supplement 51 on IP QoS. We do not address capacity reservation aspects here, or subscription, authorisation, and accounting, though they are critical aspects of a premium service offering as well.

The following steps outline the process at high level:

1) Determine the desired UNI-UNI performance objectives and any acceptable alternatives (e.g., the desired Y.1541 Network QoS Class).

2) Determine the User-Network Interfaces (UNI) and Network-Network Interfaces (NNI) that appear in the end-to-end path.

3) Determine the performance of each segment of the path (each operator domain from UNI to NNI, NNI to NNI, etc.) for each parameter with an end-to-end objective. If there is uncertainty which NNI will be traversed from among several possibilities, then separate calculations can take each one into account (although instances should be minimised, especially where the performance differences are significant).

4) Combine the segment performance levels according to combination rules.

5) Determine if the combined performance estimate meets the desired objectives.

6) If the objectives were not achieved, then take one or more of the following actions:

   a) Offer to meet modified performance objectives (User Negotiation).

   b) Seek alternative partner networks (an alternative combination of NNI to NNI segments, or Path Negotiation).

There are only three pieces of information exchanged among the partner networks:

- The End-to-End Objectives
- The Path UNI and NNI list, including operator identifications
- The performance of each domain between specific edge interfaces

Assuming that this process will be automated (with on-path signalling), then the Ingress Edge Router at each UNI/NNI may play the primary role for each Autonomous System (AS) on the Source-Destination path (step 3 above). When a QoS Signalling request enters an AS, the following operations might take place:

1) The Edge Router identifies the packet as one requiring exception processing (possibly after inspecting the protocol number in the IP header), and sends the packet to the central processor (the packet has not been processed previously in this AS).

2) The router processor inspects the Destination Address and determines the BGP Next Hop (or other equivalent egress point) for this AS. This provides the Local Loopback Addresses of the Ingress and Egress Edge Routers and NI.

3) The AS Ingress and Egress points can be mapped to a matrix of Performance Measurements (likely stored elsewhere on a server known to the router, so the router might encapsulate the signalling packet with the Ingress/Egress points into one packet and forward it to the measurement server). The Performance Matrix would be updated frequently as new Loss, Delay and Delay Variation measurements become available, and the most recent valid measurements are always used.

4) The signalling packet is augmented with the AS number and the edge-edge performance measurements (again, the measurement server might perform this function, and it may encapsulate the signalling packet in an IP header to send it back to the Edge Router.)

5) The Edge Router (extracts and) forwards the augmented signalling packet along the normal path.

6) Interior routers in the same AS would inspect the packet, find that their AS is already listed, and take no action on the performance fields.

Note that this is a process using operator domain (AS) performance as the building blocks. Other processes use network elements and the links between them as the building blocks, such as those envisioned for Integrated Services supported by RSVP signalling. It may be possible to perform capacity/traffic management on a element-by-element basis, while managing performance aspects on a domain basis as long as sufficient capacity is available on the path through the domain.

A.5 Detailed Example of a Weighted Network Segment Approach

We consider worst case scenarios that may result from this allocation methodology for services in Network Y1541 QoS class 0.

These scenarios occur when all participants in an end to end connection use their maximum impairment allocations. This situation will be rare in actual networks as real network elements cannot be that precisely engineered and some margin will typically exist in each segment.

Case 1 and 2 consider an end to end service across a total air path distance of 4000 km (e.g. Trans U.S.A.) with 3 core network segment operators involved in the end to end connection.

A.5-1 Case 1: Each core provider decides that 100% of the core budget is used for IPTD (no IPDV in core)

Table A.5-1

	Link air path distance	IPTD budget	Additional IPTD for Distance	Core budget used for IPTD	Total IPTD	IPDV (inc balance of core budget)	IPLR
Access provider 1		25ms			25ms	15ms	4×10^{-4}
Core provider A	300km		0	10ms	10ms	0	1×10^{-5}
Core provider B	3000km		12 ms	10ms	22ms	0	1×10^{-5}
Core provider C	700km		0	10ms	10ms	0	1×10^{-5}
Access provider 2		25ms			25ms	15ms	4×10^{-4}
Total CE to CE	**4000km**				**92ms**	**30ms**	**8.3×10^{-4}**

A.5-2 Case 2: Each core provider decides that 100% of the non geographic core network segment budget is used for IPDV.

Table A.5-2

	Link air path distance	IPTD budget	Additional IPTD for distance	Core budget used for IPTD	Total IPTD	IPDV (inc balance of core budget)	IPLR
Access provider 1		25ms			25ms	15ms	4×10^{-4}
Core provider A	300km		0	0	0ms	10	1×10^{-5}
Core provider B	3000km		12 ms	0	12ms	10	1×10^{-5}
Core provider C	700km		0	0	0ms	10	1×10^{-5}
Access provider 2		25ms			25ms	15	4×10^{-4}
Total CE to CE	**4000km**				**62ms**	**60ms***	**8.3×10^{-4}**

* The total for IPDV in the table is shown as an additive sum. But concatenated IPDV is not additive. The net effect is that even in this extreme case it is likely the actual end to end IPDV would be within the 50ms IPDV target of Class 0.

A.5-3 Case 3: Trans continental service involving 5 core providers, for Y.1541 class 1 end to end service

In this case, each core provider has elected to use their core network segment budget in different ways. The example highlights the impact of making these choices independently of other providers where more than three core network segments are used.

Table A.5-3

	Link air path distance	IPTD budget	Additional IPTD for distance	Core budget used for IPTD	Total IPTD	IPDV (inc balance of core budget)	IPLR
Access provider 1		25ms			25ms	15 ms	4×10^{-4}
Core provider A	300km		0 ms	4 ms	10ms	6 ms	1×10^{-5}
Core provider B	3000km		12 ms	6 ms	22ms	4 ms	1×10^{-5}
Core provider C	10,000km		55 ms	5 ms	60 ms	5 ms	1×10^{-5}
Core provider D	2,000km		5 ms	6 ms	11 ms	4 ms	1×10^{-5}
Core provider E	400km		0 ms	3 ms	3 ms	7 ms	1×10^{-5}
Access provider 2		25ms		0 ms	25ms	15 ms	4×10^{-4}
Total CE to CE	**17,000km**				**156 ms**	**56 ms***	**8.5×10^{-4}**

* The total for IPDV in the table is shown as an additive sum. But concatenated IPDV is not additive. The net effect is that even in this extreme case it is likely the actual end to end IPDV would be within the 50ms IPDV target of Class 1.

Appendix B

Guidance for Providers

B.1 Qualitative Guidance Statements

Composition of the end-to-end objectives highlights the performance areas to emphasise. When working to achieve Y.1541 Class 2, an operator knows that delay variation is unspecified and can use different techniques to achieve those objectives than might be used to serve traffic with Class 0 or 1 objectives.

Performance guidance need not be quantitative (<2 ms of delay per 100 miles) to be useful. General guidance like:

> "Minimise delay by keeping the route to air distance ratio as small as economically and geographically feasible."

should achieve the nearly the same result. Economic factors cannot be ignored in this exercise. These factors usually set the point of diminishing returns when seeking to improve performance in any area.

Other simple statements of performance guidance are:

> "Minimise delay by providing sufficient link capacity to keep queue occupation low."
>
> "Minimise delay variation by giving queue scheduler priority to traffic that is sensitive to variation."
>
> "Minimise delay variation by grooming or shaping traffic that is sensitive to variation."
>
> "Minimise packet loss by planning sufficient link capacity to avoid queue tail-drops."

It is certain that additional guidance statements will be developed; this set is just the start.

B.2 Circumstances when Guidance is Useful

There are several different phases in the life of a network, for example when new construction or expansion is in progress. Another would be a stable phase where the network's geographic assets are fixed, and customers are connected to the network at the closest existing node. Capacity may be added in either phase. Adding links from network locations to reach remote customer sites is simply the expected growth under normal/stable operation, unless new network nodes (points-of presence or concentration) are constructed.

During construction or expansion, Table B-1 indicates how guidance may influence various aspects of network design.

Table B-1 – Areas for Action Given Qualitative Design Guidance

Performance Enhancement Area	Design Aspects		
Delay	Location of Nodes	Capacity (avoid queuing)	
Delay Variation	Capacity (avoid queuing)	QoS Mechanism Provisioning	
Loss Ratio	Failure protection Strategy/Restoration Time	Capacity (avoid queue overflow = drops)	Transport Facility Types (bit errors cause loss)

During stable operation, these same three forms of guidance translate into:

- monitoring and maintaining the network according to design levels plus some tolerance
- managing load to avoid bottlenecks or congestion
- adding capacity when necessary

In a competitive environment, networks that fail to follow this simple guidance will not be chosen as partners when achieving performance objectives is at stake.

WORKING GROUP 4
DELIVERABLES

CONTROL AND SIGNALLING CAPABILITY

2.15 Signalling requirements for IP QoS (*Status P*)

2.15 – Signalling requirements for IP-QoS*

Summary

This test was published as Supplement 51 to ITU-T Q-series Recommendations. It specifies IP-QoS signalling requirements for the development of new or enhanced specifications.

It identifies the capabilities for IP-QoS signalling. In addition, it describes the essential features and models for the development of functional entity actions in support of IP-QoS signalling.

Table of Contents

* Status P: This deliverable has already been passed to ITU-T Study Group 13 and published as ITU-T Q-series Supplement 51.

2.15 – Signalling requirements for IP-QoS

1 Scope

This Supplement provides the requirements for signalling information regarding IP-based quality-of-service (QoS) at the interface between the user and the network (UNI), across interfaces between different networks (NNI), including access networks. These requirements and the signalling information elements identified will enable the development of a signalling protocol(s) capable of the request, negotiation and ultimately delivery of known IP QoS classes from UNI to UNI, spanning NNIs as required.

The signalling requirements also address signalling information related to traffic priority and admission control, as these are also central to truly comprehensive QoS.

This Supplement specifies the signalling requirements for control plane and transport control signalling in the support of Quality of Service, without presuming how these requirements may be met. It is based upon the following ITU-T Recs: Y.1221 [9], Y.1291 [8], Y.1540 [6], and Y.1541 [7].

Figure 1 depicts the scope of this Supplement. Note that the figure does not imply that signalling data and user data will necessarily flow on the same links from network to network.

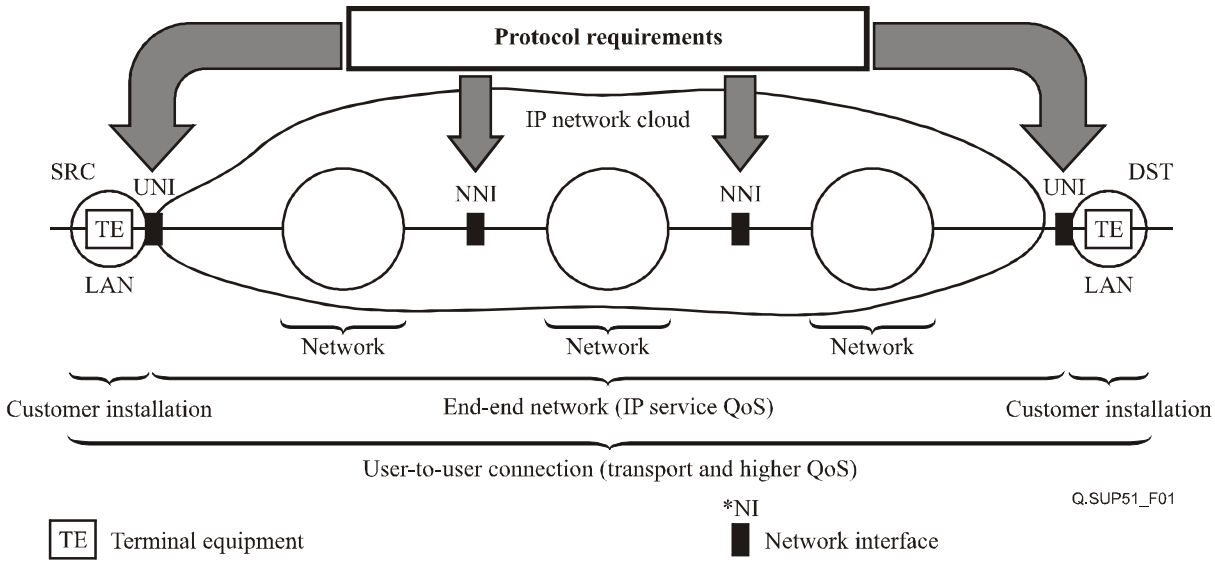


Figure 1 – The Scope of QoS signalling requirements

It is expected that continued study of IP QoS signalling requirements will address interworking and interoperability to allow hybrid signalling solutions.

2 Introduction

Although QoS is by definition (in multiple ISO, ITU-T and other standards) based on the experience of the service user, the mechanisms for achieving differentiated packet treatment are themselves taken all too often as being the same as "real" end-to-end QoS.

To meet specific network performance requirements such as those specified for the QoS classes of ITU-T Rec. Y.1541 [7], a network provider needs to implement services such as those specified in ITU-T Rec. Y.1221 [9].

To implement the transfer capabilities defined in ITU-T Rec. Y.1221 [9], a network needs to provide specific user plane functionality at UNI, NNI, and INI interfaces. A network may be provisioned to meet the performance requirements of ITU-T Rec. Y.1541 [7] either statically or dynamically on a per flow basis using a protocol that meets the requirements specified in this Supplement.

Static network provisioning is typically performed by a network engineering team using a network management system. Static provisioning typically takes into account both overall network performance requirements and performance requirements for individual customers based on traffic contracts between the customer and the network provider.

Dynamic network provisioning at a UNI and/or NNI node allows the ability to dynamically request a traffic contract for an IP flow (as defined in ITU-T Rec. Y.1221 [9]) from a specific source node to one or more destination nodes. In response to the request, the network determines if resources are available to satisfy the request and provision the network.

True QoS goes beyond just the delay and loss that can occur in the transport of IP packets. The requirements include:

– bandwidth/capacity needed by the application, and
– the priority with which such bandwidth will be maintained during congestion and with which it will be restored after various failure events.

As these aspects of QoS can be related to routing, they go beyond the resource management of the packet transport. To make the protocol envisioned by this Supplement comprehensive, requirements on priority and admission controls are also considered.

To achieve the "Hard QoS" guarantee, networks must incorporate the following functions:

1) Network resource management with QoS sensitive scalability.
2) Intra-domain and inter-domain routing with QoS sensitivity.
3) Session admission control with QoS sensitivity.

These functions must be provided whether path-coupled or path-decoupled signalling techniques are utilized within the network.

The requirements in this Supplement are intended to apply to implementations that operate using path-coupled QoS control mode, path-decoupled QoS control mode, or both modes in tandem.

The subject of QoS signalling has generated much interest in the industry. In particular, it is noted that some related work is under way in the IETF NSIS (Next Step in Signalling) Working Group focused on general IP signalling protocols that could be used to achieve different purposes such as QoS and security. The requirements of signalling protocols have been addressed in RFC 3726 [10], in which QoS has been considered as the first-use case. The effort within the IETF is complementary to the contents of this Supplement.

The IP QoS signalling solution needs to be scalable.

3 References

This Technical Report incorporates, by dated or undated reference, provision for referencing material from other publications. These references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this document only when incorporated into it by amendment or revision. For undated references, the latest edition of the publication applies.

[1] IETF RFC 791 (1981), *Internet Protocol*.

[2] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.

[3] IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

[4] IETF RFC 768 (1980), *User Datagram Protocol*.

[5] IETF RFC 793 (1981), *Transmission Control Protocol*.

[6] ITU-T Recommendation Y.1540 (2002), *Internet protocol data communication service – IP packet transfer and availability performance parameters*.

[7] ITU-T Recommendation Y.1541 (2002), *Network performance objectives for IP-based services*.

[8] ITU-T Recommendation Y.1291 (2004), *An architectural framework for support of Quality of Service in packet networks*.

[9] ITU-T Recommendation Y.1221 (2002), *Traffic control and congestion control in IP-based networks*.

[10] IETF RFC 3726 (2004), *Requirements for Signalling Protocols*.

[11] IETF RFC 3260 (2002), *New Terminology and Clarifications for Diffserv*.

[12] ITU-T Recommendation G.109 (1999), *Definition of categories of speech transmission quality*.

[13] ITU-T Recommendation G.1010 (2001), *End-user multimedia QoS categories.*

[14] ITU-T Recommendation P.911 (1998), *Subjective audiovisual quality assessment methods for multimedia applications*.

[15] ITU-T Recommendation Q.1224 (1997), *Distributed functional plane for intelligent network Capability Set 2*.

4 Definitions

4.1 **BCFE**: The BCFE is an entity that performs the Resource and Admission Control functions related to QoS requests as well as routing functions.

4.2 **IP service endpoint**: A functional entity which includes one type of IP signalling endpoint and the user.

4.3 **IP signalling endpoint**: The termination point of an IP signalling path.

4.4 **IP transport packet size**: Length of the payload of an IP transport protocol contained in an IP packet.

4.5 **network entity**: The network element responsible for terminating the IP signalling protocol.

4.6 **QoS class**: Identifies the category of the information that is received and transmitted in the U-plane.

4.7 **SeCFE**: The SeCFE (Session Control Functional Entity) is an entity that provides the call/session control function.

4.8 **SFE**: The SFE (Switching Functional Entity) is an entity that performs stream classification, i.e., QoS guarantee.

4.9 **SvCFE**: The SvCFE (Service Control Functional Entity) is an entity that provides value-added service functionality.

4.10 **Terminal Equipment (TE)**: A specific implementation of an IP signalling endpoint.

4.11 **transport connection**: A bidirectional user plane association between two IP service endpoints at the transport layer.

4.12 **transport sink address**: Contains the IP address and port number, where the sender expects to receive U-plane information.

4.13 **unidirectional QoS path**: A unidirectional QoS path is a path along which the user data packets flow in the same direction.

4.14 **user**: An entity served by the IP signalling protocol.

5 Abbreviations

BCFE Bearer Control Functional Entity

CC Connection Control

CCI Connection Control Interface

CN Core Network

CPN Customer Premises Network

DiffServ Differentiated Services

FE Functional Entity

GW Gateway

IETF Internet Engineering Task Force

IN Intelligent Network

INI Inter-Network Interface

IP Internet Protocol

IPDV IP Packet Delay Variation

IPLR IP Packet Loss Ratio

IPTD IP Packet Transfer Delay

MCU Multipoint Control Unit

MPLS Multi-Protocol Label Switching

NC Network Control

NCI Network Control Interface

NNI	Network-Network Interface
NSIS	Next Step in Signalling
QoS	Quality of Service
SC	Switch Control
SCI	Switching Control Interface
SeCFE	Session Control Functional Entity
SFE	Switching Functional Entity
SvCFE	Service Control Functional Entity
TE	Terminal Equipment
UDP	User Datagram Protocol
UNI	User-Network Interface
VOD	Video On Demand
VoIP	Voice over IP

6 Functional model

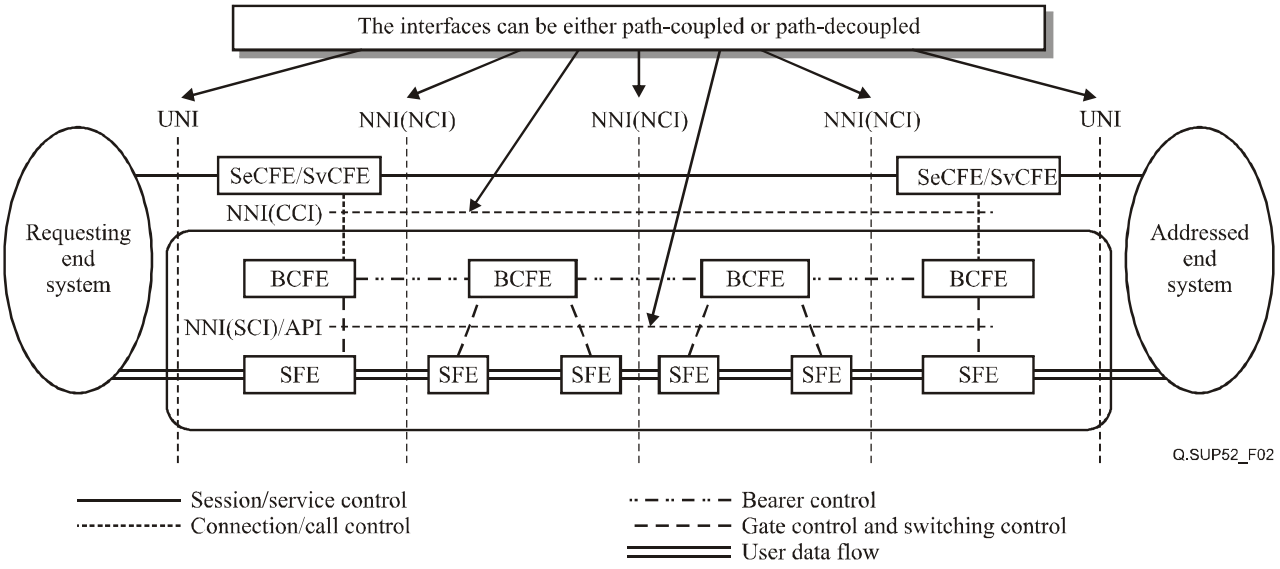


Figure 2 – The functional model of IP QoS signalling requirements

See Appendix I for the detail flows of the interfaces, Appendix II for an instance of functional model of IP QoS signalling requirements, and Appendix III for the description of trust relationships among functional entities. Such a description is considered important for deployment in a multi-operator environment.

Figure 2 depicts the functional model consisting of SeCFE, BCFE, SFE, CCIs and SCIs. It also shows an example of a service-dependent system by illustrating a Session Control FE (SeCFE) and its interface to the service-independent network. Other physical systems that can be used to provide services, such as an intelligent peripheral, could conceptually be included but are not illustrated.

The proposed modular IP QoS components and the interfaces that interconnect them relate to the functional model as follows:

a) **SeCFE/SvCFE** – An end user interacts with the SeCFE (Session Control Functional Entity)/SvCFE (Service Control Functional Entity) in order to request some service. The SeCFE/SvCFE initiates a QoS request, usually the SeCFE/SvCFE decides the parameters of a communications arrangement (such as bandwidth, quality of service, etc.). If an acceptable set of parameters can be negotiated, the SeCFE uses the services provided by the BCFE to establish, maintain and disconnect the network resources necessary to provide the negotiated arrangement.

   1) The SeCFE may appear in one of a number of forms, e.g., as a soft switch, an MCU, a VOD control server, etc. The SeCFE operates at the call/session layer, it performs call/session control, extracts QoS requirements for service connection, and initiates QoS requests to the BCFE of the bearer control plane in transport layer.

   2) The SvCFE is located within the network domain of the serving node visited by the mobile user. This functional entity provides generic network-based services to all mobile customers. These services have been referred to as default IN services which may be different in each network domain. The SvCFE and the SeCFE associated with the visited serving node are always in the same network domain; therefore, the one-to-one signalling association between these two functional entities is never supported by an inter-domain NNI signalling capability. The network SvCFE performs processing and provides access to data that is specialized for a particular service application. SvCFE extends the generic negotiation and control capabilities provided by SeCFE to support specific end-user services. Within IN terminology, this function is also called the SCF, additional information of which can be found in ITU-T Rec. Q.1224 [15].

b) **BCFE** – BCFEs (Bearer Control Functional Entities) are responsible for establishing, modifying and releasing the network resources necessary to provide the negotiated arrangement. One connection controller interacts with a peer BCFE to establish and disconnect network facilities on a link-by-link basis. BCFE components provide a generic and flexible connection model that encompasses multimedia and multiparty call requirements. BCFEs control SFEs via an SC Interface.

   The BCFE receives a QoS request from the SeCFE/SvCFE, based on a service stream. (For the MPLS case, the BCFE performs service routing. For the non-MPLS case, it performs the identification of the logical path.) After path-analysis, like service routing or the logical-path identification, it delivers the path-analysis results to the SFE.

   The BCFE needs certain network topology information and resource status information in order to be able to evaluate QoS requests and generate QoS configuration data, depending on the selected QoS control mode. The nature of this information depends on the transport layer technology, the requirements and protocols for such an interface are out of the scope of this Supplement.

c) **SFE** – SFEs (Switching Functional Entities) cross-connect a virtual connection at one port with a virtual connection at another port. Via one or more cross-connects at various SFEs located between users, a virtual connection is created between the users. The characteristics of this virtual connection are based on the call parameters negotiated at the SeCFE/SvCFE level and the route is determined by BCFE level. Based on instructions received over the SCI, the SFE, controlled by the BCFE, creates and destroys cross-connects. (For the MPLS case, it also performs MPLS transfer.)

d) **Connection control interface** – The CCI is the interface between the call/session layer and bearer control plane of transport layer.

e) **Network control interface** – The NCI is the inter-BCFE interfaces for the cases where it is necessary for two BCFEs to communicate directly.

f) **Switching control interface** – The SCI is the interface between the bearer control plane of transport layer and transport plane of transport layer.

The functional elements are structured into 2 layers, namely the call and session layer and the transport layer. The transport layer is further subdivided into the bearer control plane and the transport plane. The bearer control plane is composed of the BCFEs. In particular, it does the resource calculation related to service request. (For the MPLS case, it is also responsible for path selection and resource allocation, which characterize the logical bearer network of this service type.) The transport plane is composed of the SFEs and the media source and sinks.

6.1 Path-Coupled

The term "Path-Coupled" refers to the situation in which the signalling forwarding path is the same as the user plane path. Figure 3 shows the various possible control and in-band (i.e., indications in packet headers) mechanisms.

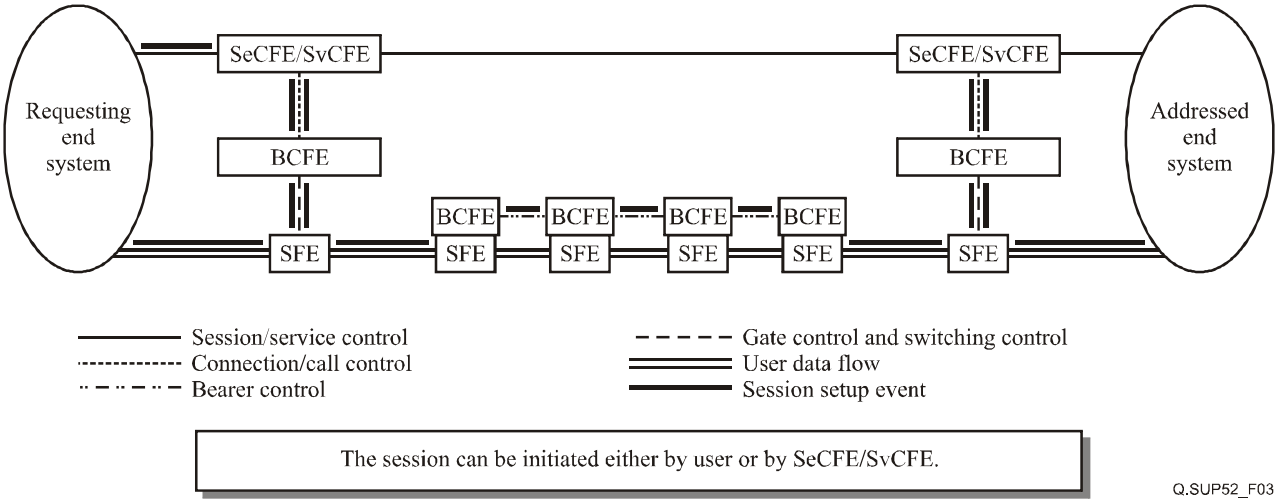


Figure 3 – Path-coupled QoS control mode

The call/session control signalling includes an indication of the QoS requirements for each session. The QoS requirements are realized using various mechanisms, e.g., packet fragmentation, over-provisioning, resource reservation (RSVP) or Diffserv. Different QoS mechanisms may be used on different sections of a session packet-forwarding path. There may be communication between call/session control nodes and packet-forwarding devices using a "gate" control protocol to control the QoS mechanism.

QoS signalling requirements are expressed in terms of attributes related to user-network signalling as well as network-network signalling. Major attributes include the following:

– the network QoS class (i.e., Table 1/Y.1541 [7]);

– the network capacity required, at both the application and network (i.e., ITU-T Rec. Y.1221 [9]) levels;

– the reliability/priority with which the service is to be sustained; and

– other elements of QoS.

Note that the complete set of classes for reliability/priority is yet to be defined.

This Supplement recognizes that an automated system for obtaining user-to-user QoS on IP networks, and on combinations of various network technologies, will require standard signalling protocols for communicating the requirements among the major entities. For the purposes of this Supplement, these entities are defined as:

1) Users and their end terminal equipment (TE); and

2) Network service providers/operators and their equipment, especially equipment implementing the interworking and signalling functions between networks, and between users and networks.

6.2 Path-decoupled

The term "path-decoupled" indicates that the signalling forwarding path is different from the user plane path.

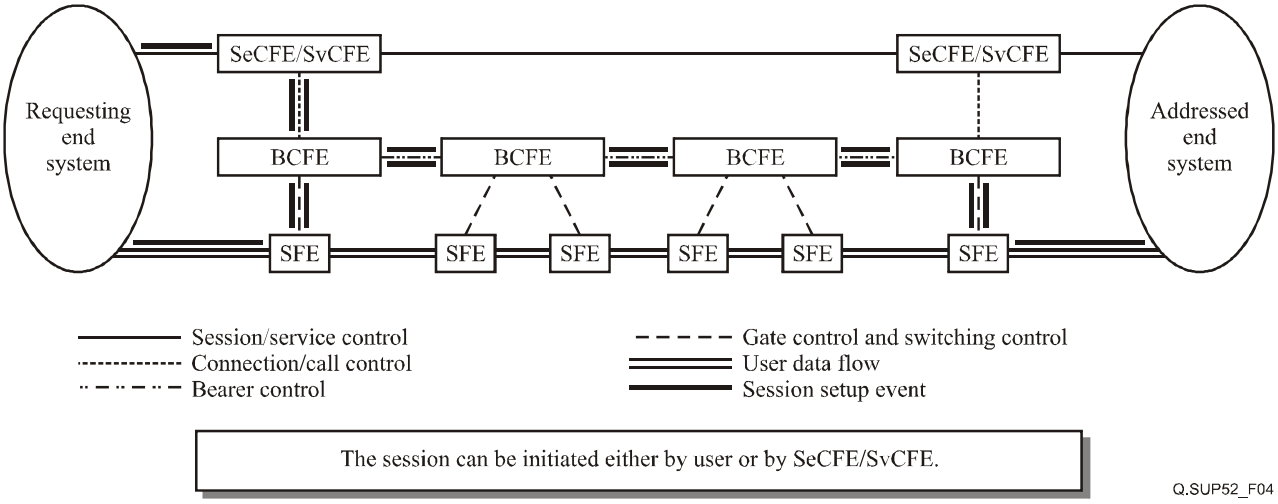


Figure 4 – Path-decoupled QoS control mode

Functionally, the framework is divided into the transport plane of transport layer, bearer control plane of transport layer and call/session control layer. The transport plane of transport layer is divided logically into basic transport plane and logical transport plane.

The basic transport plane means the IP network physical entity that is composed of the SFEs, bearing all types of IP service packets, including voice, fax, video, file transmission and web service.

In the case of the transport plane with the MPLS capability (this case is referred to as "the MPLS case" in what follows), the logical transport plane is planned and configured in advance with MPLS LSP technology.

For the transport plane without the MPLS capability (this case is referred to as "the non-MPLS case" in what follows), the logical transport plane means the networks that are planned and configured logically from the information of the routing topology on the transport plane. Each logical transport plane bears a specific service type or specific-QoS-level IP service packets, such as voice service or expedited forwarding service.

The bearer control plane of the transport layer is composed of the bearer control functional entities. It manages the network resources (bandwidth, priority, transfer delay, transfer delay jitter, etc.) of the transport plane, and controls the resource enablement, allocates the resources and routes for the service request of every QoS service stream, to meet the service stream QoS requirement.

The call/session layer is composed of session control functional entities or service control functional entities that handle the service subscriptions. It determines the service stream required QoS and requests the service stream bearer path from the bearer control plane of transport layer. The SeCFEs/SvCFEs include the soft switch that processes real-time communication call signalling such as VoIP and videotelephony, and the VoD server of the requested of video on demand, etc.

For easy management and stable network, the IP basic network needs to be divided into different management areas, which can be consistent with the division of the routing areas. In each management area, one BCFE uniformly manages the network resources, for the resource enablement control, resource allocation and routing in this management area. The resource managers in different management areas, through their signalling interaction, select a QoS-required path for the subscriber service streams across the management areas for the MPLS case.

In Figure 4 the BCFE serves as a physically independent control and management plane. The building blocks interact primarily through signalling at a per-flow level and on the basis of per- logic transport plane resource management. There is a clear signalling interface between control plane and data plane.

7 Requirements

Authentication of user and network peers is a prerequisite for QoS signalling. Authentication may be accomplished by static extension of the zone of trust, or through an authentication protocol, which is beyond the scope of these requirements.

7.1 User-network signalling

The following requirements apply to QoS signalling between users (or their terminal equipment) and the responsible network entity.

7.1.1 Attributes of a user QoS request

It shall be possible to derive the following service level parameters as part of the process of requesting service:

1) QoS class from ITU-T Rec. Y.1541 [7][5];
2) peak rate (Rp);
3) peak bucket size (Bp);
4) sustainable rate (Rs);
5) sustainable bucket size (Bs);
6) maximum allowed packet size (M);
7) IP DS field as specified in RFC 2474 [3].

It should be possible to derive the following service level parameters as part of the process of requesting service:

1) the reliability/priority with which the service is to be sustained, and
2) other elements of QoS.

Note that the complete set of classes for reliability/priority is to be defined.

Users must be able to initiate requests for service quality with the following main attributes:

– the network QoS class (e.g., Table 1/Y.1541 [7]);
– the network capacity required, at both the application and network (e.g., ITU-T Rec. Y.1221 [9]) levels;
– the reliability/priority with which the service is to be sustained; and

5 The values of IP loss ratio, IP transfer delay, and IP delay variation as specified in ITU-T Rec. Y.1221 [9] may be derived by specifying the QoS class from ITU-T Rec. Y.1541 [7] as a signalling parameter.

– other elements of QoS.

Note that the complete set of classes for reliability/priority is to be defined.

Optional attributes include the user application type and quality from among several quality categories, when such categories are available. The type of application may be completely specified from the chosen quality category.

Each of these attributes shall be signalled in independent fields in signalling messages.

Terminal Equipment (TE) should compose the detailed request on the user's behalf, possibly based on configurations set by the user or equipment installer. Many TE have the flexibility to match the user's request for application quality with network QoS classes by selecting parameters such as source coder type and packet size.

7.1.2 Omitting attributes of a user QoS request

Network QoS class, capacity, and reliability/priority are required attributes; others are optional. The network provider may assign default values for omitted attributes.

For example, speech quality categories have been defined in ITU-T Rec. G.109 [12], but there is no comparable standard range of quality categories for Web browsing, financial transactions, or many other applications of networks (each is associated with a limited quality range in ITU-T Rec. G.1010 [13]). ITU-T Rec. P.911 [14] tabulates quality categories for multimedia communication (also known as video/audio/data conferencing) and television applications. Users may simply wish to make requests for capacity, network QoS class, and reliability.

7.1.3 Form of a verifiable user QoS request

The user/TE must make its QoS request in terms the network understands, especially the parameters for network QoS. The network QoS classes and network capacity specifications in the signalling protocol must contain values that are verifiable by users (the classes in ITU-T Rec. Y.1541 [7] meet that requirement). TE may conduct measurements to ensure that the committed performance and capacity levels are achieved by the network(s).

7.1.4 Special case of user QoS request to support voiceband channels

When the user/TE request is for a voiceband channel (to support speech or voiceband modems), the QoS request (or other associated message) should contain the preferred voiceband codec and packet size. Other optional parameters may be included to indicate, for example, the use of silence suppression, the need for network echo cancellation, and alternate codecs/packet sizes.

Many of the capacity attributes will be determined by this codec choice. Also, the network operation benefits from knowledge of the codec when the need for voice transcoding can be identified (and possibly avoided). However, much of the negotiation of application parameters takes place beyond the network's purview.

7.1.5 Flow control for user QoS requests and re-requests

The TE must wait X seconds before re-submitting a request, and may have a maximum of Y simultaneous requests outstanding. Time-outs for re-submission will increase exponentially. The protocol must be "congestion-aware", using failed requests as implicit indications of congestion or using explicit notification of congestion, if available.

7.1.6 Network response to user QoS requests

Network service providers should be able to communicate the following messages and attributes (in the case of user-network interaction):

1) An identification code for the request exchange, to be used in this response and all messages that follow (such as user ACK, or release, and also in network-network messages). When used together with other information, such as Src address, each request can be uniquely referenced.

2) The simple acknowledgement and acceptance of user/TE requests.

3) The performance level expected. The ability to achieve a performance level that is better than an aspect of the QoS class response, if the network operator desires. This indication may be made for a single performance parameter, or for a combination of parameters.

4) The ability to reject a request and, at the same time, to offer a modified service level that can be met. The response may modify the request and may include commitments to an alternate QoS Class, a lower capacity, and other indications such as those in item 3.

The processing of each request and determination of acceptance require considerable work on behalf of the network provider/operator. However, these are simple tasks from the signalling point of view, and the rejections with alternatives are illustrated in Appendix V. Networks may wish to indicate a maximum time interval for which the response is valid.

7.1.7 User answer to network QoS response

The final decision to accept or reject an offered service is left to the user/TE. This completes a request-offer-answer exchange.

7.2 QoS signalling at the network-network interface

This clause treats the case where multiple networks cooperate to realize the end-to-end connectivity desired. Beyond the applications considerations mentioned above, network providers/operators primarily deal with network QoS classes, network capacity, and reliability. network-network signalling is the principle way for networks to determine multi-network compliance with QoS classes, since fixed performance allocations are not currently possible on IP networks.

Network-Network signalling shall support the determination of the QoS class offered to the user/TE, by communicating both the network QoS class requested, and the extent to which each specified parameter is already consumed. This implies that each network knows the performance from the entrance node to the (most likely) exit node(s) for the network that has the best opportunity to complete the end-end path. Policies may also determine the next network chosen. The best-next network receives the network-network signalling request.

Networks shall determine if the desired capacity and reliability are available to support the specified network QoS class from entrance to exit node(s).

7.2.1 Attributes of a network QoS request

The attributes of the network's request are:

– the network QoS class (e.g., Table 1/Y.1541 [7]), along with the consumption of individual objectives that are specified by the class;

– the network capacity required, at both the application and network (e.g., ITU-T Rec Y.1221 [9]) levels;

– the interconnecting point(s), where user/TE traffic will leave the requesting network and enter the next network;

– the reliability/priority with which the service is to be sustained; and
– other elements of QoS.

Note that the complete set of classes for reliability/priority is yet to be defined.

Optional attributes include the user application type and the quality category, when such categories are available and meaningful.

Each of these attributes shall be signalled in independent fields in signalling messages.

7.2.2 Omitting attributes of a network QoS request

Network QoS class, capacity, and reliability/priority are required attributes; others are optional.

7.2.3 Performance requirements for QoS requests and re-requests

An important aspect of the requirements for a signalling protocol is the performance requirement associated with that protocol. The most important areas where signalling performance requirements need to be established is the average/maximum latency for the establishment of service and the average/maximum latency for the re-establishment of service in the event of a network failure. The latency requirements described above for the signalling protocol depend on the performance characteristics of the underlying transport network. Because of this, performance requirements for the transport network must be specified along with the latency requirements for the signalling protocol. The combination of these factors leads to the following formal performance requirements for the signalling protocol.

1) Networks designed to meet the signalling protocol requirements specified in this clause should be capable of supporting the network performance objectives of QoS class 2 in ITU-T Rec. Y.1541 [7].
2) Signalling protocol endpoints that generate signalling messages should be capable of setting the IP DS field of those messages to a value that is associated with the statistical bandwidth transfer capability defined in ITU-T Rec. Y.1221 [9].
3) The average delay from the time of a UNI or NNI request for service to the acceptance or rejection of this service request by the network should be <800 ms.
4) The maximum delay from the time of a UNI or NNI request for service to the acceptance or rejection of this service request by the network should be <1500 ms.
5) The average delay from the time of a network failure to the time of re-establishment of service at any UNI or NNI interface should be <800 ms. (This does not address restoration of failed links.)
6) The maximum delay from the time of a network failure to the time of re-establishment of service at any UNI or NNI interface should be <1500 ms.

7.2.4 Response to a network QoS request

Network providers shall be able to respond with the following messages and attributes (in the case of network-network interaction):

1) The ability to correlate all responses and subsequent requests to the original request is required. An identification code is one example.
2) The simple acknowledgement and acceptance of requests.
3) The ability to indicate a performance level that exceeds an aspect of the request/response is required, but the indication to other entities is a network option.
4) The terminating network supporting the destination UNI shall offer a modified service level if the original service level cannot be met. The modified service may include commitment to an alternate QoS class, a lower capacity, etc.

It is possible that a chain of network-network QoS requests will encounter a network that does not support the QoS signalling protocol or QoS classes in general. If this network is an essential section of the end-to-end path, then several results are possible. One is to reject the request, but at the same time offer an unspecified class (e.g., class 5 of ITU-T Rec. Y.1541 [7]), possibly with the indication of some additional parameter values.

When making entrance-to-exit performance commitments, only one of the interconnecting links will be included for all networks, except the first network which shall include both the link to the UNI and the link to the NNI (subsequent networks will include the exit link to the next interface, either NNI or UNI).

7.2.5 Accumulating performance for additional requests

Signalling must communicate the consumption of the network (source-UNI to destination-UNI) QoS objectives. The fields used in signalling may take two forms, listed below, but the signalling messages must use one form consistently. See Appendix V for examples based on the Y.1541 [7] network QoS classes.

The forwarded request contains only the achieved values and the requested/achieved class number require signalling fields.

Each network communicates its contribution to the achieved performance level. A complete tabulation of the accumulated performance would allow corrective network actions if the requested class were not achieved.

7.3 QoS Release

Users and networks shall be able to signal when a previously requested network resource is no longer needed.

7.4 Performance

For reasons of signalling performance, the following areas should be addressed:

a) the number of messages required to establish, maintain and clear QoS requests should be kept to a minimum; and

b) the format of the IP signalling protocol information should be chosen to minimize message-processing delays at the endpoints.

7.5 Symmetry of information transfer capability

The QoS signalling protocol shall support symmetric QoS requests.

Asymmetric QoS requests are optional. That is, the end-to-end requests may be bidirectional where the information transfer capability in each direction might be different.

7.6 Contention resolution

The QoS signalling protocol shall be able to resolve all contentions with respect to resource allocation and collision.

7.7 Error reporting

The QoS signalling protocol shall include mechanisms for detecting and reporting signalling procedural errors or other failures detected by the TE/network to IP management. Service failures may also be reported to the user.

7.8 Unrecoverable failures

The TE and network entities shall include mechanisms for returning the QoS protocol instance to a stable state after detection of unrecoverable failures.

7.9 Forward and backward compatibility

The QoS signalling protocol shall include a forward compatibility mechanism and backward compatibility rules.

7.10 Parameters and values for transport connections

The signalling protocol(s) at UNI and NNI interfaces should be capable of specifying the following additional parameters as part of the process of requesting service:

1) IP header fields: source + destination address (RFC 791 [1], RFC 2460 [2]);
2) IP DS field (RFC 2474 [3], RFC 3260 [11]); and
3) Source + destination port as specified in RFC 768 [4] and RFC 793 [5].

7.11 User-initiated QoS resource modification

Either user may be able to modify the resources associated with an active transport connection, represented by the information contained in the transport connection messages.

Collision of connection resource modification requests shall be avoided by the served user.

Modification shall be performed with no loss of IP transport contents.

The use of the preferred transport connection messages is to avoid the need for subsequent modification of the connection resources immediately after the establishment.

User/TE (IP endpoints) should determine, through the use of end-end application level capability signalling, the ability and support to use resources beyond those currently in use. The support/lack of support of the capability to modify transport connection messages for a transport connection must be indicated by the originating IP endpoint. The terminating IP endpoint must indicate the support/lack of support of the modification capability of the transport connection messages. Only when both endpoints indicate modification support can modification be attempted.

This capability uses the following objects:

– Transport connection message modification support request,
– Transport connection message modification support response.

7.12 Emergency service

Emergency services shall be supported with the highest available quality of service depending on the regulatory environment.

7.13 Reliability/priority attributes

Reliability/priority attributes are the same for user-network and network-network signalling requirements. Reliability for a service can be expressed in the form of a priority level with which that service requires a particular type of network function (e.g., connection admission control priority). Hence, reliability can be requested in the form of a priority class for that specific network function. Two types of network functions apply for reliability/priority classes: connection admission control and network restoration.

From the viewpoint of signalling, there should be a limited number of priority classes for all network functions in order to ensure scalability (e.g., 4 classes). The signalling protocol needs to be able to provide the capability to effectively convey these priority requests once priority level attributes are established in standards forums. See Appendix V for more information on these attributes.

8 Interfaces description of requirements

8.1 Call/connection control interface

See Figure IV.1 for a typical process of QoS signalling in CC interface.

The QoS signalling between the call/session layer and the bearer control plane of transport layer should accomplish the following functions:

1) *Request for resources to support the service*

   Call/session layer initiates a QoS request to the bearer control plane of transport layer, with main parameters as follows:

   – Connection ID: The unique ID for each request.

     It is a requirement to have a "connection ID" to allow the sender and receiver to match a request with following responses, related modifications and cancellations. It is left for protocol design to determine which side generates that connection ID.

   – Stream information: information to identify an IP data stream.

   – QoS parameters: A description of the service quality requirements of a stream.

2) *Modification of resources to support service*

   With respect to some services, it may be necessary to modify the QoS requirements at anytime during the time the service is running. According to call/session layer requirements, bearer control plane of transport layer modifies the bandwidth that was applied for use the previous time. Multi-time modification is supported. Main parameters:

   – Connection ID: The unique ID for each request.

   – Stream information: information to identify an IP data stream.

   – QoS parameters: A description of the service quality requirements of a stream.

3) *Acceptance of resources to support service*

   Upon completing QoS resource allocation, bearer control plane of transport layer responds to the call/session layer by sending elements of success information. Main parameters are:

   – Connection ID.

   – Accepted QoS parameters: Among multi-optional QoS capabilities, the accepted QoS capability is selected.

4) *Rejection of resources to support service*

   In the case that the bearer control plane of transport layer cannot meet the QoS request of the call/session layer, it will send a rejection for resources to support service to the call/session layer. Main parameters:

   – Connection ID.

   – Rejection cause.

5) *Report about resources to support service*

In the case of any change in the allocated bandwidth information (the resource seized by the connection is no longer available, etc.; for example), the bearer control plane of transport layer should report it to the call/session layer. Main parameters:

– Connection ID.

– Current status.

6) *Release of resources to support service*

When a service is terminated, the call/session layer should initiate a request to bearer control plane of transport layer for releasing the resource that it has been requested to allocate. According to the call/session layer requirement, the bearer control plane of transport layer takes the bandwidth back. Main parameters:

– Connection ID.

– Release cause.

7) *Response to release of resources*

The cancellation of resources should be confirmed to the session. Main parameters are:

– Connection ID.

– Execution Results.

8.2 Network control interface

See Figure IV.2 for a typical process of the bearer control plane QoS signalling in NC interface.

The QoS signalling in the bearer control plane should accomplish the following functions:

1) *Request for resources to support service*

The current BCFE initiates a QoS request to the next hop BCFE for an interface, with the following main parameters:

– Connection ID: The unique ID for each request.

It is a requirement to have a "connection ID" to allow the sender and receiver to match a request with following responses, related modifications and cancellations. It is left for protocol design to determine which side generates that connection ID.

– Stream information: information to identify an IP data stream.

– QoS parameters: A description of the service quality requirements of a stream. Many international standards are available for reference in this respect, hence no further description here.

– Path information selected in the local domain and the sequent domain (for the MPLS case): By means of consultation, data stream bearer path LSP sets are distributed between the BCFEs, so conditions of LSP paths selected in the local domain should be provided for each other among BCFEs, so that a peer BCFE can correctly select a transit path LSP. For a bidirectional path, both forward path and backward path are available, such as MPLS label stack.

– Address information of the inter-domain interface: The address of the egress interface in the local domain (for the non-MPLS case).

2) *Modification of resources to support service*

With respect to some services, it may be necessary to modify the QoS requirements at any time during the service running. According to the request by the upstream BCFE, a BCFE modifies the bandwidth that was applied for use the previous time. Multi-time modification is supported. Main parameters are:

– Connection ID: The unique ID for each request.
– Stream information: information to identify an IP data stream.
– QoS parameters: A description of the service quality requirements of a stream. Many international standards are available for reference in this respect, hence no further description here.
– Path information selected in the local domain (for the MPLS case).
– Address information of the inter-domain interface (for the non-MPLS case).

3) *Acceptance of request for resources to support service*

Upon allocating the local domain resources, the BCFE responds by sending elements of success information to the upstream BCFE. Main parameters are:

– Connection ID.
– Accepted QoS parameters: Among multi-optional QoS capabilities, the accepted QoS capability is selected.
– Path information selected in the local domain and the sequent domain (for the MPLS case).
– Address information of the inter-domain interface: The address of the egress interface in the local domain (for the non-MPLS case).

4) *Rejection of request for resources to support service*

When the BCFE finds out that the QoS request of the upper BCFE cannot be satisfied, it will send a rejection response to the upper BCFE. Main parameters are:

– Connection ID.
– Rejection cause.

5) *Report about resources to support service*

In case of any change in the allocated bandwidth information (the resource seized by the connection is no longer available, etc.; for example), BCFE should report it to the upstream BCFE. Main parameters are:

– Connection ID.
– Current status.

6) *Release of resources to support service*

The upstream BCFE requests the downstream BCFE for releasing the resource that has been requested for allocation. Main parameters are:

– Connection ID.
– Release cause.

7) *Response to release for resources*

The cancellation of resources should be confirmed to the bearer control of the transport layer. Main parameters are:

– Connection ID.
– Execution results.

8.3 Switch control interface

See Figure IV.3 for a typical process of QoS signalling in SC interface.

Since this interface carries the configuration information related to QoS requests, the parameters of these messages may vary for different network layer technologies.

This interface transports the QoS parameters after being translated into network technology-dependent parameters. There are the following requirements for QoS signalling interface between the bearer control plane of transport layer and the transport plane of transport layer.

1) *QoS configuration information delivery*

According to the request of the session/call layer, or an adjacent BCFE, the BCFE determines a service route and delivers the final strategy to the corresponding SFE. Main parameters are:

- Connection ID.
- Stream information: information to identify an IP data stream.
- QoS parameters.
- Other technology-specific information (e.g., selected information of the entire path, and delivered-is-complete path information that has been allocated for the MPLS case).

2) *QoS configuration information modification*

With respect to some services, it may be necessary to modify the QoS requirements at any time during the service running. According to the request by the session/call layer, or an adjacent BCFE, a BCFE modifies the bandwidth that was applied for use the previous time. The BCFE determines a service route, and delivers the modified strategy to the corresponding SFE. BCFE and SFE support multi-time modification. Main parameters are:

- Connection ID.
- Stream information: information to identify an IP data stream;
- QoS parameters.
- Other technology-specific information (e.g., selected information of the entire path, and delivered is complete path information that has been allocated for the MPLS case).

3) *QoS configuration response*

The SFE sets QoS configuration information, and returns a success/failure indication. Main parameters are:

- Connection ID.
- Execution results.

4) *Resource status report*

This message is sent in the event of changes in the SFE resource information (e.g., SFE fault, LSP is not available, etc.); the BCFE will maintain the related bandwidth information. Main parameters are:

- Resource identifier (i.e., the LSP identifier, in the MPLS case).
- Current status.

5) *QoS configuration cancellation*

When a connection is finished, the configuration information delivered on the connection should be cancelled. Main parameters are:

- Connection ID.
- Cause code.

Appendix I

IP signalling flows

Note that the section of IP Signalling Flows is in the main body in some other TRQ(s).

The signalling information flows contained in the appendices represent a non-exhaustive set of alternatives in support of the requirements contained in the main body of this Supplement.

I.1 Path-coupled bearer control

The following diagrams illustrate the establishment (successful), connection resource modification (successful) of a QoS path.

I.1.1 Successful path-coupled transport connection establishment information flows

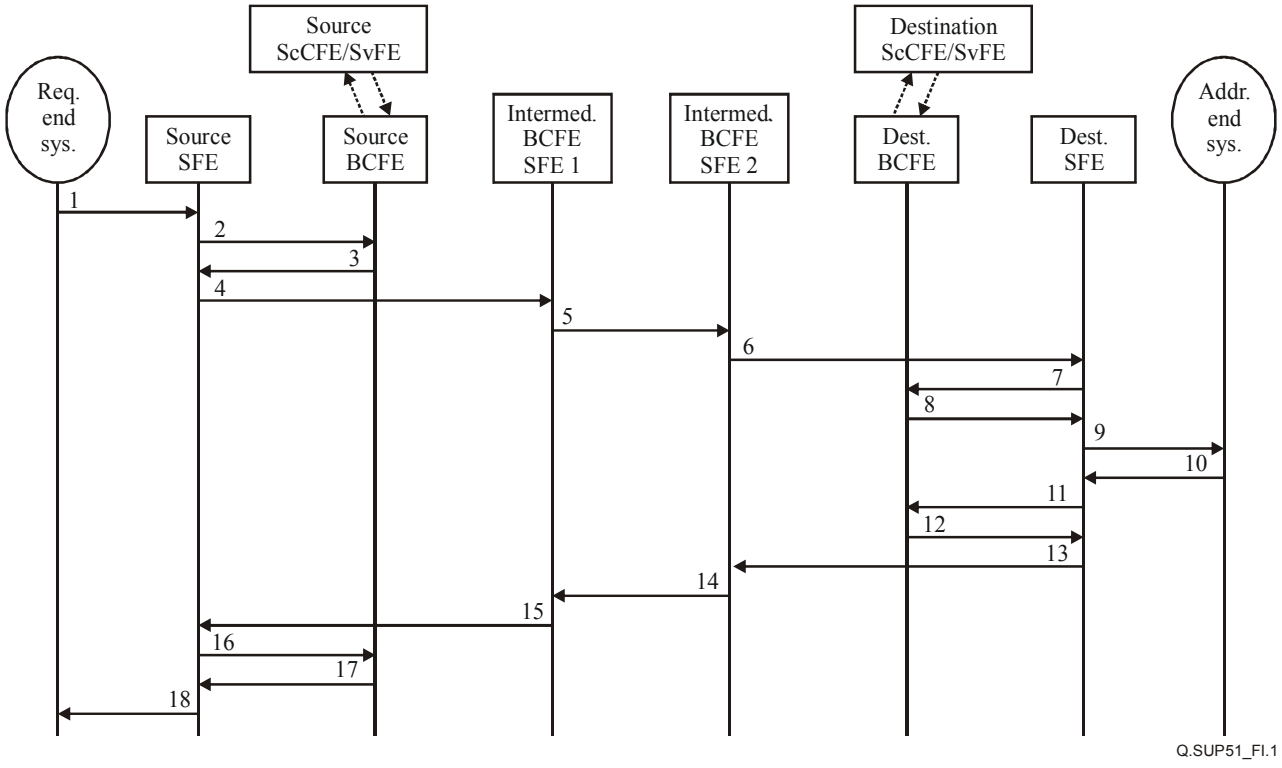


Figure I.1 – Successful path-coupled transport connection establishment information flows

Below is the descriptive text associated with the path-coupled information flow illustrated in Figure I.1.

1 IP Setup-Request.readyOriginating end system to Source SFE

——————————————————————>

User information	**Connection information**
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow: The requesting endpoint starts to establish an IP network connection.

Processing upon receipt: The addressed endpoint assures that enough resources in the endpoint remain for the new IP network connection. It then issues Information Flow 2 on the next leg.

2 IP Setup-Request.readySource SFE to source BCFE

——————————————————————>

User information	**Connection information**
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

3 IP Setup-Request.readySource BCFE to source SFE

<

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator
	Path-mode indicator

Initiation of information flow:

Processing upon receipt:

4 IP Setup-Request.readySource SFE to intermediate BCFE/SFE1

>

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

5 IP Setup-Request.readyIntermediate BCFE/SFE1 to intermediate BCFE/SFE2

——————————————————————>

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

6 IP Setup-Request.readyIntermediate BCFE/SFE2 to destination SFE

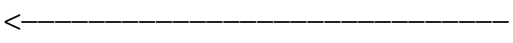
——————————————————————>

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

7 IP Setup-Request.readyDestination SFE to destination BCFE

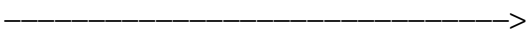


User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

8 IP Setup-Request.readyDestination BCFE to destination SFE



User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator
	Path-mode indicator

Initiation of information flow:

Processing upon receipt:

9 IP Setup-Request.readyDestination SFE to destination end system

——————————————————————>

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

10 IP Setup-Request.commit Destination end system to destination SFE

<——————————————————————

User information	Connection information
(none)	Signalling transport connection characteristics modification support response
	IP sink address of A
	IP sink address of B

Processing upon receipt:

11 IP Setup-Request.commit Destination SFE to destination BCFE

<——————————————————————

User information	Connection information
(none)	Signalling transport connection characteristics modification support response
	IP sink address of A
	IP sink address of B

Processing upon receipt:

12 IP Setup-Request.commit Destination BCFE to destination SFE

——————————————————————>

User information	Connection information
(none)	Signalling transport connection characteristics modification support response
	IP sink address of A
	IP sink address of B

Processing upon receipt:

13 IP Setup-Request.commit Destination SFE to intermediate BCFE/SFE2

<————————————————————

User information	Connection information
(none)	Signalling transport connection characteristics modification support response IP sink address of A IP sink address of B

Processing upon receipt:

14 IP Setup-Request.commit Intermediate BCFE/SFE2 to intermediate BCFE/SFE1

<————————————————————

User information	Connection information
(none)	Signalling transport connection characteristics modification support response IP sink address of A IP sink address of B

Processing upon receipt:

15 IP Setup-Request.commit Intermediate BCFE/SFE1 to source SFE

<————————————————————

User information	Connection information
(none)	Signalling transport connection characteristics modification support response IP sink address of A IP sink address of B

16 IP Setup-Request.commit Source SFE to source BCFE

————————————————————>

User information	Connection information
(none)	Signalling transport connection characteristics modification support response IP sink address of A IP sink address of B

17 IP Setup-Request.commit Source BCFE to source SFE

<————————————————————

User information	Connection information
(none)	Signalling transport connection characteristics modification support response IP sink address of A IP sink address of B

18	IP Setup-Request.commit	Source SFE to originating end system	
		<————————————	
	User information		**Connection information**
	(none)		Signalling transport connection Characteristics modification support response IP sink address of A IP sink address of B

Processing upon receipt: The requesting endpoint informs the IP served user about the completion of the requested IP network connection establishment.

I.1.2 Successful path-coupled, with QoS request modification transport connection establishment information flows

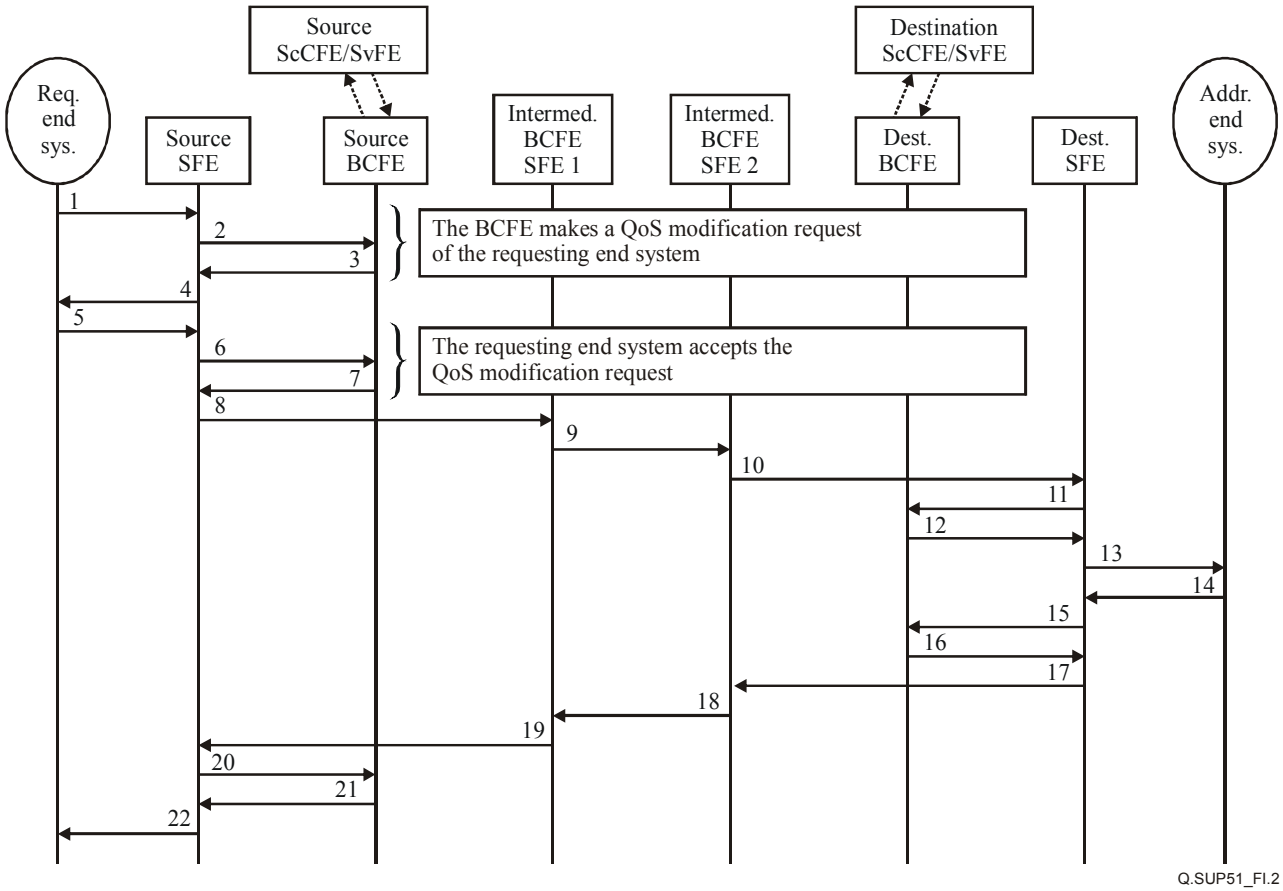


Figure I.2 – Successful path-coupled, with QoS request modification transport connection establishment information flows

Below is the descriptive text associated with the path-coupled, with QoS request modification information flow illustrated in Figure I.2.

1 IP Setup-Request.readyOriginating end system to source SFE

——————————————————>

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow: The requesting endpoint starts to establish an IP network connection.

Processing upon receipt: The addressed endpoint assures that enough resources in the endpoint remain for the new IP network connection. It then issues Information Flow 2 on the next leg.

2 IP Setup-Request.readySource SFE to source BCFE

——————————————————>

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

3 IP Modify-request Source BCFE to source SFE

<——————————————————

User information	Connection information
IP served user-generated reference	QoS modification request
Served user transport information	

Initiation of information flow:

Processing upon receipt:

4 IP Modify-request Source SFE to originating end system

<————————————————————————

User information	Connection information
IP served user-generated reference	QoS modification request
Served user transport information	

Initiation of information flow:

Processing upon receipt:

5 IP Accept-MODrequest Originating end system to source SFE

————————————————————————>

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

6 IP Accept-MODrequest Source SFE to source BCFE

————————————————————————>

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

7 IP Setup-Request.readySource BCFE to source SFE

<

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator
	Path-mode indicator

Initiation of information flow:

Processing upon receipt:

8 IP Setup-Request.readySource SFE to intermediate BCFE/SFE1

>

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

9 IP Setup-Request.readyIntermediate BCFE/SFE1 to intermediate BCFE/SFE2

——————————————————————>

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

10 IP Setup-Request.readyIntermediate BCFE/SFE2 to destination SFE

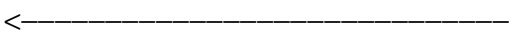
——————————————————————>

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport Preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

11 IP Setup-Request.readyDestination SFE to destination BCFE

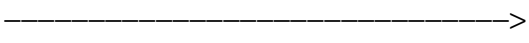


User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

12 IP Setup-Request.readyDestination BCFE to destination SFE



User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator
	Path-mode indicator

Initiation of information flow:

Processing upon receipt:

13 IP Setup-Request.readyDestination SFE to destination end system

——————————————————————>

User information	Connection information
IP served user-generated reference	Signalling transport connection characteristics
Served user transport information	Signalling transport preferred connection characteristics (optional)
	Signalling transport connection characteristics modification support request
	QoS class
	IP transport type
	IP sink address of A
	Called end point address transport
	Priority indicator

Initiation of information flow:

Processing upon receipt:

14 IP Setup-Request.commit Destination end system to destination SFE

<——————————————————————

User information	Connection information
(none)	Signalling transport connection characteristics modification support response
	IP sink address of A
	IP sink address of B

Processing upon receipt:

15 IP Setup-Request.commit Destination SFE to destination BCFE

<——————————————————————

User information	Connection information
(none)	Signalling transport connection characteristics modification support response
	IP sink address of A
	IP sink address of B

Processing upon receipt:

16 IP Setup-Request.commit Destination BCFE to destination SFE

——————————————————————>

User information	Connection information
(none)	Signalling transport connection characteristics modification support response
	IP sink address of A
	IP sink address of B

Processing upon receipt:

17 IP Setup-Request.commit Destination SFE to intermediate BCFE/SFE2

<————————————————————————

User information	Connection information
(none)	Signalling transport connection characteristics modification support response
	IP sink address of A
	IP sink address of B

Processing upon receipt:

18 IP Setup-Request.commit Intermediate BCFE/SFE2 to intermediate BCFE/SFE1

<————————————————————————

User information	Connection information
(none)	Signalling transport connection characteristics modification support response
	IP sink address of A
	IP sink address of B

Processing upon receipt:

19 IP Setup-Request.commit Intermediate BCFE/SFE1 to source SFE

<————————————————————————

User information	Connection information
(none)	Signalling transport connection characteristics modification support response
	IP sink address of A
	IP sink address of B

20 IP Setup-Request.commit Source SFE to source BCFE

————————————————————————>

User information	Connection information
(none)	Signalling transport connection characteristics modification support response
	IP sink address of A
	IP sink address of B

21 IP Setup-Request.commit Source BCFE to source SFE

<————————————————————————

User information	Connection information
(none)	Signalling transport connection characteristics modification support response
	IP sink address of A
	IP sink address of B

22 IP Setup-Request.commit Source SFE to originating end system

<————————————————————————

User information	Connection information
(none)	Signalling transport connection characteristics modification support response
	IP sink address of A
	IP sink address of B

Processing upon receipt: The requesting endpoint informs the IP served user about the completion of the requested IP network connection establishment

I.2 Path-decoupled bearer control

Within the signalling flows, the following functional entities have certain roles. They are described below.

Destination BCFE	The destination BCFE receives a QoS request based on a service stream, sent by the previous hop BCFE. When it finds out that the destination IP of the service stream belongs to the BCFE domain that is under its administration, if the request is a bidirectional one, the destination BCFE will deliver the routing result of the QoS path from the destination to the source directly to the edge router, and return the response message of the QoS path from the source to the destination to the previous hop BCFE.
Destination SFE	The destination SFE is an SFE to which a certain service stream destination belongs. The destination SFE transmits a data packet directly to a user or transfers it to another domain.
Initiator BCFE	The Initiator BCFE receives a QoS request based on a service stream, sent by the SeCFE or SvCFE. For the MPLS case it performs service routing, while for the non-MPLS case it performs the identification of the logical path.
Intermediate BCFE	The intermediate BCFE receives a QoS request based on a service stream, sent by the previous hop BCFE, queries the BCFE route table, and provides distribution of resources in the local domain.
Source BCFE	The source BCFE receives a QoS request based on a service stream, sent by the SeCFE or SvCFE or the previous hop source-seeking BCFE.
Source-seeking BCFE	The source-seeking BCFE receives a QoS request based on a service stream, sent by the previous hop BCFE, and queries the "Source BCFE" route to find out the next hop BCFE, to which it will transfer the request. The difference between the source-seeking BCFE and the intermediate BCFE is that the former transfers a request for resources according to the source address home of the service stream.

Source SFE	The source SFE is an SFE to which a certain service stream belongs. It performs stream classification. It may implement a session admission control strategy according to QoS commands.

With respect to some requests, it is necessary to allocate QoS paths from the caller parties to the called parties, and vice versa. In order to accelerate the QoS signalling process, the signalling process for paths in two directions to be allocated for one request may be provided.

I.2.1 BCFE source addressing information flows

In order to hide the network topology of the bearer control layer to the service control layer, the SeCFE/SvCFE does not need to know where the source BCFE for each call is specifically located. The SeCFE/SvCFE only needs to initiate a request to any BCFE and the request will be transferred to the source BCFE via the source-seeking BCFE process, so that a normal process of the request for resources can be started.

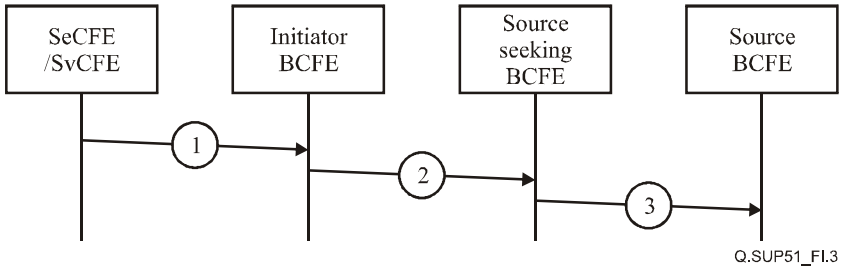


Figure I.3 – BCFE source addressing information flows

The flows illustrated in Figure I.3 are as follows:

1 IP Setup-Request.readySeCFE/SvCFE to initiator BCFE

——————————————————>

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	QoS parameter

Processing upon receipt: It performs the seeking of the real source BCFE. The initiator BCFE checks whether the source address of flow information in the QoS request belongs to the management of the Administrant Domain which the initiator BCFE takes charge of. When it finds that the source address of flow information in the QoS request does not belong to its Administrant Domain, it issues Information Flow 2.

2 IP Setup-Request.ready Initiator BCFE to source-seeking BCFE

——————————————————>

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	QoS parameter

Processing upon receipt: The source-seeking BCFE checks whether the source address of flow information in the QoS request belongs to the management of the Administrant Domain which the source-seeking BCFE takes charge of. When it finds that the source address of flow information in the QoS request does not belong to its Administrant Domain, it acts as a source-seeking BCFE. The source-seeking BCFE queries the "Source BCFE" route to find out the next hop BCFE, to which it will transfer the request. Then it issues Information Flow 3.

3 IP Setup-Request.readySource-seeking BCFE to source BCFE

——————————————————————>

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	QoS parameter

Processing upon receipt: The BCFE checks whether the source address of flow information in the QoS request belongs to the management of the Administrant Domain which the BCFE takes charge of. When it finds that the source address of flow information in the QoS request belongs to its Administrant Domain, the process of addressing source BCFE is completed and this BCFE acts as a source BCFE.

I.2.2 Unidirectional QoS path establishment information flows

There are two approaches in the QoS path establishment procedures. The difference is the existence of the provisional response from BCFE to SeCFE/SvCFE, by which the BCFE notifies to SeCFE/SvCFE that the resource allocation is successful, just before confirming the local policies to the corresponding SFE. When the SeCFE/SvCFE receives the provisional response, it changes the state of the service control from "waiting for the successful completion of resource allocation" to the next state by issuing the awaited service control messages. This approach can be applied when the resource management is integrated with service control in which the completion of the resource allocation is required before the progress and completion of the session establishment. Some VoIP services may require the completion of resource allocation before the called party's state transition into the alerting.

In Figure I.4, the scenario where the resource request is processed without the provisional response is called "1-phase case". If the request is processed with this response it is called "2-phase case".

NOTE 1 – The flows drawn in dashed lines are used only in the 2-phase case.

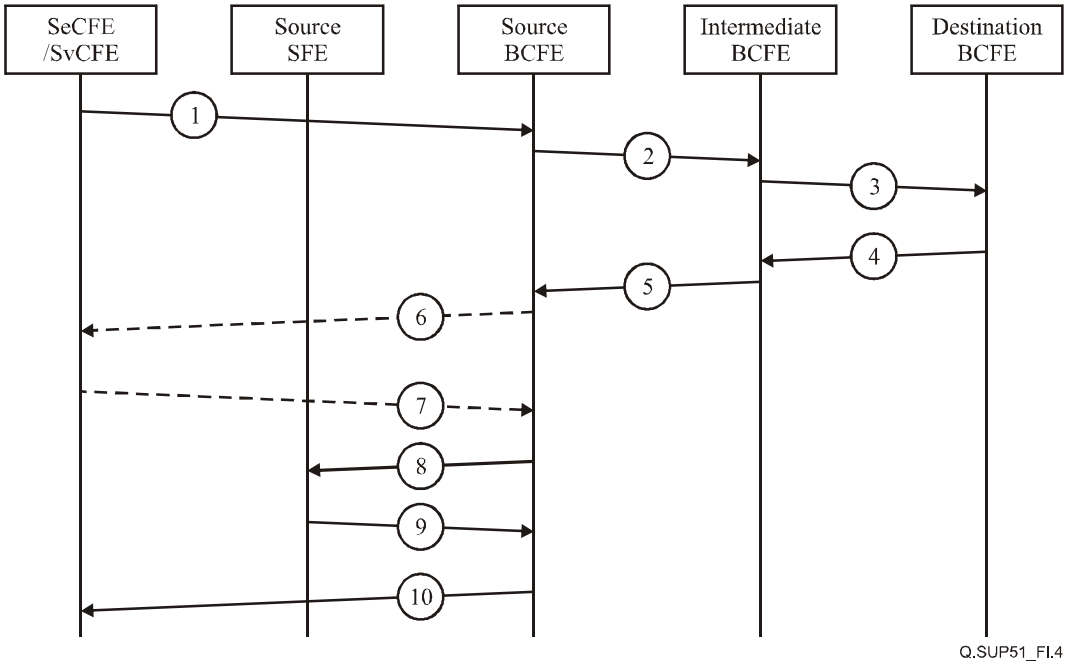


Figure I.4 – Forward unidirectional QoS path establishment information flows

The flows illustrated in Figure I.4 are as follows:

1 IP Setup-Request.readySeCFE/SvCFE to source BCFE

——————————————————————>

User information	**Connection information**
IP flows description information	Connection ID
Service type (optional)	QoS parameter

Initiation of information flow: When the SeCFE/SvCFE receives the request to establish an IP connection and finds a set of information required for the resource request (e.g., IP flows descriptions information, Service type (optional), Connection ID, and QoS parameter), the SeCFE/SvCFE issues the Information Flow 1 as a resource request.

Processing upon receipt: The source BCFE (also an initiator BCFE) allocates the path resources of the local domain. It then issues Information Flow 2.

2 IP Setup-Request.readySource BCFE to intermediate BCFE

——————————————————————>

User information	**Connection information**
IP flows description information	Connection ID
Service type (optional)	QoS parameter
	Policy-based routing information selected in the local domain and the sequent domain (for the MPLS case)
	Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The intermediate BCFE allocates the intermediate path resources. It then issues Information Flow 3.

3 IP Setup-Request.readyIntermediate BCFE to destination BCFE

——————————————————————>

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	QoS parameter
	Policy-based routing information selected in the local domain and the sequent domain (for the MPLS case)
	Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The result of the destination BCFE route decides the final path resource. The destination BCFE responds to the intermediate BCFE. It then issues Information Flow 4.

4 IP Setup-Request.commit Destination BCFE to intermediate BCFE

<——————————————————————

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	Accepted QoS parameter
	Policy-based routing information selected in the local domain and the sequent domain (for the MPLS case)
	Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The intermediate BCFE responds to the source BCFE. It then issues Information Flow 5.

5 IP Setup-Request.commit Intermediate BCFE to source BCFE

<——————————————————————

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	Accepted QoS parameter
	Policy-based routing information selected in the local domain and the sequent domain (for the MPLS case)
	Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: It then issues Information Flow 6.

6 IP Setup-Request.commit Source BCFE to SeCFE/SvCFE (Optional)

<——————————————————————

User information	Connection information
IP flows description information	Connection ID
	Accepted QoS parameters

Processing upon receipt: The SeCFE/SvCFE then informs the results of the resource allocation to its peer entity which performs the session control signalling. Upon receiving the request to cut through the IP connection with the allocated resources from the entity of session control signalling, the SeCFE/SvCFE then issues Information Flow 7 to the source BCFE.

7 IP Setup-Request.commit SeCFE/SvCFE to source BCFE (Optional)

——————————————————>

User information	**Connection information**
	Connection ID

Processing upon receipt: The source BCFE then issues Information Flow 8 to the source SFE. Until this time, based on the results of a piece of complete path resource information, the source BCFE forms a piece of stream QoS configuration information to deliver a piece of configuration information to the source SFE.

8 IP Setup-Request.commit Source BCFE to source SFE

<——————————————————

User information	**Connection information**
IP flows description information	Connection ID
Service type (optional)	Accepted QoS parameter
	Selected information of the entire path and complete policy-based routing information that has been allocated (for the MPLS case).

Processing upon receipt: The source SFE installs the configuration information to control the data stream transfer. It then issues Information Flow 9.

9 IP Setup-Request.commit Source SFE to source BCFE

——————————————————>

User information	**Connection information**
(None)	Connection ID
	Execution results

Processing upon receipt: It then issues Information Flow 10.

10 IP Setup-Request.commit Source BCFE to SeCFE/SvCFE

<——————————————————

User information	**Connection information**
IP flows description information	Connection ID
	Accepted QoS parameters

Processing upon receipt: The SeCFE/SvCFE informs the results of the cut-through to the entity which performs the session control signalling between the requesting QoS TE and the addressed QoS TE.

NOTE 2 – With regard to the interworking between the resource control flows applied to the CC interface and the session control flows applied among the requesting QoS TE, SeCFE/SvCFE, and the addressed QoS TE, it depends on the procedural requirement for the service signalling, e.g., the negotiation of QoS requirements among the requesting/addressed QoS TE and the SeCFE/SvCFE.

I.2.3 Bidirectional QoS path establishment information flows

There are two methods to establish bidirectional QoS path-supporting symmetric QoS requests, one is to allocate the path of the two directions at one time, which can be applied in the case where the transport plane has a capability to perform the explicit routing for reducing the time of the signalling procedures (see I.2.3.1); the other is to use two unidirectional information flows (see I.2.3.2).

The differences between unified-allocated forward-and-backward-resource information flows and separately-allocated forward-and-backward-resource information flows are:

– Path information of two directions should be needed for the source BCFE and intermediate BCFE to initiate a resource request. For a bidirectional path with unified-allocated forward-and-backward-resource information flows, both forward and backward paths are needed.

– Path information of two directions should also be needed for the destination BCFE and intermediate BCFE to initiate a resource response.

– The destination BCFE needs to deliver a piece of QoS configuration information from the called to the caller to the destination SFE.

I.2.3.1 Unified-allocated forward-and-backward-resource information flows

NOTE 1 – The flows drawn in dashed lines in Figure I.5 are used only in the 2-phase case.

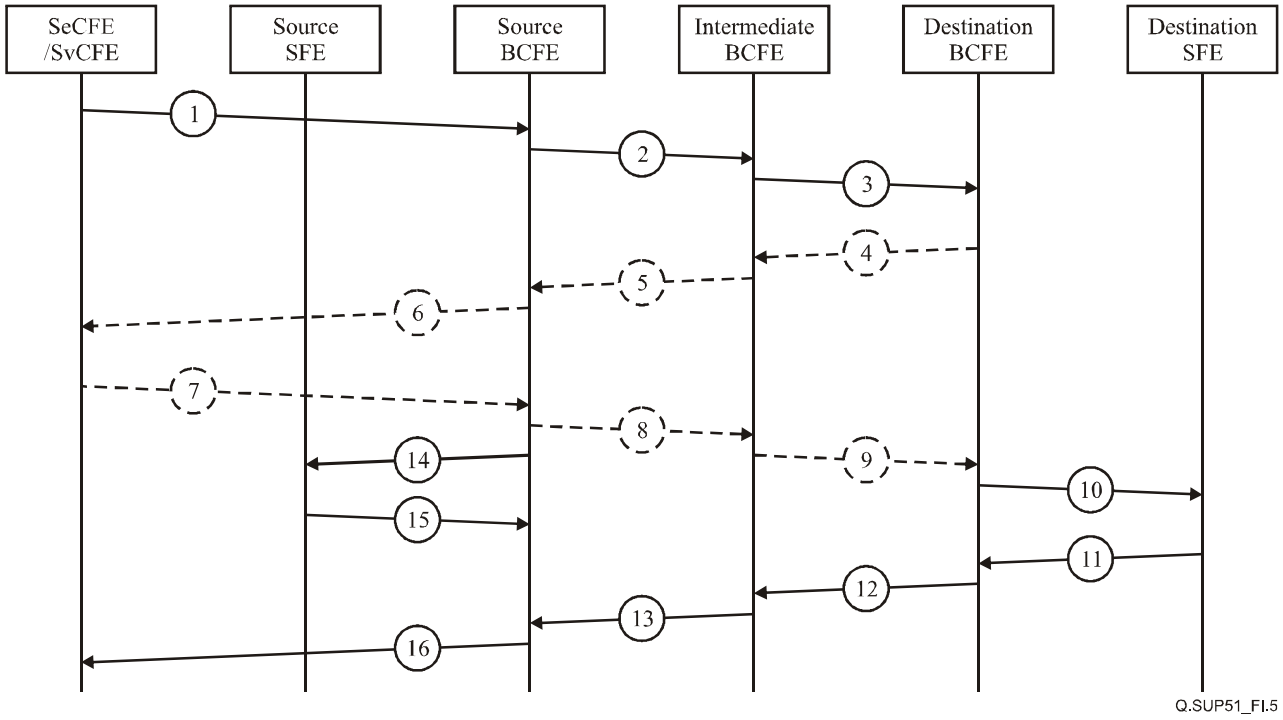


Figure I.5 – Bidirectional QoS path establishment information flows with unified-allocated signalling path

There are two separate subgroups of signalling flows: in the 2-phase case, group A consists of the messages (8, 9, 10, 11, 12, 13), where 8 is the first flow of group A; in the 1-phase case, group A consists of the messages (2, 3, 10, 11, 12, 13), where 2 is the first flow of group A. Group B consists of the messages (14, 15), where 14 is the first flow of group B. Only after the last messages of both groups (i.e., 13 and 15) reach the source BCFE, message 16 can be submitted.

The flows illustrated in Figure I.5 are as follows:

1 IP Setup-Request.readySeCFE/SvCFE to source BCFE

——————————————————>

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	QoS parameter

Processing upon receipt: The source BCFE allocates the path resources of the local domain. It then issues Information Flow 2.

2 IP Setup-Request.readySource BCFE to intermediate BCFE

——————————————————>

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	QoS parameter
	Policy-based routing information selected in the local domain and the sequent domain (for the MPLS case)
	Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The intermediate BCFE allocates the intermediate path resources. It then issues Information Flow 3.

3 IP Setup-Request.readyIntermediate BCFE to destination BCFE

——————————————————>

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	QoS parameter
	Policy-based routing information selected in the local domain and the sequent domain (for the MPLS case)
	Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The result of the destination BCFE route decides the final path resource. The BCFE responds to the intermediate BCFE. It then issues Information Flow 4.

4 IP Setup-Request.commit Destination BCFE to intermediate BCFE (only in 2-phase case)

<——————————————————

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	Accepted QoS parameter
	Policy-based routing information selected in the local domain and the sequent domain (for the MPLS case)
	Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The intermediate BCFE responds to the source BCFE. It then issues Information Flow 5.

5 IP Setup-Request.commit Intermediate BCFE to source BCFE (only in 2-phase case)

<————————————————————————

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	Accepted QoS parameter
	Policy-based routing information selected in the local domain and the sequent domain (for the MPLS case)
	Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The source BCFE issues Information Flow 6.

6 IP Setup-Request.commit Source BCFE to SeCFE/SvCFE (only in 2-phase case)

<————————————————————————

User information	Connection information
IP flows description information	Connection ID
	Accepted QoS parameters

Processing upon receipt: The SeCFE/SvCFE then informs the results of the resource allocation to the entity which performs the session control signalling between the source QoS TE and the sink QoS TE. Upon receiving the request to cut through the IP connection with the allocated resources from the entity of session control signalling, the SeCFE/SvCFE then issues Information Flow 13 to the source BCFE.

7 IP Setup-Request.commit SeCFE/SvCFE to source BCFE (only in 2-phase case)

————————————————————————>

User information	Connection information
	Connection ID

Processing upon receipt: The source BCFE then issues Information Flow 8 and Information Flow 14 at the same time. Flow 14 is issued in order to control the stream QoS configuration information of the source SFE and Flow 8 is to control the configuration information of the opposite side SFE.

8 IP Setup-Request.readySource BCFE to intermediate BCFE (only in 2-phase case)

————————————————————————>

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	QoS parameter
	Policy-based routing information selected in the local domain and the sequent domain (for the MPLS case)
	Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The intermediate BCFE finds out the next hop until the destination BCFE. It then issues Information Flow 9.

9 IP Setup-Request.ready Intermediate BCFE to destination BCFE (only in 2-phase case)

——————————————————————>

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	QoS parameter
	Policy-based routing information selected in the local domain and the sequent domain (for the MPLS case)
	Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The destination BCFE controls the destination SFE for the stream with the direction from the destination SFE to the source SFE. Upon getting a piece of complete path resource information, the destination BCFE forms a piece of stream QoS configuration information to deliver a piece of configuration information to the destination SFE. It then issues Information Flow 10.

10 IP Setup-Request.readyDestination BCFE to destination SFE

——————————————————————>

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	Accepted QoS parameter
	Selected information of the entire path and complete policy-based routing information that has been allocated (for the MPLS case).

Processing upon receipt: The destination SFE installs the configuration information to control the data stream transfer. It then issues Information Flow 11.

11 IP Setup-Request.commit Destination SFE to destination BCFE

<——————————————————————

User information	Connection information
(None)	Connection ID
	Execution results

Processing upon receipt: The destination BCFE responds to the intermediate BCFE. It then issues Information Flow 12.

12 IP Setup-Request.commit Destination BCFE to intermediate BCFE

<——————————————————————

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	Accepted QoS parameter
	Policy-based routing information selected in the local domain and the sequent domain (for the MPLS case)
	Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: The intermediate BCFE responds to the source BCFE. It then issues Information Flow 13.

13 IP Setup-Request.commit Intermediate BCFE to source BCFE

<————————————————————————

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	Accepted QoS parameter
	Policy-based routing information selected in the local domain and the subsequent domain (for the MPLS case)
	Address information of the inter-domain interface (for the non-MPLS case)

Processing upon receipt: After receiving Information Flow 13, which is the response for "backward message flows", as well as Information Flow 15, which is the response for "forward message flows", the source and initiator BCFE issues Information Flow 16.

14 IP Setup-Request.commit Source BCFE to source SFE

<————————————————————————

User information	Connection information
IP flows description information	Connection ID
Service type (optional)	Accepted QoS parameter
	Selected information of the entire path and complete policy-based routing information that has been allocated (for the MPLS case).

Processing upon receipt: The source SFE installs the configuration information to control the data stream transfer. It then issues Information Flow 15.

15 IP Setup-Request.commit Source SFE to source BCFE

————————————————————————>

User information	Connection information
(None)	Connection ID
	Execution results

Processing upon receipt: After receiving Information Flow 13, which is the response for "forward message flows", as well as Information Flow 15, which is the response for "backward message flows", and means that resources have been allocated in both direction, the source and initiator BCFE issues Information Flow 16.

16 IP Setup-Request.commit Source BCFE to SeCFE/SvCFE

<————————————————————————

User information	Connection information
IP flows description information	Connection ID
	Accepted QoS parameters

Processing upon receipt: The SeCFE/SvCFE informs the results of the cut-through to the entity which performs the session control signalling between the Source QoS TE and the Sink QoS TE.

NOTE 2 – As regards the interworking between the resource control flows applied to the CC interface and the session control flows applied among the source QoS TE, SeCFE/SvCFE, and the sink QoS TE, it depends on the procedural requirement for the service signalling, e.g., the negotiation of QoS requirements among the source/sink QoS TE and the SeCFE/SvCFE.

I.2.3.2 Separately-allocated forward-and-backward-resource information flows

Figure I.6 shows the separately-allocated forward-and-backward-resource information flows. For the backward information flows, if both of calling and called part SeCFE/SvCFE take part in the procedure, we can use the second figure; if only one of the calling and called part SeCFE/SvCFE take part in the procedure, we can use the third figure.

In the case of one of the calling and called part SeCFE/SvCFE taking part in the procedure, this is performed with two parallel unidirectional information flows described in section I.2.2 except the following points;

– Information flow 1 is shared between both cases. Information 10 is also identical. In the 2-phase case, information flows 6 and 7 are also shared with each diagram.

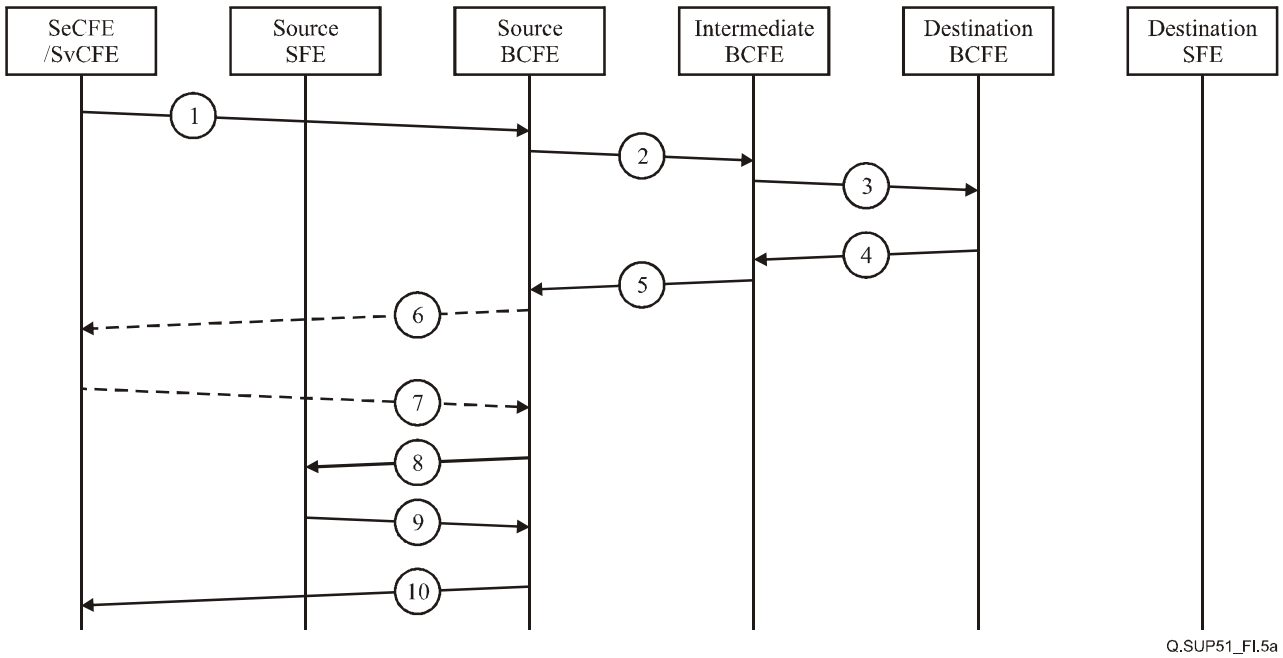
– The BCFE receiving information flow 1 splits the signalling sequence into two sequences with opposite directions. In the 2-phase case, this split is also performed after receiving information flow 7.

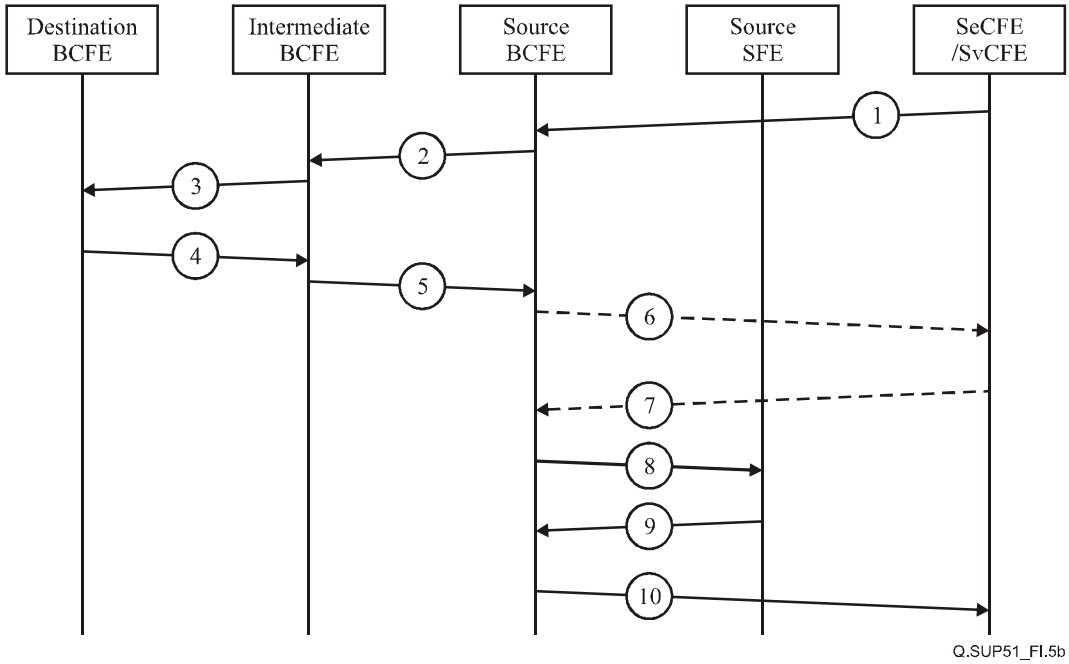
– The BCFE receiving information flow 1 also waits for the response of each sequence (information flows 9 and S8), and then consolidates these two signalling sequences into a single sequence. In the 2-phase case, this consolidation is also performed before issuing information flow 6.

– For performing the resource control in the direction where the initiating BCFE is not the source BCFE, the source BCFE seeking flows (described in section I.2.1) are applied as described with information flows (S1, S2, S3, S4, S5, S6, S7, S8).

NOTE – The flows drawn in dashed lines in Figure I.6 are used only in the 2-phase case.

Figure I.6 – Separately-allocated forward-and-backward-resource information flows *(start)*





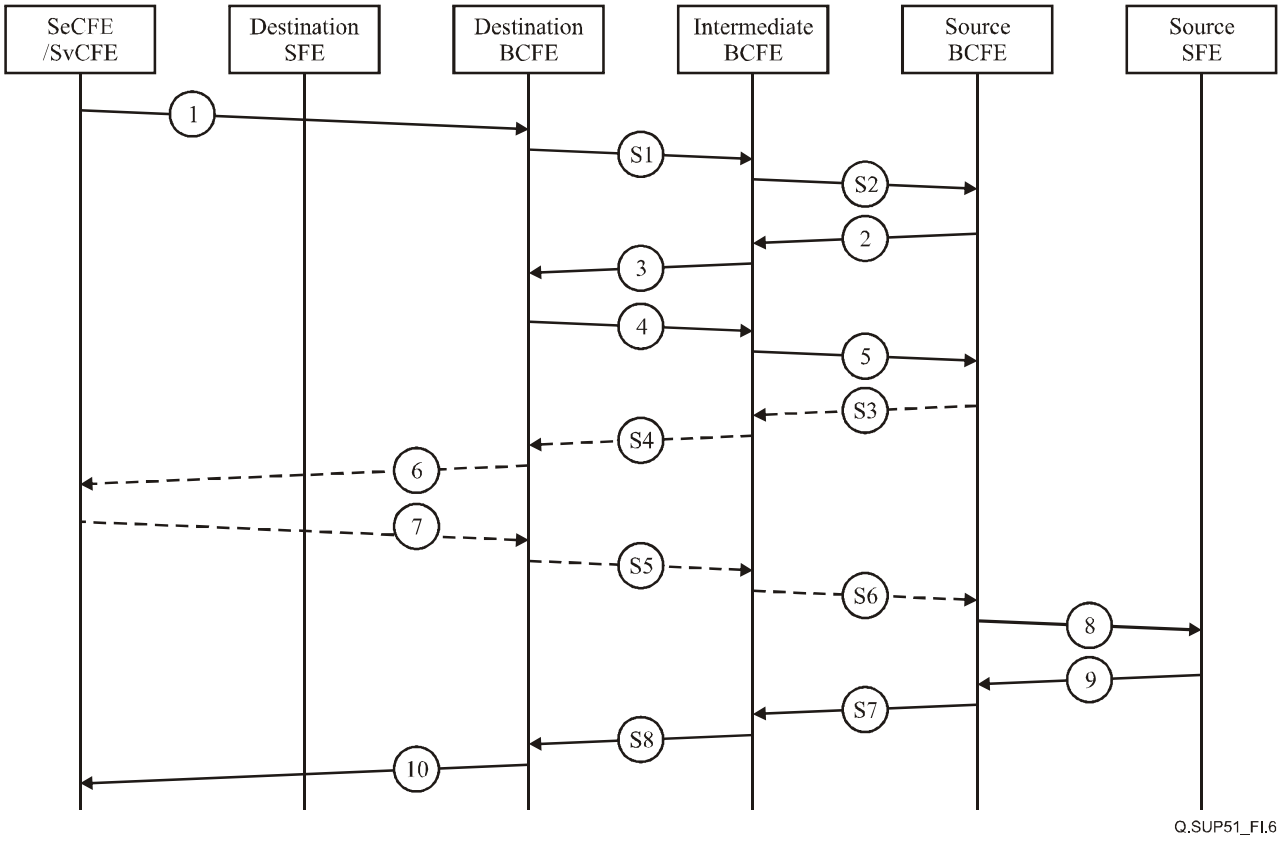


Figure I.6 – Separately-allocated forward-and-backward-resource information flows *(end)*

Appendix II

An instance of functional model of IP QoS signalling requirements

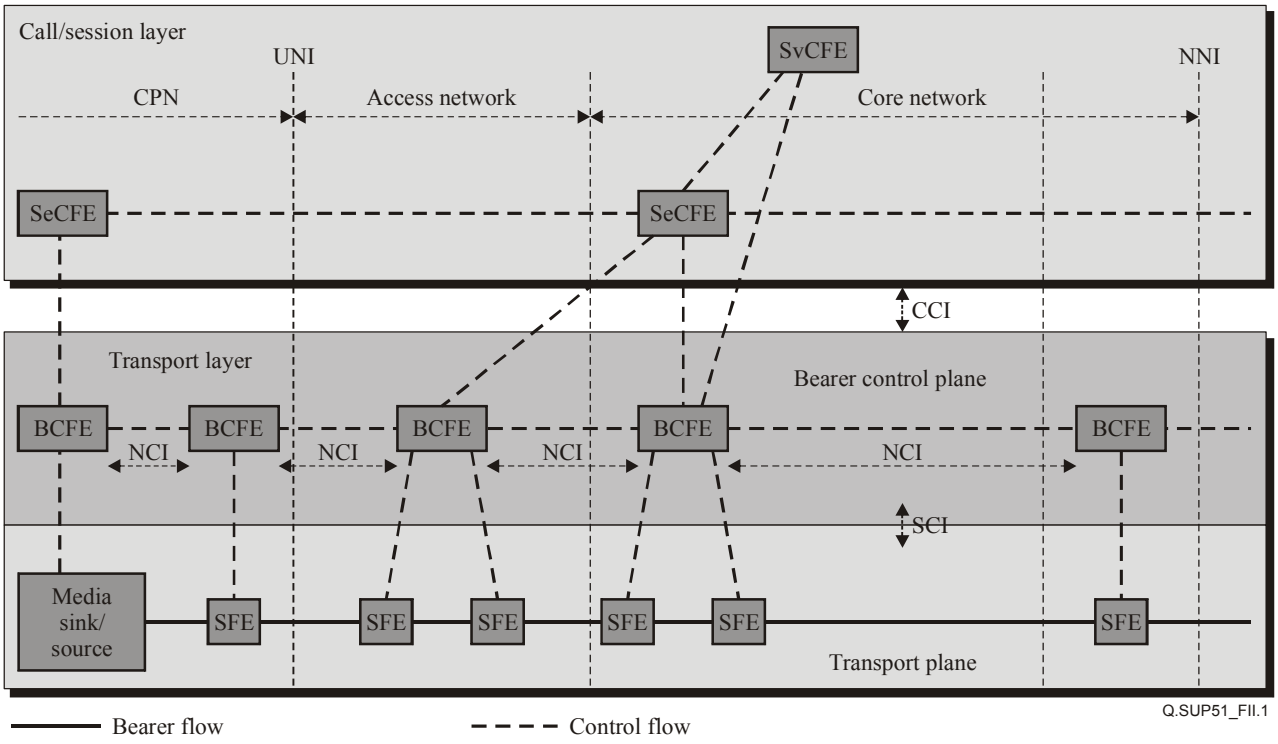


Figure II.1 – The functional model of IP QoS signalling requirements

Appendix III

Multi-operator scenario

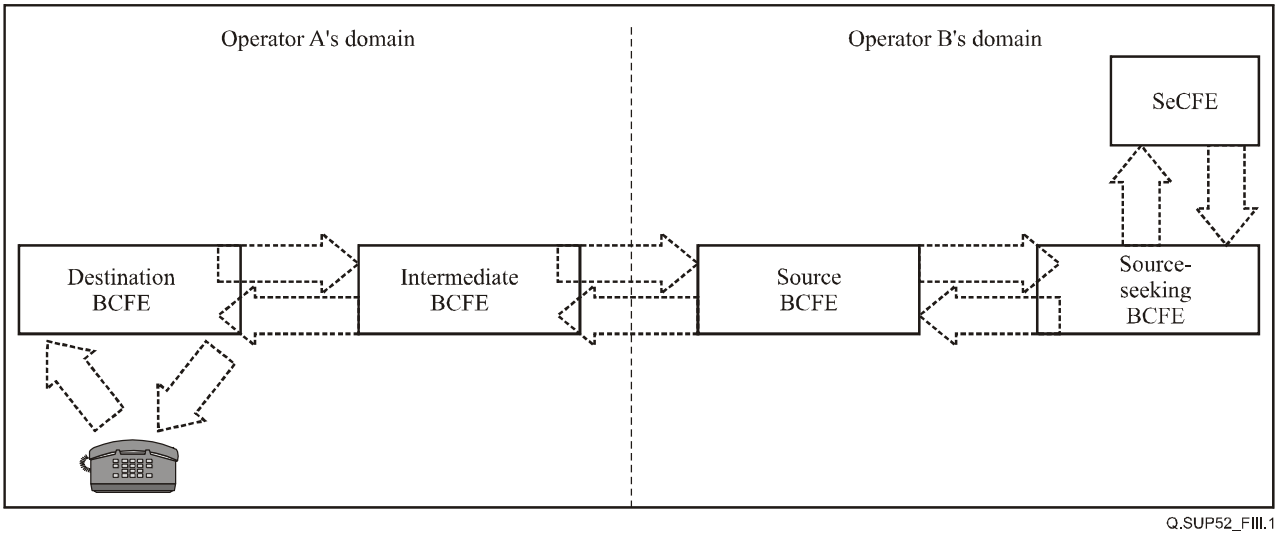


Figure III.1 – Multi-operator scenario

In Figure III.1 operator A is responsible for the terminating section of the IP stream. Only the QoS bearer setup requests are shown. Operator B offers the network service at call/session control level and initiates QoS requests.

Operator A is responsible for:

– Taking into consideration the QoS requests generated by operator B;

– Informing operator B of the available QoS parameters for the call/session;

– Enforcing the agreed QoS parameters within the network domain which it manages.

Operator B is responsible for:

– Generating appropriate QoS requests in accordance with the service offered to the end user;

– Enforcing the agreed QoS parameters within the network domain which it manages.

In this scenario, the end-end efficiency depends on the cooperation of operators A and B who would establish mutual agreements in order for the service to be rendered. A trusted relationship is therefore assumed between BCFEs belonging to different operators. In order to achieve this requirement, additional security features not described in this Supplement (e.g., mutual authentication), may be necessary.

Appendix IV

Typical process of QoS signalling in interfaces

Figure IV.1 shows a typical process of QoS signalling in CC interface:

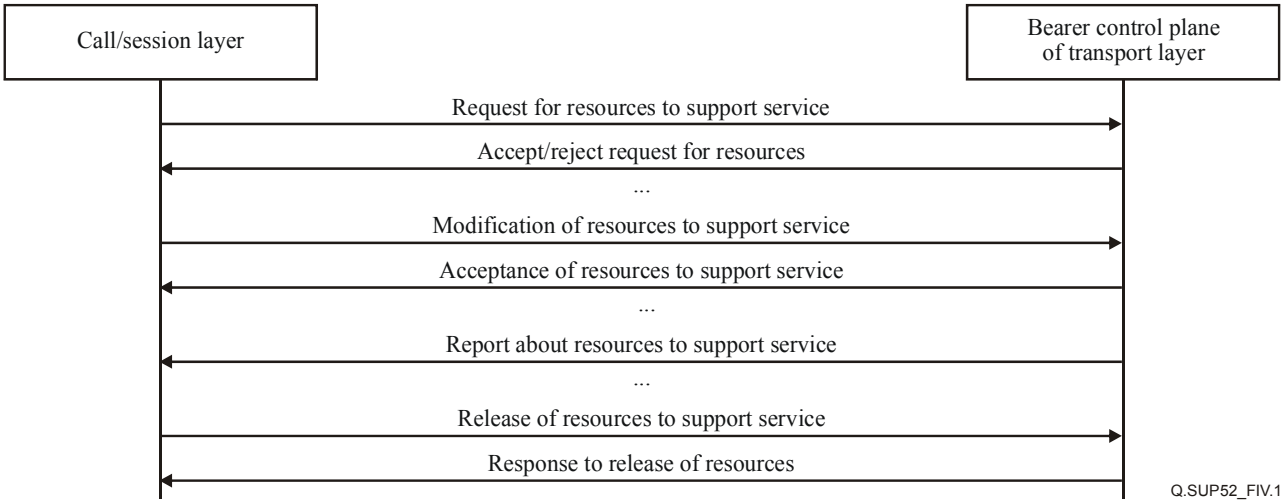


Figure IV.1 – Process of QoS signalling in CC interface

Figure IV.2 shows a typical process of the bearer control plane QoS signalling in NC interface.

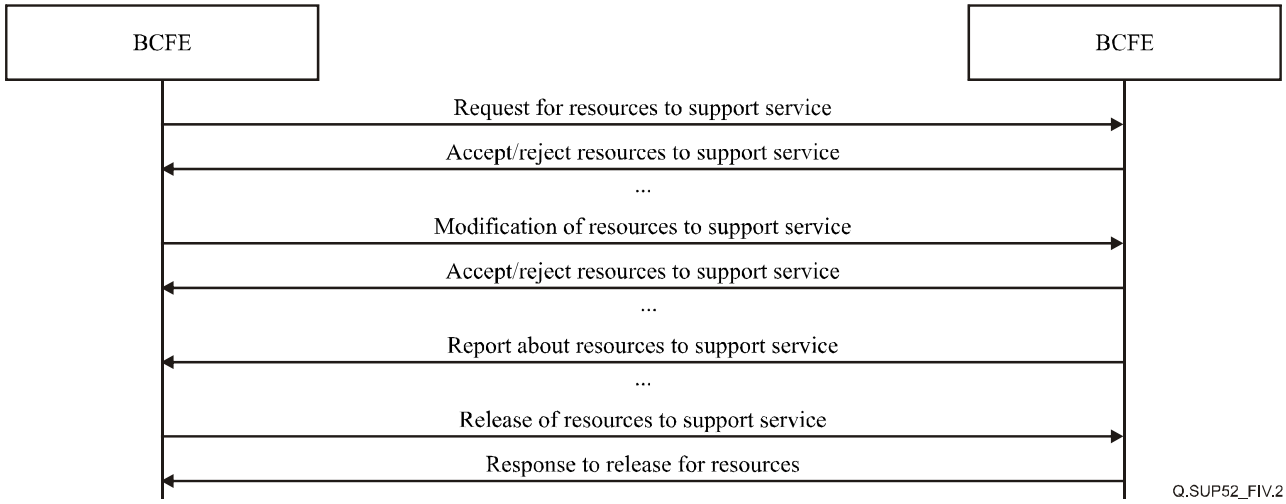


Figure IV.2 – Process of bearer control plane QoS signalling in NC interface

Figure IV.3 shows a typical process of QoS signalling in SC interface.

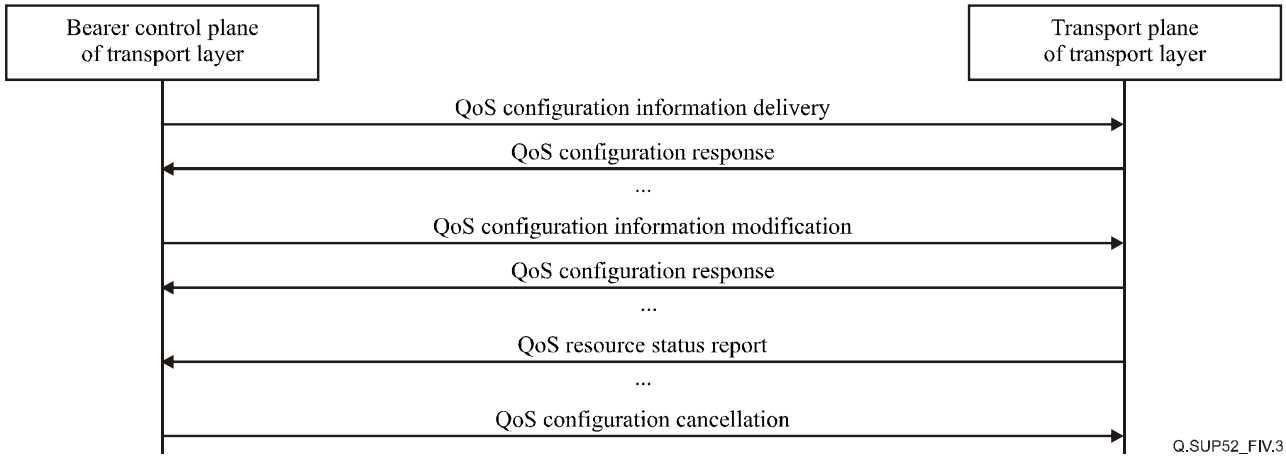


Figure IV.3 – Process of QoS signalling in SC interface

Appendix V

Examples to support QoS signalling requirements based on Y.1541 network QoS classes, and additional information on reliability/priority

V.1 User-network signalling in support of network QoS class

An example of network response 3 (see 7.1.6) (QoS class acceptance and parameter level indication) is a case where the network provider commits to the requested class and indicates the achieved performance for delay and delay variation supporting the class 0 objectives. The values indicated are simply estimates of performance, and the only binding commitment is to the QoS class. In the following tables, acceptance of the QoS class indicates commitment to its objectives.

Table V.1 – Example of QoS Class acceptance with specified parameter indications

Field name	Value	Mandatoryf ield?
QoS class requested	Class 0	Yes
QoS class response	Accept	Yes
Mean transfer delay (IPTD)	80 ms	No
99.9% – min Delay Var. (IPDV)	20 ms	No
Loss (IPLR)		No
Errored packets (IPER)		No

An example of network response 4 (see 7.1.6) (QoS class rejection and alternate class commitment and indications) is a case where the network provider rejects the requested class and offers another class with a specified parameter indication for delay.

Table V.2 – Example of QoS class rejection with alternative offer and indications

Field name	Value	Mandatoryf ield?
QoS Class requested	Class 0	Yes
QoS class response	Reject	Yes
QoS class offered	Class 1	No
Mean transfer delay (IPTD)	180 ms	No
99.9% – min Delay Var. (IPDV)		No
Loss (IPLR)		No
Errored packets (IPER)		No

V.2 Network-network signalling

Signalling must communicate the consumption of the network (source-UNI to destination-UNI) QoS objectives. The fields used in signalling may take several forms:

Table V.3 – Example of accumulating and signalling current performance

	Requested	Currently achieved
QoS class	Class 0	Class 0
Mean transfer delay (IPTD)	100 ms	20 ms
99.9% – min Delay Var. (IPDV)	0 ms	10 ms
Loss (IPLR)	10^{-3}	$<10^{-3}$
Errored packets (IPER)	10^{-4}	$<10^{-4}$
Status of parameter indications		Allowed

Note that the requested parameter values are fully specified by the QoS class, but are included in this table for simple comparison. Only the achieved values and the requested/achieved class number require signalling fields.

The network receiving this message determines its performance from entrance node to the destination, or to the most likely exit node to the best-next network. The network would add its contribution to the currently achieved fields (according to a specified set of summation rules for each parameter), and send these fields on to the next network or back toward the requesting user. Participating networks can indicate their willingness to indicate specific parameter values (where a single negative preference overrides others). In case the requested QoS class is not achieved, the response can contain the committed performance in excess of the offered class, using the currently achieved values.

The ability for each network to enter and communicate its contribution to the achieved performance level is a network option, an example of which is shown in Table V.4:

Table V.4 – Example of accumulating and signalling current performance

	Requested	Network 1	Network 2	Currently achieved
QoS class	Class 0	Class 0	Class 0	Class 0
Mean transfer delay (IPTD)	100 ms	20 ms	10 ms	30 ms
99.9% – min Delay Var. (IPDV)	50 ms	10 ms	10 ms	15 ms
Loss (IPLR)	10^{-3}	$<10^{-3}$	$<10^{-3}$	$<10^{-3}$
Errored packets (IPER)	10^{-4}	$<10^{-4}$	$<10^{-4}$	$<10^{-4}$
Status of parameter indications		Allowed	Allowed	Allowed

A complete tabulation of the accumulated performance would allow corrective network actions if the requested class were not achieved.

Summation rules are simple for transfer delay. Average values for each network are added to the currently achieved value. More study is needed to determine the summation rules for delay variation and other parameters.

V.3 Future development of classes to support reliability and priority attributes

Reliability/priority attributes are the same for user-network and network-network signalling requirements. No formal standards exist with respect to the qualitative (e.g., number of priority classes) or quantitative (e.g., time-to-restore) aspects of reliability. To that extent, the following assumptions are made in determining reliability attributes:

– Reliability for a service can be expressed as a priority with which that service requires a particular type of network function (e.g., connection admission control priority). Hence, reliability can be requested in the form of a priority class for that specific network function.

– From the viewpoint of signalling, there will be a limited number of priority classes for all network functions in order to ensure scalability (e.g., 4 classes).

Two types of priority class attributes are defined:

– Connection admission control priority class: The urgency with which a service connection is desired (e.g., high, normal, best effort).

– Restoration priority class: The urgency with which a service requires successful restoration under failure conditions (e.g., high, normal, best effort).

Appendix VI

Path-coupled and path-decoupled interoperability scenarios and scenarios with/without the participation of SeCFE/SvCFE

[Editor's note:

The description of mixed scenarios does not raise new requirement, but instead describes a "best current practice" how to combine both modes and

The description of Scenarios with/without the participation of SeCFE/SvCFE also gives only an example how signalling may be used. As this requirement paper should remain protocol-neutral, no mentioning of protocols belongs into the main part.]

VI.1 Path-coupled and path-decoupled interoperability scenarios

The path-coupled and path-decoupled interoperability scenarios are shown in Table VI.1.

Table VI.1 – Interworking/interoperability scenarios

Interworking scenario	UNI	NNI	NNI	UNI
1	Path-coupled	Path-coupled	Path-coupled	Path-decoupled
2	Path-coupled	Path-decoupled	Path-decoupled	Path-coupled
3	Path-coupled	Path-decoupled	Path-decoupled	Path-decoupled
4	Path-decoupled	Path-coupled	Path-coupled	Path-coupled
5	Path-decoupled	Path-coupled	Path-coupled	Path-decoupled
6	Path-decoupled	Path-decoupled	Path-decoupled	Path-coupled
7	Path-coupled	Path-coupled	Path-decoupled	Path-decoupled
8	Path-decoupled	Path-coupled	Path-decoupled	Path-coupled

VI.2 Scenarios with/without the participation of SeCFE/SvCFE

Figure VI.1 illustrates the scenario without the participation of SeCFE/SvCFE (e.g., Internet web browsing, http, email, etc.).

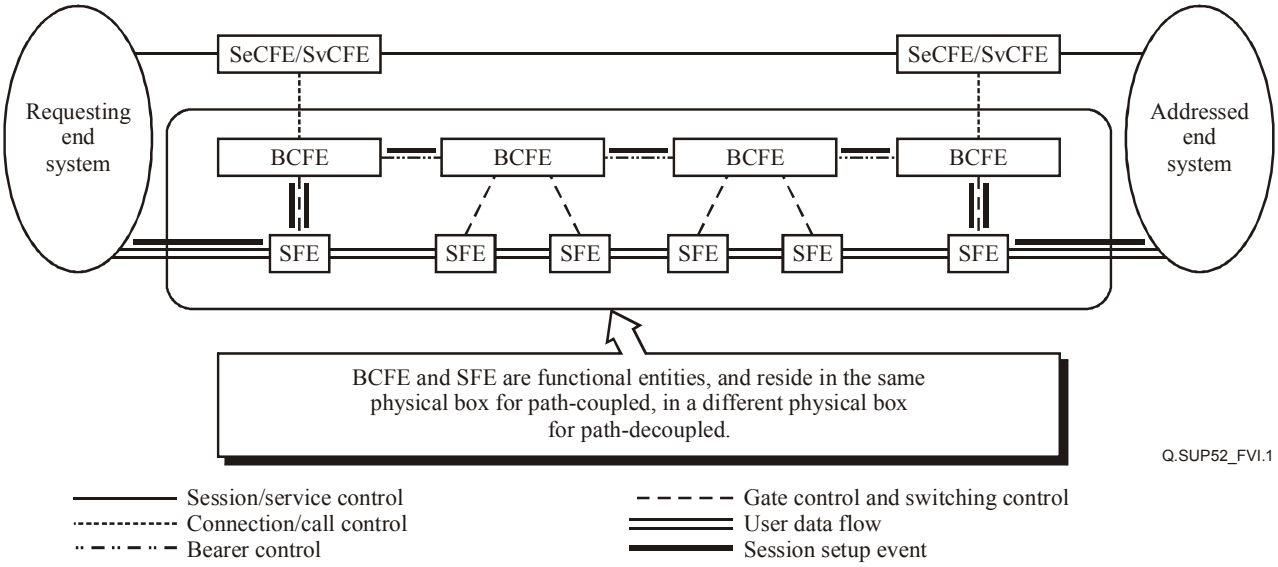


Figure VI.1 – Scenarios without the participation of SeCFE/SvCFE

Figure VI.2 illustrates the scenario with the participation of SeCFE/SvCFE.

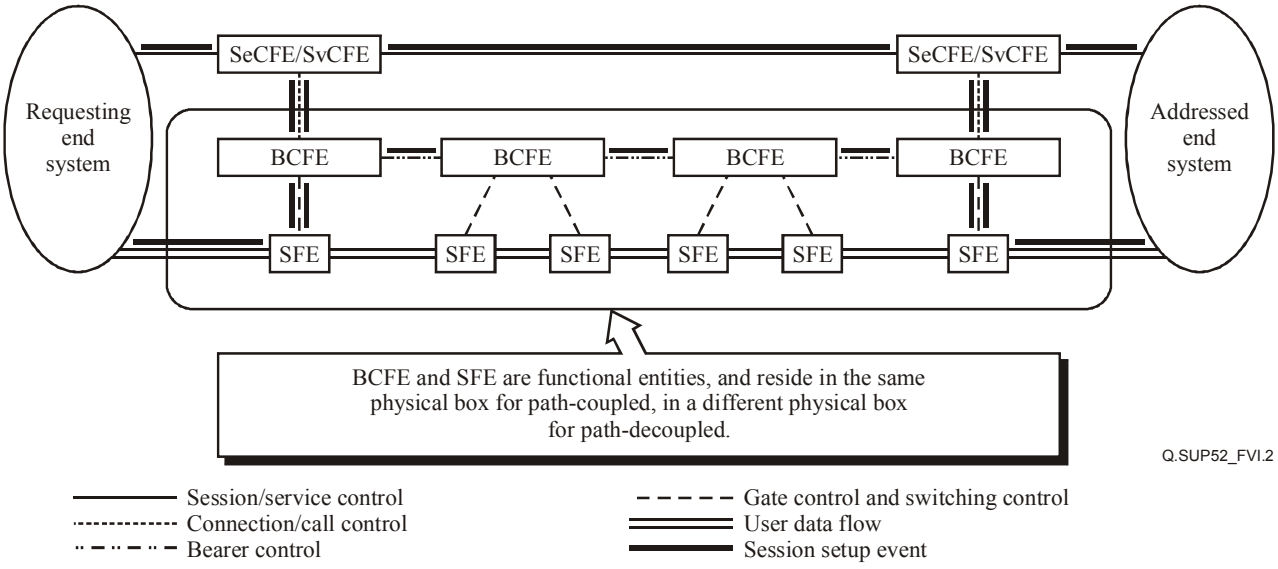


Figure VI.2 – Scenarios with the participation of SeCFE/SvCFE

WORKING GROUP 5
DELIVERABLES

SECURITY CAPABILITY

2.16 Security requirements for NGN – Release 1 (*Status A*)

2.17 Guidelines for NGN-security for Release 1 (*Status D*)

2.16 – Security Requirements for NGN – Release 1*

Table of Contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

2.16 – Security Requirements for NGN Release 1

1 Scope

This document provides the security requirements for NGN Release 1. This document provides requirements related to NGN services and NGN users including the transport and service strata interfaces.

The security requirements specified in this Recommendation reflect consideration of the following security dimensions as specified in ITU-T Recommendation X.805:

- Access control
- Authentication
- Non-repudiation
- Data confidentiality
- Communication security
- Data integrity
- Availability
- Privacy

The requirements are also consistent with the security threats identified in ITU-T Recommendation X.805 and the Guidelines for NGN security.

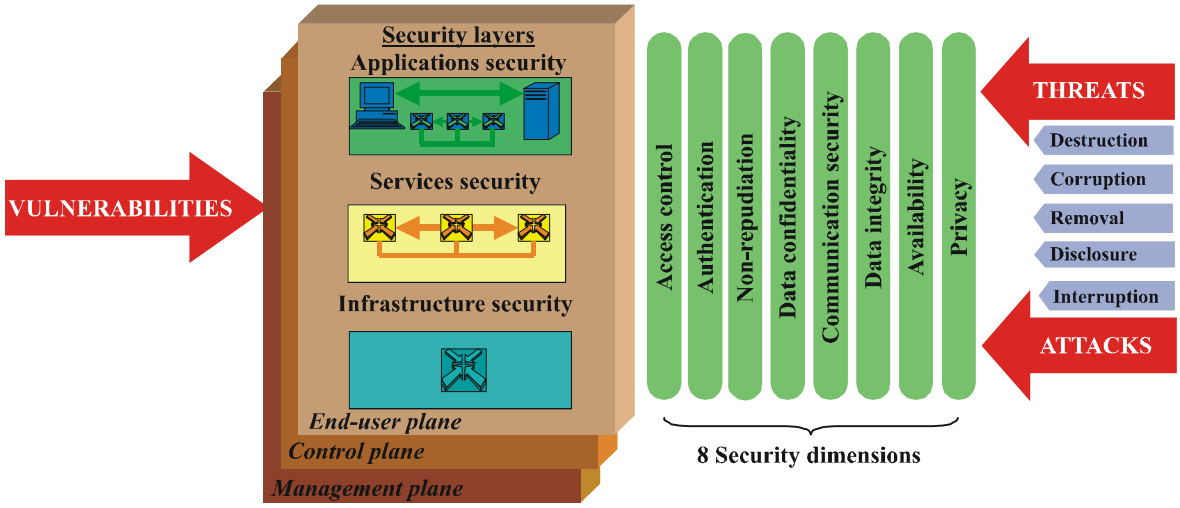


Figure 1 – Security architecture for end-to-end network security

The NGN security architecture should flexibly support various security policies and mechanisms to allow for interconnection with untrusted networks, e.g. the Internet, and untrusted terminals, e.g. terminals associated with WLAN and home networks. The architecture allows for interconnection of networks to provide security across concatenated networks and therefore allows network providers to offer a commitment of security to each other and customers.

The NGN security architecture should also address customer security needs which include: privacy, protection of customer data in databases beyond the UNI, etc.

2 Definitions and Abbreviations

2.1 Definitions

Emergency Telecommunications Service: National service providing authorized priority communications to facilitate the work of emergency personnel in times of disaster.

Telecommunications Disaster Relief: International service providing authorized priority communications to facilitate the work of emergency personnel in times of disaster. TDR facilitates the interworking between different national implementations of ETS to allow end-to-end priority communications.

2.2 Abbreviations and Acronyms

AAA	Authentication, Authorization, Accounting
BB	Broad Band
CSCF	Call Server Control Function
ETS	Emergency Telecommunications Service
GW	Gateway
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
IP-CAN	IP Connectivity Access Network
ISDN	Integrated Services Digital Network
MM	Multimedia
NGN	Next Generation Network
NW	Network
PSTN	Public Switched Telephone Network
RTSP	Real Time Streaming Protocol
SCT	Switched Circuit Technology
SIP	Session Initiation Protocol
TDR	Telecommunications for Disaster Relief
TE	Terminal Equipment
UA	User Agent
UE	User Equipment
UICC	Universal Integrated Circuit Card

3 Introduction

Figure 2 below depicts Transport and service configration of the NGN from Draft FGNGN-FRA [1]. This document recognizes and addresses the security requirements associated with the interfaces between:

- customer premises equipment and NGN access networks (UNI interconnection)
- NGN networks (NNI interconnection)
- NGNs and other networks, e.g. PSTN/ISDN, Internet
- Third party application provider equipment and NGNs (ANI) – This is out of scope of NGN Release 1

In the figure the customer and access networks are intended to be representative and are not intended to be all inclusive. Additionally, no attempt has been made to show the partitioning of networks into separate administrative domains. The developed security requirements in this document are sufficient to address these interconnection requirements and should not prevent an administrative domain from adequately protecting itself, from a security point of view.

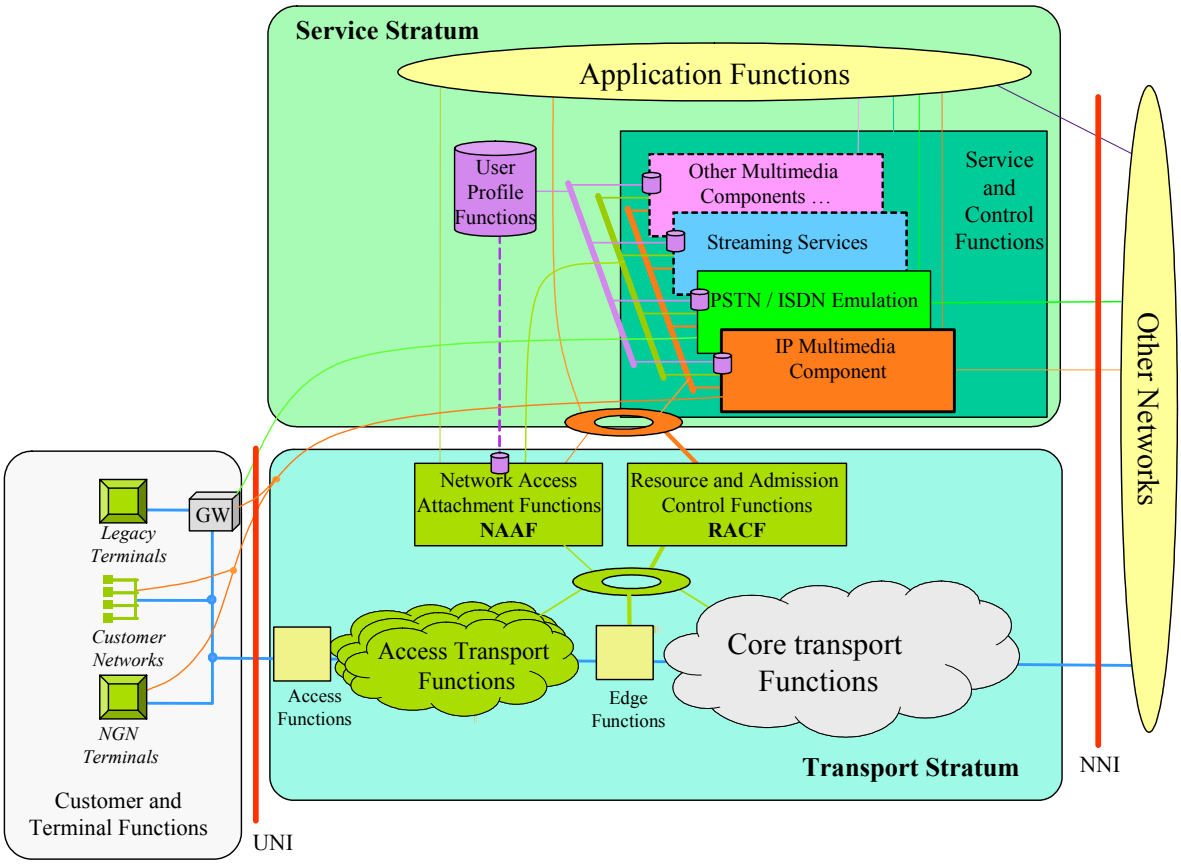


Figure 2 – Transport and service configration of the NGN

4 General Security Requirements

The following is a list of general security requirements:

i) NGN security shall support interoperability; in particular among the various NGN security mechanisms. Minimum standardized security features shall be available worldwide.

ii) Key management shall be available, (preferably integrated and automated)

iii) An NGN shall provide the possibility to establish trust relationships with other networks and with users. This includes the capability of the network to authenticate and authorize a single subscriber and another network.

iv) Authentication and authorization shall be performed at both service and transport strata (user-to-network, network-to-user, network-to-network).

An NGN shall be capable of supporting a service that can ensure source address authentication. This should be possible also in presence of NAT transversal.

v) The NGN architecture shall allow for network operators to limit the visibility of the network topology and resources to authorized entities.

vi) An NGN shall support multiple security zones. Isolation in security terms may be required between different security zones.

vii) An NGN shall allow provision of security measures to block unwanted traffic.

viii) An NGN shall allow provision of security measures against unauthorized access to network resources, devices, services and subscriber data (profile).

ix) The security of NGN network management resources (OSS, database, etc.) shall be ensured.

x) An NGN shall be capable of supporting a service which can ensure Integrity of the communication

xi) An NGN shall be capable of supporting a service which can ensure confidentiality of communications.

xii) An NGN shall be capable of supporting a service that can prove the origin of received data as a particular subscriber or address, and a service that can prove the delivery of data to a particular subscriber or address. This should be possible also in presence of NAT transversal

xiii) Security functionality shall be installed on the boundary between the networks and passage of data should be controlled through it. This includes functions such as filtering data packets and signalling information according the rules specified e.g. refusal of communication from particular applications or users

5 General Security Objectives

The following is a list of general security objectives:

i) NGN security features should be extensible, and flexible enough to satisfy various needs.

ii) Security requirements should take the performance, usability, scalability and cost constraints of NGN into account.

iii) Security methods should be based on existing and well-understood security standards as appropriate.

iv) The NGN security architecture shall be globally scalable (within network operator domains, across multiple network operators domains, in security provisioning)

v) The NGN security architecture should respect the logical or physical separation of signalling and control traffic, user traffic, and management traffic.

vi) NGN security shall be securely provisioned and securely managed.

vii) An NGN should provide security from all perspectives: service, network operator and subscriber.

viii) Security methods should not generally affect the quality of provided services.

ix) Security should provide simple, secure provisioning and configuration for subscribers and providers (Plug & Play)

x) Appropriate security levels should be maintained even when multicast functionality is used.

xi) The service discovery capabilities should support a variety of scoping criteria (e.g. location, cost, etc.) to provide appropriate scaling, with appropriate mechanisms to ensure security and privacy.

xii) The address resolution system shall be a special system used only by this network, and certain security measures shall be in place. This system may use databases that are internal or external to the NGN.

6 Objectives and requirements specific for security dimensions

The objectives and requirements described here are specific to particular security dimensions such as authentication. They are common to all interfaces.

6.1 Access control

i) NGN providers shall restrict network access to authorized subscriber terminals.

1) Authorization by other network providers may be accepted.

2) Authorization may be done in an implicit manner.

ii) It shall be possible for NGN to prevent intruders from obtaining unauthorised access to NGN services by masquerading as authorised users.

iii) The access control will be in accordance with the mobile subscriber's security policies.

6.2 Authentication

i) It shall be possible for NGN providers to authenticate subscribers at the start of, and during, service delivery.

1) A SIM functionality shall be required for subscriber to access any NGN service except for emergency services.

ii) It shall be possible for NGN users to authenticate the network at the start of, and during, service delivery.

6.3 Non-repudiation

6.4 Data confidentiality

i) It shall be possible for NGN providers to protect the confidentiality of subscriber traffic by cryptographical means.

ii) It shall be possible for NGN providers to protect confidentiality of control messages by cryptographical means.

6.5 Communication security

i) NGN shall provide mechanisms for ensuring that information is not unlawfully diverted or intercepted.

6.6 Data integrity

i) It shall be possible for NGN providers to protect the integrity of subscriber traffic by cryptographic means.

ii) It shall be possible for NGN providers to protect integrity of control messages by cryptographical means if security policy requests.

6.7 Availability

i) To mitigate DoS attacks, spreading of viruses or worms and other attacks, NGN should support provision of security measures to prevent or terminate communications with the non-compliant end-user equipment. These measures may be suspended to allow emergency communications.

ii) An NGN should allow provision of security measures to filter out packets and traffic that is considered harmful by the NGN provider's security policy.

6.8 Privacy

NGN shall protect the subscriber's private information such as location data, identities, phone numbers, network addresses or call-accounting data.

7 Security requirements for the Transport Stratum

7.1 NGN Customer Network domain

7.1.1 Customer gateway to customer device

The protection of Data Confidentiality and Authentication between devices should be provided. Availability protection should be ensured in different network states.

7.1.2 Customer device to customer

Authenticity of home devices should be verified by home subscriber. Authorization and accountability should also be required.

7.2 Customer Network to IP-CAN interface (UNI)

Access control, Authorization and Authentication are required capabilities which must be invoked before IP-CAN resources are made available in response to requests from Customer Network domains.

7.3 The IP-CAN function (UNI to NNI)

Security requirements specific to a network should also apply to the IP-CAN domain transport facilities and access signalling control systems, e.g. RACS (Resource and Admission Control Subsystem). Specifically security requires that data flows be monitored to identify unusual activities resulting from attacks.

Access control and authentication must be implemented on the access network to prevent unauthorized access and use of resources. Two kinds of resources are controlled in the access: the network and the services on network. In network access, the subscriber/subscriber terminal should be identified and authenticated. Access control of services is provided by the service control function, and the access network can be used to enhance such functions.

7.4 Core Network function

Security requirements specific to a core network should also apply to the transport network facilities and signalling control systems, e.g. SIP (Session Initiation Protocol). Communication security between core network entities should be provided.

7.5 NGN Customer Network to NGN Customer Network Interface

Remote customer to customer gateway

In order to prevent unauthorized users from intercepting communications, which might cause disclosure of information, authenticity of the remote customer and a customer in visited network should be verified. Data confidentiality should be protected at the same time. Availability should also be ensured.

Remote subscriber to a device in customer network

In order to prevent unauthorized or illegal users from intercepting, authenticity of remote subscriber identity should be verified. Data confidentiality should be protected at the same time. Availability and integrity should also be ensured. Accountability requires that remote subscriber be able to trace the target a device in customer's network accurately.

8 Security requirements for the Service Stratum

8.1 IMS core network security architecture

IMS access security should not be dependent on the technology used by the IP-CAN security.

For use with IMS, an access security capability shall be provided, based on 3GPP and 3GPP2 documentation. In those cases where 3GPP and 3GPP2 specifications differ, the preference should be given to the specifications that provide more options for achieving particular security solution. For example, the 3GPP security solutions rely exclusively on Authentication Key Agreement (AKA) method and smart cards for authentication and key distribution, while 3GPP2 solutions provide additional options. In this particular case, the NGN security solutions should include at least those solutions that have been specified by 3GPP2 (which already include the 3GPP solutions).

Figure 2 below provides a visual representation of the IMS architecture as provided in 3GPP/3GPP2 documents on IMS security architecture. In this figure there are five different kinds of interfaces, or security associations, identified each representing a different set of needs for security protection for IMS and they are numbered 1, 2, 3, 4 and 5. Please note that in 3GPP2 specifications HSS (Home Subscriber Server) is defined as a logical entity comprised of the AAA server and several supporting capabilities and databases, e.g. Home Location Register, Domain Name Servers, security and network access databases. For those with a background in 3GPP and 3GPP2 the Gm reference point is identified as interface number 2 and the Cx-interface is identified as interface number 3.

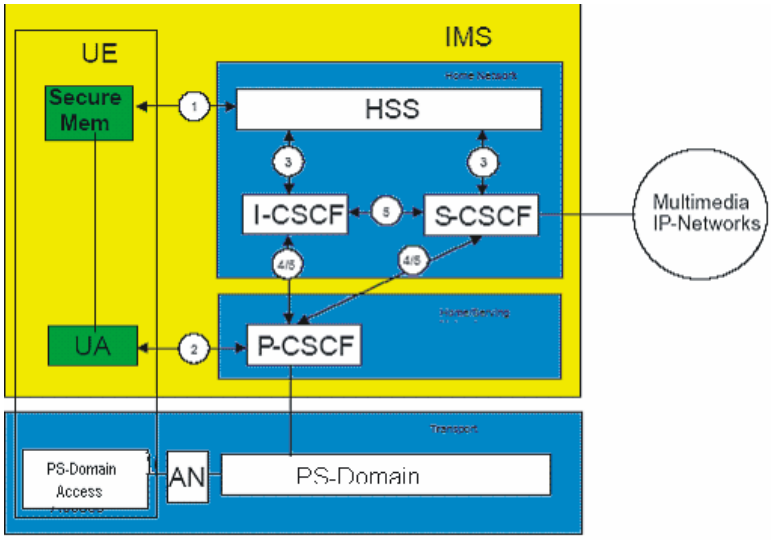


Figure 2 – The IMS security architecture

8.2 IMS security Architecture Interface Requirements

There are interface requirements associated with each of the numbered interfaces identified in the IMS security architecture figure.

8.2.1 Interface #1

Mutual authentication between the UE and the S-CSCF shall be provided.

Authorization is a required function which must be invoked before IMS resources are initially made available in response to a subscriber request from Home Network domains.

Authentication is a required function which must be invoked before IMS resources are subsequently made available in response to a subscriber request from Home Network domains.

IMS security mechanisms shall be independent of the IP-CAN security mechanism.

IMS access security should not be dependent on the technology used by the IP-CAN security and should be based on 3GPP and 3GPP2 security approaches.

Mutual authentication is required between the UE and the HN.

IMS security mechanisms based on the use of UICC card or equivalent are outside the scope of this document.

8.2.2 Interface #2

A secure link is required between the UE and a P-CSCF to ensure a security association (SA) is available to provide protection for the Gm interface.

Data origin authentication shall be provided i.e. the corroboration that the source of data received is as claimed.

8.2.3 Interface #3

A secure link is required between the HSS and the S-CSCF to ensure a security association (SA) is available to provide protection for the Cx-interface.

8.2.4 Interface #4

Security is required between different networks for SIP capable nodes.

This requirement is only applicable when the P-CSCF resides in the Visited Network (VN). If the P-CSCF resides in the Home Network (HN) then requirement number five below applies.

8.2.5 Interface #5

Security is required within the network between SIP capable nodes. Note that this security association also applies when the P-CSCF resides in the HN.

There exist other interfaces and reference points in IMS, which have not been addressed above. Those interfaces and reference points reside within the IMS, either within the same security domain or between different security domains.

8.3 Transport domain to NGN core network

Security is required for the "Go like" interface between the service control and the resource control sub-systems. This should include all requirements for implementing solutions according to 3GPP or 3GPP2 specifications.

8.4 Application to core network interface

Access control, Authorization and Authentication are required functions which must be invoked before the IMS responds to Application requests for resources.

8.5 Application domain security

Application domain security is out of scope for Release 1 requirements, it is assumed that applications built on top of core networks that use an IMS architecture are responsible for their own security and may have their special security requirements.

8.6 NGN Customer Network to Application interface

Security between the NGN customer interface (UNI) and the Application interface (API – UNI) is not addressed in this document, however, these requirements address the security of the transport connection/sessions between these interfaces. Applications should have their own incremental security requirements

8.7 VoIP security requirements

Standard security solutions for VoIP in NGN should:

- Provide protection for voice communications
- Protect identities of the parties involved in communication from unlawful disclosure
- Be designed with a goal to minimize impact on Quality of Service (QoS)
- Support NAT and firewall traversal

Use of the IPsec techniques for securing VoIP traffic on the networks that employ NATs and firewalls requires additional studies.

8.8 ETS and TDR security objectives and requirements

8.8.1 ETS and TDR security objectives

The general objective is for NGNs to be capable of supporting secure ETS and TDR communications. ETS is a national service and TDR is an international service providing authorized priority communications to facilitate the work of emergency personnel in times of disaster. The international TDR service facilitates the interworking between different national implementations of ETS to allow end-to-end priority communications.

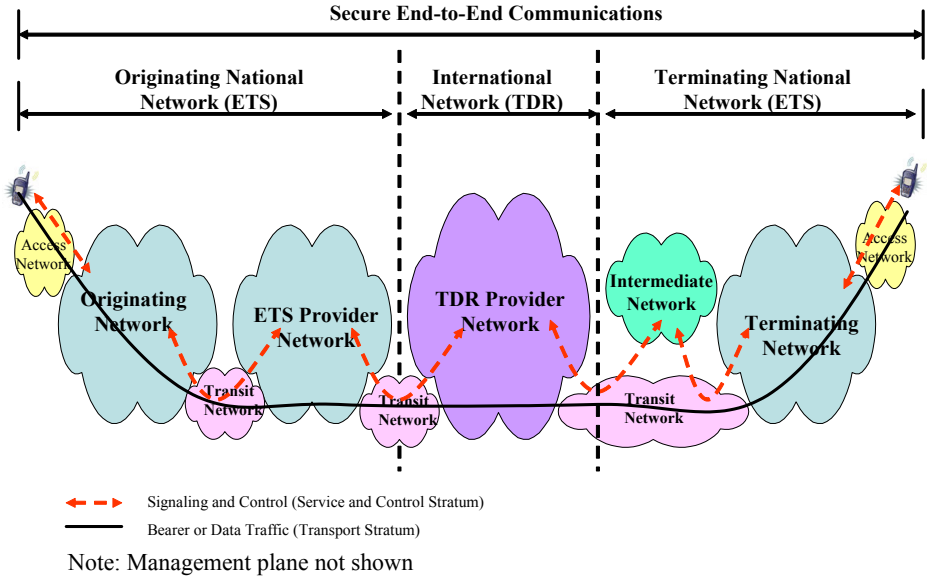


Figure 4 – Example End-to-End ETS and TDR Communications between National Networks

Figure 4 illustrates an example end-to-end ETS and TDR communication between different national networks. The example illustrates that end-to-end communications would involve multiple network segments and administrative domains (e.g., Access Network, Originating Network, ETS Provider Network, TDR Provider Network, Intermediate Network and Terminating Network).

The objective is to support security capabilities to protect ETS and TDR communications end-to-end across multiple network administrative domains. Specifically, this includes protecting the following:

- ETS and TDR Signalling and Control (Service Stratum, including control functions)
- ETS and TDR Bearer and Data Traffic (Transport Stratum), and
- ETS and TDR Management Data (Management Stratum)

8.8.2 ETS and TDR security requirements

8.8.2.1 General requirements

The following general security requirements shall be supported for ETS and TDR:

1) Security capabilities to protect end-to-end ETS and TDR communications across multiple network administration domains shall be supported.

2) Security capabilities to provide identity management and authentication of users and networks across multiple network administration domains shall be supported.

3) Security capabilities to protect interworking between TDR (international implementations) and ETS (national implementations) shall be supported to allow secure end-to-end communications.

4) Security mechanisms (e.g., encryption) used to protect ETS and TDR communications shall allow preservation of priority information.

8.8.2.2 Authentication, authorization and access control

The following authentication, authorization and access control capabilities (but not limited) shall be supported for ETS and TDR:

- Security capabilities to protect mechanisms used to authenticate and authorize ETS/TDR users and devices.
- Security capabilities to protect mechanisms used to bind ETS/TDR end user with associated devices.
- Security capabilities to protect mechanisms used to share authentication information (e.g., confirm that a user has been authenticated) across multiple network administrative domains.
- Security capabilities to protect mechanisms used for mutual authentication of users and entities. This includes mechanisms for ETS/TDR users to authenticate the called party or communicating entities (e.g., website, content server, etc) for ETS/TDR communications.
- Security capabilities to protect mechanisms used to authentication networks. This includes mechanisms used to authenticate the network handing off an ETS/TDR communication (e.g., originating network) and authentication of the network receiving the ETS/TDR communication (e.g., intermediate or terminating networks).
- Security capabilities to protect against unauthorized access to ETS/TDR information and resources (e.g., user information in authentication servers and management systems).

8.8.2.3 Confidentiality and privacy

The following confidential capabilities (but not limited) shall be supported for ETS and TDR:

- Security capabilities to provide confidentiality protection of the ETS and TDR signalling and control
- Security capabilities to provide confidentiality protection of ETS and TDR bearer and data traffic (e.g., voice, video or data)
- Security capabilities to provide confidentiality protection of ETS and TDR user and communicating entities identities, and subscription information
- Security capabilities to provide confidentiality protection of ETS and TDR user location

The following privacy capabilities (but not limited) shall be supported for ETS and TDR information:

- Security capabilities to provide privacy protection of TDR and ETS information (e.g., information derived from the observation of network activities such as web-sites that a user has visited, a user's geographic location, and the IP addresses and DNS names of devices in a service provider network)
- Security capabilities to provide privacy protection against observing of ETS and TDR usage information (e.g., usage patters such as ETS traffic volume, origination and termination locations, time, etc.).

8.8.2.4 Data Integrity

The following data integrity capabilities (but not limited) shall be supported for ETS and TDR:

- Security mechanisms to provide integrity protection of ETS and TDR communications (e.g., protection against unauthorized modification, deletion, creation, or replay). This includes mechanisms to provide notification of information tampering or modification.
- Security mechanisms to provide integrity protection of ETS and TDR information (e.g., priority marking, voice, data and video)
- Security mechanisms to provide integrity protection of ETS and TDR specific configuration data (e.g., priority information stored in policy decision functions, user priority level, etc).

8.8.2.5 Communication

The following capability (but not limited) shall be supported to protect ETS and TDR communications:

- Security mechanisms to protect the information flows between authorized entities for ETS and TDR communications against intrusions (e.g., mechanisms to prevent interception, hijacking or replay of ETS/TDR signalling or bearer/data traffic)

8.8.2.6 Availability

The following capabilities (but not limited) shall be supported to protect the availability ETS and TDR communications and resources:

- Security mechanisms to protect the availability of ETS and TDR communications (e.g., protection of ETS and TDR signalling and control, and bearer/data traffic against Denial of Service (DoS) attacks).

Security mechanisms to protect the availability of TDR and ETS specific resources and information (e.g., authentication/authorization databases, priority information stored in policy decision function, and dedicated network resources against Denial of Service (DoS) and other forms of attacks).

8.9 Open service platform to valued-added service provider security

Authentication and authorization are needed before Value-added Service access Open Service Platform.

Data confidentiality and integrity should be considered when transmitting data and signalling between Open Service Platform and Value-added Service.

Content filter and monitor should be considered while Value-added Service access Open Service Platform.

Security protection with different trust level could be selected by service provider for protecting the communication between Value-added Service and Open Service Platform.

2.17 – Guidelines for NGN-security for Release 1*

Table of Contents

* Status D: The FGNGN considers that this deliverable is not yet mature, requiring discussion and technical input to complete development.

2.17 – Guidelines for NGN-security for Release 1

1 Scope

This document describes general principles and guidelines for building secure Next Generation Network. The document adopts major concepts of ITU-T Recommendation X.805 as a foundation for developing the detailed recommendations for the end-to-end NGN security. The document also provides more detailed examination of such essential for the NGN security issues as IMS access security and security for NAT/firewall traversal.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Document are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ITU-T Recommendation X.800 (1991), *Security Architecture for Open Systems Interconnection for CCITT ApplicationsITU-T Recommendation*.

[2] ITU-T Recommendation X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

[3] ITU-T Recommendation X.805 (2003), *Security Architecture for Systems Providing End-to-end Communications*.

[4] FGNGN document, *Functional Requirements and Architecture of the NGN (FRA)*.

[5] FGNGN document, *Functional Requirements and Architecture for Resource and Admission Control in Next Generation Networks (RACF)*.

[6] ETSI TS 133 203 (2005), *Universal Mobile Telecommunications System (UMTS);3G security; Access security for IP-based services*.

[7] 3GPP2 S.S0086 (2004), *IMS Security Framework.*

[8] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

[9] IETF RFC 2402 (1998), *IP Authentication Header*.

[10] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*.

[11] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH*.

[12] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm With Explicit IV*.

[13] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*.

[14] IETF RFC 2407 (1998), *The Internet IP Security Domain of Interpretation for ISAKMP*.

[15] IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*.

[16] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

[17] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use With IPsec*.

[18] IETF RFC 2411 (1998), *IP Security Document Roadmap*.

[19] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*.

[20] IETF RFC 3168 (2001), *The Addition of Explicit Congestion Notification (ECN) to IP*.

[21] IETF RFC 4109 (2005), *Algorithms for Internet Key Exchange version 1 (IKEv1)*.

[22] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[23] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.

[24] FGNGN document, *Security Requirements for NGN Release 1*.

[27] IETF RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*.

[28] IETF RFC 3948 (2005), *UDP Encapsulation of IPsec ESP Packets*.

[29] IETF RFC 3847 (2004), *Restart Signaling for Intermediate System to Intermediate System (IS-IS)*.

[30] IETF RFC 3715 (2004), *IPsec-Network Address Translation (NAT) Compatibility Requirements*.

3 Terms and definitions

Third party service and application provider trusted: A value-added service and application provider that can be trusted by the network operator. It may be a subordinate organization or partner of the network operator that has high level of security trustworthiness .

Third party service and application provider not trusted: The value-added service and application provider that cannot be trusted by network operators. It can be independent service and application providers which have lower level security trustworthiness.

Open service and application platform: A service and application platform provided by a network operator that has an open interface for value-added services and applications.

Accountability: The property that ensures that the actions of an entity may be traced uniquely to the entity [1].

Authentication: The corroboration that the source of data received is as claimed [1].

Authorization: The granting of rights, which includes the granting of access based on access rights [1].

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [1].

Integrity: The property that data has not been altered or destroyed in an unauthorized manner [1].

Availability: The property of being accessible and useable upon demand by an authorized entity [1].

4 Abbreviations and acronyms

ALG Application Layer Gateway

DNS Domain Name System

ETS Emergency Telecommunications Service

IP-CAN	IP-Connectivity Access Network
IPsec	IP Security
LSP	Label-switched Path
MGT	Management
MPLS	Multi-protocol Label Switching
NAT	Network Address Translation
OSI	Open Systems Interconnection
QoS	Quality of Service
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TDR	Telecommunications for Disaster Relief
TLS	Transport Layer Security
VoIP	Voice over IP

5 NGN threat model and Security Dimensions

The security threat model as well as other fundamental materials have been addressed in the following ITU-T Recommendations:

- Recommendation X.800 [1] defines the general security-related architectural elements which can be applied appropriately in the circumstances for which protection of communication between open systems is required.

  (This Recommendation establishes, within the framework of the Reference Model of X.200 [2], guidelines and constraints to improve existing Recommendations or to develop new Recommendations in the context of OSI in order to allow secure communications and thus provide a consistent approach to security in OSI.)

- Recommendation X.805 [3] defines a network security architecture for providing end-to-end network security.

  (The architecture can be applied to various kinds of networks where the end-to-end security is a concern and independently of the network's underlying technology. This Recommendation defines the general security-related architectural elements that are necessary for providing end-to-end security. The objective of this Recommendation is to serve as a foundation for developing the detailed recommendations for the end-to-end network security.)

Parties interested in security considerations related to NGN are invited to read these base security documents, as it is assumed the reader of this document is aware of the information presented in those Recommendations.

The Recommendation X.800 [1] and X.805 [3] identify the following security threats to the networks that are applicable to NGN:

a) Destruction of information and/or other resources

b) Corruption or modification of information

c) Theft, removal or loss of information and/or other resources

d) Disclosure of information

e) Interruption of services.

The table 1 from the Recommendation X.805 [3] lists the Security Dimensions and describes mapping of Security Dimensions to security threats: the letter 'Y' in a cell formed by the intersection of the table's columns and rows designate that a particular security threat is opposed by a corresponding security dimension.

Table 1 – Mapping of security dimensions to security threats

Security dimension	Security threat				
	Destruction of information or other resources	Corruption or modification of information	Theft, removal or loss of information and other resources	Disclosure of information	Interruption of services
Access control	Y	Y	Y	Y	
Authentication			Y	Y	
Non-repudiation	Y	Y	Y	Y	Y
Data confidentiality			Y	Y	
Communication security			Y	Y	
Data integrity	Y	Y			
Availability	Y				Y
Privacy				Y	

The generic threats identified above exist in the NGN environment.

This general approach of specifying threats and the security measures that are to counter them can be applied to all components of the NGN. The NGN components depicted in Figure 1, "Transport and service configration of the NGN", are described in detail in the NGN document *Functional Requirements and Architecture of the NGN (FRA)* [4]. Security considerations section of the NGN output document *Functional Requirements and Architecture for Resource and Admission Control in Next Generation Networks (RACF)* [5] presents an example of applying the security concepts of the Recommendations X.800 and X.805 to a specific component of the NGN.

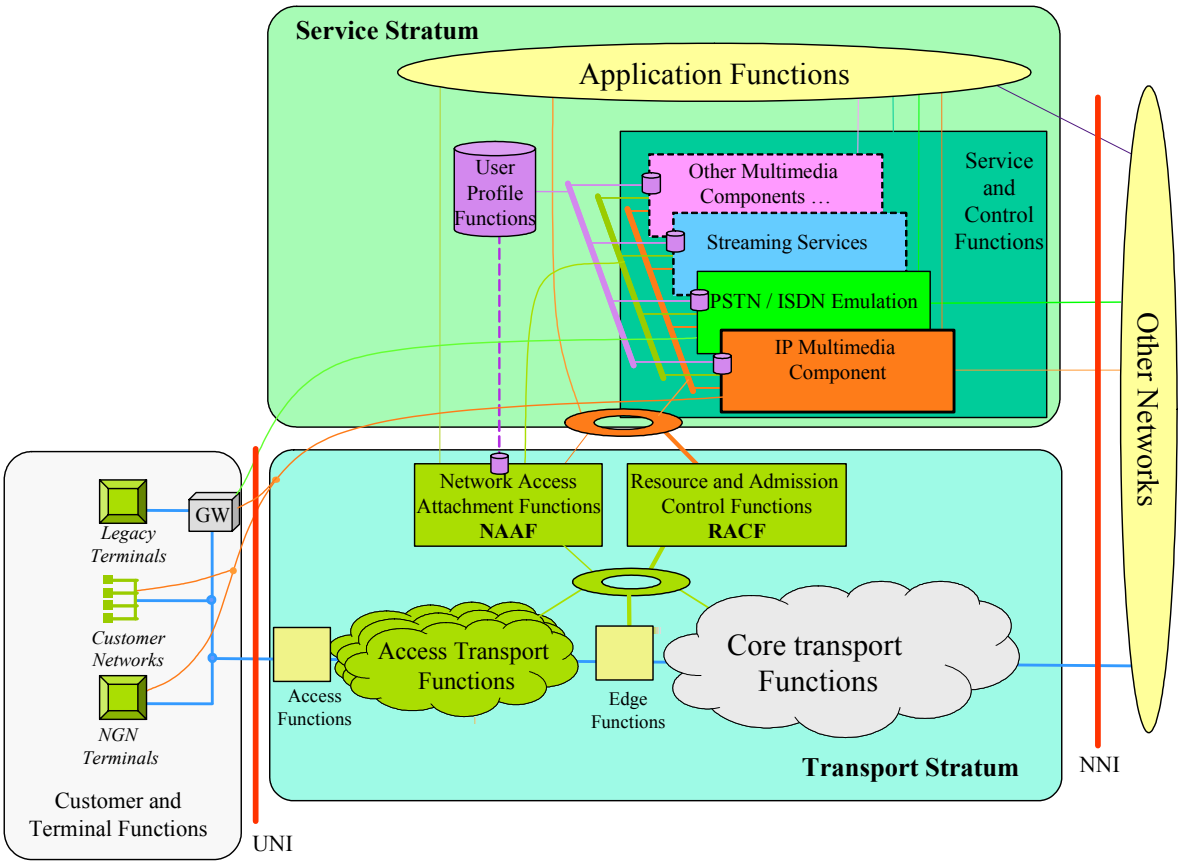


Figure 1 – Transport and service configration of the NGN

6 NGN Security Models

6.1 A four layer conceptual model for NGN security and the granularity of protection

In the NGN architecture, the network could be divided into a service stratum and transport stratum. Each of these can be subdivided into two layers:

- In the service stratum the application layer and service layer can be defined; and
- In the transport stratum the packet layer and link layer can be defined.

Application Layer

The Application Layer focuses on the network-based applications accessed by Service Provider's customers. These applications could include web browsing, email, basic file transport applications, etc. Security applied at the Application Layer is to protect customers and network.

Service Layer

The Service Layer addresses various services that Service Providers provide to their customers. These services include domain name services, value-added services, QoS, etc. Security applied at the Services Layer is to protect service providers and their customers.

Packet Layer

The Packet Layer addresses packet flow that network facilities support to transport information. For NGN, it is considered that IP will be the primary protocol used to provide NGN services to end-users as well as supporting legacy services. Thus, security applied at the packet layer is focused on the protecting IP packets.

Link Layer

Link Layer addresses frame data transmission between directly connected network facilities. The main task of the link layer is to take a raw transmission facility and transform it into a line that appears free of transmission errors in the upper layer. It accomplishes this task by having the link layer sender: break the input data up into data frames (typically a few hundred bytes); transmit the frames sequentially; and process the acknowledgment frames sent back by the receiver. Security applied at the link layer focuses on protecting the link frames and as a result does not provide protection beyond a single link.

This layered system of providing security leads to consideration of the various levels of the granularity of protection. For example, because link layer security would provide protection for everything that passes over the link, it could be considered as providing coarse granularity. On the other hand, because security implemented at the application layer only protects that application, it could be considered as providing fine granularity. As a result:

- Compared with the other three levels of the granularity, the security applied at the link layer is the coarsest, but the efficiency is always the highest.
- Granularity of protection of security applied at packet layer is finer than at link layer, but coarser than at service layer. Security applied at the packet layer is less efficient than security applied at the link layer and more efficient than security applied at the packet layer.
- Granularity of protection of security applied at the service layer is finer than at the packet layer, but coarser than application layer. Security applied at the service layer is less efficient than security applied at the packet layer and more efficient than security applied at the packet application layer.
- Granularity of protection of security applied at the application layer is finer than service layer. Security applied at the application layer is less efficient than security applied at the service layer.

Choosing a security mechanism that operates at the appropriate layer and provides needed security is required for a cost-effective solution. This could also be referred to as selecting the right degree of granularity.

While a security mechanism implemented at a lower layer provides a degree of protection for the higher layers, this protection could be insufficient. On the other hand end-to-end security can be achieved at the application layer. However, limiting security solely to the application layer means that each application must be security-aware.

Assessment of the required granularity of protection should take into account expected usage patterns, implementation layers, and deployment considerations. A secure set of machines (e.g. network operation centre with strictly secured access) may require only subnet granularity. On the other hand, security of a particular application may need to be addressed by the security mechanisms embedded within the application. Use of an external security mechanism, to an application, may severely affect the application's deployment.

6.2 Security Associations model for NGN

One of the distinct characteristics of NGN, is the separation of strata and planes. This separation is illustrated by Figure 2.

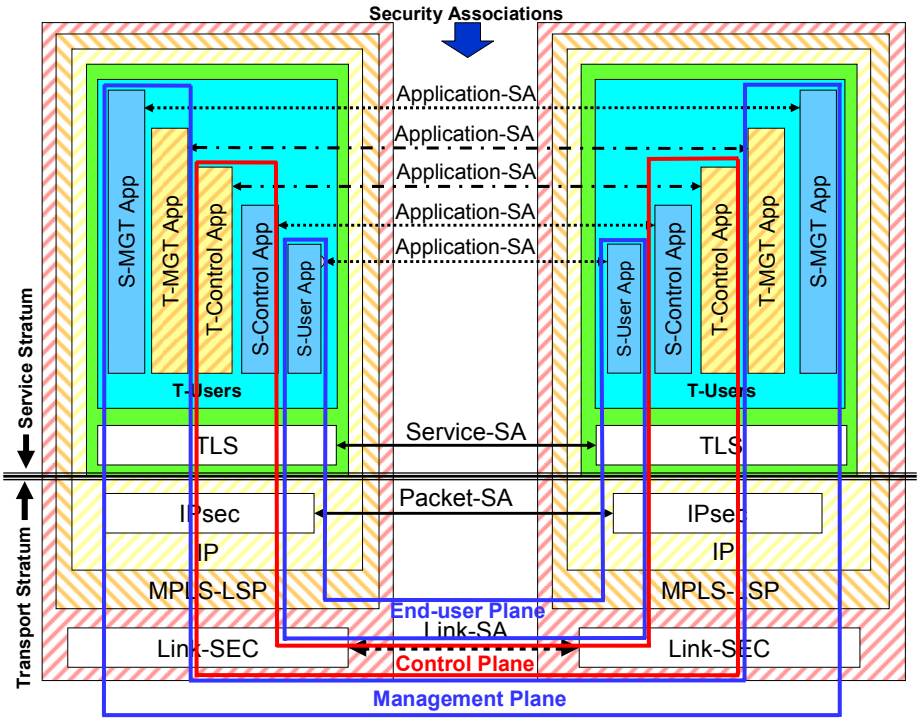


Figure 2 – Security association model for NGN

Various security association exist within the NGN model. Security Association (SA) denotes secure transmission between two network entities based on authentication, the negotiation of the method of encryption and the exchange of encryption keys. In the NGNs the SAs can be established between the entities that belong to various network and security layers, security planes and strata. Figure 2 depicts security associations in the Transport Stratum and the Service Stratum. The Link Security function is depicted at the bottom of the Transport Stratum. The IP, IPsec and MPLS LSP are shown above the Link Security function of the Transport Stratum. The application functions reside above the TLS (TLS protocol is specified in [22]) function, which is at the bottom of the Service Stratum.

In this figure a security association for each of the specific applications and for TLS provide complete Service Stratum security. Packet Security Association is provided by IPsec (IPsec protocol is specified in [8] – [21]) within the Transport Stratum.

Figure 2 also depicts the End-user, Control and Management Planes. Security of these planes is focused on the protection of the respective network activities. There should be no dependency between the security protection of these planes. For example, if the network control functions are compromised, the management capabilities should be available for mitigation of the attack.

(1) End-user Plane security

The end-user security plane addresses security of access and use of the service provider's network by customers. This plane also represents actual end-user data flows.

(2) Control Plane security

The control security plane is concerned with protection of the activities that enable the efficient delivery of information, services and applications across the network. It typically involves machine-to-machine communications of information that allows the machines (e.g., switches or routers) to determine how best to route or switch traffic across the underlying transport network. This type of information is sometimes referred to as control or signalling information.

(3) Management Plane security

The management security plane is concerned with the protection of operations, administration, maintenance and provisioning functions of the network elements, transmission facilities, back-office systems (operations support systems, business support systems, customer care systems, etc.)

7 Security of the NGN subsystems

This section provides an overview of several components of the NGN security. The security of these components, although they may have some dependencies on each other, can be addressed separately in terms of documentation.

7.1 IP-Connectivity Access Network (IP-CAN)

External to IMS, it is assumed that the IP-CAN is secure, i.e., security is provided by the IP-CAN architecture, which provides transport for both media and signalling, and this security architecture is orthogonal to the security specified for the IMS. IP-CAN security shall be able to provide confidentiality.

Confidentiality can be attained by network layer security mechanism, such as encapsulation security payload (ESP) of IPsec, which is a general security protocol for IP. IPsec is an end-to-end protocol, usually works between hosts in transport mode or routers in tunnel mode. Because of the end-to-end feature of IPsec, it is not widely deployed as an important mechanism of access security. Some SDOs develop layer 2 security mechanisms that provide segment by segment security service for data. The link layer security mechanism is being defined for IEEE 802 data link layer in IEEE 802.1 committee. Confidentiality, integrity and anti-replay service are provided by the protocol. In DOCSIS 1.1 baseline privacy interface plus (BPI+) security services are defined for DOCSIS1.1 data link layer. There are quite a lot some other such security mechanisms for different data link protocols. The implementer of IP-CAN should consider the availability and propriety of such mechanism.

Two kinds of IP-CAN resource shall be access-controlled: the network and the services on network. In network access, the user/user terminal should be identified and authenticated. Access control of service is often implemented by service control function, and access network can be used to enhance such function. Access control often relies on the result of authentication and use IP filter to implement control. Address, port, protocol ID, user ID and other information of packet or session are checked to decide whether it is qualified to access network or service.

Access control and authentication are usually implemented on access network to avoid unauthorized access. There are variety of mechanisms to implement them. In IETF Protocol carrying Authentication of Network Access (PANA) is being developed to define a generic mechanism for access network, and it is proper to be applied in IP-CAN because it is independent of link technologies. There are also other link layer authentication mechanism, such as PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE). EAP is a widely deployed authentication protocol in these mechanisms because of its flexibility to adapt to various authentication algorithms. IP filter controls the access of IP packets to network, and access control list (ACL) is often implemented to filter IP packets.

7.2 IMS network domain and IMS-to-non-IMS network security

IMS functional entities are realized by physical entities in the Core Network; the interconnection among the network entities must be secured. A generic means of network domain security, (e.g., in standard IETF protocols) should be available in all core network entities, including those providing IMS.

IMS security should protect data and signalling. This protection should be based on IPsec ESP with use of IKE or, preferably, IKEv2 protocols and in accordance with 3GPP and 3GPP2 specifications.

Security for IMS-to-non-IMS network interfaces, (i.e. between the IMS subsystem of NGN and other subsystems of NGN) should provide protection for data and signalling. Such protection should be based on the TLS protocol.

User authentication data should be available to other network domains for the purpose of supporting roaming on Wi-Fi and LAN access connections.

Protection of the bearer level services should be provided by the Secure Real-time Transport Protocol (SRTP) [23].

7.3 IMS access

Users of the IMS must be authorized to use the IMS and, once authorized for IMS services, the user must be authenticated for each access. IMS access security should not be dependent on the technology used by the IP-CAN security. For use with IMS, access security capability shall be provided, based on 3GPP and 3GPP2 documentation. In those cases where 3GPP and 3GPP2 specifications differ, the preference should be given to the solutions that provide more options for achieving security. Of course, selection of a standard that allows a variety of solutions must not lead to lowering of the level of security. For example, the 3GPP security solutions rely exclusively on Authentication Key Agreement (AKA) method and smart cards for authentication and key distribution, while 3GPP2 solutions provide additional options. In this particular case, the NGN security solutions should include at least those solutions that have been specified by 3GPP2 (which already include the 3GPP solutions).

Extensions to resolve issues of intervening NAT and firewalls should be negotiated with both 3GPP and 3GPP2, in order to achieve a single harmonized solution. Secure traversal of NAT and firewall devices is especially essential for VoIP traffic. The Session Border Controller devices are capable of supporting traversal for VoIP and should be employed by NGN. Session Border Controllers can also provide control, auditing, recording, and filtering of VoIP call streams that must cross enterprise security boundaries.

Figure 3 below provides a visual representation of the IMS architecture as provided in 3GPP/3GPP2 documents [6], [7] on IMS security architecture. In this figure there are five different kinds of interfaces, or security associations, identified each representing a different set of needs for security protection for IMS and they are numbered 1, 2, 3, 4 and 5. For those with a background in 3GPP and 3GPP2 the Gm reference point is identified as interface number 2 and the Cx-interface is identified as interface number 3.

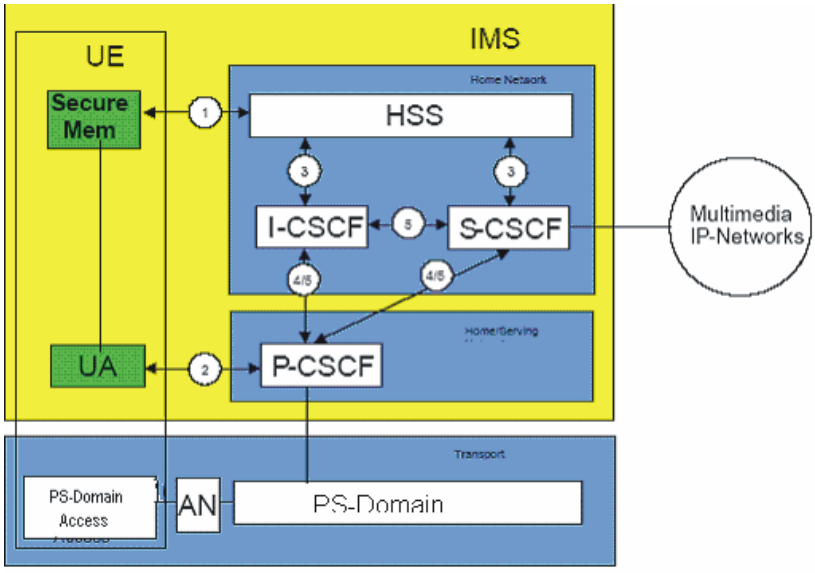


Figure 3 – The IMS security architecture

The requirements described below are identified in the *Security Requirements for NGN Release 1* [24] document.

Requirements associated with the numbered interfaces

1. Mutual authentication between the UE and the S-CSCF shall be provided.
2. A secure link is required between the UE and a P-CSCF to ensure a security association (SA) is available to provide protection for the Gm interface.

   Data origin authentication shall be provided i.e. the corroboration that the source of data received is as claimed.
3. A secure link is required between the HSS and the S-CSCF to ensure a security association (SA) is available to provide protection for the Cx-interface
4. Security is required between different networks for SIP capable nodes.

   This requirement is only applicable when the P-CSCF resides in the Visited Network (VN). If the P-CSCF resides in the Home Network (HN) then requirement number five below applies.
5. Security is required within the network between SIP capable nodes. Note that this security association also applies when the P-CSCF resides in the HN.

There are other interfaces and reference points in IMS, which have not been addressed above. Those interfaces and reference points reside within the IMS, either within the same security domain or between different security domains.

7.4 Framework for open platform for services and applications in NGN

Availability of open services and applications is one of the most important features of NGN architecture. Third party providers of services and applications use APIs provided by the open services and applications platform to develop value-added services and applications. According to different levels of credibility to network providers, the providers of value-added services and applications can be divided into those trusted by network providers and those that are not. The former may be network providers themselves, subordinate organizations or partners which can be regard as trusted providers of services and applications by network operators. While the latter may be independent providers of services and applications that can be regarded as non-trusted.

Because NGN has features of open and distributed controls, there are various threats to the open services and applications platforms and value-added services and applications, (e.g., destruction or modification of information, disclosure of information, interruption of services and applications, etc.) It is essential to protect the open services and applications platform and the value-added services and applications from those security threats.

Figure 4 depicts security framework for open services and applications platform. The figure depicts various security dimensions that protect communications between value-added services and applications and the open services and applications platform. According to different scenarios, the services and applications providers need to implement different security dimensions to provide the required security capabilities. The best protection could be provided when the trusted, as well as non-trusted, service and application providers implement all security dimensions. However, in order to improve the performance and cost, the trusted service and application providers may implement only a subset of the security dimensions that are determined to be essential.

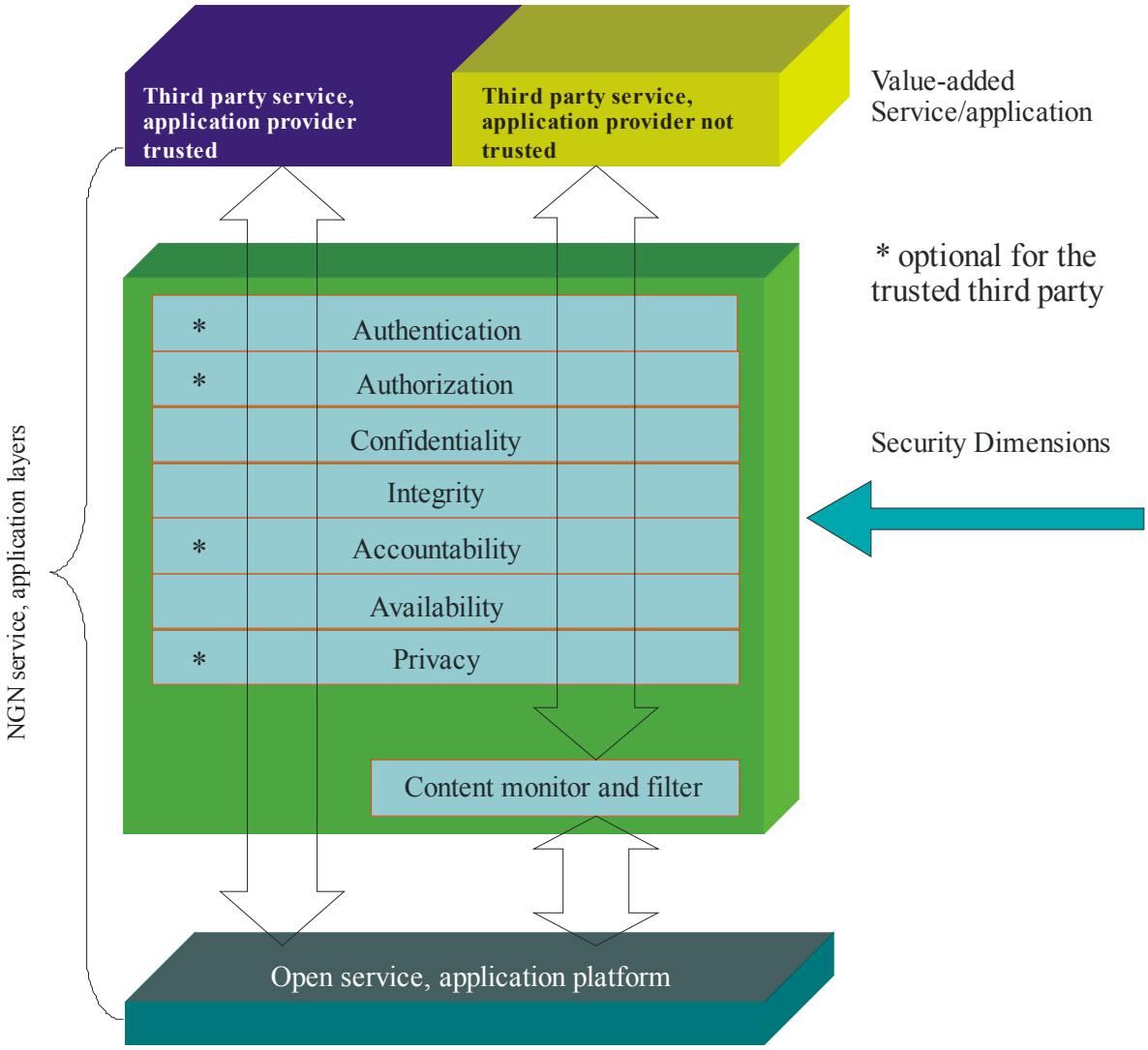


Figure 4 – Security Framework for Open Services and Applications Platform.

If value-added services are provided by a third party that is trusted, it is not necessary to monitor and filter the content transmitted from the trusted third party to the service and application platform. If information is transmitted through open network, its integrity should be protected and availability should be ensured. For some sensitive information, confidentiality is also required. Some security dimensions that are marked by * in Figure 4 are optional for the trusted third party because the trusted third party could be considered as an integral part of the service and application platform providers. These optional security dimensions are authentication, authorization, accountability and privacy.

If valued-added services are provided by a third party that is not trusted, it is necessary to monitor and filter the content transmitted from the un-trusted third party to the service and application platform. These measures could prevent fraud and illegal actions and ensure accurate charging. In non-trusted environment, the identity of the third party providing value-added services and applications should be verified. Data confidentiality should be ensured for protection of sensitive information. Availability, integrity and privacy should be ensured in different network states. Accountability is also necessary for tracing activities of the non-trusted providers of value-added services and applications.

7.5 Emergency Telecommunications Service (ETS) and Telecommunications for Disaster Relief (TDR) Security

7.5.1 Overview

Availability and security of ETS and TDR depends on NGN security. This section provides guidelines for ETS and TDR security. A brief description of the TDR and ETS is provided to aid in the understanding of the security needs and objectives.

7.5.2 TDR and ETS Descriptions

Telecommunications for Disaster Relief (TDR) – TDR is an international service providing authorized priority communications to facilitate the work of emergency personnel in times of disaster. TDR facilitates the interworking between different national implementations of ETS to allow end-to-end priority communications.

Emergency Telecommunications Service (ETS) – ETS is a national service providing authorized priority communications to facilitate the work of emergency personnel in times of disaster.

ETS is intended for use in a variety of national networks and provides priority call/session setup capabilities that are used to support emergency response/recovery activities. ETS provides priority connectivity for authorized user from any originating point in the public network and to any destination point in the public network. It may include support of priority connectivity and communications across multiple network types (e.g., circuit-switched networks, wireless network/mobile radio access, cable, satellite, or packet-based multi-media networks). ETS may include priority for network access, network call setup, and delivery of the call. In addition, ETS requires specific non-call associated signalling and priority handling of all related non-call associated signalling.

7.5.3 Security Planning for ETS and TDR

The availability and security of ETS and TDR communications in NGNs depend on the following:

(a) General NGN Security – The generic mitigation capabilities, mechanisms and policies supported for NGN access and transport services and application services.

(b) ETS and TDR Specific Security – Mitigation capabilities, mechanisms and policies specific to TDR and ETS communications. The uniqueness of TDR and ETS (i.e., specific priority marking) communications may expose these services to specific security risks and vulnerabilities (e.g., denial of service attacks) that require special considerations.

(c) Authentication and authorization of TDR and ETS users and networks in an NGN environment.

Figure 5 illustrates an example end-to-end ETS and TDR communication between different national networks. The example illustrates that end-to-end communications may involve multiple network segments and administrative domains (e.g., Access Network, Originating Network, ETS Provider Network, TDR Provider Network, Intermediate Network and Terminating Network). Each network would have specific security responsibilities within its administration domain to facilitate end-to-end security and availability of TDR and ETS communications.

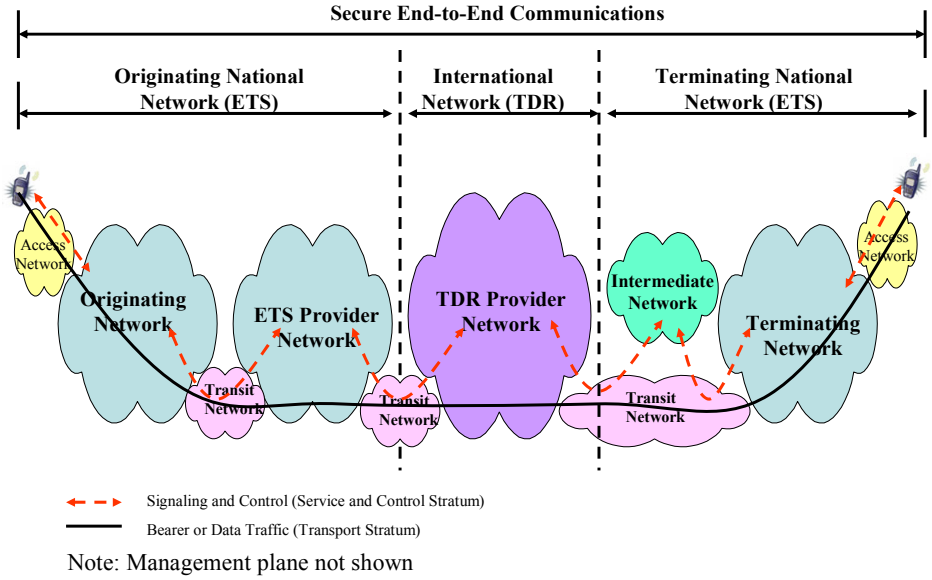


Figure 5 – Example End-to-End ETS and TDR Communications between National Networks

The general guidelines or security planning to protect ETS and TDR signalling, bearer and data, and management related data and information (e.g., user profile information), but are not limited to:

- Each network administrative domain should establish and enforce security policies and implement mitigation capabilities for ETS and TDR within its domain. Specifically, it is recommended that mitigation capabilities and security practices beyond those needed for other services (i.e., mitigation capabilities, practices and policy specific to ETS/TDR) should be identified and enforced. For example, mitigation capabilities to prevent use of TDR and ETS services and resources by unauthorized users, and to prevent denial of service and other types of attacks.
- Each network administrative domain should establish method/procedures for identifying ETS/TDR communications, identity management and, authentication of users and networks across multiple network administration domains. For example, Service Level Agreements (SLAs) should establish and enforce security policy for authenticating each domain for handing off and receiving ETS/TDR communications.
- Each network administrative domain should establish and enforce security policies to protect ETS and TDR management related data and information (e.g., user profile information).
- Each network administrative domain should establish and enforce security policies to allow secure interworking between ETS and TDR.

7.6 Overview of existing standard solutions related to NAT/firewall traversal

The real-time services are an essential part of the IP Multimedia Service (IMS) component of NGN. One of the main challenges hindering the acceptance of real-time services (e.g. VoIP) is a standards-based solution for traversing intermediary nodes such as Network Address Translation (NAT) and firewall boxes. The existing standards solution cause significant security problems. For environments needing a secure connection (bearer channel, signalling channel or both), Application Layer Gateways (ALG) traditionally used for adding intelligence to intermediary nodes to handle applications such as VoIP. Presence of the ALGs create difficulties for encrypted traffic. Security measures such as encryption that are designed to protect signalling data from malicious network entities have the effect of hiding the data from the ALG.

Since ALGs cannot examine the data being transported, they block VoIP bearer traffic. So VoIP cannot be supported in secure environments. User Agents wishing to set up a secure connection to achieve data confidentiality and data integrity for signalling, also find that the current systems do not support this capability. Additionally, since the NAT changes the source address, the hash produced by the initiating host in a digital signature will not be confirmed by the receiving host and an error message will be generated.

The existing standards security solutions for networks with NAT and firewall devices should be evaluated for the use in the NGN. The next sections give an overview of several such solutions. The applicability of these solutions to NGN is for further study.

7.6.1 Simple traversal of UDP through NATs (STUN)

STUN is a light weight protocol that allows applications to discover the presence and types of NATs and firewalls that exist between a user/client and the Internet. In addition, it enables applications to determine the public IP addresses allocated to them by the NAT (address binding). STUN works for many types of NATs. The protocol is specified in the IETF RFC 3489 [27].

7.6.2 Traversal Using Relay NAT (TURN)

The Internet Draft *Traversal Using Relay NAT (TURN)* specifies the TURN protocol that enables an element behind NAT or firewall to receive incoming data over TCP or UDP connections. STUN allows a client to obtain a transport address (and IP address and port), which may be useful for receiving packets from a peer. However, addresses obtained by STUN may not be usable by all peers. Those addresses work depending on the topological conditions of the network. TURN proposes a solution that complements STUN. TURN allows a client to obtain a transport address at which it can receive media from any peer that is able to send packets to the public Internet. The protocol is studied in the Internet Draft *Traversal Using Relay NAT (TURN)*, (work in progress), J. Rosenberg, et al.

7.6.3 Interactive Connectivity Establishment (ICE)

The Internet Draft *Interactive Connectivity Establishment (ICE)* specifies a methodology for NAT traversal for multimedia session establishment protocols. This draft does not specify a new protocol, rather it describes the ICE methodology which uses existing protocols, such as STUN, TURN and Real Specific IP (RSIP). ICE requires mutual cooperation of endpoints in a SIP dialog. ICE does not require extensions from STUN, TURN or RSIP. However, it requires some additional SDP attributes. The Internet Draft *Interactive Connectivity Establishment (ICE)*, (work in progress), J. Rosenberg, et al. has been published.

7.6.4 Compatibility of NATs and IPsec in VoIP networks

Because NATs hide the source addresses of the devices that are behind the NAT, compatibility of NATs and IPsec is problematic. Particularly, when NATs are used the authentication of the sender of the data is an issue that must be addressed.

The IETF standard solution to the problem of NAT traversal – UDP encapsulation of IPsec should be considered for use with VoIP. This solution is specified in the IETF RFC 3948 *UDP Encapsulation of IPsec ESP Packets* [28]. This RFC specifies protocol that defines methods to facilitate the encapsulation and decapsulation of the IP Encapsulating Security Payload (ESP) packets inside UDP packets traversing NATs. Whenever negotiated, encapsulation is used with Internet Key Exchange (IKE). The negotiation of the use of UDP encapsulation of IPsec packets through NAT boxes in IKE is described in RFC 3847 [29]. This RFC also specifies how to detect one or more network address translation devices (NATs) between IPsec hosts. These two RFCs specify a solution that meets IETF IPsec-NAT compatibility requirements that are described in RFC 3715 [30]. The implementation of this standard solution should allow VoIP IPsec traffic to traverse NATs. Use of shared secret negotiated through IKE could provide a solution to the authentication problem.

7.6.5 Security concerns related to STUN, TURN and ICE

It should be noted that STUN, TURN and ICE protocols have a number of security concerns, as stated in Security Consideration sections of each of the relevant RFCs.

Along with security issues, the impact of these protocols on the network performance (which is especially important for VoIP) should be studied.

WORKING GROUP 6
DELIVERABLES

EVOLUTION

2.18 Evolution of networks to NGN (*Status A*)

2.19 PSTN/ISDN evolution to NGN (*Status A*)

2.20 PSTN/ISDN emulation and simulation (*Status A*)

2.18 – Evolution of Networks to NGN*

Table of Contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

2.18 – Evolution of Networks to NGN

1 Scope

This draft identifies principles and aspects for evolution of the existing networks to Next Generation Networks (NGNs) based on Global Information Infrastructure (GII) concept and related Recommendations Y.2001 [1] and Y.2011 [2].

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this draft. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this draft are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this draft does not give it, as a stand-alone document, the status of a Recommendation.

[1] ITU-T Recommendation Y.2001 (2004), *NGN overview*

[2] ITU-T draft Recommendation Y.2011 (2004), *General principles and general reference model for next generation networks*

[3] ITU-T Recommendation G.964 (2001), *V-interfaces at the digital local exchange (LE) - V5.1 interface (based on 2048 kbit/s) for the support of access network (AN)*

[4] ITU-T draft Recommendation X.462 (1996), *Information technology - Message Handling Systems (MHS) Management: Logging information*

[5] ITU-T Recommendation Q.1741.3 (2003) *IMT-2000 references to release 5 of GSM evolved UMTS core network*

[6] ITU-T Recommendation G.100 (2001), *Definitions used in Recommendations on general characteristics of international telephone connections and circuits*

[7] ITU-T Recommendation F.700 (2000), *Framework Recommendation for multimedia services*

[8] ITU-T Recommendation Y.1411 (2003), *ATM-MPLS network interworking – Cell mode user plane interworking*.

3 Definitions

This draft defines or uses the following terms:

3.1 **Access Gateway (AG):** A unit that provides subscribers with various service access (e.g. PSTN, ISDN, V5.x, xDSL, LAN etc.) and connects them to the packet node (IP or ATM) of an NGN.

3.2 **Access Network (AN):** See Recommendation G.964 [3].

3.3 **Accounting**: See Recommendation X.462 [4]. For convenience the definition is repeated here: "The action of collecting information on the operations performed within a system and the effects thereof."

3.4 **Application:** A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

3.5 **Application Server (AS)**: A unit that supports service execution, e.g. to control Call Servers and NGN special resources (e.g. media server, message server).

3.6 **Billing -** See Recommendation Q.1741.3 [5]. For convenience the definition is repeated here: "A function whereby CDRs generated by the charging function are transformed into bills requiring payment."

3.7 **Call Server:** The core element of a CS-based PSTN/ISDN emulation component, which is responsible for call control, gateway (Access GW, Media GW, and Packet GW) control, media resource control, routing, user profile and subscriber authentication, authorization and accounting. Depending on its role, it can be called as "Access Call Server", "Breakout Call Server", "Interworking Call Server", or "Gateway Call Server".

3.8 **Charging** - See Recommendation Q.1741.3 [5]. For convenience the definition is repeated here: "A function whereby information related to a chargeable event is formatted and transferred in order to make it possible to determine usage for which the charged party may be billed."

3.9 **Customer network:** A telecommunications network belonging to the customer and located in the customer premise(s). The customer network is connected to the user side of an access network

3.10 **Evolution to NGN:** A process in which whole or parts of the existing networks are replaced or upgraded to the corresponding NGN components providing similar or better functionality, while attempting to maintain the services provided by the original network and the possibility of additional capabilities.

3.11 **Gateway:** A unit that interconnects different networks and performs the necessary translation between the protocols used in these networks.

3.12 **Network Node Interface (NNI):** The interface of a network node (node as defined in Rec. E.351) which is used to interconnect with another network node. Note: This interface is not constrained to a single protocol. In the case of interconnection between an NGN network and a legacy network it will also depend on the type of network connecting to NGN and where the mediation is performed if any.

3.13 **Next Generation Network (NGN):** See Recommendation Y.2001 [1].

3.14 **Node:** A network element (e.g. switch, router, exchange) providing switching and/or routing capabilities.

3.15 **PABX:** See Recommendation G.100 [6]

3.16 **Public Switched Telephone Network (PSTN):** See Recommendation G.100 [6].

3.17 **Signalling Gateway (SG):** A unit that provides signalling conversion between the NGN and the other networks (e.g. STP in SS7).

3.18 **Telecommunication service:** See Recommendation F.700 [7].

3.19 **Transit Gateway (TG)**: A unit that provides an interface between the packet nodes of the NGN and the circuit switched node of the PSTN/ISDN providing any needed conversion to the bearer traffic.

3.20 User Network Interface (UNI): An interface between the user equipment and a network termination at which interface the access protocols apply. Note: This interface is not constrained to a single protocol.

4 Abbreviations and acronyms

This draft uses the following abbreviations:

AG	Access Gateway
AN	Access Network
API	Application Programming Interface
AS	Application Server
ATM	Asynchronous Transfer Mode
CS	Call Server
CDR	Call Detail Record
ETS	Emergency Telecommunications Service
FR	Frame Relay
GII	Global information infrastructure
GW	Gateway
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAN	Local Area Network
MED	Mediation
NGN	Next Generation Network
OAM	Operation, Administration and Maintenance
PABX	Private Automatic Branch eXchange
PLMN	Public Land Mobile Network
PSTN	Public Switching Telecommunication Network
QoS	Quality of Service
SCP	Service Control Point
SG	Signalling Gateway
SS7	Signalling System number 7
STP	Signalling Transfer Point
TDR	Telecommunications for Disaster Relief
TG	Transit Gateway
DSL	Digital Subscriber Line

5 Conventions

TBD

6 Evolution principles

Evolution to NGN should allow continuation of the existing network capabilities and in addition facilitate implementation of new capabilities. Evolution to NGN should respect the integrity of services provided by the existing networks and should facilitate introduction of new services. Considering that provision of NGN is an evolutionary process it is necessary to define a step-by-step approach leading to the NGN as a target network. This approach should consider the following objectives:

- separation of transport, control, management and service functions.
- reduction of cost for the network infrastructure and its maintenance
- maximum reuse of the existing resources
- achieving comparable QoS level as provided in the existing network
- optimum use of the new technologies
- rapid implementation of new services and technologies enabling introduction of new applications
- provision of mechanisms enabling user's full utilisation of the applications and network resources.

7 Aspects to consider when evolving to NGN

Network operators will potentially choose a different evolution path depending on their actual resources. While considering the evolution path it is essential the following aspects be considered:

7.1 Transport

7.1.1 Leased line provisioning

TBD

7.2 Signalling and control

TBD

7.3 Management

TBD

7.4 Services

7.4.1 Bearer

TBD

7.4.2 Supplementary

TBD

7.5 Operation, administration and maintenance (OAM)

TBD

7.6 Resource allocation

TBD

7.7 Naming numbering and addressing

TBD

7.8 Accounting, charging and billing

It is generally accepted that the introduction of NGN will result in changes to the existing "accounting, charging and billing" procedures. However, these changes will not be immediate. During the transition period, maintaining the existing procedures, to the extent practical, may be required.

Evolution from existing networks to NGN will also imply replacement of the existing sources of the accounting data generation. Thus the following accounting aspects may be affected:

a) Information content

b) Interfaces to other systems

c) Data format

d) Data security, i.e. data protection, transmission security and confidentiality

As shown in Figure 7-1 following scenarios are considered when evolving to NGN. The timing or preference for selection of these scenarios is operator dependent.

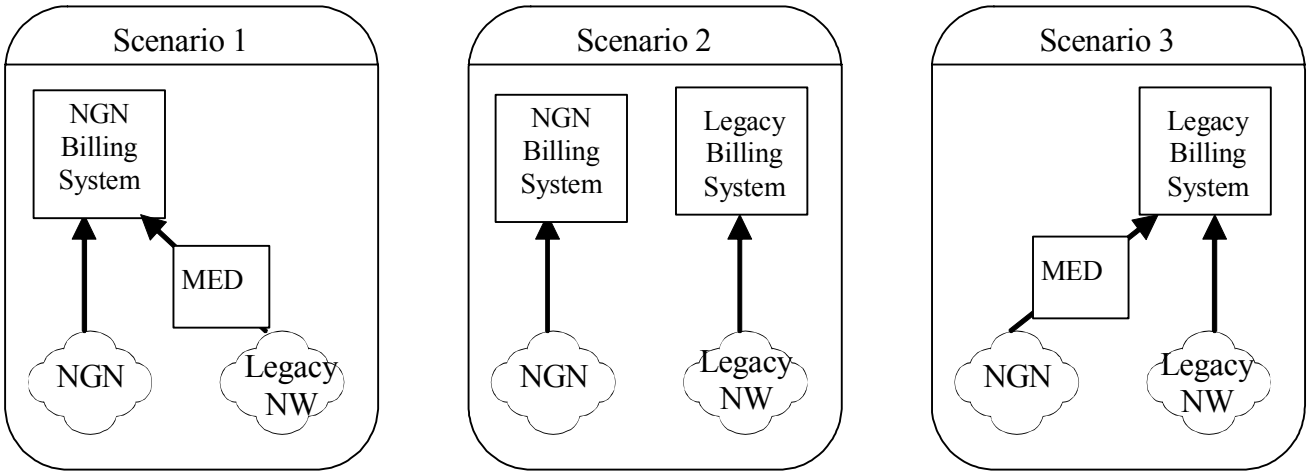


Figure 7-1 – Billing system evolution scenarios

Mediation (MED) is an entity which allows transfer and processing of Call Detail Records (CDRs) from the legacy network to the NGN billing system or from the NGN to the legacy billing system.

Scenario 1

For this scenario an NGN billing system is considered to handle both legacy networks and the NGN. For this case all accounting aspects are affected.

Scenario 2

A new billing system is developed for NGN while using existing legacy system for the legacy network. For this case all accounting aspects are to be considered for NGN.

Scenario 3

For this scenario a legacy billing system is considered to handle both legacy networks and the NGN. For this case all accounting aspects are affected.

7.9 Interworking

Interworking as defined in Y.1411 [8] is used to express interactions between networks, between end-systems, or between parts thereof, with the aim of providing a functional entity capable of supporting an end-to-end communication. Evolution to NGN should take the following into consideration.

- Ability to inter-work with non-IMS based networks such as PSTN/ISDN, Public Land Mobile Network (PLMN) and public IP networks
- Ability for inter-domain, inter-area or inter-network interworking
- Support for authentication and authorization
- Ability to perform call admission control
- Support for accounting, charging and billing

8 Service requirements by national regulatory bodies

TBD

9 Emergency communications in NGN

Evolution of the network shall provide continuity of the existing emergency communications in addition to potentially providing new emergency communications capabilities.

Requirements for the support of emergency communications are described in NGN Release 1 Requirements. Emergency communications includes:

- Individual-to-authority communications, e.g., calls to emergency service providers.
- Authority-to-authority communications, e.g. Telecommunications for Disaster Relief (TDR) and Emergency Telecommunications Services (ETS).
- Authority-to-individual communications, e.g. community notification services. TDR and ETS also provide requirements for authority-to-individual communications.

10 Security aspects of evolution

Evolution of network security should allow continuation of the existing network security capabilities and in addition provide new mitigation and prevention capabilities against new security threats.

Several aspects may be considered:

- Achieving acceptable security level by combination of different layer security methods
- Similar user security experience while evolving networks to NGN
- No over-provision of security measures.

Appendix I

Priorities

Network and service providers may choose different evolution path based on their existing and forecasted resources. This approach may encompass different technologies and have different priorities.

Therefore there is a need to prepare a set of documents to help evolution of the existing networks towards NGN. Taking into consideration that potentially there are different evolution approaches (at least as many as the existing networks), it is crucial to consider items provided in clause 8 for each network and to not violate the evolution and interworking principles described in clauses 6 and 7. The following provides list of networks or technologies which may be considered for evolution.

- PSTN / ISDN
- FR
- ATM
- IPv4
- Mobile Network
- Other scenarios

2.19 – PSTN/ISDN Evolution to NGN*

Introduction

Next Generation Network (NGN) is believed to provide new opportunities for and capabilities to the network and service providers. Considering that existing networks have different life span and vast amount of capital has been spent on them, complete replacement of their components is not considered to be either advisable or possible. So, a phased approach should be considered for evolution of existing networks to NGN.

Public Switched Telephone Network/Integrated Services Digital Network (PSTN/ISDN) being one of the first networks, is considered to be prime candidate for evolution. For PSTN/ISDN evolution to NGN a phased approach is considered in this draft.

Table of Contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

2.19 – PSTN/ISDN Evolution to NGN

1 Scope

Public Switched Telephone Network/Integrated Services Digital Network (PSTN/ISDN) being one of the networks in telecommunication is considered to be a prime candidate for evolution to Next Generation Network (NGN) [1 & 2]. Because of widespread deployment and use of PSTN/ISDN, evolution to NGN should be considered as a step-wise approach.

This draft describes possible ways of evolving PSTN/ISDN to NGN. Both IP Multi-media Sub-System (IMS)-based and Call Server (CS)-based are described. It describes aspects which need to be considered including evolution of transport, management, signalling and control parts of PSTN/ISDN to NGN. Evolution scenarios are also provided in this document.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this draft. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this draft are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this draft does not give it, as a stand-alone document, the status of a Recommendation.

[1] ITU-T Recommendation Y.2001 (2004), *NGN overview*

[2] ITU-T draft Recommendation Y.2011 (2004), *General principles and general reference model for next generation networks*

[3] ITU-T Recommendation G.964 (2001), *V-interfaces at the digital local exchange (LE) – V5.1 interface (based on 2048 kbit/s) for the support of access network (AN)*

[4] ITU-T Recommendation G.965 (2001), *V-interfaces at the digital local exchange (LE) - V5.2 interface (based on 2048 kbit/s) for the support of access network (AN)*

[5] ITU-T Recommendation Q.310-332 (1988), *Specifications of Signalling System R1*

[6] ITU-T Recommendation Q.400-490 (1988), *Specifications of Signalling System R2*

[7] IETF RFC 3372 (2002), *Session Initiation Protocol for Telephones (SIP-T): Context and Architectures*

[8] ITU-T Recommendation Q.1912.5 (2004), *Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part.*

[9] ITU-T Recommendation M.3400 (2000), *TMN Management Functions*

[10] ITU-T Recommendation M.3010 (2000), *Principles for a Telecommunications management network*

[11] ITU-T Recommendation G.100 (2001), *Definitions used in Recommendations on general characteristics of international telephone connections and circuits*

[12] ITU-T draft Recommendation Y.ngn-account (August 29 – September 9 2005), *Requirements and framework allowing accounting, charging and billing capabilities in NGN*

[13] ETSI specification TS 122 115 v6.5.0 (2005-09), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Service aspects; Charging and billing*

3 Definitions

This draft uses or defines the following terms:

3.1 **Media Server (MS):** A network element providing the Media Resource Processing Function for telecommunication services in NGN.

3.2 **NGN-AG:** An Access Gateway, which interfaces to IP Multimedia Component using SIP and providing PSTN/ISDN simulation services.

3.3 **Remote User Access Module (RUAM):** A unit that physically terminates subscriber lines and converts the analogue signals into a digital format. The RUAM is physically remote from the Local Exchange.

3.4 **User Access Module (UAM):** A unit that physically terminates subscriber lines and converts the analogue signals into a digital format. The UAM is collocated with a Local Exchange (LE), and is connected to the Local Exchange.

4 Abbreviations and acronyms

This draft uses the following abbreviations.

AG	Access Gateway
AS	Application Server
AN	Access Network
ATM	Asynchronous Transfer Mode
BICC	Bearer Independent Call Control
CAS	Channel Associated Signalling
CBR	Constant Bit Rate
CCS	Common Channel Signalling
CS	Call Server
IN	Intelligent Network
INAP	Intelligent Network Application Part
IP	Internet Protocol
ISDN	Integrated Service Digital Network
LE	Local Exchange
LL	Leased Line

MS	Media Server
OSS	Operation Support System
PABX	Private Automatic Branch Exchange
PCM	Pulse Code Modulation
POTS	Plain Old Telephone Service
PRI	Primary Rate Interface
PSN	Packet Switch Network
PSTN	Public Switching Telephone Network
QoS	Quality of Service
RUAM	Remote User Access Module
SCE	Service Creation Environment
SCP	Service Control Point
SG	Signalling Gateway
SIP	Session Initiation Protocol
SSF	Service Switching Function
SSP	Service Switching Point
STP	Signalling Transfer Point
TDM	Time Division Multiplexing
TE	Transit Exchange
TG	Transit Gateway
TMN	Telecommunication Management Network
UAM	User Access Module
VoIP	Voice over IP

5 Conventions

TBD

6 PSTN/ISDN evolution to NGN

PSTN/ISDN is the prime candidate for evolution to NGN and as such all their aspects should be carefully examined and appropriate measures should be taken.

In general PSTN/ISDN networks are comprised of the following entities each with one or multiple functionalities:

- Transport (access plus core): User Access Module (UAM), Remote User Access Module (RUAM), Access Network (AN) via V.5 [3 & 4] interface connected to the core switches and core switches themselves
- Control and signalling: exchange hosts
- Management: management of exchanges
- Service: exchange hosts and auxiliary network (e.g. IN)

In PSTN/ISDN most of the functionalities are located in a single exchange and may use proprietary protocols. However, in the NGN functionalities may be distributed amongst several elements. The following clauses provide detailed steps for evolution of PSTN/ISDN to NGN.

7 Aspects to consider when evolving to NGN

For evolution of PSTN/ISDN to NGN aspects identified in the following sub-clausesare to be considered:

7.1 Transport

Transport is an important part of any network. It encompasses functions related to:

- User premises equipments (e.g. terminals, PABXs, routers) ;
- The access network equipments (e.g. line terminating modules, remote or local concentrators, multiplexers); and
- The core network equipments (e.g. local exchanges, transmission facilities, transit and international exchanges)

All transport related aspects which may be affected by evolution to NGN should be considered.

7.1.1 Leased line provisioning

Provision of leased lines is network specific.

7.2 Signalling and control

PSTN/ISDN uses signalling systems such as R1 [5], R2 [6], Common Channel Signallig (CCS) and Channel Associated Signalling (CAS). All these signalling systems are for the circuit switched networks. Since NGN is packet-based, other suitable types of signalling (e.g., BICC, SIP-T [7], SIP-I [8], etc.) may be required. Also, signalling function and call control function may reside in more than one NGN element.

Since the NGN has to work with the PSTN/ISDN and other networks, interworking between NGN signalling systems and the legacy network signalling systems is required.

It is further anticipated that signalling aspects for access and core networks be independent in order to have the possibility of a step-wise approach for evolution to NGN.

7.3 Management

PSTN/ISDN management is comprised of activities from core exchange network, access network, intelligent network and the Operation Support System (OSS). Recommendations M.3400 [9] and M.3010 [10] provide management principles for PSTN/ISDN.

NGN management system is comprised of three planes, namely the network management plane, the network control plane and the service management plane. Each of the three planes implements corresponding management functions to each layer in the NGN layered model. Standard interfaces between these planes need to be defined and are beyond scope of this document.

Evolution of PSTN/ISDN management (i.e. operations, administration and management) systems requires the ability to support the transition of PSTN/ISDN through intermediate stages towards NGN. More information may be available in documents related to NGN management.

7.4 Services

PSTN/ISDN services which are traditionally provided by PSTN/ISDN exchanges may be provided by Application Servers (ASs) in NGN. As well some services may be implemented on the Call Server (CS).

- It is expected that some or all of the legacy services will be provided by NGN. However, there is no guarantee that all services be provided when PSTN/ISDN is simulated.
- Use of legacy terminals via adaptation to the NGN is expected in order to support existing services.
- It is assumed that legacy services may be upgraded on the basis of relevant features inherently provided by NGN (e.g. Presence management).

An example of PSTN/ISDN service evolution is shown in Appendix I.

7.4.1 Bearer

While evolving from PSTN/ISDN to NGN, continuity of bearer services should be provided.

PSTN/ISDN Simulation provides functionality that is similar but not identical to existing ISDN bearer services.

PSTN/ISDN emulation shall provide support for all bearer services offered by PSTN/ISDN. However, there is no requirement for NGN to support all ISDN bearer services identified in I.230 series.

Use of NGN to connect two PSTN/ISDN networks shall be transparent for all bearer services.

7.4.2 Supplementary

While evolving from PSTN/ISDN to NGN, continuity of supplementary services should be provided to the extent practical. PSTN/ISDN emulation shall provide support for all supplementary services offered by PSTN/ISDN. PSTN/ISDN simulation provides functionality that is similar but not identical to existing PSTN/ISDN services. The NGN need not support all ISDN supplementary services identified in I.250 series of Recommendations. NGN must appear transparent when used to connect supplementary services between two PSTN/ISDNs.

7.5 Operation, administration and maintenance (OAM)

TBD

7.6 Resource allocation

TBD

7.7 Naming numbering and addressing

The NGN naming, numbering and addressing schemes in consistency with Recommendation Y.2001 [1] shall be able to inter-work with existing E.164 numbering scheme.

7.8 Accounting, charging and billing

It is generally accepted that the introduction of NGN will result in changes to the existing "accounting, charging and billing" procedures. However, these changes will not be immediate. During the transition period, maintaining the existing procedures, to the extent practical, may be required.

Evolution from existing networks to NGN will also imply replacement of the existing sources of the accounting data generation. New business models for NGN services may increase number of business roles involved in charging.

Thus the following accounting aspects may be affected:

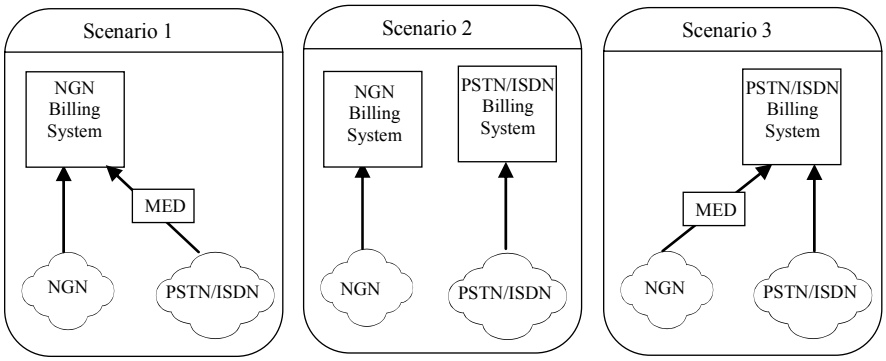
a) Information content

b) Interfaces to other systems

c) Data format

d) Data security, i.e. data protection, transmission security and confidentiality

Three following scenarios are considered when evolving to NGN. The timing or preference for selection of these scenarios is operator dependent.



Mediation (MED) is an entity which allows transfer and processing of Call Detail Records (CDRs) from the PSTN/ISDN to the NGN billing system or from the NGN to PSTN/ISDN billing system.

Scenario 1

For this scenario an NGN billing system is considered to handle both PSTN/ISDN and the NGN. For this case all accounting aspects are affected.

Scenario 2

For this scenario a new billing system is developed for NGN while keeping the existing PSTN/ISDN billing system. For this case all accounting aspects are to be considered for NGN.

Scenario 3

For this scenario a legacy billing system is considered to handle both PSTN/ISDN and the NGN. For this case all accounting aspects are affected.

7.8.1 Considerations

The NGN shall support both offline and online charging. For evolution to NGN the following factors shall be considered. However, this does not constitute a comprehensive list.

- Information content – the information contained in the CDRs shall be consistent with the information already provided in PSTN/ISDN. In particular the following data should be provided:
  - Calling and/or called user identification

  - Date and time of the event
  - Type of the service or event
  - Call duration or session duration

  It is also necessary to provide new NGN specific, information such as:
  - Bandwidth
  - QoS
  - Media type
- Data sources
  - Call Server
  - Media server
  - Access Gateway
  - Trunking Gateway
  - Application server
- Data format requirements
  - Optimal encoding complexity
  - Convenience of data collection and record construction
  - Optimal data size
  - Efficient data storage
- Interfaces to other systems
  - For real time and bulk methods of collecting accounting data.
  - For on-line and off-line charging
  - For other services such Advice of Charge and credit Limit

Specific detailed requirements are addressed in Y.NGN-account [12] and ETSI TS 122 115 [13].

7.9 Interworking

TBD

7.10 Routing

When NGN coexists with PSTN/ISDN, the routing scheme should allow the carriers to control where their traffic enters and leaves the NGN. This will make it possible for the carrier to optimize use of their network resources.

8 Service requirements by national regulatory bodies

It is desirable that NGN provides:

- the basic telephone service with the same or better quality and availability as the existing PSTN/ISDN;
- the capability for accurate charging and accounting;
- capabilities to support number portability ;
- capability for the user to select the carrier for local and long-distance calls;
- the availability of directory inquiry service for PSTN/ISDN and the NGN users;

- support of Emergency Communications as stated in clause 9;
- support for all users, including the disabled. Support should provide at least the same capabilities as the existing PSTN/ISDN. NGN offers the opportunity for more advanced support, e.g. network capabilities for text to speech;
- privacy of user's information;
- mechanisms to support lawful interception and monitoring of various media types of communications such as voice, data, video, e-mail, messaging, etc. Such a mechanism may be required of a network provider for providing access to Content of Communication (CC) and Intercept Related Information (IRI) by Law Enforcement Agencies (LEA), to satisfy the requirements of administrations and International treaties;
- interoperability between NGN and e.g. PSTN and wireless telecommunication network.

The list of required services in public telecommunications systems in each country is based on national regulation. This document is not addressing detailed national regulatory requirement.

9 Emergency communications in NGN

It is desirable that NGN provides:

- capability to support priority mechanisms for Emergency Communications in multimedia services (e.g., voice, data, and video). Emergency communications includes: a) individual-to-authority communications, i.e., calls to emergency service providers; b) authority-to-authority communications; and c) authority-to-individual communications. Telecommunications for Disaster Relief (TDR) and Emergency Telecommunications Services (ETS) could be both authority-to-authority and authority-to-individual communications and community notification services could be authority-to-individual communications;
- support for calls to emergency service providers which may be free of charge for the calling user. Such calls must include information on how to enable emergency services to call back the calling user, and including at least the accurate location information about the calling user at the time of call initiation, e.g. to be provided to the emergency response centres, routing of the call to the Public Safety Answering Point (PSAP) - regardless of whether the user is fixed, mobile or nomadic. Accurate location may be such information as postal address, geographic coordinates or other information like cell indicators. Both network and user location information shall be provided, if available;
- the capability to ensure that calling line identification presentation (or the equivalent information in IMS) is not ruled out on a per call, per line or per identity basis for calls to the emergency call number;
- network integrity, as far as possible, in order to support critical communications such as TDR support in a crisis situation.

10 Security aspects of evolution

The NGN shall provide at least the same security level as for the existing PSTN/ISDN. As PSTN/ISDN is transitioning to NGN new concerns and threats, unknown in PSTN/ISDN, may be encountered. Therefore additional measures may be required to guarantee at least the current security level.

Different security dimensions, depending on the access method, shall be taken into account to fulfill this demand:

- Authentication
- Non-repudiation
- Data confidentiality
- Communication security
- Data integrity
- Availability
- Privacy

The NGN security means may be used to secure PSTN/ISDN simulation and emulation scenarios. The complete list of requirements for NGN security is beyond the scope of this document.

11 Evolution scenarios

All the NGN evolution scenarios rely upon the separation of functionalities of transport, control, service and management aspects.

The evolution scenarios imply one or more steps, depending on the extent to which these separations are implemented.

Possible scenarios for evolution of the PSTN/ISDN are presented in the following sub-clauses:

11.1 Core network

11.1.1 CS-Based

General

The Call server (CS) is the core element for PSTN/ISDN emulation. It is responsible for call control, gateway control, media resource control, routing, user profile and subscriber authentication, authorization and accounting. The Call Server may provide PSTN/ISDN basic service and supplementary services, and may provide value added services through service interaction with an external Service Control Point (SCP) and/or Application Server (AS) in the Service/Application layer. A fully compliant Call Server implementation need only implement some of the components identified here, although it is possible to combine multiple functions in a single entity.

A Call Server can perform one or more of the following roles.

- Access Call Server (ACS) - A call server can implement access gateway control and media resource control functions, and thus can providing PSTN/ISDN basic service and supplementary services.
- Breakout Call Server (BCS) - A call server can implement interworking functions to allow interconnection with PSTN/ISDN networks.
- Interworking Call Server (ICS) - A call server can provide interoperability between PSTN/ISDN emulation components and IP multimedia components within a single NGN domain.
- Gateway Call Server (GCS) - A call server can provide interoperability between different NGN domains from different operators.

Consolidation of local exchanges and remotes for evolution to NGN

In order to prepare the PSTN/ISDN for the evolution to a Packet Switched Network (PSN) and as an initial step some of the Local Exchanges (LEs) are removed and all their functionalities such as control, accounting, etc. are transferred to those remaining LEs. Affected User Access Module (UAM), Private Automatic Branch eXchange (PABX), and Access Network (AN) are connected to the remaining LEs. Further consolidation occurs when User Access Modules (UAM) become Remote User Access Modules (RUAM) which, are connected to the remaining LEs. Figure 11-1 shows this preparatory step.

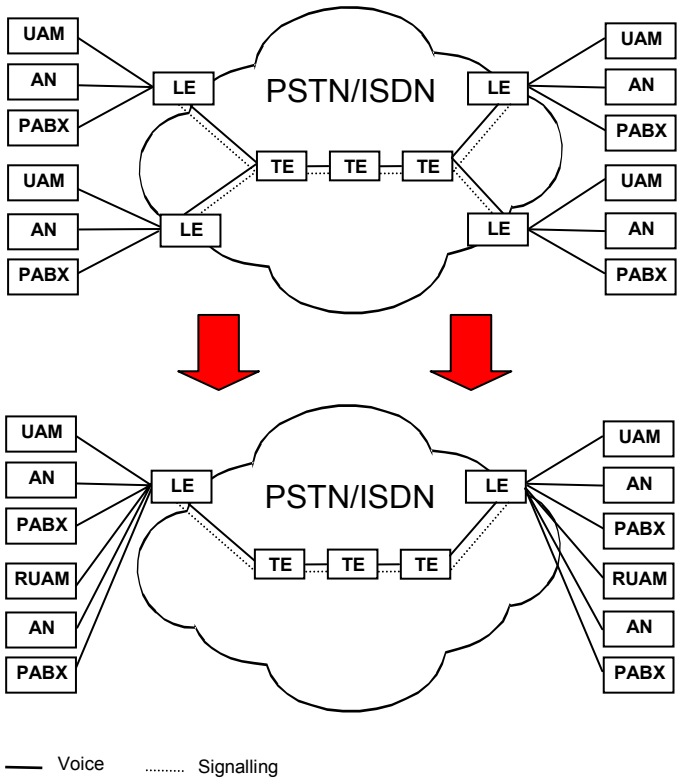


Figure 11-1 – Preparation for evolution to NGN

Scenario 1 – PSTN/ISDN and PSN co-exist initially

The most likely initial approach for evolution of PSTN/ISDN to PSN will involve a path that requires the PSTN/ISDN to co-exist with PSN during a transition period as shown in Figure 11-2. This scenario follows that approach. There are two steps in this scenario as explained below.

Step 1

In this step some of the Local Exchanges (LEs) are replaced by the Access Gateways (AG). Functions originally provided by the removed LEs are furnished by the AGs and the Call Server (CS). In addition some of the access elements such as User Access Modules (UAMs), Remote User Access Modules (RUAMs), and Private Automatic Branch eXchanges (PABXs) which were originally connected to the removed LEs become directly connected to Access Gateways (AGs). Additional Access Gateways (AGs) may also be deployed to support new subscribers can directly connect to them. The Transit and Signalling Gateways (TGs & SGs) are deployed for interconnection between PSN and the TEs of the legacy network as well as other operators' PSTNs/ISDNs. The Access and the Transit Gateways (AGs & TGs) are all controlled by the Call Server (CS).

Step 2

In this step the remaining Local Exchanges (LEs) are replaced by the Access Gateways and the Transit Exchanges (TEs) are removed and their control functions are performed by Call Server (CS). The Transit and Signalling Gateways (TGs & SGs) are deployed for interconnection between PSN and other operators' PSTNs/ISDNs. The Access and the Transit Gateways (AGs & TGs) are all controlled by Call Server (CS).

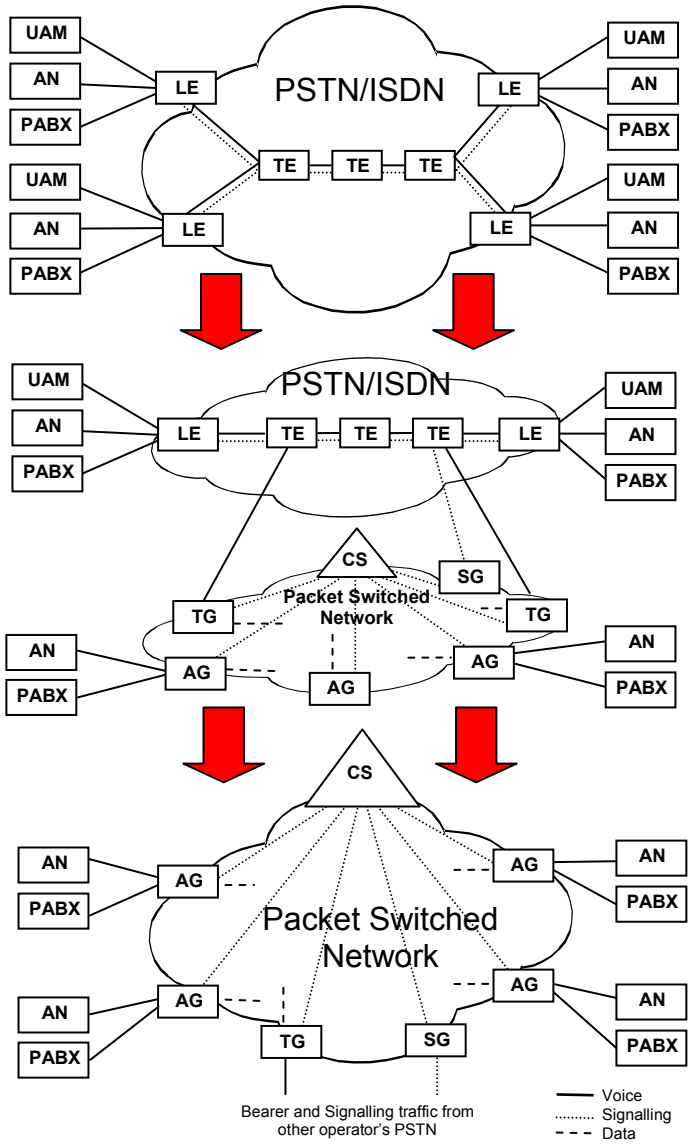


Figure 11-2 – Realisation of scenario 1

Scenario 2 – Use of SGs and TGs as an initial approach

This scenario consists of two steps as shown in Figure 11-3 and explained below.

Step 1

In this step PSTN/ISDN is replaced by PSN and the TE functions are performed by the TGs and the SGs under the control of the Call Server (CS). The local exchanges (LEs) are connected to the PSN via Transit Gateways (TGs) and Signalling Gateways (SGs). The Transit and Signalling Gateways (TGs & SGs) are also deployed for interconnection between PSN and other operators' PSTNs/ISDNs.

Step 2

In this step the Local Exchanges (LEs) and some of the access elements such as User Access Modules (UAMs) and Remote User Access Modules (RUAMs) are removed and their functions are provided by the Access Gateways (AGs) and Call Server (CS). The Private Automatic Branch eXchanges (PABXs) are directly connected to Access Gateways (AGs). The Access Networks (AN's) are either replaced by the Access Gateways (AGs) or are connected to the Access Gateways (AGs). The Transit and Signalling Gateways (TGs & SGs) are deployed for interconnection between PSN and other operators' PSTNs/ISDNs. The Access and the Transit (AGs & TGs) are all controlled by Call Server (CS).

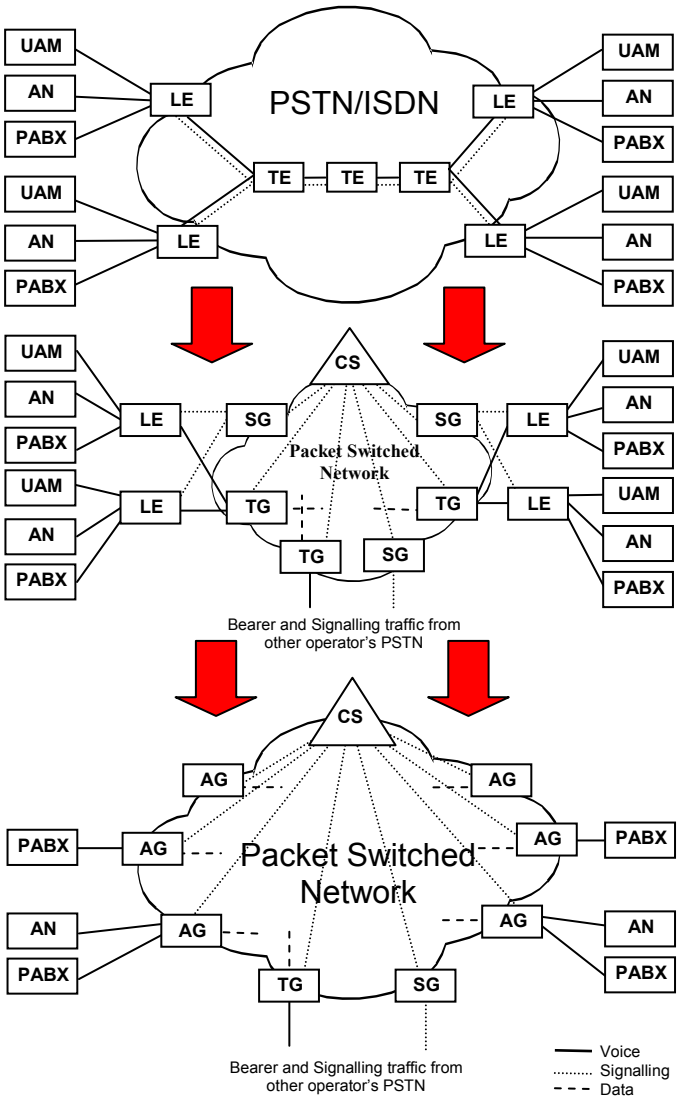


Figure 11-3 – Realisation of scenario 2

Scenario 3 – The one-step approach

In this scenario the PSTN/ISDN is replaced with Packet Switched Network (PSN) in only one step as shown in Figure 11-4. The local exchanges (LEs) are replaced by the Access Gateways (AGs) and their functions are divided between the AGs and the Call Server (CS). Specifically the call control and accounting functions are all transferred to the Call Server. All access elements such as User Access Modules (UAMs), Remote User Access Modules (RUAMs), and Private Automatic Branch eXchanges (PABXs) are connected to Access Gateways (AGs). The Access Networks (AN's) are either replaced by the Access Gateways (AGs) or are connected to Packet Based Network through the AGs. The Transit Gateways (TGs) under the control of

the Call server (CS), and the Signalling Gateways (SGs), are deployed to replace the TE functions and provide interconnection between PSN and other operators' PSTNs/ISDNs.

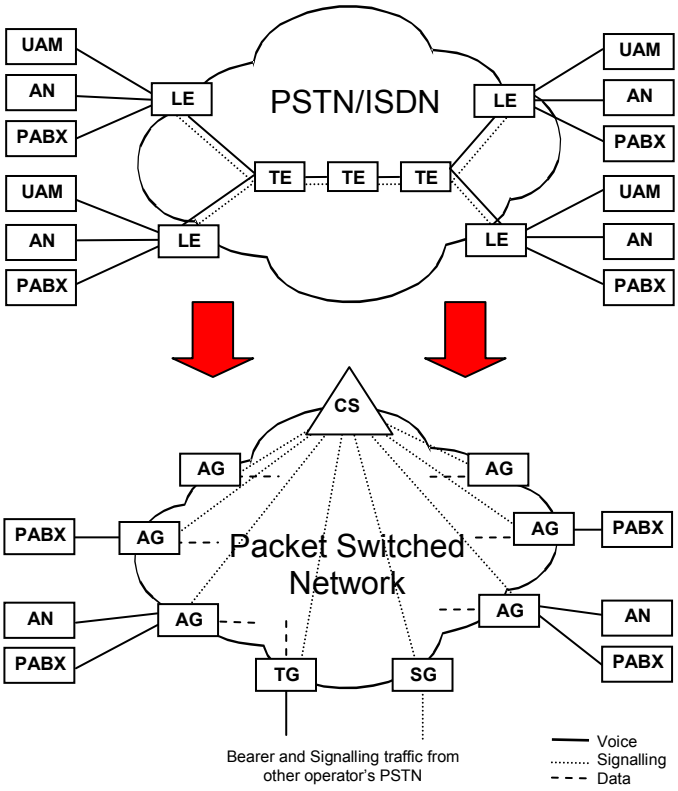


Figure 11-4 – Realisation of scenario 3

11.1.2 IMS-based

Figure 11-5 shows a scenario where PSTN/ISDN evolves directly to a PSN based on the IMS core network architecture. The end-users access the network using NGN user equipment or legacy user equipment connected via an AG. The Transit and Signalling Gateways (TGs & SGs) are deployed for interconnection between the NGN and other operators' PSTNs/ISDNs.

11.1.3 Concurrent CS-based and IMS-based

Concurrent CS-based and IMS-based implementations can occur when an existing operator deploys a separate IMS-based network for new services and supports the remainder of the services using a CS-based approach. These two types of network implementations need to interoperate. Interoperation is possible if SIP is used, but this is beyond the scope of this document.

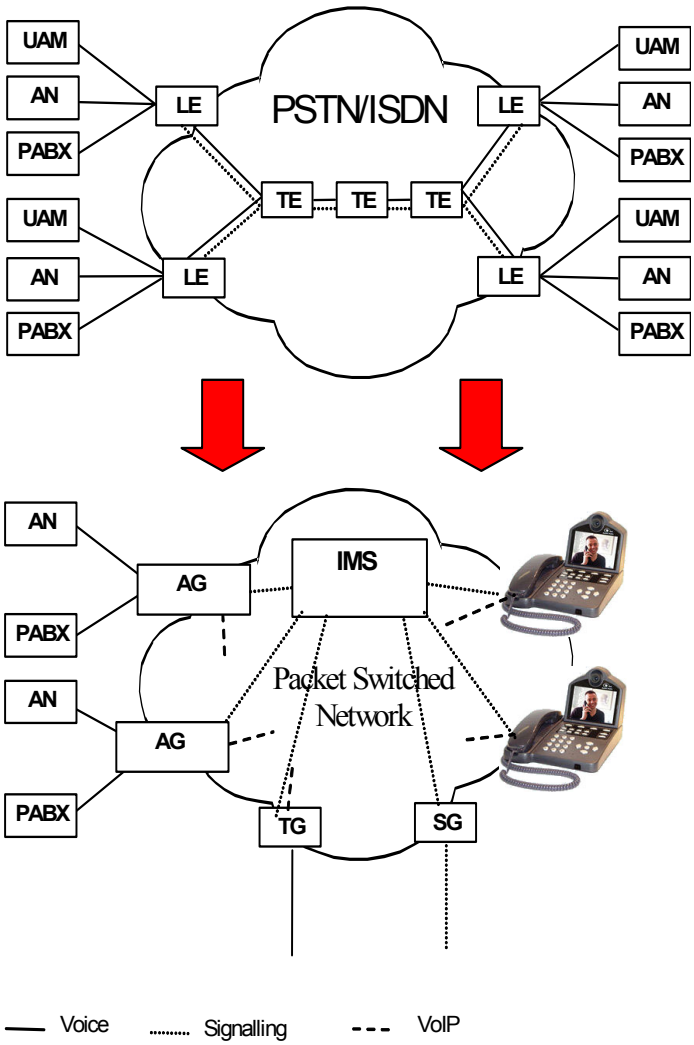


Figure 11-5 – IMS-based PSTN/ISDN evolution to NGN

11.2 Access Network evolution

11.2.1 Evolution of xDSL access to NGN

Evolution of Access Network is shown in three possible steps.

Step 1

There are three traditional Access Network interfaces: V5.x [3 &4], analogue POTS Interface and digital ISDN Interface. They connect subscribers to core PSTN/ISDN over Local Exchanges (LE). There is xDSL interface, which connects a legacy terminal over wired copper lines. Possible initial data link layer protocol for xDSL is ATM.

Legacy users are able to select narrowband and broadband access at the same time. There is subscriber's end-user equipment (xDSL modem) and a Digital Subscriber Line Access Multiplexer (DSLAM) on the operator side. Since xDSL interfaces enable users to connect to the Internet it will be used to connect the legacy terminals to NGN.

Access Network, for another user domain with V 5.x [3 & 4] interface can be left as it is shown on figure or it can be completely replaced by Access Gateway (AG) connected to NGN directly.

Step 2

In this step LE and V5.x [3&4] entities are replaced by an AG. Customer Premise Equipment (CPE) with xDSL modem supported legacy subscribers and may enable them broadband access to NGN. CPE with xDSL modem should have an adaptation function to enable legacy terminal communicate with other subscribers connected to NGN. IP subscribers may also use xDSL interface as transport medium to NGN. Protocol for xDSL interface may be Ethernet which enable broadband data flows and services, e.g. Video on Demand (VoD), Broadcast TV (BTV), Voice over IP (VoIP).

Step 3

In this step twisted copper lines are replaced by optical fibre, either Fibre to The Curb (FTTC) or Fibre To The Home (FTTH) to increase transmission speed. Protocol for this transmission medium may be Ethernet.

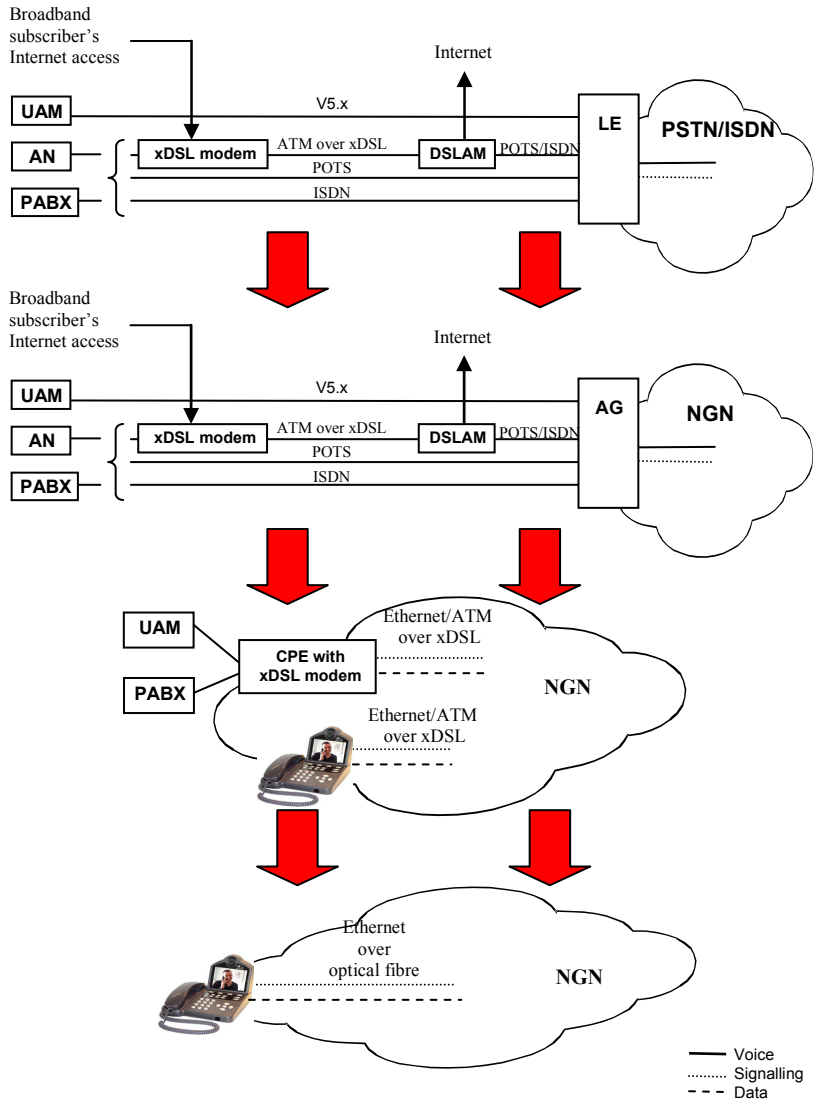


Figure 11-6 – Evolution of xDSL access to NGN

11.3 Signalling and control scenarios

A possible scenario for evolution of signalling in the core network consists of three steps.

Step 1

In this step Signalling Transfer Point (STP) functionality is transferred from the Transit Exchanges (TE) to the independent units creating an STP mesh network (partial or complete).

Step 2

In this step STPs are upgraded to the Signalling Gateways (SG) and are placed on the edge between PSTN/ISDN and NGN. In this case both the legacy network and NGN coexist with each other.

Step 3

In this final step, which is taken when all LEs and TEs are replaced by NGN and there is no more any need to have Signalling Gateways.

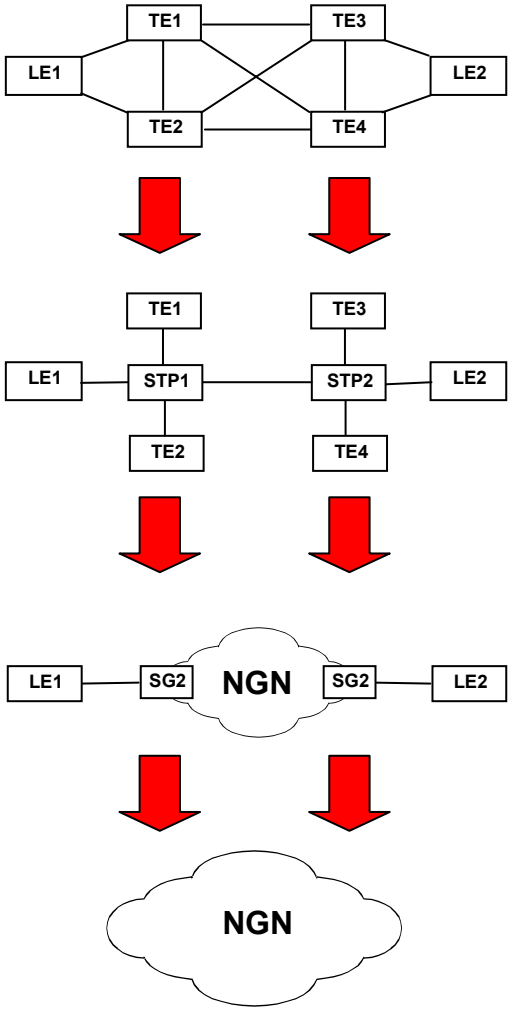


Figure 11-7 – Realisation of signalling evolution scenario

11.4 Management scenarios

Evolution of PSTN/ISDN management system could be done in several possible ways. In one scenario PSTN/ISDN is evolved to NGN but the PSTN/ISDN management system will be used to manage the newly evolved NGN. In another scenario an NGN management system managing an NGN would also manage a PSTN/ISDN. This topic needs further consideration.

11.5 Services evolution scenarios

Possible scenarios for evolution of services in PSTN/ISDN based on IN may be as follows:

Scenario 1

In this scenario it is proposed to reuse existing IN services in NGN by implementation of SSF in CS. Both PSTN/ISDN and NGN networks exist

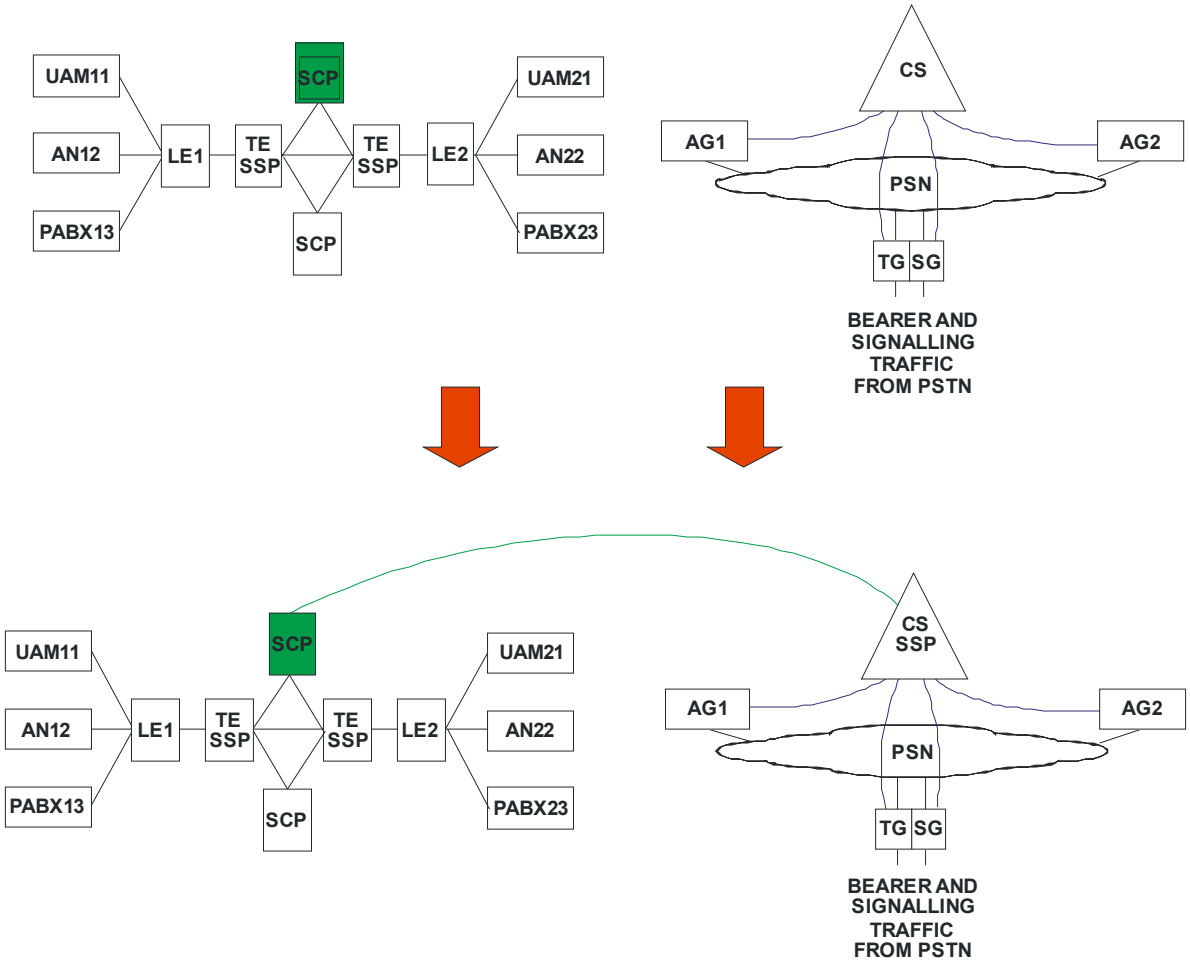


Figure 11-10 – Realisation of scenario 1

On the opposite way reversal scenario could be considered.

The Service Control Point (SCP) can be integrated to the Application Server and become part of the Application Server. So, the services created by the Service Creation Environment (SCE) can be directly loaded to the SCP module of the new Application Server.

An example of SCP integrated to the Application Server is shown in Appendix II.

Scenario 2

In this scenario in order to provide some intelligent service in PSTN/ISDN, IVR is used for processing DTMF signal and announcement.

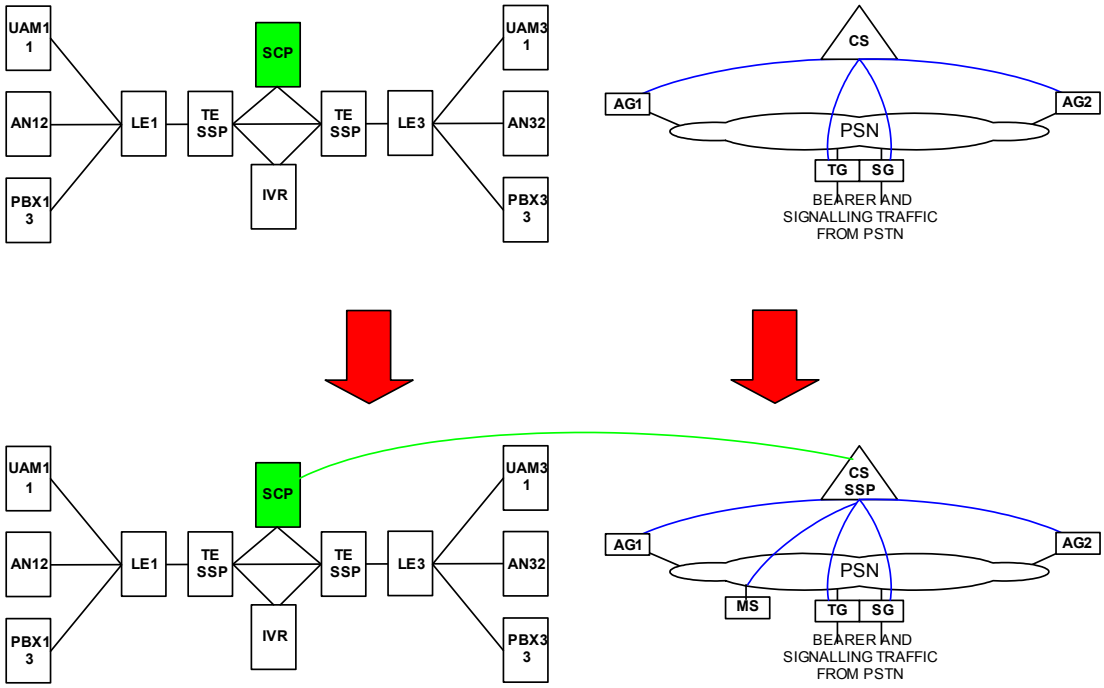


Figure 11-11 – Realisation of scenario 2

Scenario 3

This scenario consists of two steps, which are executed consecutively.

Step 1:

This is a step in which the traditional IN services are provided with SCP, and new value-added services are implemented in AS. During the network evolution, the service triggering function can be realized via CS or IMS. The CS or IMS connects to SCP via Intelligent Network Application Protocol (INAP) interface, and simultaneously connects to AS via SIP interface.

Step 2:

Once the evolution to the NGN is completed all the value-added services will be provided by AS.

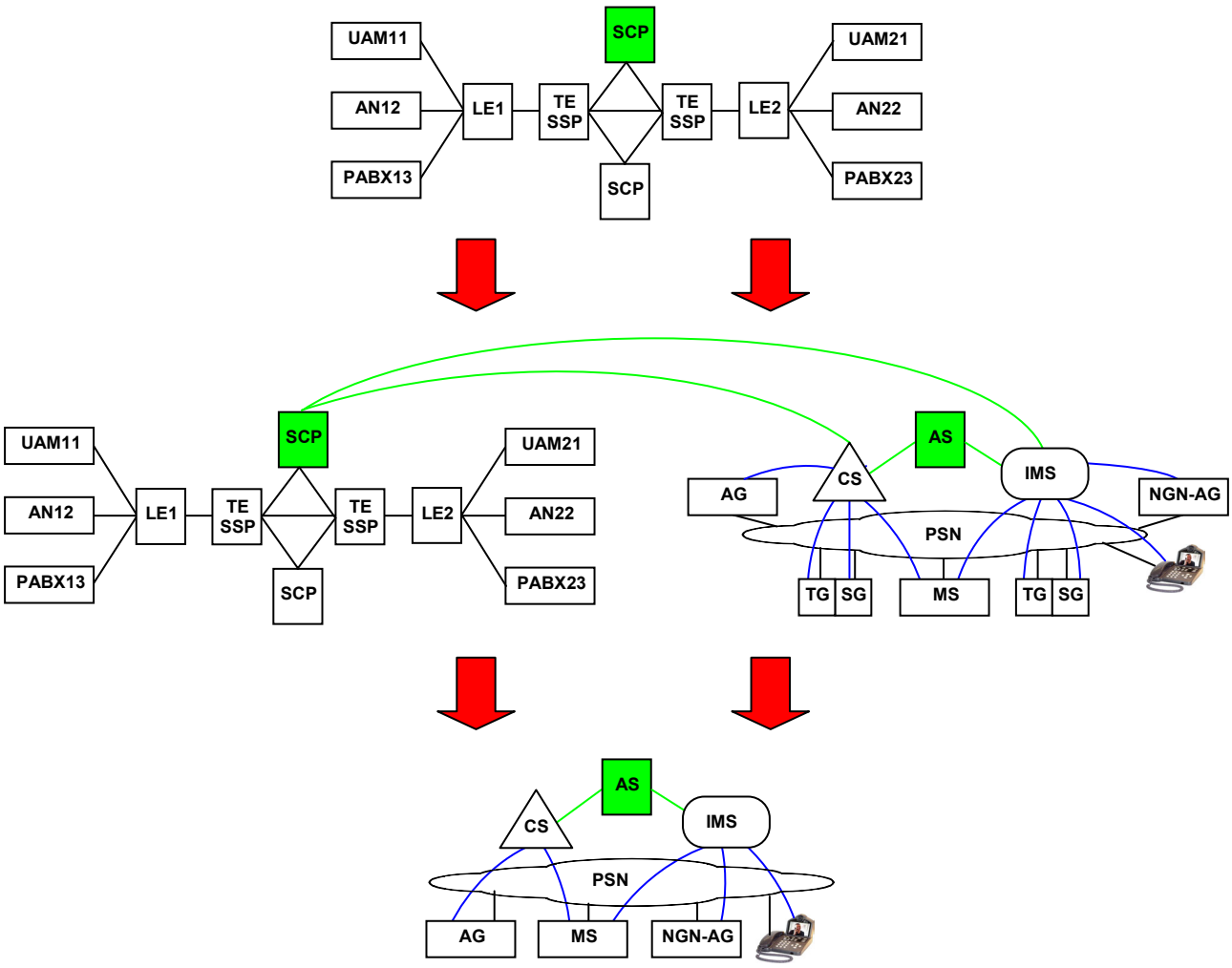


Figure 11-12 – Realisation of scenario 3

Appendix I

Examples of PSTN/ISDN service evolution

(This appendix does not form an integral part of this draft)

This appendix illustrates one example for the deployment of PSTN/ISDN service evolution as following:

- Implementation of SSF function of the IN network in the control layer (using open interface INAP allows for treating the IN network elements as the elements of NGN service layer).
- Duplication/implementation of the service logic from PSTN/ISDN host in NGN service layer (application server - AS). Division of service logic from control.
- Inclusion of SCP of the IN network into NGN service layer - SSP-SCP communication through NGN IP packet network.
- Common SCE for all elements of NGN service layer - optional step.

For the separation of the service function during evolution of PSTN/ISDN, service process in local exchange can be transferred simply to a tandem exchange through data configuration. Only tandem exchanges are upgraded according to the above described steps. In this way, the collection of information at billing centre becomes simpler too, because all the services are converged at the tandem exchanges, only the information of tandem exchanges needs to be collected rather than that of all the local exchanges.

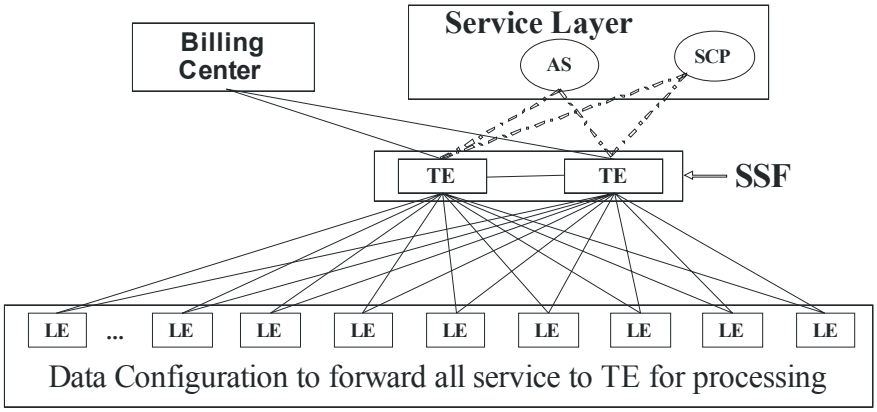


Figure I-1 – Service evolution from PSTN/ISDN to NGN

Appendix II

Examples of SCP being integrated to the Application Server

(This appendix does not form an integral part of this draft)

The following figure shows the SCP is integrated to the Application Server as a whole:

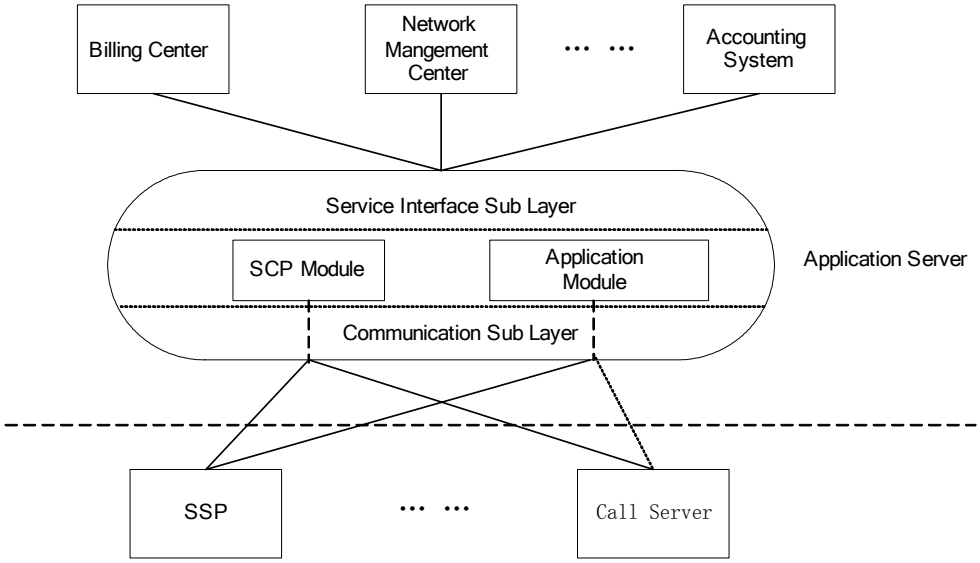


Figure I-2 – The SCP is integrated to the Application Server as a whole

In this networking mode, the SCP is integrated to the Application Server and becomes a part of the Application Server. The bottom layer of the new Application Server is established in a uniform communication layer. The services created by the SCE in the traditional IN can be directly loaded to the SCP module of the new Application Server. The new services developed by using open interfaces (such as Parlay APIs) can run on the Application module. The SCP module and the Application module have a uniform service interface layer with unified data configuration, operation & maintenance and external interfaces.

2.20 – PSTN/ISDN emulation and simulation*

Introduction

NGN Next Generation Network (NGN) is believed to provide new opportunities for and capabilities to the network and service providers. Considering that existing networks have different life span and vast amount of capital has been spent on them, complete replacement of their components is not considered to be either advisable or possible.

The PSTN/ISDN services are widely used and the end users are accustomed to it. NGN is expected to provide PSTN/ISDN-like services.

Since a completely simulated network may take considerable time to be implemented, then PSTN/ISDN emulation is needed. In this case the legacy terminals enjoy the ability of having identical services as those provided by PSTN/ISDN.

This draft addresses PSTN/ISDN emulation and simulation.

Table of Contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

2.20 – PSTN/ISDN emulation and simulation

1 Scope

The Public Switched Telephone Network/Integrated Services Digital Network (PSTN/ISDN) being one of the first telecommunication networks, is considered to be a prime candidate for evolution to Next Generation Network (NGN).

The PSTN/ISDN provides many features that a service provider can offer to the end-users. As such, when evolving to NGN, there is the expectation that all or at least some of these features may continue to be provided.

The PSTN/ISDN Emulation could potentially provide PSTN/ISDN service capabilities and interfaces and maintain the end-user experience unchanged irrespective of the changing of the core network.

PSTN/ISDN Simulation could potentially provide PSTN/ISDN-like service capabilities that fulfil the end-users need. However, there is no guarantee that PSTN/ISDN simulation can provide all features that have been available to the PSTN/ISDN user. Simulated PSTN/ISDN may provide additional new features and capabilities that have not been available to the users of PSTN/ISDN.

This draft describes PSTN/ISDN emulation and simulation.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this draft. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this draft are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this draft does not give it, as a stand-alone document, the status of a Recommendation.

[1] ITU-T Recommendation Y.1411 (2003), *ATM-MPLS network interworking – Cell mode user plane interworking*

[2] ITU-T Recommendation I.411 (1993), *ISDN user-network interfaces – reference configurations*

[3] ITU-T Recommendation I.413 (1993), *B-ISDN user-network interface*

[4] ITU-T Recommendation G.964 (2001), *V-interfaces at the digital local exchange (LE) – V5.1 interface (based on 2048 kbit/s) for the support of access network (AN)*

[5] ITU-T Recommendation G.965 (2001), *V-interfaces at the digital local exchange (LE) – V5.2 interface (based on 2048 kbit/s) for the support of access network (AN)*

[6] ITU-T Recommendation H.248 and its annexes, *Gateway control protocol*

[7] IETF RFC 2719 (1999), *Framework Architecture for Signalling Transport*

[8] IETF RFC 2960 (2000), *Stream Control Transmission Protocol*

[9] IETF RFC 3057 (2001), *ISDN Q.921-User Adaptation Layer*

[10] IETF RFC 3331 (2002), *Signalling System 7 (SS7) Message Transfer Part 2 (MTP2) – User Adaptation Layer*

[11] IETF RFC 3332 (2002), *Signalling System 7 (SS7) Message Transfer Part 3 (MTP3) – User Adaptation Layer (M3UA)*

[12] ITU-T Recommendation Q.761 (1999), Signalling System No. 7 – ISDN User Part functional description

[13] ITU-T Recommendation Q.762 (1999), Signalling System No. 7 – ISDN User Part general functions of messages and signals

[14] ITU-T Recommendation Q.763 (1999), Signalling System No. 7 – ISDN User Part formats and codes

[15] ITU-T Recommendation Q.764 (1999), Signalling System No. 7 – ISDN User Part signalling procedures

[16] ITU-T Recommendation Q.1912.5 (2004), Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part

[17] IETF RFC3261 (2002), SIP: Session Initiation Protocol

[18] ITU-T Recommendation Q.1901 (2000), Bearer independent call control protocol

[19] ITU-T Recommendation Q.1902.1 (2001), Bearer independent call control protocol (Capability Set 2): Functional description

[20] ITU-T Recommendation Q.1902.2 (2001), Bearer independent call control protocol (Capability Set 2) and signalling system No. 7 ISDN user part: General functions of messages and parameters

[21] ITU-T Recommendation Q.1902.3 (2001), Bearer independent call control protocol (Capability Set 2) and signalling system No. 7 ISDN user part: formats and codes

[22] ITU-T Recommendation Q.1902.4 (2001), Bearer independent call control protocol (Capability Set 2): Basic call procedures

[23] ITU-T Recommendation Q.1902.5 (2001), Bearer independent call control protocol (Capability Set 2): Exceptions to the application transport mechanism in the context of BICC

[24] ITU-T Recommendation Q.1902.6 (2001), Bearer independent call control protocol (Capability Set 2): Generic signalling procedures for the support of the ISDN user part supplementary services and for bearer redirection

[25] ITU-T Recommendation M.3400 (2000), TMN Management Functions

[26] ITU-T Recommendation M.3010 (2000), Principles for a Telecommunications management network

[27] ETSI specification TS 123 228 V6.6.0 (2004-06), IP multimedia Subsystem (IMS), stage 2, Release 6

3 Definitions

This draft uses or defines the following terms:

3.1 Interworking: See Recommendation Y.1411 [1]. For convenience the definition is repeated here: The term "interworking" is used to express interactions between networks, between end systems, or between

parts thereof, with the aim of providing a functional entity capable of supporting an end-to-end communication. The interactions required to provide a functional entity rely on functions and on the means to select these functions.

3.2 NGN-AG: An Access Gateway, which interfaces to IP Multimedia Component using SIP and providing PSTN/ISDN simulation services.

3.3 PSTN/ISDN Emulation: Provides PSTN/ISDN service capabilities and interfaces using adaptation to an IP infrastructure.

NOTE: Not all service capabilities and interfaces have to be present to provide an emulation.

3.4 PSTN/ISDN Simulation: Provides PSTN/ISDN-like service capabilities using session control over IP interfaces and infrastructure.

NOTE: This definition allows for the possibility of simulation providing a complete mapping of the PSTN / ISDN service set (complete simulation).

3.5 User equipment: A device or devices allowing a user access to network services. This term refers to a terminal (e.g. dedicated voice terminal or multipurpose personal computer) that is connected to an NGN, which may be through a user network or other devices.

NOTE: definition is based on Q.1741.3

4 Abbreviations

This draft uses the following abbreviations.

ADF	Adaptation Function
IF	Interface
IMS	IP multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Service Digital Network
ISUP	ISDN User Part
IW	Interworking
NGN	Next Generation Network
NNI	Network Node Interface
PABX	Private Automatic Branch Exchange
PSTN	Public Switching Telecommunications Network
SIP	Session Initiation Protocol
SS7	Signalling System No. 7
UNI	User Network Interface

5 Conventions

TBD.

6 Evolution of PSTN/ISDN to NGN

PSTN/ISDN offers a number of features and capabilities to the end-users. Thus, when evolving to NGN, there is the expectation that all or at least some of these features may continue to be provided.

6.1 PSTN/ISDN emulation and simulation

PSTN/ISDN emulation provides most of the existing PSTN/ISDN service capabilities and interfaces using adaptation to an IP infrastructure. Although PSTN/ISDN emulation standards support all PSTN/ISDN supplementary services, individual Carriers may choose to deploy PSTN/ISDN emulation with support for only a sub-set of PSTN/ISDN supplementary services.

PSTN/ISDN simulation could also provide PSTN/ISDN-like service capabilities that potentially fulfil the same end-user need as existing PSTN/ISDN services. However, there is no guarantee that PSTN/ISDN simulation would provide all features that have been available to the PSTN/ISDN user. In addition, simulated PSTN/ISDN may provide additional new features and capabilities that have not been available to the users of PSTN/ISDN.

Figure 6-1 provides a high level presentation of how emulation and simulation is performed and the relationship between different networks and NGN.

As shown in Figure 6-1, there are several ways that an user equipment can be connected to an NGN providing either emulation or simulation of PSTN/ISDN.

Pattern 1: In this case the legacy user equipment is connected to an NGN through an adaptation function (e.g. ADF2) at the network side of the UNI. This configuration is used to emulate PSTN/ISDN. In this case the legacy user equipment continues to be used.

Pattern 2: In this case the legacy user equipment is connected to an NGN through an adaptation function (e.g. ADF1) at the user side of the UNI. This configuration is used when there is a desire to use legacy user equipment while PSTN/ISDN is being simulated.

Pattern 3: In this case the NGN user equipment directly connects to NGN.

An example of this network structure based on these three classifications is provided in Appendix I.

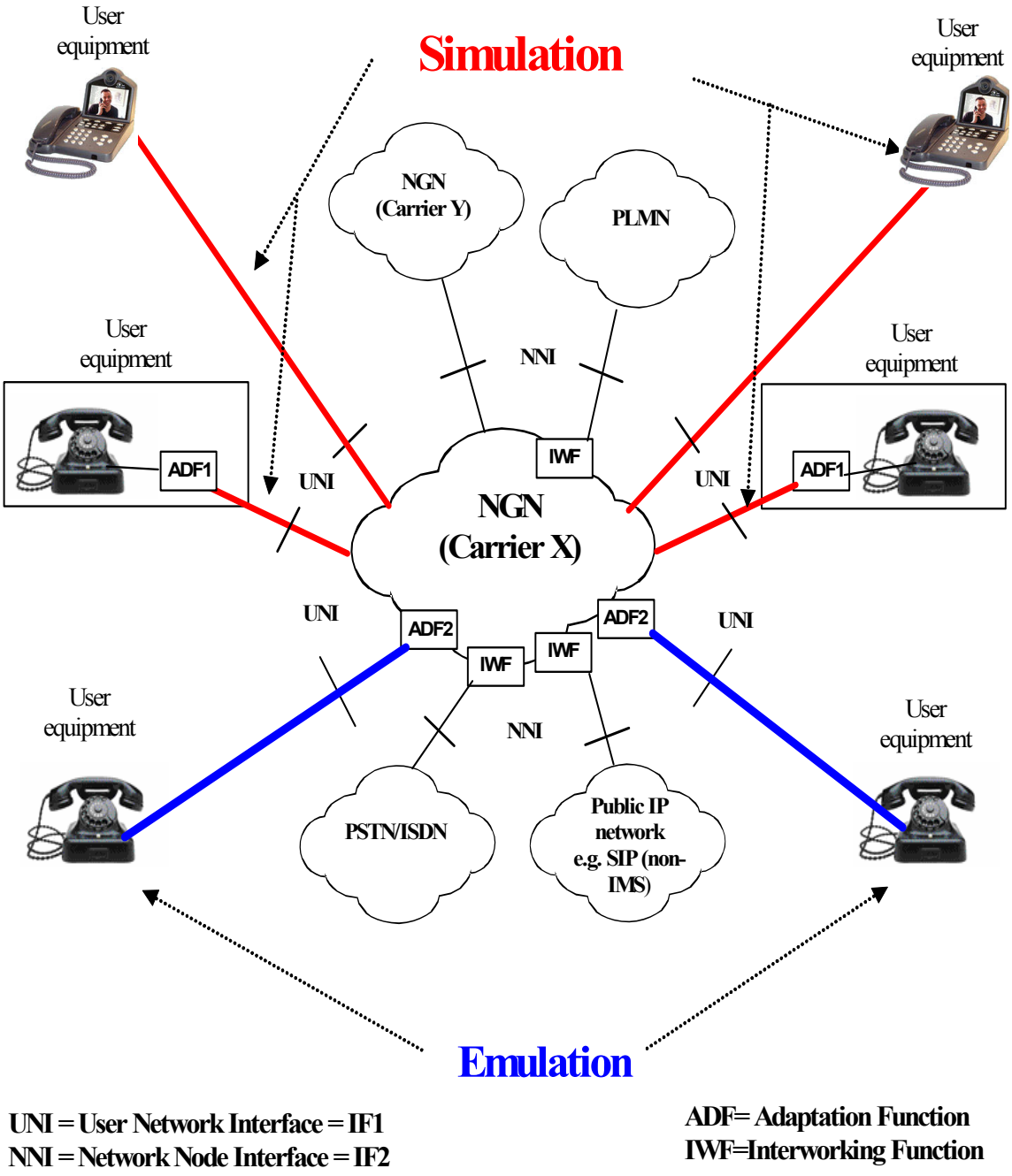


Figure 6-1 – Emulation, simulation, interoperability and interworking with NGN

6.2 Interfaces

In discussing PSTN/ISDN emulation and simulation several different networks are considered to accommodate both IMS-based and non-IMS-based scenarios. Two interfaces are to be dealt with. These are User Network Interface (UNI) and Network Node Interface (NNI). The following provides details for these interfaces.

Interface type 1, IF_1: This interface is between the user equipment and a network element in NGN which may also contain an adaptation function. This is a User Network Interface (UNI). It can be:

- Between an NGN user equipment and the NGN
- Between an IP user equipment and public IP network

- Analogue telephone interface between the legacy user equipment and PSTN/ISDN
- S, T or coincident S/T reference point for ISDN Basic Rate via a Network Termination 1 (NT1) [2]
- S_B, T_B or coincident S_B / T_B Reference Point for ISDN Primary Rate via a Network Termination 1 (NT1) [3]
- Access Networks using V5 signalling, PSTN interface provided according to national mappings, V5.1 [4] and V5.2 [5] interfaces for support of Access Network (AN)
- National variants of the above

Interface type 2, IF_2: This is a Network Node Interface (NNI). It can be between:

- NGNs
- An NGN and the PSTN/ISDN
- An NGN and a Public IP network.

6.3 Adaptations

Adaptation Function type 1 (ADF1): ADF1 allows the NGN to provide a full NGN account, including user and service profiles, to user equipment. From an NGN perspective, the user is receiving a normal NGN service that is essentially indistinguishable from any other NGN service. (As is the case with all NGN services, in practical implementations it is still subject to limitations of the user equipment).

Adaptation Function type 2 (ADF2): ADF2 allows the User Equipment to receive a standard PSTN/ISDN service, which is essentially indistinguishable from the PSTN/ISDN service provided by legacy technologies. From an NGN perspective, a "PSTN/ISDN emulation" service is being provided. In general, user and service profiles will not be associated with this account.

ADF1 and ADF2 can be implemented in gateways, and provide protocol and media translation / adaptation between a legacy user equipment and the NGN.

7 Aspects to consider

7.1 Transport

TBD

7.2 Signalling and control

7.2.1 Signalling for PSTN/ISDN emulation

The following examples of signalling protocols are used to show how PSTN/ISDN emulation is performed using call servers.

The H.248 protocol [6] is used by A-CS to control Access Gateway.

The SIGTRAN protocol [7 to 11] is used for interaction between B-CS and SG.

The ISUP protocol [12 to15] is used by SG for interworking between SG and PSTN/ISDN network.

The SIP-I protocol [16] is used by G-CS for interoperability between different PES domains.

The SIP protocol [17] is used by I-CS for interoperability between PES and IMS components.

The signalling used among A-CS, B-CS, G-CS and I-CS is the SIP-I or BICC [18 to 24] protocol.

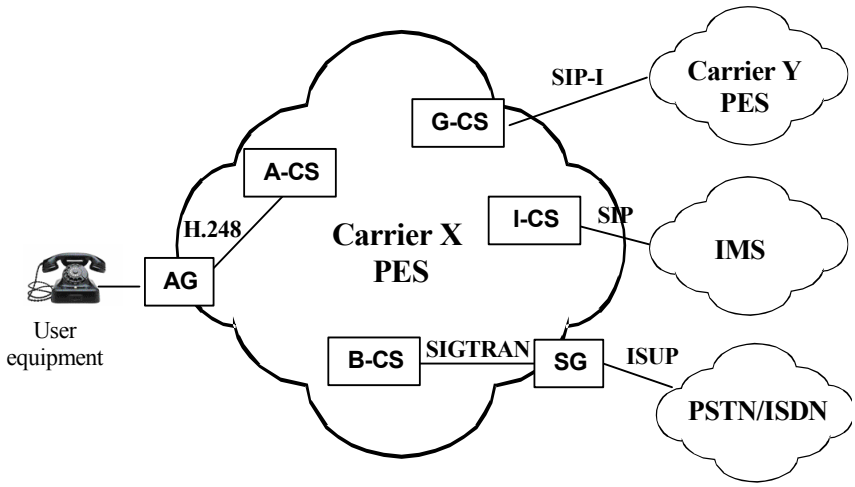


Figure 7-1 – Signalling for PSTN/ISDN emulation

7.2.2 Signalling for PSTN/ISDN simulation

The following examples of signalling protocols are used to show how PSTN/ISDN simulation is performed using SIP servers.

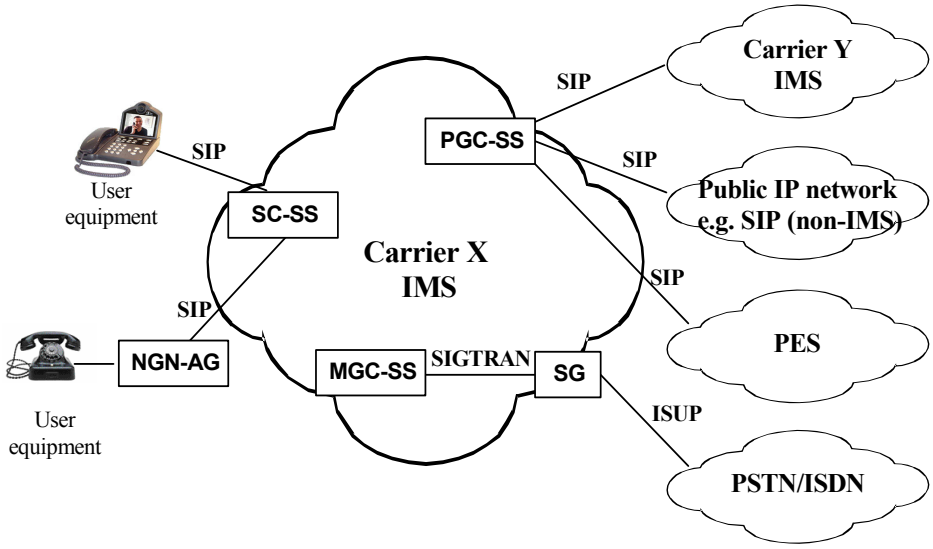


Figure 7-2 – Signalling for PSTN/ISDN simulation

In the figure, the SIP Server which is responsible for session control is named as Session Control SIP Server (SC-SS). The SIP Server which realizes interworking with PSTN/ISDN network is named as Media Gateway Control SIP Server (MGC-SS). The SIP Server which realizes interoperability with other NGN domains or other packet-based networks is named as Packet Gateway Control SIP Server (PGC-SS).

The SIP protocol is used by SC-SS to control NGN end system (e.g. SIP phone) or NGN-Access Gateway (e.g. SIP Access Gateway).

The SIGTRAN protocol is used for interaction between MGC-SS and SG.

The ISUP protocol is used by SG for interworking between SG and PSTN/ISDN network.

The SIP protocol is used by PGC-SS for interoperability between different IMS domains, or between IMS and PES components, or between IMS and other IP network.

The signalling used among SC-SS, MGC-SS and PGC-SS is SIP protocol.

7.3 Management

The management system of PSTN/ISDN includes exchange network management, access network management, intelligent network management and Operation Support System (OSS). Recommendations M.3400 [25] and M.3010 [26] provide management principles for PSTN/ISDN.

Referring to the management module defined in TMN, the NGN management system is comprised of three planes, namely the network element management plane, the network control plane and the service management plane. The three planes each implement corresponding management functions to each layer in the NGN layered model. Standard interfaces between these planes will be defined.

7.4 Services

In this clause both bearer and supplementary services are discussed. It is also anticipated that PSTN/ISDN emulation and simulation would support both narrowband and broadband services to the extent possible.

7.4.1 Bearer

ISDN bearer services are described and defined in I.230 series of Recommendations.

7.4.1.1 Emulation

NGN does not redefine any of the ISDN bearer services.

Although ISDN emulation supports all ISDN bearer services, individual Carriers may choose to deploy ISDN emulation which supports only a sub-set of ISDN bearer services.

7.4.1.2 Simulation

When ISDN simulation is performed, some of these services may be provided though the services themselves may not necessarily have the full functionality defined in the above referred-to service specifications.

NOTE: "Simulation" is said to be "based-on" PSTN/ISDN services in order to provide PSTN/ISDN-like services.

7.4.2 Supplementary

ISDN supplementary services as defined in I.250 series of Recommendations.

7.4.2.1 Emulation

NGN does not redefine any of the PSTN/ISDN supplementary services.

Although PSTN/ISDN emulation standards allow for support all PSTN/ISDN supplementary services, individual Carriers may choose to deploy PSTN/ISDN emulation which support only a sub-set of PSTN/ISDN supplementary services.

7.4.2.2 Simulation

When ISDN simulation is performed, some of these services may be provided though the services themselves may not necessarily have the full functionality defined in the above referred to service specifications.

In case of interworking of multiple networks, it is desirable to provide, as much as possible, affected supplementary services.

NOTE: "Simulation" is said to be "based-on" PSTN/ISDN services in order to provide PSTN/ISDN-like services.

Additional services, e.g. SIP based, may also be available.

7.5 Operation, administration and maintenance (OAM)

TBD

7.6 Resource allocation

TBD

7.7 Naming, numbering and addressing

TBD

7.8 Accounting, charging and billing

TBD

7.9 Interworking

TBD

8 Service requirements by national regulatory bodies

It is desirable that NGN provides:

- the basic telephone service with the same or better quality and availability as the existing PSTN/ISDN;
- the capability for accurate charging and accounting;
- capabilities to support number portability ;
- capability for the user to select the carrier for local and long-distance calls;
- the availability of directory inquiry service for PSTN/ISDN and the NGN users;
- support of Emergency Communications as stated in clause 14;
- support for all users, including the disabled. Support should provide at least the same capabilities as the existing PSTN/ISDN. NGN offers the opportunity for more advanced support, e.g. network capabilities for text to speech;
- privacy of user's information;
- mechanisms to support lawful interception and monitoring of various media types of communications such as voice, data, video, e-mail, messaging, etc. Such a mechanism may be required of a network provider for providing access to Content of Communication (CC) and Intercept Related Information (IRI) by Law Enforcement Agencies (LEA), to satisfy the requirements of administrations and International treaties;
- interoperability between NGN and e.g. PSTN and wireless telecommunication network.

The list of required services in public telecommunications systems in each country is based on national regulation. This document is not addressing detailed national regulatory requirement.

9 Emergency communications in NGN

It is desirable that NGN provides:

- capability to support priority mechanisms for Emergency Communications in multimedia services (e.g., voice, data, and video). Emergency communications includes: a) individual-to-authority communications, i.e., calls to emergency service providers; b) authority-to-authority communications; and c) authority-to-individual communications. Telecommunications for Disaster Relief (TDR) and Emergency Telecommunications Services (ETS) could be both authority-to-authority and authority-to-individual communications and community notification services could be authority-to-individual communications;
- support for calls to emergency service providers which may be free of charge for the calling user. Such calls must include information on how to enable emergency services to call back the calling user, and including at least the accurate location information about the calling user at the time of call initiation, e.g. to be provided to the emergency response centres, routing of the call to the Public Safety Answering Point (PSAP) – regardless of whether the user is fixed, mobile or nomadic. Accurate location may be such information as postal address, geographic coordinates or other information like cell indicators. Both network and user location information shall be provided, if available;
- the capability to ensure that calling line identification presentation (or the equivalent information in IMS) is not ruled out on a per call, per line or per identity basis for calls to the emergency call number;
- network integrity, as far as possible, in order to support critical communications such as TDR support in a crisis situation.

10 Security aspects of evolution

TBD

11 Emulation and simulation scenarios

11.1 Emulation

In this scenario, the core network of a traditional PSTN/ISDN is replaced with an NGN but the legacy user equipment remains unchanged. The legacy user equipments are connected to NGN using an adaptation function, identified here as ADF2. Adaptation is done after the UNI (i.e. IF1). Emulation should provide support for all PSTN/ISDN services. However, individual Carriers may choose to deploy PSTN/ISDN emulation with support for only a subset of PSTN/ISDN supplementary services.

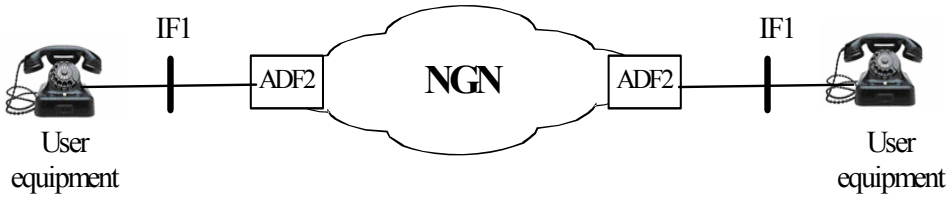


Figure 11-1 – PSTN/ISDN emulation

11.2 Simulation

All scenarios in this sub-clause are based on the IP Multimedia Sub-System (IMS) model with the addition of Core transit network. Originating/Terminating network and the Originating/Terminating Subscriber's home networks are called "visiting network" and "home network" in IMS terminology [27]. Description of all interfaces is provided in Annex A of this draft. Scenarios shown here are samples of what can be present. Depending on what network is present, other scenarios can be constructed.

The following scenarios could provide PSTN/ISDN-like service capabilities. Simulated PSTN/ISDN may provide additional new features and capabilities that have not been available to the users of PSTN/ISDN. However, there is no guarantee that all existing features available to the PSTN/ISDN end users would continue to be provided.

Scenario 1: All networks present

This is a scenario with all networks present.

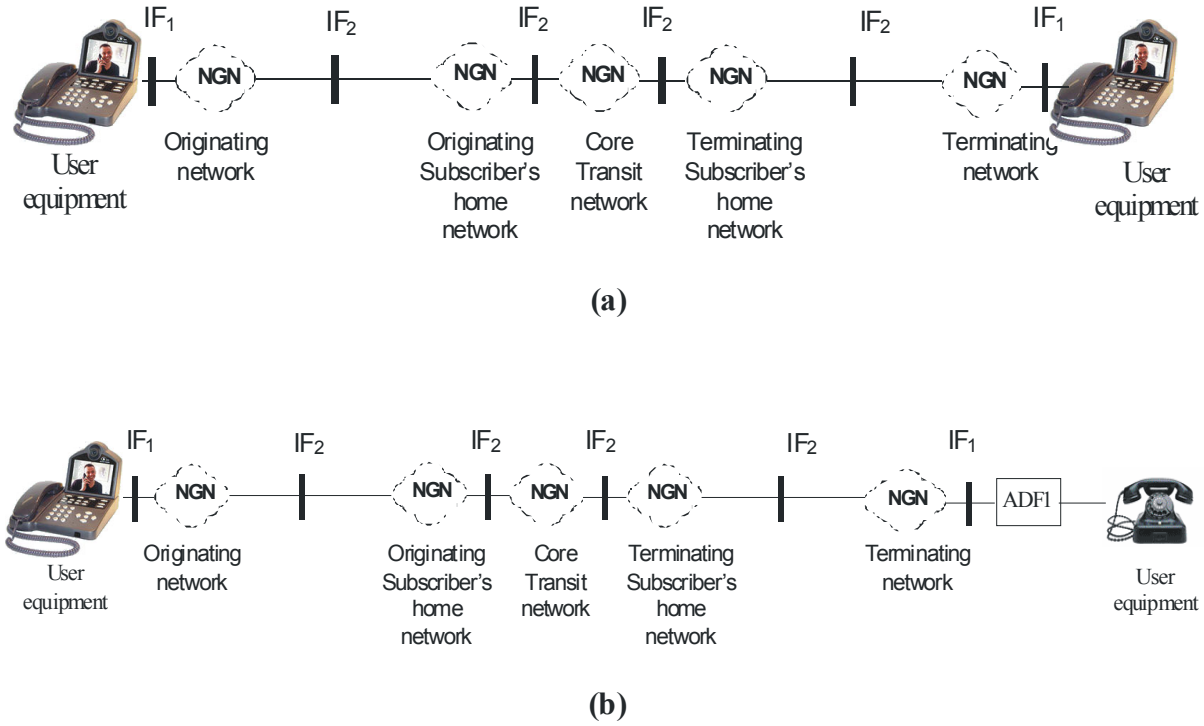
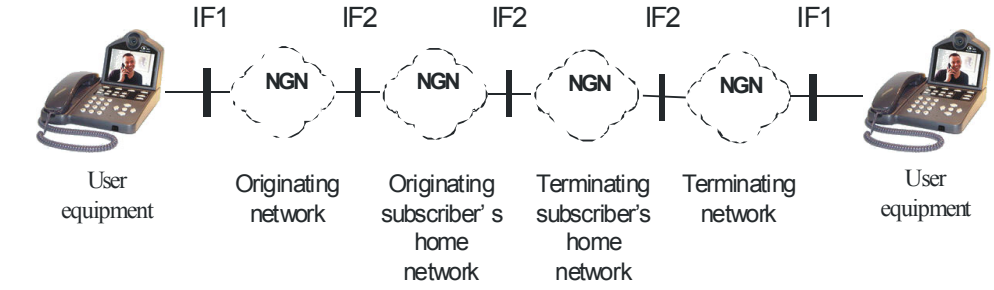


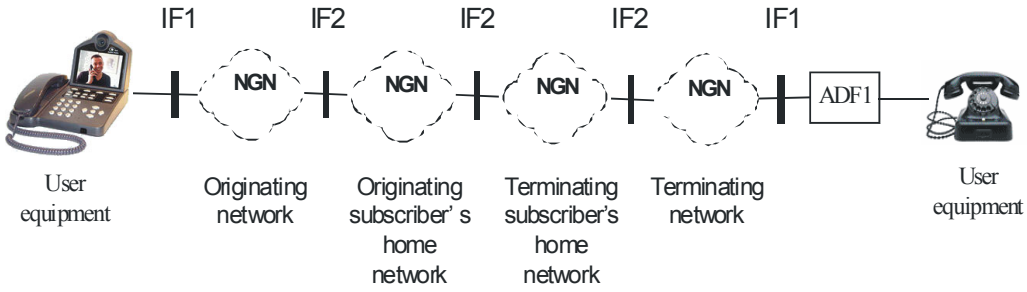
Figure 11-2 – PSTN/ISDN simulation-all networks present

Scenario 2: Core Transit network not present

This scenario is as the previous one less the Core Transit network. This scenario is identical to the IMS model.



(a)



(b)

Figure 11-3 – PSTN/ISDN simulation-Core Transit network not present

Scenario 3: Single network scenario

This is the simplest possible scenario in which there is only one network behaving as the Originating, Transit and Termination network.

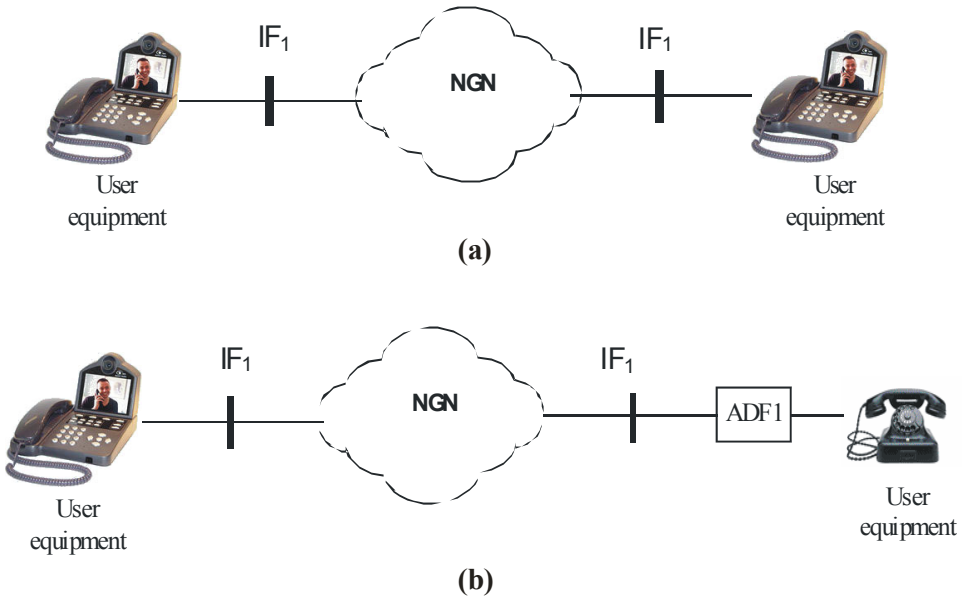
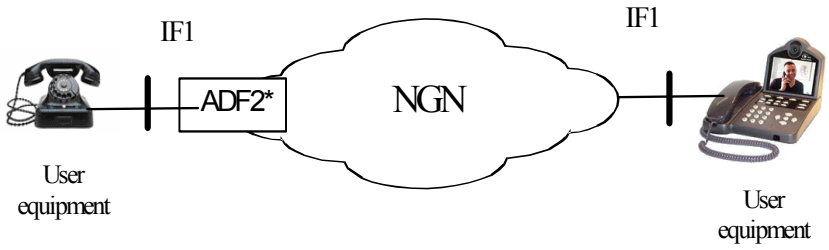


Figure 11-4 – PSTN/ISDN simulation-Originating and Terminating networks the same

11.3 Legacy and NGN user equipment connected through an NGN

This scenario presents a case in which one user equipment is a legacy while the other is an NGN user equipment. Other scenarios involving these user equipments are possible depending if the NGN is Core Transit, Terminating (Originating) or Terminating (Originating) Subscriber's home network or any combination of them. For the NGN user equipment only PSTN/ISDN – like services are supported. ADF2 provides mapping from PSTN/ISDN to NGN. Thus this scenario supports only PSTN/ISDN-like services.



* Note: For certain network services, ADF2 may provide some functionality normally associated with ADF1.

Figure 11-5 – Legacy and NGN end systems connected through an NGN

11.4 Scenarios involving interworking

Interworking occurs when there are two networks of different nature communicating with each other.

NGN and PSTN/ISDN – Scenario 1

In this scenario, one user equipment is NGN and the other is a legacy user equipment. The legacy user equipment is directly connected to PSTN/ISDN. Here PSTN/ISDN is mapped to NGN and vice versa. Considering that PTSN/ISDN simulation supports PSTN/ISDN-like services, therefore, this would be the limiting factor and only those PSTN/ISDN services are supported that can also be supported (or provided) by simulated PSTN/ISDN.

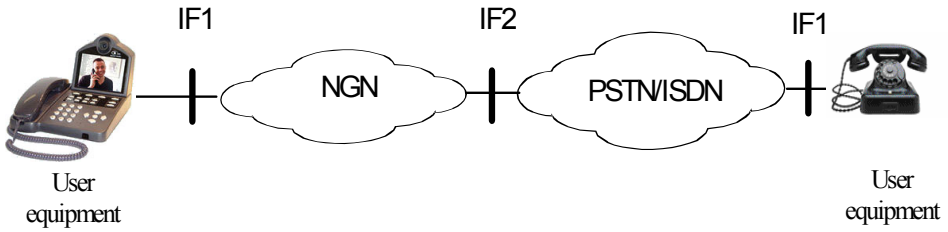


Figure 11-6 – PSTN/ISDN Interworking with NGN– Scenario 1

NGN and PSTN/ISDN – Scenario 2

In this scenario, the two legacy user equipments are at the two ends. However, one is connected directly to PSTN/ISDN and the other goes through an NGN via adaptation, i.e. ADF2. The NGN supports PSTN/ISDN emulation to support end-to-end PSTN/ISDN services.

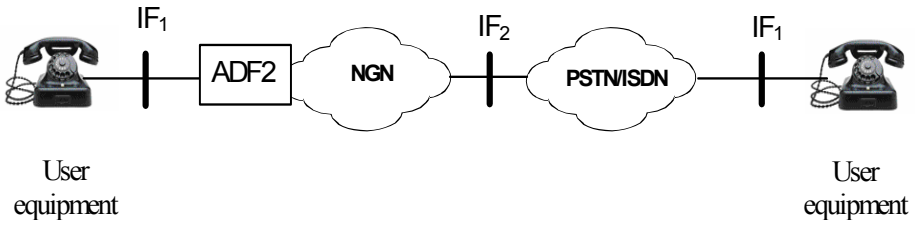


Figure 11-7 – Interworking between PSTN/ISDN and NGN –Scenario 2

NGN and Public IP network – Scenario 1

In this scenario, one end is an NGN user equipment and the other end is an IP user equipment going through a Public IP network. The Public IP network may be, but is not limited to, Internet and IP cable network. The NGN would support only PSTN/ISDN-like services. Services supported by Public IP network may be similar to NGN or may differ. Thus only services are supported which are similar in the two networks.

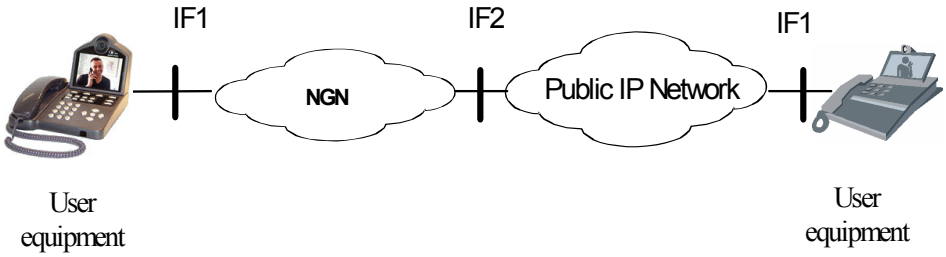


Figure 11-8 – NGN Interworking with Public IP Network – Scenario 1

NGN and Public IP network – Scenario 2

In this scenario, one end is a legacy user equipment going through an NGN through an adaptation function, and the other end is an IP user equipment going through a Public IP network. The Public IP network may be, but is not limited to, Internet and IP cable network. ADF2 provides mapping from PSTN/ISDN to NGN. The end-to-end service provided is PSTN/ISDN-like service. Services supported by Public IP network may be similar to NGN or may differ. Thus like in previous scenario only services which are similar in two networks can be supported.

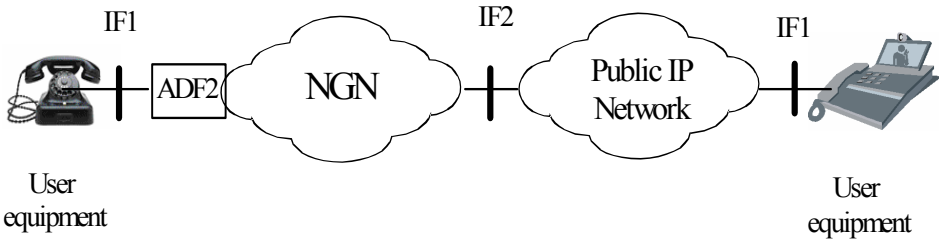


Figure 11-9 – NGN Interworking with Public IP Network – Scenario 2

Interworking between CS-based and IMS-Based NGN

This scenario describes the network evolution using both emulation and simulation. This can happen when an operator deploys an IMS-based network and another operator uses CS-based emulation. There is a need for interworking between the CS-based and IMS-based networks. This is possible by SIP, but this is beyond the scope of this document.

11.5 Emulation and simulation scenarios involving customer networks

In this scenario an NGN customer network connects directly to an NGN via a Type 1 interface (IF1).

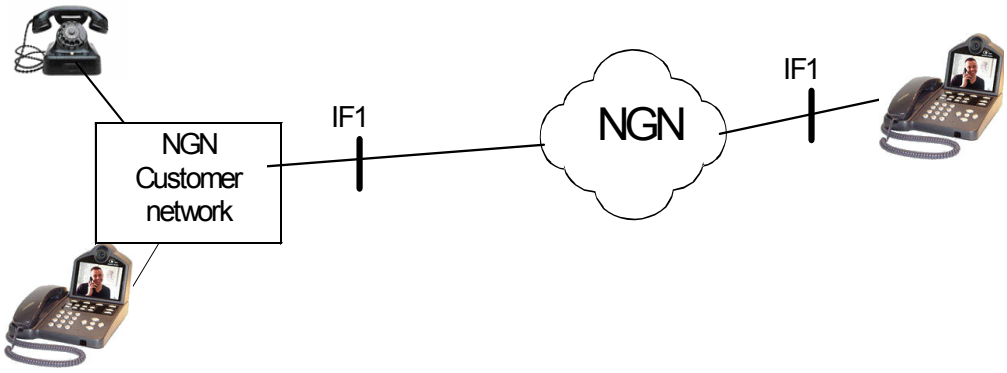


Figure 11-10 – An NGN customer network connected to an NGN

Appendix I – Examples of emulation and simulation network structure

I.1 Examples of emulation and simulation network structure

Examples of network structures based on the above classifications will now be given. Including the following descriptions in the document will facilitate easier understanding between emulation and simulation network structures.

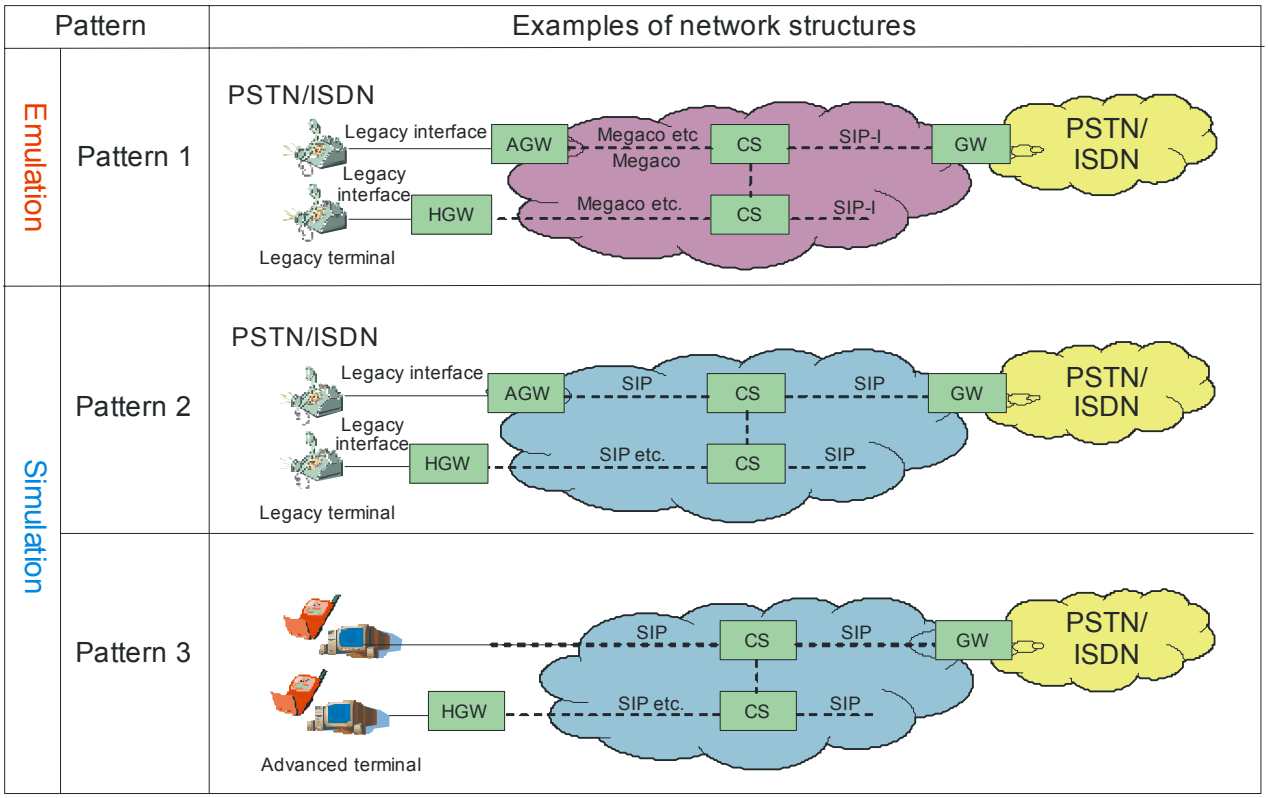


Figure I-1 – Examples of emulation and simulation network structures

I.2 Basic connection patterns

The basic connection patterns are determined based on Emulation/Simulation and whether or not there is interworking with PSTN/ISDN. In the case that they are first divided into category A or B according to whether interworking with PSTN/ISDN or not, the basic connection patterns are classified as follows.

Category A

In the category A, NGN connects all terminals directly.

- Pattern A-1: NGN connects all terminals using emulation.
- Pattern A-2: NGN connects all terminals using simulation.
- Pattern A-3: NGN connects some terminals using emulation and others using simulation.

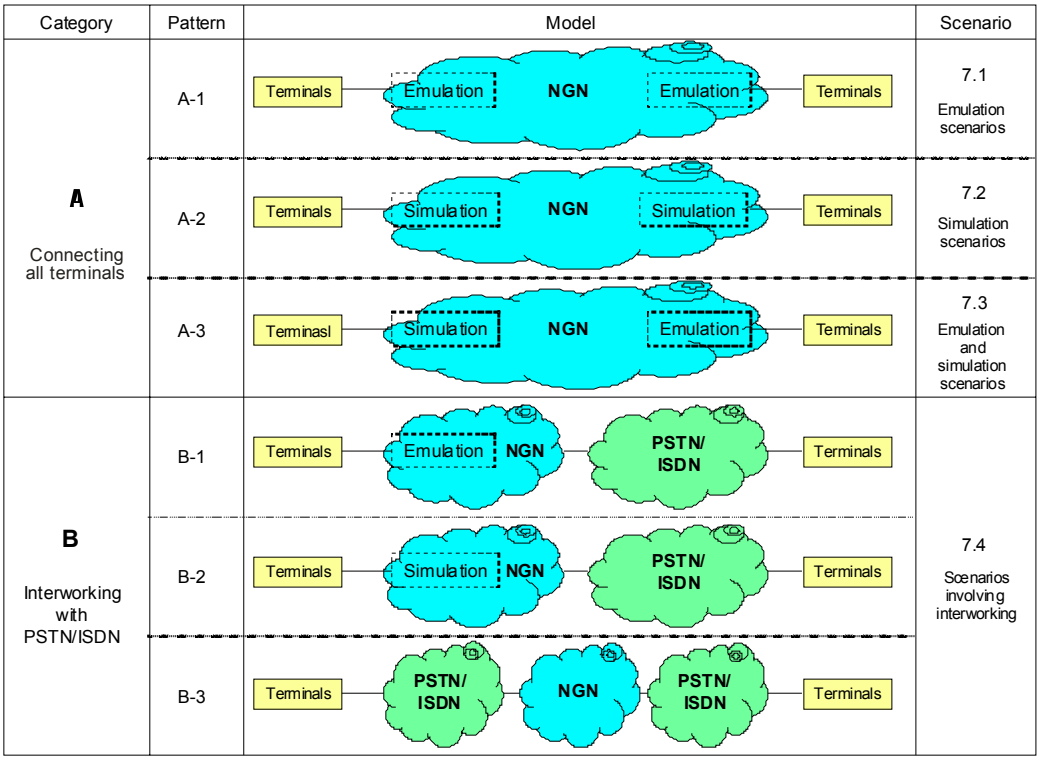


Figure I-2 – The basic connection patterns

Category B

In the category B, NGN interworks with PSTN/ISDN.

- Pattern B-1: NGN connects some terminals using emulation, and interworks with PSTN/ISDN.
- Pattern B-2: NGN connects some terminals using simulation, and interworks with PSTN/ISDN.
- Pattern B-3: NGN interworks with two different PSTN/ISDNs.

SECTION 3

BEYOND RELEASE 1 DELIVERABLES

WORKING GROUP 2
DELIVERABLES

FUNCTIONAL ARCHITECTURE AND MOBILITY

3.1 Softrouter requirements (*Status D*)

3.2 Converged services framework functional requirements and architecture (*Status D*)

3.1 – Softrouter requirements*

Introduction

The routing architecture platform of next generation networks should provide great flexibility and capabilities in terms of managing and operating the network. Traditionally, a networking device can be split along three dimensions/planes that provide distinct services: management plane, control plane and the data/forwarding plane. The management plane has typically been seen as a logically separate entity and has been developed as such, while the forwarding plane and control plane are usually tightly integrated with the communication between the data plane and control plane done over a proprietary API. We can evolve today's networks into more flexible next generation networks if we are able to eliminate the tight integration of the control plane and the data plane and instead use a standard API for communication between the two planes. Note that with this mechanism one can continue to build a networking device that has the control plane and the data plane tightly integrated into a single device. The difference, however, is that the communication between the two planes is now done over the standard interface. The flexibility provided by such as interface is quite enormous in terms of extending the capabilities of a device. One can now use any third party applications or one can develop their own application and execute them on a server and communicate with the device over the standard interface. A similar philosophy has already been accepted in the telephony world in the form of the softswitch network architecture. A similar case, in terms of benefits, can be made if we apply this philosophy to the data world.

Dis-aggregation of a traditional network element such as a router encompasses the following three aspects: (1) Decoupling of the complex control plane processing functions from the data plane or forwarding plane functions (2) Execution of control plane functions on dedicated, external, reliable and scalable control plane servers and (3) Standard communication interface between the control plane servers and the forwarding plane elements.

Traditionally, the control plane functionality is executed over general-purpose processors while the data-plane/fast-path functionality is based on ASICs or network processors. Providing a standard set of communication interfaces with various elements inside the networking element enables each entity to evolve independently, while providing many other benefits of the architecture such as improved control plane scalability, reliability and security.

* Status D: The FGNGN considers that this deliverable is not yet mature, requiring discussion and technical input to complete development.

Table of contents

3.1 – Softrouter requirements

1 Scope

The scope of this document is to provide general requirements for the various entities involved in a softrouter-based network architecture. Specifically, it describes requirements on the functionality and architecture of various entities and the interface (protocol) requirements among the various entities.

2 References

[1] IETF RFC 3654 - Requirements for Separation of IP Control and Forwarding

3 Related Work

There is an effort at the IETF ForCES working group to define a framework and associated mechanisms for standardizing the exchange of information between the logically separate functionality of the control plane and the forwarding plane. The main focus of the working group is related to forwarding and control elements that are in very close proximity to each other (in the same room or even co-located).

However, since the effort at the IETF is very limited – narrowly focuses on the communication interface standardization – the effort here is to expand the scope to consider it from the network architecture perspective and determine the possibilities of realizing new, more reliable, more flexible and more secure networks; while utilizing the standard communication interface between the control plane and the forwarding plane.

4 Abbreviations and Acronyms

The definitions made in this paragraph are derived from the definitions in [1] but differ in meaning and scope.

AE: **Addressable Entity** – A physical entity that is directly addressable using some methodology such as IP, MAC etc.

CE: **Control Element** – The CE is a logical entity providing layer 3 control functionality for the purpose of packet forwarding. A CE controls one or multiple FEs belonging to the same NE. A CE is associated with exactly one NE. However, an NE may have one or more CEs. A CE may consist of multiple, distributed, redundant sub-components (PCEs) to implement the control functionality.

FE: **Forwarding Element** – The FE is a logical entity providing layer 3 packet forwarding functionality. An FE can only be associated with exactly one NE at a given point of time. The FE's control may be migrated to a different CE, if needed. An FE must be able to process protocols for communication with its CE and for FE discovery. An FE may utilize fractional, whole or multiple PFEs. IP TTL and IP options may be modified on a per FE granularity.

NE: **Network Element** – The NE is a logical entity performing the traditional layer 3 routing functionality according to [1]. It consists of one or more CEs and FEs. FEs and CEs of the same NE may be

separated by multiple hops. IP TTL and IP options may be modified on a per FE granularity. This means that the data plane sees a NE as multiple hops whereas the control plane sees a NE as a single hop.

PCE: **Physical Control Element** – A hardware platform that implements layer 3 router control functions. A PCE may host partial CEs (CE sub-components) or multiple CEs.

PFE: **Physical Forwarding Element** – A hardware platform that implements layer 3 packet forwarding functionality. A PFE may host multiple FEs but not partial FEs.

External Link: External links are layer 3 packet-forwarding links that leave the packet-forwarding plane of an NE to connect with neighboring NEs. In other words, enternal links are Inter-NE links.

Internal Link: Internal links are layer 3 packet-forwarding links that interconnect FEs of the same NE. In other words, the internal links are Intra-NE links. The link between FEs and CE are not considered internal links.

Control Link: Control links interconnect CEs with FEs. Direct control links connect CEs with FEs without any intermediate FEs or NEs. Indirect control links span intermediate FEs and NEs.

Pre-Association Phase: Period of time during which the CE and FE discover each other's existence and attempt to bind themselves. It includes the determination of which CE and which FE can be part of a given NE (This, obviously, is preceded by the determination of which PCEs/PFEs are part of a given CE/FE).

Post-Association Phase: Period of time during which FEs and CEs know their mutual bindings and establish communication over a protocol.

5 Overview

The softrouter architecture logically breaks independent entities into separate network elements and provides a standard communication interface between these elements. The softrouter NE mainly comprises of the control element and the forwarding element along with their respective interconnection links and protocols. The CE is responsible for the control plane functionalities such as routing protocols, signaling protocols etc. in addition to controlling the forwarding element itself. The FE is responsible for packet processing and handling. The CE controls the FE by suitably manipulating various resources on the FE – e.g. forwarding table entries, NAT tables, filter tables etc. In general the CE dictates the packet forwarding behavior by such table manipulations, while the FE acts or applies the policies on the packets as dictated by the CE.

In addition to the functional entities such as CE and FE, the NE comprises of three types of distinct links that interconnect the entities. These are the control links, internal links and external links. Control links interconnect the CEs with the FEs and only control traffic flows over it. Internal links interconnect FEs to other FEs within the same NE and are used for internal packet forwarding between FEs. Finally, external links are those which are exposed to the external world, and which connect to other NEs.

A conceptual network architecture is depicted in Fig. 1, which shows the data network completely made up of softrouter elements. Note however that the architecture doesn't require Greenfield networks for deployment. One should be able to deploy the softrouter architecture elements within existing data networks.

From the network perspective, we need the capability of deploying softrouter elements within the network that can be geographically or logically distributed but can still be viewed as a single network entity. The ability to control forwarding elements that are geographically distributed provides for a very flexible architecture. However, this very requirement adds additional complexity to the overall solution since it would require a mechanism to discover these elements.

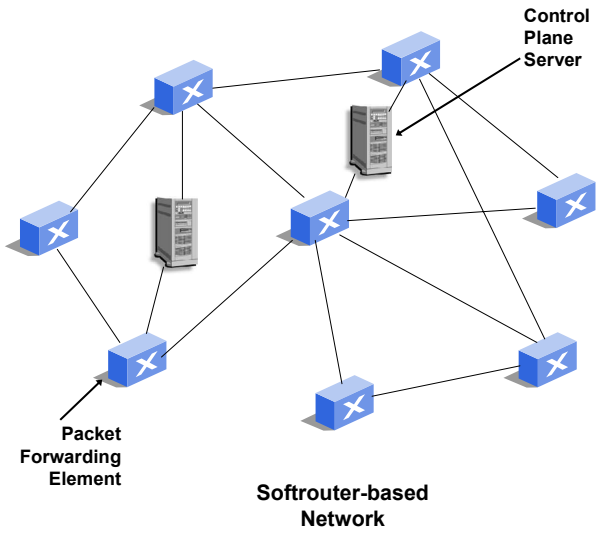


Figure 1 – Network architecture using Softrouters

When the CEs and FEs are separated by multi-hops from each other, routing a control packet from the CE to the FE itself becomes an issue – because intermediate elements of the network between the CE and FE may not necessarily be under the control of this particular CE. Once the respective elements have been discovered and routing protocols started, routing control packets over multiple hops will not be an issue. It is possible to solve the multi-hop scenario using a discovery mechanism that operates independently of the routing protocols. This discovery mechanism needs to be operated on all elements – i.e. CE as well as FE.

6 Requirements

6.1 NE Architecture Requirements

- Collection of PCEs (CEs) and PFEs (FEs) that may be geographically distributed should have the ability to be logically assembled together to function as a single network element as seen from the network's perspective.
- There should be no hop limitation between the CEs and the FEs.
- The CEs must be able to make use of a physically or logically separate signaling network, if one exists, by ensuring all control plane messages traverse this signaling network only.
- Every element should have the capability to operate the discovery protocol.
- The elements should be able to be interconnected using any underlying technology such as Ethernet, ATM etc.
- The packets enter an NE on external links of one FE and may leave the NE on the same or another external link of the same or other FEs within the NE. In other words, a packet may travel zero or more internal links before leaving the NE. [The architecture must allow for the ability of a packet to traverse multiple FEs before leaving the NE.]
- The architecture must prevent unauthorized elements from joining the NE. An unauthorized CE should not be allowed to control any FEs nor should an authorized CE allow any unauthorized FEs to join the NE.
- The architecture should allow the CEs and FEs to join and leave the NE dynamically.

- The NE should have the capability to support hundreds of FEs and one or more CEs.
- The NE should be able to support all traditional protocols.

6.2 CE Specific Requirements

- The PCE can either be co-located or physically separated from the PFEs. It can operate as an independent server.
- CE should have the capability to execute all control plane protocols.
- There must be a mechanism for the CE to query system resources on the FE.
- The architecture should support a mechanism for the CE to obtain the interconnected FE topology. Further, there should be no restrictions on the way the FEs are interconnected or how many FEs may be connected within a given NE.
- Individual protocols may be optimized in this architecture to improve performance, reliability and security. A CE to CE protocol may be used for this purpose.

6.3 FE specific Requirements

- An FE should only accept control messages from its own set of CEs that have authority to control it. Any messages from a CE outside this set should be discarded.
- FEs must support a minimal set of capabilities such as link status detection, resource discovery etc. that are necessary for establishing network connectivity.
- The FE must support monitoring and error reporting capabilities. Any change in the system resources such as unavailability of interfaces, line cards etc. should be reported back to the CE asynchronously.
- The FEs must be able to redirect protocol packets received from the peers. It should allow the CE to configure filters to perform such packet redirection. It should have the ability to deliver packets generated by the CE on all or specific interfaces.

6.4 Discovery and Intra-NE protocol Requirements

- The elements should have the ability to discover each other. In other words, the FEs should have the ability to discover who their respective CEs are and the CE should have the ability to discover all FEs that it has the authority to control.
- Determining the explicit set of which CE controls which FE can either be done through configuration or by some other mechanism. What is important is that at the time of discovery, this information should be available for the elements to couple with each other.
- The discovery protocol may have multiple components to it – one of which may be to enable routing packets from a CE to a particular FE and vice-versa. This routing of packets may be hop-by-hop, if need be (i.e. not necessarily using the fast path, but each hop receiving the message and determining the next hop to send to).
- The architecture should have support for discovering the inter-FE or intra-NE topology – needed for determining appropriate route paths for packets traversing the NE.
- The intra-NE path traversal of the packet should be tolerant to internal link failures. In other words, it should be possible for the packet to be routed through an alternative internal path, if one exists.
- The ability to dynamically determine a failure and update the path would require some form of routing protocol within the NE, which may be distinct from the routing protocols such as OSPF running between NEs.

6.5 CE-FE Interface Protocol Requirements

- The model should allow a CE to determine the capabilities and resources of an FE in a given NE. The CE should have the ability to control and manage these FE capabilities through configuration.
- The protocol between the FE and the CE (here-after called the FE-CE protocol) should support event-notification and query/response mechanism. The event notification is an event-driven message that is used to asynchronously report changes in system capabilities – e.g. an interface going up or down on the FE should immediately be reported to the CE. Further, the CE should have the ability to query any status or statistical information from the FE.
- The FE-CE protocol should be able to operate in a multi-hop environment, wherein the CE and the FE are separated from each other by more than one layer three hops. This feature allows architectural flexibility in terms of using geographically dispersed elements organized to operate as a single NE.
- The FE-CE protocol should have the ability to communicate securely.
  - It should be able to repel man-in-the-middle or impersonation attacks
  - It should have the ability to throttle messaging over the control channel to prevent DoS attacks
  - Ability to verify/authenticate configuration message before they are applied to the elements.
  - Ability to configure FEs to filter attack packets. The CE itself can do this configuration, or in the case where the control channel is already flooded with attack packets such that no control packets from the CE reach the FE, there must be mechanism to install filters on the FE directly (off-band).
- The FE-CE protocol should provide a means for expressing message priority
- The FE-CE protocol should have the ability to handle hundreds of FEs in a given NE. This implies that the protocol on the CE will have hundreds of termination points and should be able to address each channel to a specific FE separately.
- The FE-CE protocol should support various levels of reliability in delivering messages
  - Mission critical message such as configuration messages (e.g. updating the FIB, filter etc.) from the CE to the FE, or change in system resource message reported from the FE to the CE should be handled with a very high degree of reliability.
  - Messages such as heartbeat messages may not require strict reliability – where timeliness is more important than reliability.
  - In the case of multi-hop scenario, transport layers such as TCP or reliable UDP may be employed for message delivery.
  - In care where the protocol is operating in a non-IP environment such as Ethernet, switch-fabric etc., and care should be taken to provide the necessary reliability that is not supported by the underlying technology.
- The FE-CE protocol should be operable over any interconnect technology – i.e. independence from the underlying data-link technology used.

6.6 Failover and Redundancy Requirements

- The architecture must support fail-over mechanisms for the CE. In other words, if a primary CE of the NE fails, the control functionality of the NE should be transferred to a secondary CE. The FEs should be able to accept configuration commands from the secondary CE, after they deem that the primary CE has failed.
- A mechanism to determine CE/FE failure should exist. This can be using heartbeat or keep-alive messages between the FE and the CE that indicates that the respective elements are functioning properly.

6.7 Security Requirements

- Both the CE and the FE should support authentication, authorization and other such security mechanisms to enable secure communication.

6.8 Management Requirements

- Standard management tools should be allowed to query the CEs and FEs to determine their current state. However, the management tools should not be allowed to directly control the configuration parameters of the FEs. The CE should handle FE configuration.

7 Security Considerations

<to be added>

3.2 – Converged services framework functional requirements and architecture*

Abstract

'Converged Services', namely those multimedia services accessible to users through what appears to be a unified network infrastructure, in a seamless fashion, are fundamental to the success of Next Generation Networks (NGN). To address this capability, the 'Converged Services Framework (CSF)' work item was created at the FGNGN #4 meeting. This is the third draft version of the 'Converged Services Framework' output document generated at the final FGNGN #9 meeting. This document is ready for transmittal to parent Study Group 13 for further consideration. A list of items for further study is identified below where contributions are invited.

The TR-CSF is a stage 2 document with the objective to define the functional architecture, requirements, and logical interfaces associated with the CSF. The work on this TR-CSF has progressed well in FGNGN; however, further work is required for its completion in Release 2. The following steps are recommended towards its completion:

1) Further development of the CSF requirements and functional architecture.

2) Mapping of CSF functions to NGN functional architecture and identifying enhancements.

3) Development of additional use case scenarios.

4) Identification of logical interfaces and protocols.

With the completion of the above stage 2 work on CSF, the TR-CSF would form the basis for the development of the Stage 3 protocol work. The appropriate groups for the development of stage 3 protocol would then be identified, based on the stage 2 requirements.

NOTE – Within the document there are several Editors notes that identify areas/issues that need to be addressed via contributions.

Summary

This document contains the output draft of "NGN Release 2 Converged Services Framework Functional Requirements and Architecture" after the 9th and the final meeting of FGNGN held at Gatwick, London (14-17 November 2005). As agreed during the meeting, the input document FGNGN-ID-01197, submitted by the co-editors, to this meeting was used as baseline for the production of this version.

Input Documents considered for this draft during this meeting are shown in the table below:

* Status D: The FGNGN considers that this deliverable is not yet mature, requiring discussion and technical input to complete development.

Table of Contents

3.2 – Converged services framework functional requirements and architecture

1 Scope

The objective of the NGN Release 2 'Converged Services Framework' (CSF) work item is to define the functional architecture, requirements, and logical interfaces associated with the CSF. The CSF takes into account backward compatibility with legacy terminals, networks and services where possible. Through CSF, legacy equipment will continue functioning in an NGN and the behaviour of new generations of NGN-compatible equipment will be ensured to operate in legacy networks.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Specification. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Specification are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ITU-T Recommendation Y.2011 (2004), 'General principles and general reference model for Next Generation Networks'

[2] ITU-T FGNGN-OD-00223 'Draft FGNGN-FRA Version 6.3'

[3] CableLabs' PacketCable Multimedia specification 'PacketCable™ Multimedia Specification PKT-SP-MM-I02-040930'

3 Definitions and terms

3.1 Definitions

[Editors' Note] Further review is requested of these definitions and contributions are invited.

Session-based services: A network controlled session is established before the content is transferred. In general, session based services are peer-to-peer communications, broadcast and multicast type communications. Examples of the session based services are not limited to, conversational services, interactive videophone, etc.

Non-Session based Services: There is no network controlled session established before the content is transferred. In general, non-session based services are of short duration (in terms of connection). Examples of the non-session based services, not limited to, instant messaging, WAP-push, Web services. In the Web service case, even though there is session established (e.g., TCP sessions) between the end points, there is no network controlled session and hence it is designed as non-session based services.

3.2 Terms

This document defines the following terms:

CC-FE Convergence Coordination Functional Entity

NS-FE Network Support Functional Entity

ES-FE Edge Support Functional Entity

CLS-FE Client Support Functional Entity

4 Acronyms

This document uses the following acronyms:

AM (PCMM) Application Manager

AS (IMS) Application Server

CC-FE Convergence Coordination Functional Entity

CLS-FE Client Support Functional Entity

CSF Converged Service Framework

ES-FE Edge Support Functional Entity

FE Functional Entity

FRA Functional Requirements and Architecture

HSS (IMS) Home Subscriber Server

iFC initial Filter Criteria

IMS IP Multimedia Subsystem

ISC IMS Service Control

ISDN Integrated Services Digital Network

NGN Next-Generation Network

NS-FE Network Support Functional Entity

OMA Open Mobile Alliance

OSA Open Service Access

OSE OMA Service Environment

OSI Open Systems Interconnection

PCMM PacketCable Multimedia

PS (PCMM) Policy Server

PSTN Public Switched Telephone Network

RKS (PacketCable) Record Keeping Server

SIP Session Initiation Protocol

SLF (IMS) Subscription Locator Function

SPT (IMS) Service Point Trigger

SUP-FE Subscriber User Profile Functional Entity

UE User Equipment

5 Overview and high-level requirements

5.1 Introduction

The separation of functions across different layers has been one of the foundations of networking. While the principles propounded by the OSI 7 layer model still apply in the context of NGN, its top three layers are interpreted in specific ways to accommodate the characteristics of an NGN environment, specifically by defining the NGN application and service control entities as part of the NGN Service Stratum [1]:

[Editors' Note] The following definition of "NGN service stratum" was originally taken from [1], however, in the context of CSF it was modified via contributions. Therefore, this definition needs to be revisited for Release 2. This issue needs to be addressed via contributions.

"NGN service stratum: That part of the NGN which provides the user functions that transfer service-related data and the functions that control and manage service resources and network services to enable user services and applications. User services may be implemented by a recursion of multiple service nodes within the service stratum. The NGN service stratum is concerned with the multiplicity of media and services to be operated between peer entities. For example, services may be related to voice, data or video applications, arranged separately or in some combination in the case of multimedia applications. From an architectural perspective, each application in the service stratum is considered to have its own user, control and management planes."

One of the fundamental requirements of NGN is the ability to deliver a wide variety of services directed to a user across a wide variety of transport networks with possibly different service deployment schemes.

The main goal of the 'Converged Service Framework' (CSF) is to provide a framework that would enable application providers to provide services that operate smoothly and consistently when crossing the boundaries of multiple access and core networks. To enable this, the framework should support features common to converged applications. These include tracking the user identity, state and profile, device identity, state and profile, session state, and location, across multiple networks.

Another key element of the CSF is that it will allow advanced services to reach into legacy networks.

5.2 High-level requirements

[Editors' Note] The following high-level requirements were introduced at the FGNGN#9 meeting. Due to time constraints these high-level requirements did not get a thorough review during the meeting. These contributions require further detailed review and contributions are invited.

The following high-level requirements are applicable to the CSF:

1) Shall function across various transport and control networks.
2) Shall enable end-users to access their services regardless of their current location, active device, or the access network in which they are registered.
3) Should operate over access networks and NGN domains that are not administered by the CSF provider.

4) Shall enable delivery of services to the end user without end-user intervention.

5) Shall enable the creation and operation of access network-independent applications.

6) Shall enable the collection, of subscriber and service related information about a user from service networks, access networks, devices and applications, subject to privacy and security considerations.

7) Shall enable the aggregation of subscriber and service related information about a particular user across multiple networks, devices and applications.

8) Shall enable the distribution of aggregated subscriber and service related information about a user to a service network, access network, device or application, subject to privacy and security considerations.

9) Shall respond to service requests by end users or applications with responses that consider the aggregated information about a user and his/her state (e.g., multiple networks, devices, applications).

10) Shall provide network-specific, application-specific or device-specific translated service requests on behalf of a received service request to allow an end user or network-agnostic application to achieve 'converged' behaviour.

11) Shall support identity management and support data and usage privacy for the subscribers.

12) Shall support session management, including hand-over of an in-progress session from one device to another device, and from one type of network to another type of network.

13) Shall provide controlled access to network resources when the business agreement permits, regardless in what network the resource resides.

14) Shall support deployment of applications across multiple networks.

15) Shall support both carrier specific and third party applications.

16) Shall support management of subscriber profile, location, presence, availability, preference and service subscription information that spans different networks and devices, subject to privacy and security considerations.

17) Shall provide controlled access information from services enablers (such as Presence, Availability, Location, registration status, QoS options, media resources, billing) irrespective of the access network, server, and device to create enhanced integrated services on a per-user basis.

18) Shall support policy management of IMS, Packet Cable and other networks.

19) Shall support Digital Rights Management and allow service providers to enable DRM when sharing content across multiple devices owned by the same user, across multiple access networks, and across multiple identities of the same user.

20) Shall support the use of network adapters which allow information to be delivered across an API between systems using different data formats and protocols.

21) Shall support access to the IMS and its services from a public or private WiFi Access Point.

22) Shall support access to the IMS and its services from a public landline broadband access network (cable or DSL).

23) Shall support access to the IMS services from non-3GPP access networks.

24) Shall support enhanced services that receive triggers from the underlying networks.

25) Shall enable converged end user service features such as Single Bill, Single Number (or Find-Me-Follow-Me), Shared Number with Family members, Single Voice Mail Box.

6 CSF functional architecture

[Editors' note] To assist in the future development of the CSF functional architecture a list of items is identified for further study on which contributions are invited. This list is contained as Appendix D, at the end of the document.

The CSF-based NGN architecture is based on the functional elements described below. The functions may be implemented in a distributed manner through the interaction of multiple functional entities.

6.1 CSF functional elements

Convergence Coordination Functional Entity (CC-FE): Provides convergence of: user identities, device, and service ownership, session management, and resource capabilities. It takes input from service provider and operator databases, manually entered profile information, and/or from the Network, Edge, and Client support functions described below. CC-FE should support coordination control for multiply invoked services in a single or multiple configurations**.**

The CC-FE resides within the Service Stratum of Release 1. The CC-FE is responsive to the following sub-elements within the Service Stratum:

– The Application functions

– The Service / User / Profile functions

– The Service and Control functions

The CC-FE is also responsive to components within the Terminal Functions.

Network Support Functional Entity (NS-FE): Provides session, access and rights information to the coordination function. The NS-FE is responsive to the following sub-elements located within the Transport Stratum:

– The Transport User / Device Profile functions

– The Transport Control and Monitoring functions

– The Media Handling functions

– The Gateway functions

NS-FE should support media service control for multiply invoked media resources in a single or multiple configurations.

Edge Support Functional Entity (ES-FE): This function interfaces to some combination of the access networks and the customer networks. It provides session, resource and identity information about itself and devices subtending it to the CC-FE. The ES-FE is responsive to the following sub-elements located within the Transport Stratum:

– Network Attachment Control functions

– The Access functions

– The Terminal functions

Client Support Functional Entity (CLS-FE): This function resides in end user clients. It provides session, resource and identity information about itself and the user to the CC-FE. The CLS-FE is responsive to components of the End User Functions shown in Figure 1. CLS-FE should support priority based service execution when multiple services are invoked in parallel, and support multiple interfaces with multiple services in a single or multiple configurations.

6.2 CSF functional components and logical interfaces

Figure 1 highlights the logical interfaces among the CSF functional entities and between CSF and the converged services/applications (AS-FE).

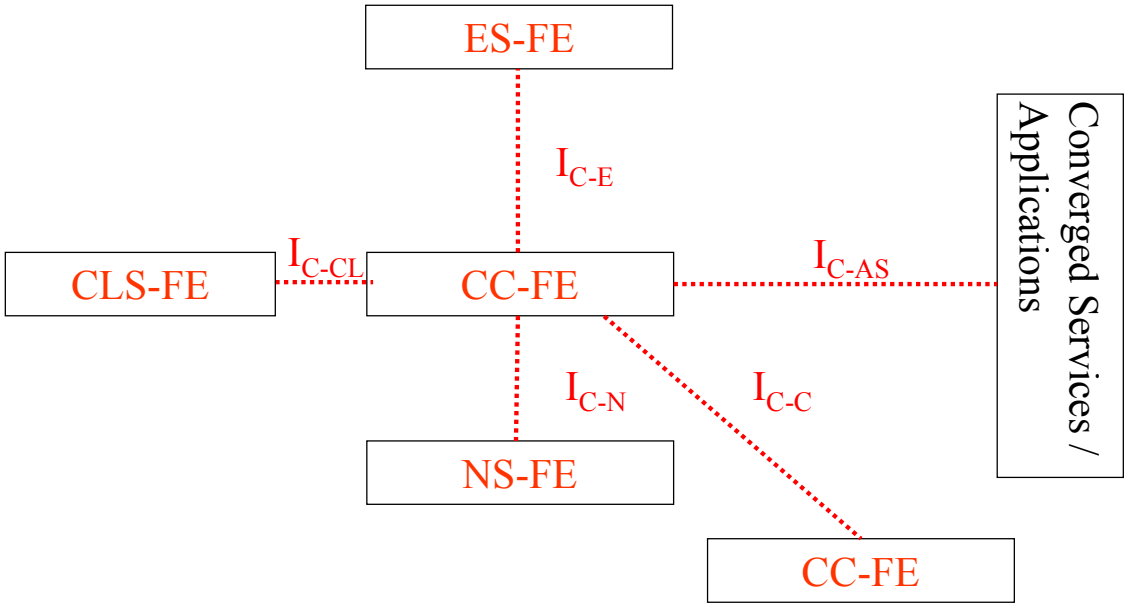


Figure 1 – Logical interfaces among the CSF functional entities

With reference to Figure 1:

i) The CC-FE, providing convergence of (at least): user identities, device, access and service ownership, session control, and resource capabilities, has logical interfaces with the other CSF sub-elements and other CC-FEs.

The CC-FE act as protocol termination point for the following logical interfaces:

- I_{C-AS}, with respect to an Application Server FE (AS-FE). This interface should provide a communication path between the application server and the CSF. Some candidate protocols for this interface are, for instance, Parlay X and SIP
- I_{C-CL}, with respect to the CSF Client Support Function (CLS-FE). This interface should provide a communication path between the end-user device and the CC-FE.
- I_{C-N}, with respect to the CSF Network Support Function (NS-FE). This interface should provide a communication path between a supporting underlying network and the CC-FE.
- I_{C-E}, with respect to the CSF Edge Support Function (ES-FE). This interface should provide a communication path between a supporting edge device or network and the CC-FE. Edge devices are those network components on the logical boundary between a customer premise and access network, and may have joint administration.

– I_{C-C}, the interface between CC-FEs in different locations. [Editors' Note] Ic-c interface needs to be described in more detail to understand its purpose. Contributions are invited.

ii) The NS-FE, providing session, access and rights information to the CC-FE

The NS-FE act as protocol termination point for the following logical interfaces:

– I_{C-N} as previously described

– Interfaces with the network in which the NS-FE is embedded

iii) The ES-FE, providing session, access and rights information to the CC-FE

The ES-FE act as protocol termination point for the following logical interfaces:

– I_{C-E} as previously defined

– Interfaces with the networks in which the ES-FE-enabled device is resident (e.g., UPnP in the LAN)

iv) The CLS-FE, providing session and state information to the CC-FE.

The CLS-FE act as protocol termination point for the following logical interfaces:

– I_{C-CL} as previously defined

– Interfaces with the devices with which the CLS-FE-enabled device is associated

6.3 CSF policy mechanism

[Editors' Note] The following high-level view of policy mechanism was introduced at the FGNGN#9 meeting. Contributions are invited for further development of this section.

This section provides the requirements for CSF policy mechanism to manage and coordinate converged services. The following figure provides the high-level view of policy mechanism.

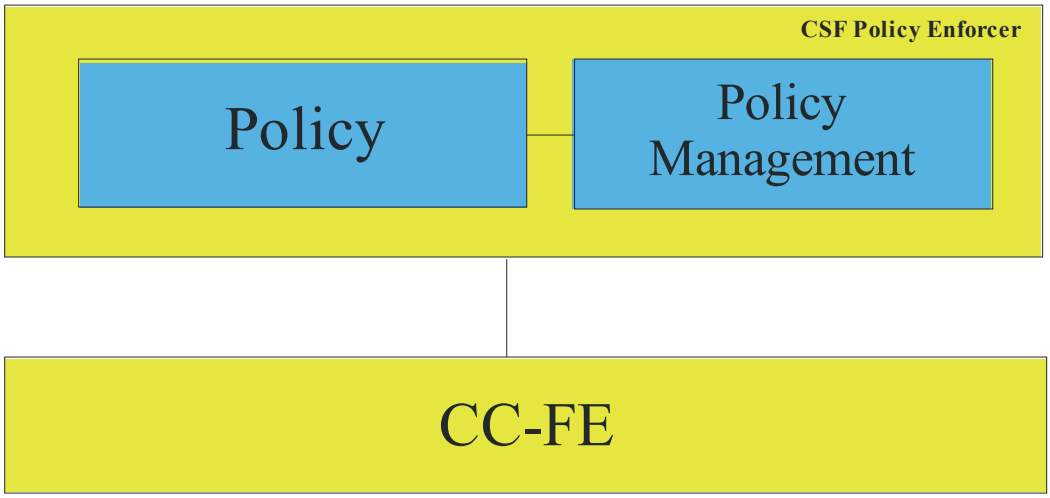


Figure 2 – CSF Policy mechanism

Policy: this function is responsible for policy access, policy condition matching and corresponding policy execution according to matched condition.

Policy Management: this function provides the functions of describing, creating, updating, deleting, provisioning and viewing of policies.

7 Context

7.1 Relationship to FGNGN FRA

Along with a new architecture [2], Next Generation Networks will bring an additional level of complexity over existing networks. The addition of support for multiple access technologies and for mobility results in the need to support a wide variety of network configurations. From the service viewpoint, NGN will support a wide variety of session-based and non-session-based services.

Session-based services can include SIP-based services (e.g., conversational services, interactive videophone), as well as non SIP-based services (video streaming and broadcasting, for instance).

Non session-based services can include SIP-based services (e.g., presence and instant messaging) as well as non SIP-based services (e.g., WAP-push, Web Services).

Moreover, NGN standards provide support for PSTN/ISDN replacement (i.e., PSTN/ISDN emulation). To provide support for all these services, several functions in both service stratum and transport stratum are needed.

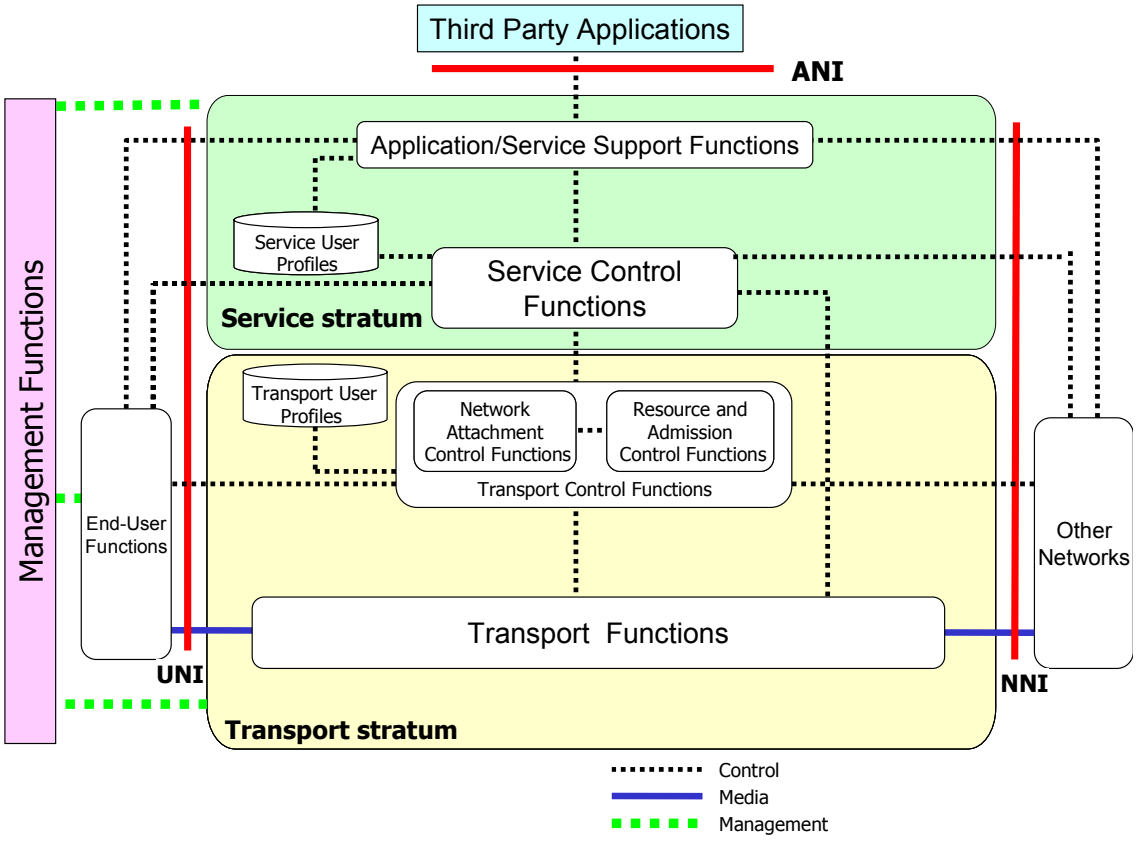


Figure 3 – The NGN architecture overview (FRA release 1)

Figure 3 shows the NGN architectural overview (as agreed in WG2 at the time of writing in reference [2]). The CSF is largely located in the Service Stratum, with Support Functions reaching into the Transport Stratum in certain cases.

The ambition of NGN Release 2 is to specify and engineer an 'overlay' system, amenable to inter-working with existing end-to-end solutions, whether they are legacy ones (cellular, Packet Cable, etc.) or IMS-based ones.

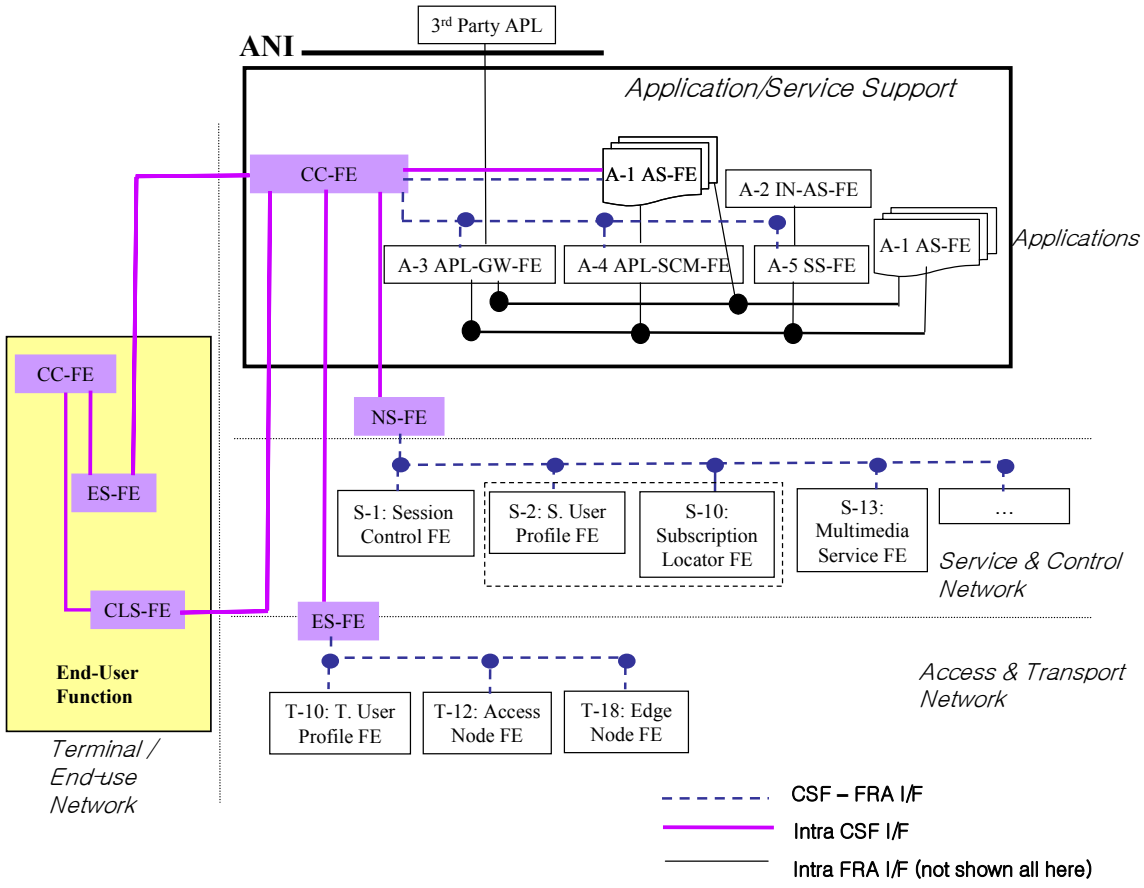


Figure 4 – The CSF relationship to FRA

In the Figure 4, three interfaces are identified. The thick line represents interfaces between CSF FEs (Intra CSF interfaces). The dotted line shows interfaces between CSF and FRA FEs. The solid lines are interfaces between FRA FEs, whose interconnections are not all shown here.

As described in Section 6, the CSF is made up of one or more convergence coordination functional entities (CC-FE), as well as supporting functional entities in the network support functional entity (NS-FE), edge support functional entity (ES-FE) and the end devices for client support functional (CLS-FE).

It should be noted that the CC-FE may be co-located with a support functional entity, such as the NS-FE. It should further be noted that other than the CC-FE, not all FEs need be present for operation. For example, CSF function may be implemented entirely in an operator's infrastructure through the use of CC-FEs and NS-FEs, and without ES-FEs or CLS-FEs.

Figure 4 depicts the high-level abstraction of the more detailed functional architecture for NGN from the FRA document [2]. The co-existence of CSF components, which consists of four Functional Entities (Convergence Coordination – CC, Network Support – NS, Edge Support – ES, and Client Support – CLS), on (with) the FRA functional architecture is shown as purple boxes in the figure. Connections among CSF components are shown with pink lines. The transport functions in green are expected to be of interest, but not communicate with the CC-FE directly.

[Editors' Note] The transport functions of interest to CSF are for further study.

Application Functions:

A1-Application Server FE: An Application Server is a functional entity that provides the intelligence for a user-level service. An AS-FE communicates with a CC-FE in a manner similar to how an AS-FE communicates with an Application Gateway AGW-FE. An AS-FE contacts a CC-FE when enacting a service on behalf of a user, to determine the user capability and state across (and independent of) the multiple access networks or devices available to the user.

A2-Application Gateway FE: The AGW-FE is an intermediary between the Application Server and Service Control FE. The AGW-FE is analogous in some respects to the CC-FE. In particular, it may sit logically between an AS-FE and an SC-FE or MS-FE. The CC-FE interacts with the AGW-FE in its communications with the "3rd party application providers" block for obtaining input from service provider and operator databases external to the NGN.

Service Functions:

S1-Session Control FE: The SC-FE is responsible for enabling access of end devices to application servers. The SC-FE should include an NS-FE behaviour to push information / respond to requests for information to a CC-FE. In particular, the SC-FE/NS-FE should provide the following categories of information to a trusted CC-FE:

- Notification of triggers related to previously specified users or devices
- Parameters related to sessions that are in progress
- Notification of user / device registration status
- Addressing, location information for devices known to be associated with a specified user

S2-User Profile FE: The SUP-FE is a database function that maintains user profile, device profile, presence, subscription, and location information for an administrative domain. The SUP-FE should include an NS-FE behaviour responsive to a CC-FE, providing access to its content according to its own rules of access privileges / trust. The NS-FE should filter its data prior to transmission to the CC-FE according to these rules. Conditioned upon establishment of trust, the NS-FE should also accept and store SUP-FE related information from a CC-FE as a proxy for a user or user device.

S13-Multimedia Service FE: The Multimedia Service FE is the non-session based equivalent of S1, the Session Control FE. It should include an NS-FE behaviour similar to that in S1 accordingly.

S3-Authentication & Authorization FE: It is expected that a CSF component may need to establish its identity and authority to access or provide information when communicating with a foreign administrative domain.

Transport Functions:

It is assumed that the transport functions are responsive to components in the service and control layers. As such, the CSF structure would not communicate directly with these components, but would get information from them through the service and control FEs described above.

Some of the transport functions of interest to the CSF are (these are for further study):

- Traffic Measurement FE
- Others FFS

7.2 Converged service description

Converged service can be defined as a service presented by inter-working or integrating component services, in a single or multiple configurations of the NGN functional architecture [2], to various types of terminals attached to various types of access networks, each with its own restrictions and capabilities.

The classification of the converged service type is possible in several ways and one is based on the functional architecture point of view:

– Type 1: converged service in a single configuration (e.g., IP Multimedia Component)

– Type 2: converged service over multiple configurations (e.g., IP Multimedia Component + Streaming Service Component)

– Type 3: converged service over multiple configurations and other networks (e.g., IP Multimedia Component + Internet service)

Figure 5 shows the three types of converged services.

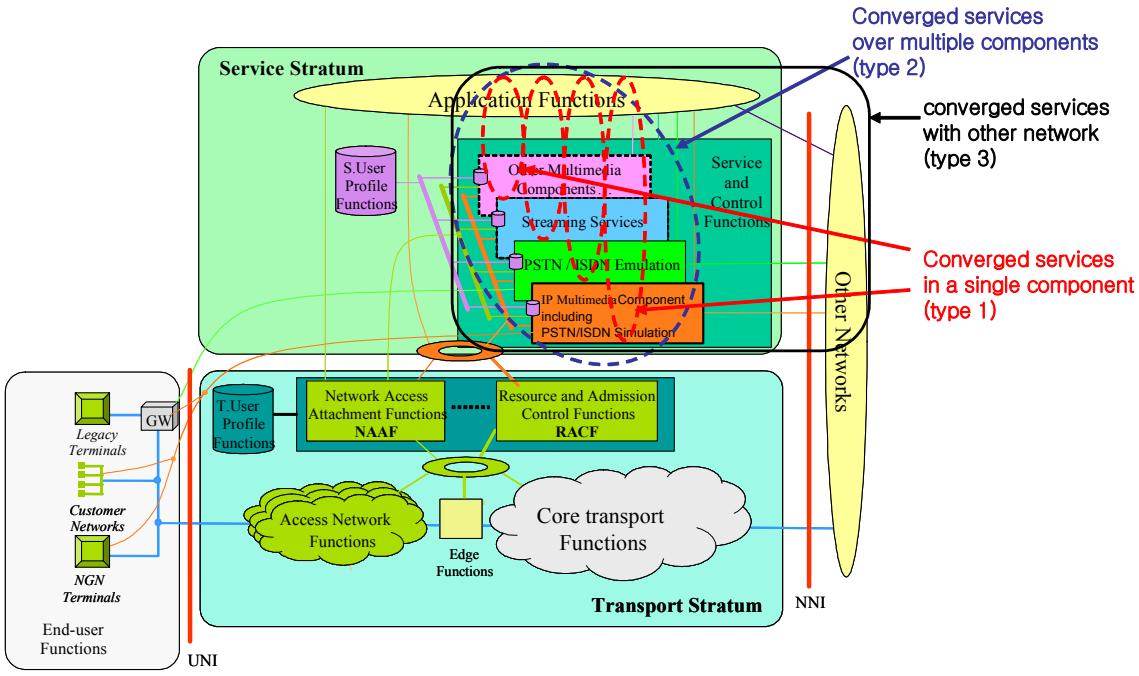


Figure 5 – Converged services types

Other typical classification is as follows according to the convergence of different types of media or access network heterogeneity:

– Voice and data converged service

– Fixed and mobile converged service

– Broadcast and communication converged service

It is useful to show the converged service examples in each type.

Examples for Type 1 converged services are described in Appendix C.1 and Appendix A.2.

Examples for Type 2 converged services are shown in Appendix C.2, C.3 and Appendix A.3.

Example for Type 3 converged service are illustrated in Appendix C.4.

Appendix A

CSF use cases

This appendix includes example use cases to highlight the functionality of the CSF.

[Editors' Note] Contributions are invited on these use cases and additional uses for inclusion.

A.1 Call Forwarding – Instant Messenger converged service

This use case shows that the converged service aggregates two types of services: a Call forwarding service and an Instant Messenger service. For this, a Call Forwarding service and an Instant Messenger service need to be registered with the CC-FE, a mobile station needs to have dual mode, such as GSM and WLAN, and a user may subscribe to this converged service, in advance. The converged service may be performed by informing the Instant Messenger service of the call status from Call Forwarding service.

Figure A.1 shows how the CC-FE coordinates the two services when the called party subscriber is busy. The purpose of this scenario is that messenger buddies can come to know that they cannot communicate with the subscriber because he is busy.

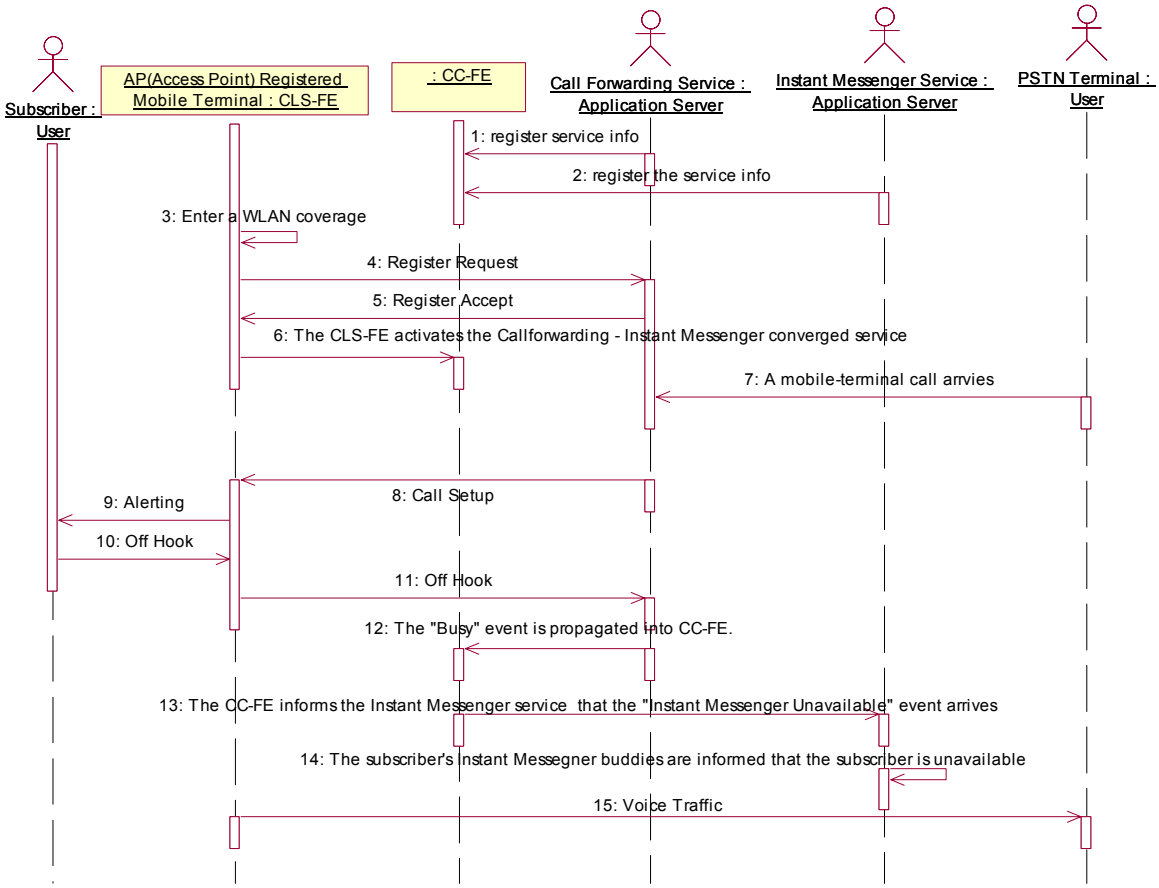


Figure A.1 – Call Forwarding – Instant Messenger Converged service use case

1) The Call Forwarding service Application Server needs to be registered with the CC-FE.

2) The Instant Messenger service Application Server needs to be registered with the CC-FE.

3) The mobile terminal(registered in the AP) enters a WLAN coverage

4) The mobile terminal sends the registration request message to the Call Forwarding service Application Server.

5) The Call Forwarding service Application Server responds to the mobile terminal.

6) The CLS-FE activates a converged service

7) A PSTN user initiates a call to the mobile terminal in the WLAN.

8) The Call Forwarding service Application Server initiates call setup.

9) The mobile terminal alerts.

10) The subscriber responds to the call.

11) The "Off Hook" event is informed of the Call Forwarding service Application Server.

12) The "Busy" event is informed of the CC-FE. And then the CC-FE generates an "Instant Messenger Unavailable" event based on the "Busy" event.

13) The CC-FE notifies the "Instant Messenger Unavailable" event to the Instant Messenger service Application Server.

14) The subscriber's Instant Messenger buddies are informed that the subscriber is unavailable

15) The call between the subscriber and the PSTN terminal user is established.

A.2 Call Forwarding -Video Conferencing converged service

This use case shows a converged service which coordinates a Call Forwarding service and a Video Conferencing service. When the subscriber starts the Video Conferencing service, her/his terminal state changes to busy. At this time, if there are other incoming calls, they need to be automatically forwarded to an alternate terminal, and Figure A.2 shows the case.

The flow is as follows:

1) The Video Conferencing service Application Server is registered with the CC-FE.

2) The Call Forwarding service Application Server is registered with the CC-FE.

3) The subscriber selects a Video Conferencing service in the CLS-FE.

4) The CLS-FE requests a coordination service.

5) The subscriber requests the Video Conferencing service.

6) The CC-FE is informed about the subscriber's "Video Conferencing active" status from the Video Conferencing service Application Server.

7) The CC-FE informs the Call Forwarding service Application Server that the subscriber is busy.

8) Any Incoming call is now forwarded to an alternative terminal by the Call Forwarding service Application Server.

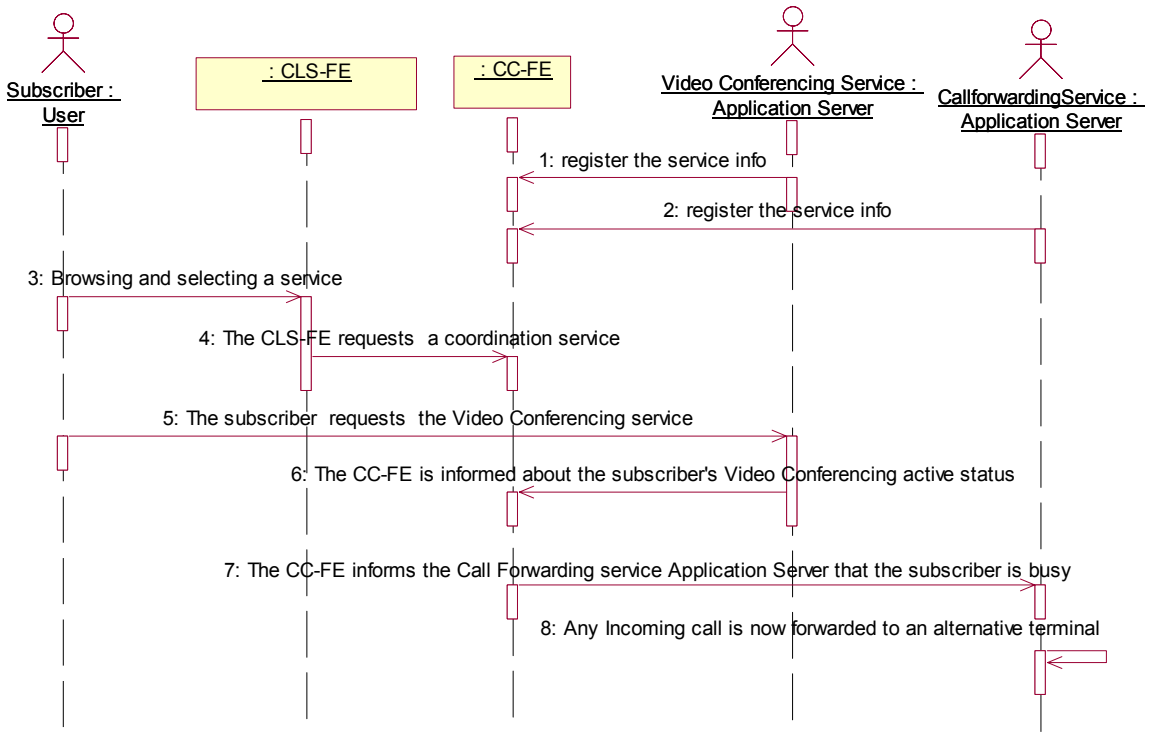


Figure A.2 – Call Forwarding – Video Conferencing converged service use case

A.3 Movement of conference call from a fixed client to mobile client

To provide service continuity across administrative domains it is necessary to provide a service coordination network entity (e.g., a CC-FE) that is aware of the user's state and can facilitate the joint operation of a user's session across these administrative boundaries. An example of service elements in need of coordination is the user's available resources and device states on both sides of the two, or more, administrative domains. The service coordination network entity is responsive to service requests from either the fixed network or mobile network

The following presents a use case scenario in which a User, Bob, is in a video conference call with another person ("Caller"). He decides to leave his location but wishes to continue his conversation on his mobile handset without interruption. Bob is able to push a button on his mobile phone and have the audio portion of the call move to his mobile phone automatically.

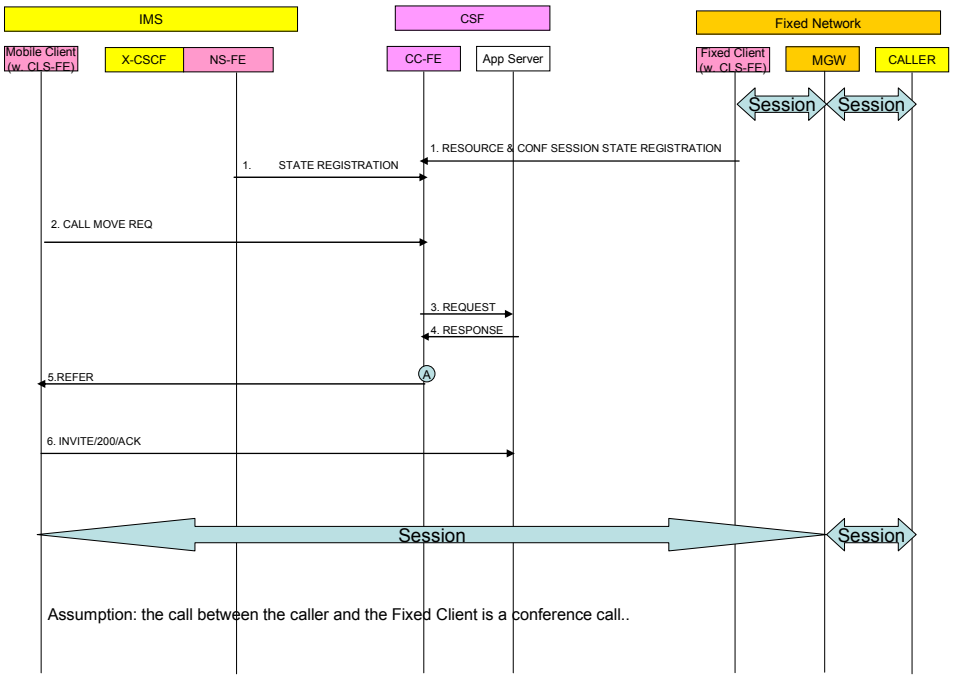


Figure A.3 – Movement of Conference call from a fixed client to a mobile client

Call Flow description:

1) Bob is in a video conference call using his desk top video phone. The CLS-FE in his desk top video phone registers its states with the CC-FE, informing its conference session ID (Conf-URI) and resource info. Other device belonging to Bob (in this case the mobile phone) also registers its states with the CC-FE via the NS-FE in the serving network (IMS).

2) The CLS-FE in the mobile phone initiates a Call Move Request to the CC-FE.

3) CC-FE processes the request and sends an inquiry to the Application Server for service logic.

4) Application Server sends the decision back to the CC-FE to move the audio portion of the call to the mobile phone. Task (A): The service logic decides that CC-FE should initiate a call to the mobile phone. The CC-FE fetches the session info of the conference call in progress [Conf-URI] and sends that as a response to the CLS-FE request.

5) Upon receiving the response from CC-FE, the CLS-FE in mobile phone initiates a request to join the conference call in progress. Task B: one possible implementation is to conference in fixed client, mobile clients and the caller and then drop the fixed client.

6) Without interruption Bob continues his conference call on the mobile phone.

Appendix B

Standards related to CSF

B.1 CSF relationship to OSA/Parlay

The CSF defines an architectural framework that provides a coherent view of information available at different network entities across dissimilar networks, with one benefit being easier creation of new services that provide a seamless user experience across multiple networks. A salient feature of the framework is that it accommodates and uses functions resident in the core network, edge devices and end-user devices. The CSF framework is further concerned with enabling smooth and consistent operation of applications across disparate networks, be they NGN, legacy or other.

While a Parlay/OSA gateway provides access to information available from one or more points in a given network, the CC-FE obtains the information from multiple networks, processes them and then provides the processed information to the applications in a manner that significantly reduces the complexity of interacting with these multiple and heterogeneous networks directly.

While Parlay/OSA allows creation of applications that function in multiple networks, CSF allows the application to function smoothly and consistently when users, devices or sessions cross the boundaries of networks or administrative domains.

B.2 CSF relationship to underlying networks

[Editors' Note] The nature of CSF relationship to underlying networks is for further study.

In some CSF instantiations, a Network Support Functional Entity is resident in the underlying network, and is administered by the operator of that network. In this case, it is helpful to illustrate the relationship of the NS-FE to the underlying network.

B.2.1 Example: CSF in an IMS-style network

An example of which components of IMS are used by the CSF, and how they extend the IMS specification set, is provided below.

The CSF operates across multiple transport and service control networks. In interacting with IMS, the CSF may act like an application server (AS) and utilize the interfaces defined for an AS. Specifically, an NS-FE uses the ISC interface to interact with the S-CSCF and obtain triggers to discover and modify sessions destined to or originated by a user.

In the Release 6 IMS, S-CSCF via the ISC interfaces directly with Application Servers. The AS selection is based on initial Filter Criteria (iFC) which are in turn based on predefined Service Point Triggers (SPT) in the Home Subscriber Server (HSS).

With the addition of a CSF overlay, the trigger criteria will have available a richer set of information through the Convergence Coordination Functional Entity (CC-FE) – such as session and resource state of the user across multiple, heterogeneous networks. The CSF also enables identity management features that enable AS to be independent/unaware of the identities of the users in individual networks.

The CSF allows session/resource state to be provided to applications via an interface.

The NS-FE may use the S_h interface to interact with the HSS and obtain information about the user and devices associated with the user in the IMS domain.

In large networks with multiple HSS, the NS-FE may use the D_h interface to interact with Subscription Locator Function (SLF) to discover HSS possessing user information.

The NS-FE uses the U_t interface to interact with the UEs. This interface is used to interact directly with an IMS UE to obtain user inputs, preferences and state of devices from the UE. Alternately, a CC-FE may use the CSF interface $I_{C\text{-}CL}$ to communicate with the Client Support Functional Entity (CLS-FEin the UE to obtain user inputs and preferences and state of devices from the UE.

It is also possible for the Network Support Function (NS-FE) to be incorporated within, e.g., the S-CSCF. If implemented in this way, the NS-FE should behave in a manner consistent with the NS-FE-to-CC-FE interface. The NS-FE-IMS interface may disappear from definition, or may need to be enhanced. This is a subject for further study.

B.2.2 Example: CSF in a wireline-style network

An example of which components a Wireline-style network are used by the CSF is provided with reference to the CableLabs' PacketCable Multimedia specification 'PacketCable™ Multimedia Specification PKT-SP-MM-I02-040930'.

The CSF is intended as an overlay across transport and service control networks. In interacting with PCMM, the CSF may act like an application manager (AM) and utilize the interfaces defined for an AM. Specifically, a PCMM-specific NS-FE uses the pkt-mm-3 interface to interact with the PacketCable Policy Server (PS) and obtain rights for different flows traversing this access network.

Additionally, the policy server is the point of contact with the CSF for interaction with protected components such as the PacketCable Record Keeping Server (RKS).

The NS-FE uses the mm-7 interface to interact with the Client (a term specified in PCMM). This interface is used by CSF to interact with the Client Support Function (CLS-FE) to directly obtain user inputs and preferences and state of devices from the Client. Alternately, a CC-FE may use the CSF interface $I_{C\text{-}CL}$ to communicate with a Client Support Functional Entity (CLS-FE) in the Client to obtain user inputs and preferences and state of devices from the Client.

It is also possible for the NS-FE to be incorporated within, e.g., the PCMM PS. If implemented in this way, the NS-FE should behave in a manner consistent with the NS-FE-to-CC-FE interface. The NS-FE-PCMM interface may disappear from definition, or may need to be enhanced. This is a subject for further study.

Appendix C

Examples of three converged service types

NGN FRA defines multiple configurations to provide wide variety of services. It is the aim of the CSF to present converged services of more than one service across the configurations to users in a unified manner.

Such capabilities to converge services for a subscriber by coordinating, collecting and binding user's status information from each configuration, is separately defined in this CSF document from FRA. This means current FRA release 1 does not fully incorporate the converged control capabilities in each FE.

This Appendix describes several example converged type scenarios and also presents relationship between CSF functions.

C.1 Type 1 Example: Converged service in a single configuration

In the case of a single configuration such as of an IP Multimedia Component, multiple services must be invoked and coordinated.

For the originating party, the origination call screen and number translation services are sequentially invoked and processed. Then for the terminating party, call forwarding on no-answer and voice mail services are invoked in sequence.

In this case, two originating services and two terminating services are converged for originating and terminating subscriber, respectively.

The CC-FE (shown as a Service broker in the figure) coordinates the interoperation between multiple services based on the converged service subscription information provided by the NS-FE, shown as part of the SUP-FE (e.g. HSS) in the figure.

Also, the CC-FE decides converged service control based on the user's presence and preference information from the NS-FE in the SUP-FE or AS-FE (e.g. Presence server). For example, the CC-FE may decide not to invoke Call Forwarding on No-Answer, but connect to the Voice Mail Server (VMS) instead.

Though the APL-SCM (APL Service Coordination Manager) function is defined to manage interaction between multiple application services [2], it only considers coordination based on the iFC through SC-FE.

However, the CC-FE makes use of more information (e.g. user's status) collecting from various network parts such as Presence server, than simple subscription information in iFC.

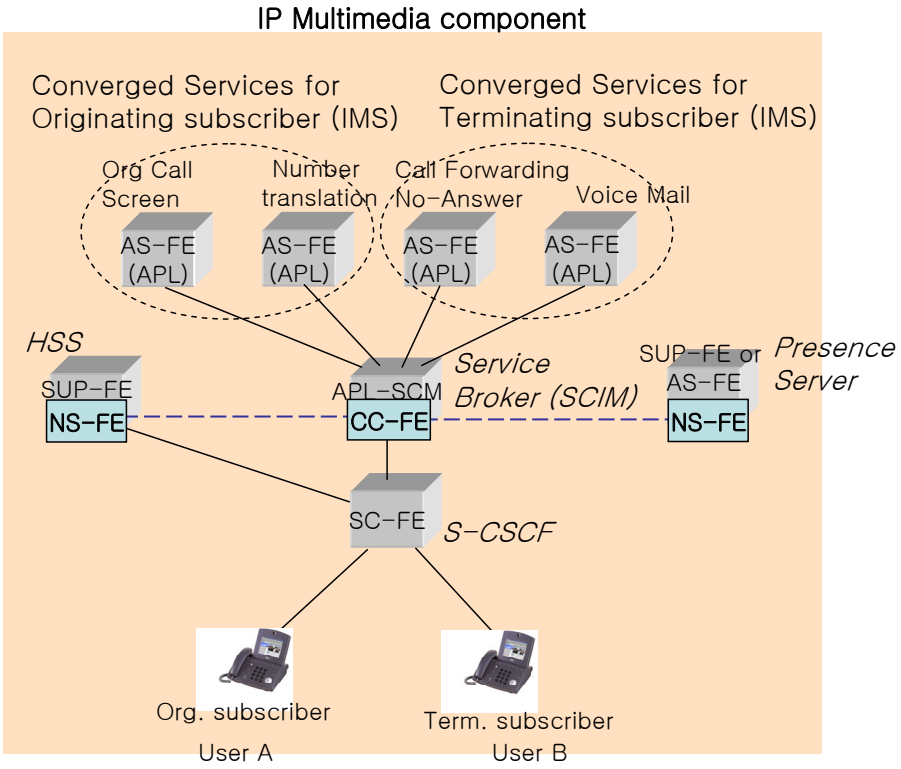


Figure C.1 – Converged service example in a single configuration

C.2 Type 2 Example: Converged service in multiple configurations – PIEA + IMS

In this example, service convergence is achieved across multiple configurations, the first being PIEA and the second being IP Multimedia Components.

User A has both a POTS and IP phone, and subscribes two services, Caller ID and Number Translation. Through service convergence, it should be possible for him to access same services from both phones.

When User A requests a call from the POTS phone, the basic Caller ID and Number translation services in PIEA are invoked. In the case that User A requests a call using the IP video phone, the Multimedia Caller ID and Number translation services will be provided by IMS.

Since the user subscribes over multiple configurations, the interaction management function of the CC-FE is required between different configurations or administrative domains.

To retrieve each profile for the user, the CC-FE refers to the NS-FE in the PIEA UPF (e.g. User Profile) or the NS-FE in the IMS SUP-FE (e.g. HSS), according to the user's network.

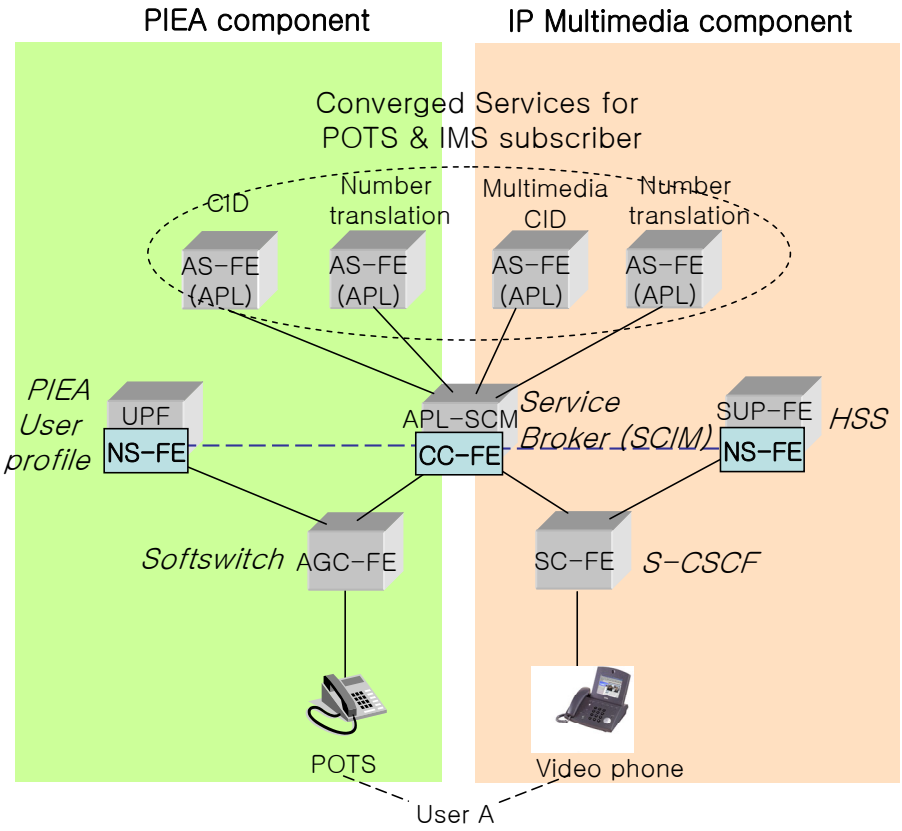


Figure C.2 – Converged service example in multiple configurations (PIEA + IMS)

C.3 Type 2 Example: Converged service in multiple configurations – IMS + VOD

This is the converged service for multiple configurations of IP Multimedia and Streaming Service Components. User A, who is a subscriber of both VoIP and IPTV, turns on and watches IPTV (or VOD). When a call arrives to user A, the CC-FE is notified of an arriving call to user A by an NS-FE in the SC-FE. The CC-FE looks up user A's service registration and determines that this state information should be sent to the NS-FE/CC-FE in the MS-FE. The NS-FE/CC-FE in the MS-FE then looks up user A's preferences and determines that IPTV traffic should be suspended. The CC-FE in APL-SCM notifies the NS-FE in the Head-end server to 'Suspend Video Traffic'. The Head-end then suspends the VOD stream until he/she hangs up the phone call.

This coordination is enabled by CC-FE that interworks with an NS-FE in the Multimedia Service FE (e.g. Head-end server) of Streaming Service Component and an NS-FE in SC-FE (e.g. S-CSCF) of IP Multimedia Component.

The NS-FE in Multimedia Service FE (MS-FE) sends user A's IPTV (VOD) connection status to the CC-FE, and when the user makes a call and is connected, the CC-FE notifies the NS-FE in the MS-FE. Then the MS-FE invokes the appropriate service logic to suspend stream to the user. When the user disconnects the call, the NS-FE in SC-FE sends notification to CC-FE and the original state is resumed.

As such, the NS-FEs from different configurations interoperate with CC-FE.

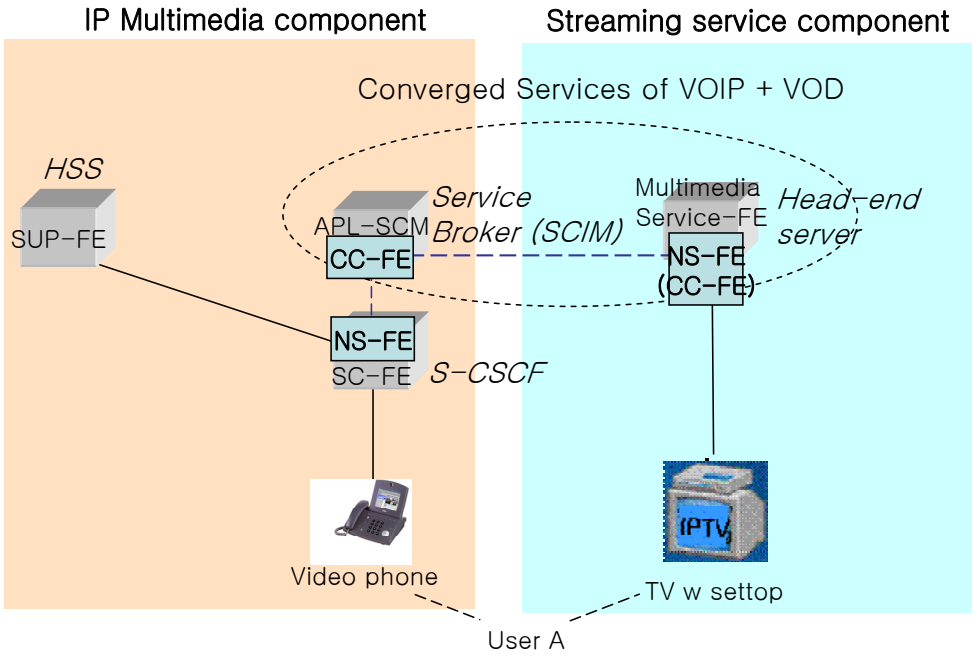


Figure C.3 – Converged service example in multiple configurations (IMS + VOD)

C.4 Type 3 Example: Converged service with other network – IMS + Internet IM server

This example shows the converged service for multiple configurations of IP Multimedia Component and an unspecified "Other network", such as the Internet.

Figure C.4 (a) shows VoIP + IM converged service scenario:

User A has a video phone and an Internet connected PC in which he uses an Instant Messenger (or Calendar, or similar service).

When the user A's phone establishes a call connection, the 'busy' status is notified to CC-FE. The CC-FE sends that information to an NS-FE in the Instant Messenger or Calendar server. The user's status of the IM or Calendar is changed to be 'busy'.

On the contrary, when the User A makes the status as 'busy' in the IM or Calendar, it informs the CC-FE, and the CC-FE notifies the NS-FE in SC-FE. Then the user A's video phone status becomes busy. Therefore as an incoming call arrives, the calling party receives the busy tone for the user A.

As an alternative interworking with IM service, the CLS-FE in user PC can notify such status of the user to the CC-FE.

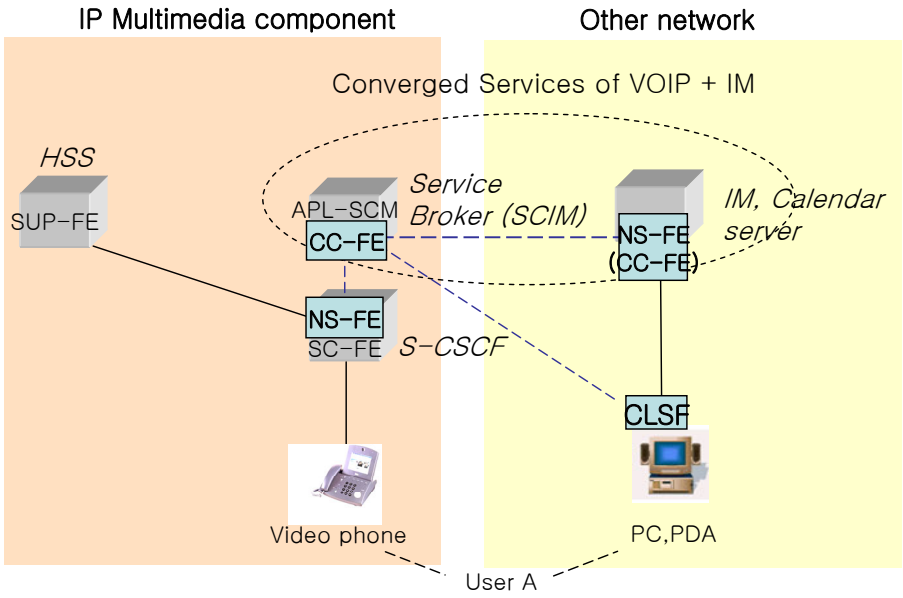
Figure C.4 (b) illustrates Game + IM converged service scenario:

When User A connects to a Game server, it is possible three alternative notifications to CC-FE: (1) from the CLS-FE on the phone; (2) from the ES-FE on the Edge Node; (3) from the NS-FE on the Game server.

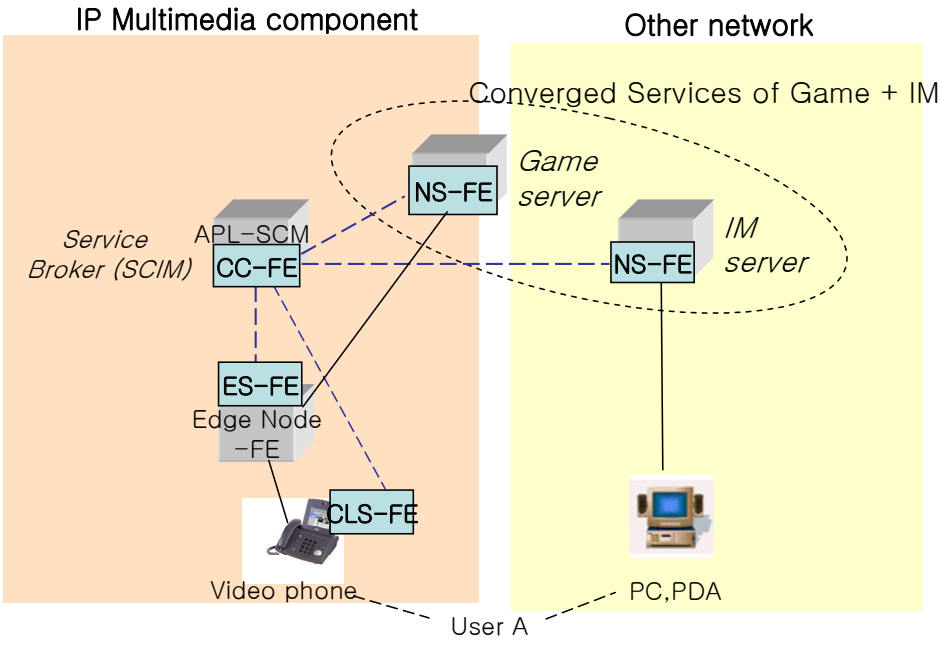
For (2), the ES-FE in Edge Node FE monitors the video phone's out-stream packets to the network based on the source IP and/or port number. Detecting such packets, ES-FE notifies to CC-FE that User A's video phone is busy (for any 'data' services other than VOIP) and then CC-FE notifies to NS-FE on IM server, which become to know User A's status is 'busy'.

Although it is not shown in the figure, the CC-FE may reside on the terminal for the Enterprise, Home network services, and peer-to-peer service such as personal broadcast service.

To intercommunicate between these two networks the CSF glues through CC-FE and NS-FE/CC-FE/CLS-FE/ES-FE in each network.



(a) IMS + Internet IM



(b) Game + Internet IM

Figure C.4 – Converged service example with other networks

The dashed line corresponds to the interfaces between CSF functions.

Appendix D

Items for further study for development of CSF functional architecture

NOTE – This appendix should be removed from this document after all items are addressed.

1) Study the OMA Service Environment (OSE) to identify how OSE fits into the CSF.

2) CSF is a Release 2 item and hence its mapping into the NGN is part of the Release 2 standardization. This mapping will assist in downstream stage 2 and stage 3 works.

3) One of the goals of the CSF is to allow Applications which may or may not have been designed together, such as those designed by disjoint parties, to co-ordinate and co-operate on a per-user basis. This aspect is not clearly spelled out in the current TR-CSF and should be addressed. Moreover, the CSF should cover both areas: in-house (operator apps) and out-house (3rd party app).

4) The elements of CSF should be reachable (either directly or through a domain-specific gateway) by those of another administrative domain subject to meeting conditional access requirements. Additional use case scenarios describing how services are coordinated across different domains are needed.

5) Within the CSF architecture, the end user device should be allowed to make its own decision, if it is capable and wants to do so. This idea needs to be captured in the TR-CSF.

WORKING GROUP 7
DELIVERABLES

FUTURE PACKET-BASED BEARER NETWORKS

3.3 Problem statement (*Status P*)

3.4 FPBN requirements (*Status A*)

3.5 FPBN high-level architecture (*Status A*)

3.6 FPBN candidate technologies (*Status D*)

3.3 – Problem statement*

Introduction

This Problem Statement is the first deliverable from WG 7 on "Future Packet Based Bearer Network". Subsequent documents will further identify the requirements for architectures (and protocols), which will fill the gaps, if any, which are identified with current architectures and systems.

Table of Contents

* Status P: This deliverable has already been passed to ITU-T Study Group 13.

3.3 – Problem statement

1 Some problems with current Packet Based Networks (PBNs)

Network operators are now facing a major turning point in the evolution of their many and various service-dedicated network platforms (such as PSTN, ATM, FR, Internet backbone, IP VPN, etc.) towards a simpler, more converged "Connectionless" and "Connection-Oriented" common service networks. Such a network must be robust, carrier-scale, and flexible, while at the same time optimizing both Capital Expenditures (CAPEX) and Operational Expenditures (OPEX).

2 References

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z. and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.

3 Definitions

cl-ps – connectionless packet switched (e.g., the IP transport network)

co-ps – connection oriented packet switched (e.g., MPLS as a server)

co-cs – connection oriented circuit switched (e.g., the traditional TDM network)

Network Mode – one of cl-ps, co-ps, or co-cs

4 Issues Facing Network Operators

Current cl-ps networks have the advantage that they provide a relatively simple operational model, and the disadvantage that they are unable to provide hard end-to-end QoS guarantees in a cost-effective way. Current co-ps networks have the advantage that they can provide guaranteed performance, but possibly at a relatively higher operational complexity. Operators therefore require that both cl-ps and co-ps modes be supported in order to be able to provide all the services that their customers require.

4.1 Support for different traffic types

Network operators require a scalable architecture that:

- enables the provision and guarantee of SLS (Service Level Specifications),
- is 'designed for uncertainty', and
- provides for different traffic types[6] and their associated service differentiation mechanisms.

Further, in order to provide such QoS based services, a network must provide a mechanism (virtual or otherwise), which provides for the logical separation of different traffic classes associated with different traffic.

6 Please refer to WG 3 for a discussion of traffic classes.

4.2 Protecting the control and management planes from user-plane traffic

Network operators require that their control and management infrastructure be protected from user traffic[7]. Thus, a network architecture must provide the capability to separate the various planes in a particular mode (e.g., cl-ps, co-ps, or co-cs). An example is the separation of data plane from control plane in the SS7 architecture.

4.3 Guaranteeing and charging for Service Level Agreements

As broadband access penetration increases and new applications emerge, the question of how to deliver QoS based services, along with the mechanisms for charging these services has become increasingly important. To this end (and at the very least), network operators will want to:

- Guarantee fair access to shared resources in the access network.
- Control load distribution to avoid focused overload in the core.
- Support hard guarantees to customers.
- Support pricing of different classes.

Any QoS architecture must provide for these functions. It is important to note that in general, the QoS functions described above are characterized by their end-to-end behaviour. However, while QoS architectures such as the IETF's Differentiated Services (DS) Architecture [RFC2475] define an end-to-end QoS model, the DS model itself is described in terms of Per-Hop Behaviours (PHBs) and edge traffic conditioning, and network operators may feel that the DS model is insufficient to provide the required end-to-end QoS guarantees.

4.4 The need to ensure emergency services get through and are maintained

Network operators are required to ensure that emergency services (e.g., 112 or 911 emergency calls) are established and are not dropped under conditions of resource shortfall. A related problem in current QoS approaches is the inability to distinguish between 'urgency' (defined as how fast a service request or user packet must get processed in the up-state to meet the application's QoS requirements) and 'importance' (defined as the survivability of a given service request or user packet compared to all other service requests or user packets when the network has insufficient resources to service all the traffic, irrespective of QoS classifications).

4.5 Provide adequate security

Network operators require that their infrastructures are secure. However, architectures that carry control and management plane information in-band (i.e., in the user plane, such as the IP network) can offer greater potential for attacks against an operator's network infrastructures. Such attacks include classical security attacks (hijacking, privacy, non-repudiation, etc), as well as attacks on network availability (e.g., Denial of Service (DoS) attacks).

4.6 Identification, location, and remediation of faults (OAM)

Clearly, network operators will require the ability to rapidly detect, locate, and remediate network faults (preferably proactively, i.e., before the customer notices). However, certain architectural choices can make such rapid fault remediation difficult or impossible. For example, consider the case of IP networks, where control and management information are carried in-band. In this case, it can be difficult or impossible to

[7] See section 5 additional discussion of security.

rapidly locate, diagnose, and repair certain classes of faults (in particular, those faults which have the property that the fault itself prevents fault detection, location, or repair).

4.7 Performance Monitoring

Network operators also require the ability to monitor the performance of their networks and the services they provide. The same architectural choices that can cause fault remediation to be difficult (or impossible) can cause similar problems for performance monitoring.

3.4 – FPBN requirements*

Introduction

This document specifies high-level requirements of a Future Packet Based Network (FPBN). The document specifies user plane, control plane and management plane requirements.

Table of Contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

3.4 – General requirements of FPBN

1 Scope

The scope of this document is requirements for architecture of FPBN comprised of transport stratum packet based path layer networks (refer to G.805 [1], G.809 [2] and Y.2011 [3]).

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this document. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this document are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this document does not give it, as a stand-alone document, the status of a Recommendation.

[1] ITU-T Recommendation G.805 (2000), Generic functional architecture of transport networks.

[2] ITU-T Recommendation G.809 (2003), Functional architecture of connectionless layer networks.

[3] ITU-T Recommendation Y.2011 (2004), General principles and general reference model for next generation networks.

[4] TR-TERM, Terms, definitions and high-level terminological framework for Next Generation Networks.

3 Terms and Definitions

Absolute QoS – See TR-TERM [4].

Access Group – See G.805.

Address – An identifier used for routing a communication to an entity.

Connection – See G.805.

Control plane – See TR-TERM.

Flow - See G.809.

Flow domain – See G.809.

User plane – See TR-TERM.

Importance – Importance is the survivability of a given packet compared to all other packets when the network has insufficient resources to service all the traffic. The importance of a given packet is independent of the delay requirements (urgency) of that packet.

Management plane – See TR-TERM.

Off-path – Off-path in a co network means it is using a separate trail. Off-path in cl-ps network means it is using a separate server layer trail.

Relative QoS – See TR-TERM.

Subnetwork – See G.805.

Trail – See G.805.

Urgency – Urgency is how fast a packet must get processed in the up-state to meet the requested QoS requirements. The urgency of a packet is conveyed in terms of the performance (delay) it requires and a packet's urgency is independent of the survivability (importance) of that packet.

4 Abbreviations

AP – Access Point (defined in G.805 and G.809)

cl-ps – Connectionless packet switched

co-ps – Connection orientated packet switched

CP – Connection Point (defined in G.805)

FP – Flow Point (defined in G.809)

FPBN – Future Packet Based Network

mp-t-mp – Multi-point to multi-point

MTU – Maximum Transmission Unit.

OAM – Operations, Administration and Maintenance

PM – Performance Management

p-t-mp – Point to multi-point

p-t-p – Point to point

QoS – Quality of Service

VPN – Virtual Private Network

5 Conventions

6 FPBN requirements

6.1 General requirements

This section specifies general requirements for the FPBN. More detailed requirements are specified in the other sections below.

The FPBN:

- Shall provide both connectionless and connection-oriented services for multiple client types.
- Shall efficiently support p-t-p and p-t-mp services.
- Should efficiently support mp-t-mp services.
- Shall support at least absolute QoS in the co-ps mode (if a co-ps mode is provided).

- Should allow a smooth migration from current cl-ps and co-ps packet networks.
- Shall interwork and co-exist with current cl-ps and co-ps packet networks.
- Shall support arbitrary network topologies and be able to expand bandwidth, topology, number-of-customers and number-of-services incrementally.
- Shall detect, and recover from, facility and equipment failures and performance degradation as appropriate to the requirements of the service.
- Shall offer the appropriate OAM functions for each plane.
- Shall completely secure the internal control and management plane traffic from external attack and shall ensure that it remains secure and stable under situations of extreme stress.
- Shall secure the management plane to prevent access to control and management functions by unauthorised users.
- Shall be able to accommodate new traffic types.
- Shall allow statistical multiplexing for efficiency.
- Shall support lawful interception of FPBN services. See FGNGN Release 1 scope.
- Shall support accounting functions by being able to monitor at least network utilisation and performance parameters.
- Shall provide the ability to distinguish between urgency (delay) and importance (survivability).
- Shall support services that require in-order delivery of packets.
- Should support logical separation of control, management and user planes
- Should support off-path control and management planes.
- Shall provide harmonised and consistent means of referring to user plane access points.
- Shall provide traffic user plane defect detection and handling (OAM) that is not reliant on the control and/or management planes and is not a function of the nature of the client being transported.
- Shall harmonise trail or connection setup and teardown with OAM activation & deactivation.
- Shall support mechanisms to avoid traffic impact during reconfiguration.
- Shall attempt to keep traffic flowing while recovering from failures.
- Shall only deliver traffic from the intended source/ingress to the intended destination(s)/egress(es) except under extremely rare multiple failure conditions.
- Shall support emergency services.
- Shall be scalable and reliable.
- Shall maintain the separation between user traffic flows as appropriate for the FPBN service that is being provided.

6.2 Detailed requirements

This section specifies requirements that are more detailed than the general requirements specified above.

6.2.1 Addressing related requirements

This section specifies addressing related requirements for the FPBN. These requirements apply to the network, not necessarily to the user packet itself.

The FPBN:

- Shall support the identification of a packet’s source and its destination within the FPBN in the cl-ps mode.

- Shall support the identification of a connection's source within the FPBN in the co-ps mode at the connection's destination.
- Should support FPBN addressing that is disjoint from any client addressing.

6.2.2 Control related requirements

This section specifies control related requirements for the FPBN.

The FPBN:

- Shall support mechanisms to safe guard against persistent (i.e. looping) traffic units in the cl-ps mode.
- Shall support mechanisms to safe guard against co-ps connections containing forwarding loops.
- Should facilitate the in-order delivery of the traffic unit.
- Shall ensure the integrity of the control information (e.g. header checksum).

6.2.3 QoS related requirements

This section specifies QoS related requirements for the FPBN.

The FPBN:

- May support queuing priority, which can be implicit or explicit.
- May support discard priority, which can be implicit or explicit.

6.2.4 Network performance management (PM) related requirements

This section specifies PM related requirements for the FPBN.

The FPBN:

- May provide utilisation information on links and nodes.
- Should provide logging of FPBN utilisation as appropriate for the FPBN services that are supported.
- Should support performance monitoring (PM).
- Shall suspend any network performance measurements (for both directions of the trail or connection) if either direction of a bi-directional trail or connection enters the unavailable state.
- Shall support network performance monitoring (PM) including availability, packet loss, delay and jitter between any two points in the network.

6.2.5 Protection related requirements

This section specifies protection related requirements for the FPBN.

The FPBN:

- May support mechanisms to recover from equipment or facility failures.

6.2.6 Payload related requirements

This section specifies payload related requirements for the FPBN.

The FPBN:

- May support mechanisms for dynamically discovering the maximum transmission unit (MTU) of a path or connection across an FPBN.
- Shall deliver packets in-sequence for the connection-oriented mode of operation.

- May support mechanisms to enable the in-sequence delivery of packets for the connectionless mode of operation.
- May support mechanisms to ensure the integrity of the adapted information.

6.2.7 OAM related requirements

This section specifies OAM related requirements for the FPBN.

The FPBN:

- Shall support simple OAM mechanisms to detect and handle defects.
- Shall support OAM mechanisms that are agnostic about the client layer that the FPBN is carrying (i.e. it shall be possible to manage the server layer using the same mechanisms independent of the client that is being transported).
- Shall support OAM defect detection and handling in the traffic user plane.
- Shall support OAM defect detection and handling (e.g. defect indication to the trail termination) on an uni-directional basis in the traffic user plane in the co-ps mode.
- Shall support the appropriate consequent actions (after defect detection) at a trail termination sink (e.g. suppression of client traffic, defect indication to the client and defect indication to the trail termination source) (for co-ps and co-cs clients).

6.2.8 Security related requirements

This section specifies security related requirements for the FPBN. The intent is to protect against and detect unauthorised end stations but not unauthorised users on authorised end stations.

The FPBN:

- Shall provide mechanisms to protect the control plane communications from security threats.
- Shall provide mechanisms to protect the management plane communications from security threats.

7 Control plane requirements

This section specifies control plane related requirements for the FPBN.

The FPBN:

- Shall support a control plane that is independent of any particular client layer control plane.
- Shall have an unambiguous and reliable means of distinguishing control packets from user plane packets and management plane packets.
- Shall allocate resources to control plane packets such that no amount of user plane traffic can cause control functions to become inoperative.
- Shall detect and recover from control plane failures and degradation as appropriate to the requirements of the services.

8 Management plane requirements

This section specifies management plane related requirements for the FPBN.

The FPBN:

- Shall support a management plane that is independent of any particular client layer management plane.

- Shall have an unambiguous and reliable means of distinguishing management packets from user plane packets and control plane packets.
- Shall allocate resources to the management plane packets such that no amount of user plane traffic can cause management functions to become inoperative.

9 Transport stratum service requirements

This section specifies transport stratum service requirements for the FPBN. The services in the transport stratum are divided into two groups; basic service and enhanced services

9.1 Basic transport stratum service requirements

This section specifies basic transport stratum service requirements for the FPBN.

The FPBN:

- Shall provide a point to point transport stratum service without adaptation.
- Shall support point to point transport stratum service including adaptation functions.
- Shall support point to multi-point transport stratum service including adaptation functions.

9.2 Enhanced transport stratum service requirements

This section specifies enhanced transport stratum service requirements for the FPBN.

The FPBN:

- Should support multi-point to multi-point transport stratum service including adaptation functions.
- Shall support connection-oriented transport stratum services with absolute QoS assurance.
- Shall support transport stratum services with relative QoS.

3.5 – FPBN high-level architecture*

Introduction

This document specifies a high-level architecture for Future Packet Based Networks (FPBNs). The document also specifies the relationship between an FPBN and the NGN strata and the interfaces in an FPBN.

In order to be able to provide a full suite of services (examples of which include Data, Video and Voice Telephony services) to their customers operators may need to utilise both the cl-ps and co-ps transport modes, because each mode is well suited to the transport of some services and not so well suited to the transport of others.

FPBN provides the topmost layer(s) of the transport stratum as defined in Y.2011. The services mentioned above form part of the service stratum as defined in Y.2011.

Table of Contents

* Status A: The FGNGN considers that this deliverable has been developed to a sufficiently mature state to be considered by ITU-T Study Group 13 for publication.

Page

3.5 – FPBN high-level architecture

1 Scope

This architecture for an FPBN addresses both cl-ps and co-ps layer networks. Co-cs layer networks used to provide the lower layer(s) of the transport stratum are outside of the scope of this document. The definition and specification of specific services is left to other NGN Recommendations and is outside of the scope of an FPBN and this document.

2 References

[1] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

[2] ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks.*

[3] ITU-T Recommendation G.809 (2003), *Functional architecture of connectionless layer networks.*

[4] ITU-T Recommendation X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model.*

[5] ITU-T Recommendation Y.2011 (2004), *General principles and general reference model for next generation networks.*

[6] TR-RACF, *Functional Requirements and Architecture for Resource and Admission Control in Next Generation Networks.*

[7] ITU-T Recommendation Y.1710 (2002), *Requirements for OAM functionality for MPLS networks.*

[8] ITU-T Recommendation Y.1711 (2004), *Operation & Maintenance mechanism for MPLS networks.*

[9] ITU-T Recommendation Y.2001 (2004), *General overview of NGN.*

[10] TR-FRA, *Functional Requirements and Architecture of the NGN.*

[11] TMF 513 V3.0, *Multi-Technology Network Management Business Agreement, NML-EML Interface.*

[12] TMF 608 V3.0, *Multi-Technology Network Management Information Agreement, NML-EML Interface.*

[13] TMF 814 V3.0, *Multi-Technology Network Management Solution Set.*

[14] TMF 517 V0.7, *Multi-Technology Operations Systems Interface Business Agreement.*

[15] TMF 608 V3.1, *Multi-Technology Network Management Information Agreement, NML-EML Interface.*

3 Terms and Definitions

Address: An identifier used for routing a communication to an entity.

Authentication: See X.800 [1].

Availability: A measure of the capability of a given entity (for example a layer network, connection, flow etc.) to maintain connectivity with the associated performance criteria that have been guaranteed by the entity being measured.

Client/server relationship: See G.805 [2].

Connection: See G.805.

Flow: See G.809 [3].

Name: an identifier (that may be resolved to an address) that uniquely identifies an entity within a particular identification domain.

Trail: See G.805.

4 Abbreviations

ATM	Asynchronous Transport Mode
cl-ps	connectionless packet switched
CPE	Customer Premises Equipment
co-cs	connection orientated circuit switched
co-ps	connection orientated packet switched
CV	Connectivity Verification
FPBN	Future Packet Based Network
FT_Sk	Flow Termination Sink
FT_So	Flow Termination Source
E-NNI	Exterior-Network to Network Interface
I-NNI	Interior-Network to Network Interface
IP	Internet Protocol
L2TP	Layer 2 Tunnelling Protocol
MPLS	Multi-Protocol Label Switching
MTNM	Multi-Technology Network Management
MTOSI	Multi-Technology Operations Systems Interface
NGN	Next Generation Network
NNI	Network to Network Interface
OAM	Operations, Administration & Maintenance
OSI BRM	Open Systems Interconnection Basic Reference Model
PPP	Point to Point Protocol
p-t-p	point to point
p-t-mp	point to multipoint
QoS	Quality of Service
RACF	Resource and Admission Control Functions
RPT	Reference Point Type

SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
TMF	TeleManagement Forum
TT_Sk	Trail Termination Sink
TT_So	Trail Termination Source
UNI	User to Network Interface
VC-4	Virtual Container Level 4

5 Convention

None

6 FPBN architecture

6.1 Framework

An FPBN is composed of Packet Based Path Layer Networks (as defined in G.805 [2], G.809 [3]) in the Transport Stratum (the functionality is similar to Layers 2 and 3 in X.200 [4]). An overview of G.805 and G.809, and the relationships to the OSI BRM, is provided in Appendix A. The Transport Stratum is depicted in Figure 1/Y.2011 [5]. Each layer network 'system' in an FPBN consists of a user plane, a control Plane and a management Plane and each of the planes within a layer network will have its own traffic forwarding component which may belong to the same layer network (if the planes are not isolated from each other) or different layer networks (if the planes are isolated from each other).

It is a requirement (identified in the FPBN requirements document) that an FPBN '*shall provide mechanisms to protect the control plane or processes that support the delivery of packets to the control plane from malicious attacks*'. An identical requirement also exists for protecting the FPBN management plane from malicious attacks. The user, control and management planes (of each layer network) should be segregated from each other in order to keep the performance, security and reliability of each plane (and that of the other planes) from being violated. Techniques for doing so include (but are not limited to) isolation between planes or special treatment of traffic belonging to the different planes. How a particular NGN network maintains the integrity of its planes is up to it, so long as the requirements detailed in the FPBN requirements document are met.

It is a requirement (identified in the FPBN requirements document) that an FPBN '*should support off-path control and management planes*' and therefore isolation is the preferred 'default' mechanism that can meet the requirements for protecting the user, control and management planes (of each layer network) from each other. The user, control and management planes can be isolated from each other by the allocation of independent co-ps or co-cs server layer network trails. The type of isolating technology is determined by several factors, such as location (e.g. access or core), network status, cost, etc. It is up to the operator to decide to what degree they wish to operate their control and management planes off-path. Another motivation for isolating the control and management planes from the user plane is to ensure that the FPBN control and management planes continue to operate even if the FPBN user plane is overloaded or faulty.

An FPBN should seek to harmonise functional components (e.g. control and management plane design and operation) across the networking modes as far as practically possible.

Figure 1 and Figure 2 show functional diagrams that depict the user plane of the FPBN architecture. The cl-ps network is drawn using G.809 conventions and the co-ps network is drawn using G.805 conventions.

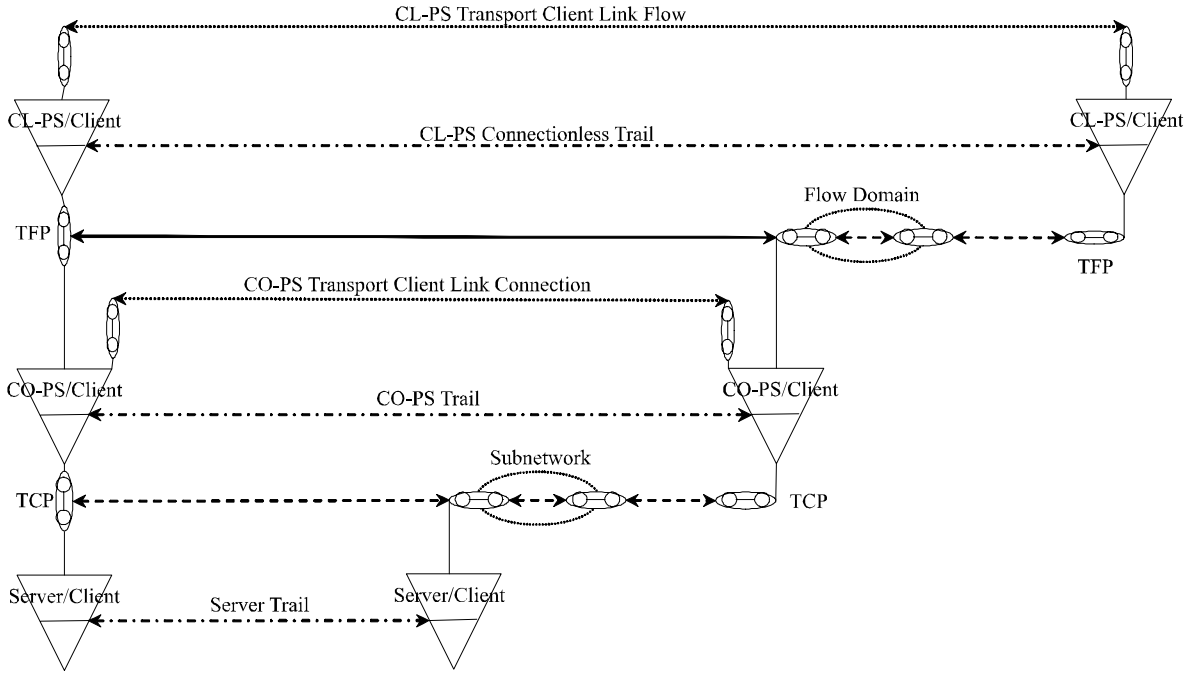


Figure 1 – Functional diagram depicting the user plane of the proposed architecture (cl-ps transport over co-ps layer network trails)

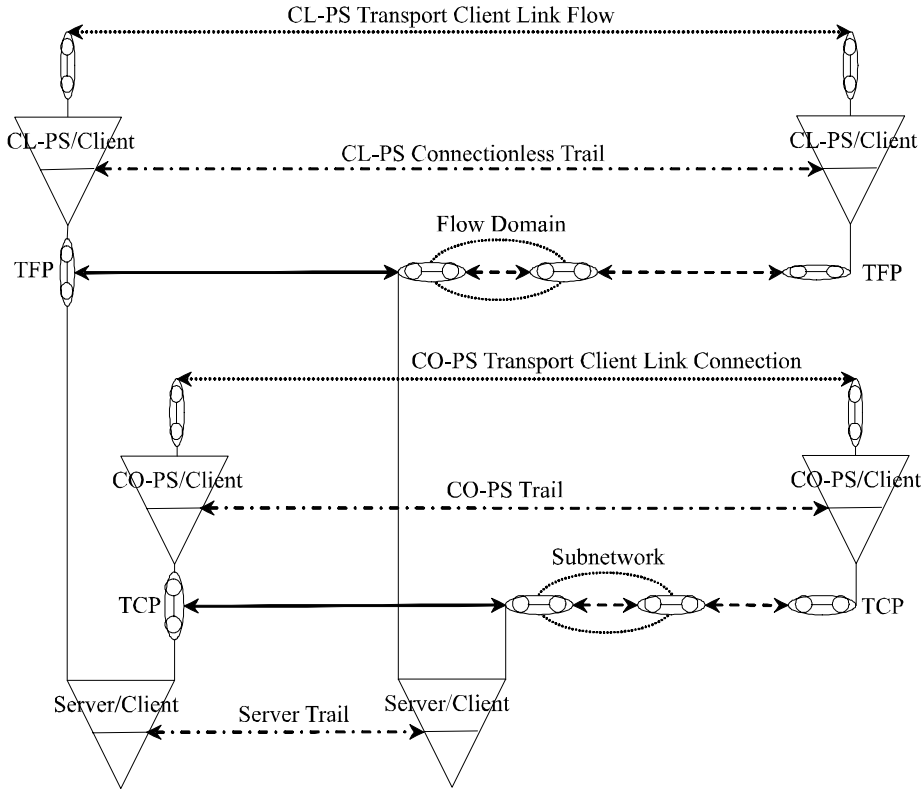


Figure 2 – Functional diagram depicting the user plane of the proposed architecture (cl-ps transport over server layer network trails)

The transport stratum may be implemented by multiple discrete layer networks that form client/server relationships. A different networking mode (cl-ps, co-ps and co-cs) may be used for each of the layer networks (this is not shown in Figure 1 and Figure 2). The number of layer networks and networking modes used is a choice for the particular operator deploying the transport stratum and is beyond the scope of this document.

In Figure 1 and Figure 2 the cl-ps and co-ps layer networks are shown separately. This separation may be physical or logical. The cl-ps layer network may use co-cs server layer network trails that are separate from the server co-cs layer network trails used by the co-ps layer network. Alternatively the separation may be logical;; i.e. the cl-ps and co-ps layer networks share the same server layer network trails. There may be some strict logical partitioning between them so that bandwidth sharing is impossible.

Similarly the cl-ps layer network may use physically separate networking equipment (e.g. routers) to the co-ps layer network or both layer networks may use the same physical networking equipment but that equipment will be logically partitioned between the cl-ps and co-ps layer networks.

In Figure 1 and Figure 2, the server layer network trail may be provided by any technology, switched or un-switched. Further client/server relationships may exist below the server layer network trail, however it should be noted that client layers inherit the impairments of their server layer networks and that this inheritance is recursive down to the duct.

In co-cs layer networks each client is explicitly allocated a dedicated amount of bandwidth from the server layer network trail. The clients are fully isolated and therefore one client's loading can not impact the performance of another client. This makes it simple to guarantee dedicated bandwidth for a client.

In co-ps layer networks each client is allocated bandwidth from a server layer network trail. However as the clients are only logically isolated one client's loading may directly impact the capacity available to another client. The appropriate allocation of bandwidth and the use of ingress admission control and policing make it possible to guarantee dedicated bandwidth for a client.

In cl-ps layer networks flows are not normally explicitly allocated to server layer network trails. Therefore the capacity available to one client flow may be impacted by the loading of other client flows. This may be mitigated by engineering the appropriate capacity in the server layer network (i.e. over provisioning) or by establishing resource reservation state per-hop and pinning routes. This makes it possible to guarantee dedicated bandwidth for a client. This procedure is implicit in a co-ps layer network. However, these techniques are not generally used for the majority of traffic in cl-ps layer networks.

NOTE – Due to the different characteristics of each networking mode it is generally advisable to stack modes that less efficiently provide dedicated bandwidth on top of modes that more efficiently provide dedicated bandwidth.

Looking at the top of Figure 1 and working down the model shows cl-ps transport over cl-ps layer network connectionless trails, which are transported over co-ps layer network trails which are in turn transported over server layer network trails. Co-ps transport is provided over co-ps layer network trails, which are in turn transported over server layer network trails.

Looking at the bottom of Figure 1 and working up the model shows a server layer network trail providing transport for a co-ps layer network. The co-ps layer network in turn provides transport for co-ps services as well as providing transport for the cl-ps layer network. Then the model shows that the cl-ps layer network provides transport for cl-ps services.

Looking at the top of Figure 2 and working down the model shows cl-ps transport over cl-ps layer network connectionless trails, which are in turn transported over server layer network trails. Co-ps transport is provided over co-ps layer network trails, which are in turn transported over server layer network trails.

Looking at the bottom of Figure 2 and working up the model shows a server layer network trail providing transport for a co-ps layer network and a cl-ps layer network. The cl-ps layer network provides cl-ps transport and the co-ps layer network provides co-ps transport.

For the cl-ps layer network depicted in Figure 1 and Figure 2, the choice of using co-ps transport or other server layer network trails or both will be a decision taken by the operator and will be dependent on a number of factors both economic and technical including (but not limited to):

- The operator's local policy.
- The traffic level guarantees the operator has made to their customers.
- The level of bandwidth granularity a given service requires.
- The volume of cl-ps traffic which is being aggregated. I.e. small volumes are likely to be better served off the co-ps mode, whilst larger volumes are likely to be better served off the co-cs mode.

An operator may choose to use any of the options above (i.e. co-ps transport, server layer network trails, or both) in order to support a cl-ps layer network. Alternatively an operator may choose to mix the above options, so for example an operator may choose to use co-ps transport for some cl-ps connectionless trails and other server layer network trails for other cl-ps connectionless trails. One reason for mixing these options is that some cl-ps links within the operator's network may require the larger/coarse bandwidth granularities provided by server layer network trails, whereas other cl-ps links may require a finer bandwidth granularity. In order to maximise the utilisation of the larger/coarse bandwidth granularities provided by server layer network trails the operator may wish to utilise the co-ps layer network as a method of mediation between the server layer network trails and cl-ps layer networks.

The specific encapsulation format used for an FPBN user plane is independent of network mode. It is the control plane or management plane that commonly determines the network mode. Therefore operators may use the same encapsulation format for both cl-ps and co-ps network modes even though the forwarding behaviour of each mode is different.

6.2 User plane

User plane resources may be allocated to different service classes, so as to adapt to the open market, competitive circumstance, services implementation and evolution.

Resources of service classes will be allocated on demand. Resources allocated to service classes are independent of each other. Different service classes have different attributes. For example, some service classes may guarantee the Packet Loss Ratio and delay of packet transport, some may guarantee Packet "Importance", some may guarantee much higher security for packets, some may provide guaranteed throughput for packet streams, and some others may provide combinations of these above attributes or even combinations with some other attributes.

It is not necessary to provision all services in a service class in the same way in an FPBN. The control plane may set up some of them, while the management plane may set up others.

As the service stratum may require a large number of service classes with different attributes, an FPBN should provide service classes in an extensible way. There are many advantages to doing so, for example voice service can be put into an independent service class so that traditional PSTN carriers can provide consistent voice service characteristics. As another example, an FPBN could provide "Carrier of Carriers" services so that the transport carrier and the service carriers can be different operators, etc.

It is a requirement (identified in the FPBN requirements document) that an FPBN '*shall provide a point to point transport stratum service without adaptation*', '*shall support point to point transport stratum service including adaptation functions*' and '*shall support point to multi-point transport stratum service including adaptation functions*'. Such transport stratum services may support link connections (or link flows) within the service stratum or within other layer networks within the transport stratum. Such link connections (or link flows) may be operated by entities other than the entity that operates the FPBN layer network that is providing the transport stratum service upon which those link connections (or link flows) are built. It is clear that a client/server relationship exists between a link connection (or link flow) and the transport stratum

service that supports that link connection (or link flow). It is also clear that in order for an FPBN to be able support different entities operating different layer networks within the transport or service strata, the client and server layer networks within such a client/server relationship must be separated such that the server layer network can provide transparent (and client agnostic) transport to the client layer network.

NOTE – When a client link connection (or link flow) extends beyond an FPBN transport stratum service without adaptation, the transport stratum service only provides transport for part of that link connection (or link flow), and adaptation is provided outside of the FPBN.

6.3 Control plane

The control plane configures the user plane to forward traffic from its source to its destination. The control plane will setup and maintain user plane service classes by allocating and scheduling FPBN resources according to the requirements of the services that an FPBN supports

To support NGN services that require QoS the FPBN control plane should support a RACF function [6].

The identifier space of the control plane may be independent of any other identifier spaces in an FPBN, see clause 0 for more details.

The control plane of a layer network should be physically or logically segregated from the other planes of that layer network. Control plane communications may use user plane trails or may use logically or physically segregated trails.

The user plane may rely on control plane mechanisms in order to provide survivability and robustness against failures. Therefore, the survivability design of the control plane is likely to be different to the survivability design of the user plane. In the case where the user plane relies on control plane mechanisms in order to provide survivability and robustness then the diversity of the topology of the control plane communications should be at least as great as the diversity provided to the user plane.

An FPBN may provide both cl-ps and co-ps user planes in order to provide both cl-ps and co-ps transport stratum services. The cl-ps user plane will be independent of the co-ps user plane and each user plane will have its own control plane.

Although the control plane of the cl-ps user plane will be isolated from the control plane of the co-ps user plane it is likely that there will be some overlap between the functions and features provided by both control planes. For example both control planes may use a routing protocol to distribute the topology of the user plane that they are controlling. An FPBN should reuse as many functions and features as possible where such functions and features are required in both control planes. For example if both control planes require a routing protocol then they should both use the same routing protocol, however the exact syntax and semantics of the routing protocol messages may differ between the two networking modes as the topology information that needs to be distributed by each mode and the requirements placed on each mode are not identical.

6.4 Management plane

The management plane provides configuration, fault reporting, billing, security, and performance management for an FPBN.

The identifier space of the management plane may be independent of any other identifier spaces in an FPBN, see clause 0 for more details.

The management plane of a layer network should be physically or logically segregated from the other planes of that layer network. Management plane communications may use user plane trails or may use logically or physically segregated trails.

An FPBN may provide both cl-ps and co-ps user planes in order to provide both cl-ps and co-ps transport stratum services. The cl-ps user plane will be independent of the co-ps user plane and each user plane will have its own management plane.

6.5 OAM, performance management and availability

An FPBN is required (as stated in the FPBN requirements document) to '*offer the appropriate OAM functions for each plane*' and to '*support performance monitoring (performance management) including availability considerations*'. OAM, performance monitoring and availability are related and this section discusses aspects of each function individually and then goes on to discuss the relationships between them.

A (server) layer network has two basic states: fully working, or broken to some degree. However, a specific client (service or layer network) of that (server) layer network will only see either a 'working' service (perhaps with some level of impairment) or a 'broken' service.

If the (server) layer network is a co-ps layer network then its trails have two basic states: available (and working within its performance objectives) or unavailable. Both these states are deterministic and can be fully specified. However, it is not possible to describe a cl-ps layer network so easily because cl-ps layer networks do not have a trail construct and therefore cl-ps layer networks can have a far wider range of what may be considered as impaired versus broken behaviour.

Within a well designed and well engineered network defects and performance degradation should be rare. However, there will be failures and/or performance problems from time to time and therefore OAM is required in order to detect and manage such problems. There are two broad categories of OAM: proactive fault detection ('always on') OAM and reactive fault location/diagnostic ('on demand') OAM.

Proactive OAM is generally responsible for the rapid detection of defects (for example by using CV flows) and initiating the necessary consequent actions. Proactive OAM should be as simple as possible so that the cost of continuously processing OAM flows is minimised. This cost of processing includes operational as well as capital costs (historically the operational cost of enabling continual OAM monitoring has been very high for some networking technologies which has resulted in operators disabling the proactive OAM in some of their layer networks). Proactive OAM should not be burdened with the complexity required for fault diagnosis or fault location identification. The role of proactive OAM is simply to detect defects in a layer network and perform the necessary consequent actions (which may include triggering reactive OAM).

Reactive OAM is responsible for providing and performing the more complex OAM functions that the proactive OAM does not perform, for example performance management measurements, defect diagnosis, defect location identification and tracing functions. These more complex OAM functions are not normally performed by proactive OAM for a number of reasons, including (but not limited to): complex OAM functions need not be performed continuously and the additional cost that they would add, to the proactive OAM component, is considered to be too large.

Performance monitoring (or performance management) is the measurement of transfer performance for a given trail when that trail is in the up state. As noted previously in clause 0, client layer networks inherit the impairments of their server layer networks and this inheritance is recursive down to the duct. Therefore the performance of a given trail is defined by the performance impairments inherited from its server layer networks plus the additional impairments introduced by the trail itself (from the layer network it is part of). This inheritance between client and server layer networks leads to a requirement that a server layer network's performance criteria shall be at least as stringent as its most stringent client layer network in order for the server layer network to be able to meet the performance criteria demanded by its client layer networks.

The availability of a given layer network is essentially a measure of the capability of that layer network to maintain connectivity in spite of one (or more) defects or failures. As noted previously because a link connection (or a link flow) in a client layer network is supported by a trail (or a connectionless trail) in that client's server layer network, a client layer network inherits certain characteristics (such as link diversity)

from its server layer network and this inheritance recurses down to the duct. This means that regardless of where in the network stack a given layer network is situated, its ability to effect disjoint routing is closely coupled to the available physical duct topology. Therefore, it is impossible to achieve routings in a client layer network that are more diverse than the physical duct topology.

In order to efficiently manage a layer network, that layer network's OAM, performance management and availability must be designed and processed in a logical order so that that layer network's OAM, performance management and availability mechanisms are extensible without adverse impact to that layer network or to the operator that 'owns' that layer network.

The recommended logical ordering is as follows. The differences between the needs and requirements of proactive OAM and reactive OAM should be well understood and then the network mode (i.e. cl-ps or co-ps for FPBNs) that the OAM will be operating in must be identified. This is because each of the two packet switched networking modes has different characteristics, defects and consequently different OAM requirements.

For each mode it is necessary to define suitable and appropriate OAM for defect detection and handling (i.e. proactive OAM), including defining which defects can occur in that networking mode. For example there is a common requirement for both packet switched networking modes to provide a CV (Connectivity Verification) mechanism and therefore both packet switched networking modes must provide a mechanism that allows a trail's termination sink to identify that trail's termination source. In the cl-ps mode the CV function effectively 'comes for free' because each and every packet contains a source address. However, verifying the connectivity of a cl-ps layer network that only supports transit flows requires some additional proactive OAM functionality. In addition to its other functions a periodic CV flow between a pair of flow or trail termination points can be used to distinguish whether that flow or trail is quiescent or broken.

For each defect identified in a given networking mode, it is necessary to define a set of entry and exit criteria (for the available and unavailable states) based on defect persistency as well as a set of consequent actions for that defect. The exact entry and exit criteria and consequent actions will depend upon the nature of the defect and the networking mode it applies to.

Once the available defects, their entry and exit criteria and any consequent actions have been defined (for the networking mode being considered), only then is it possible to start to address mechanisms for taking performance management measurements and assessing a given trail, connection, flow or layer network against any performance management SLAs that have been agreed. This is because performance measurements, at least for SLA purposes, are only meaningful when the network entity considered is in the available state.

It should be noted that it is not just performance management that is dependent on the correct order of processing as outlined above. Some other examples include:

- Network element specification (in terms of registers and threshold crossing exception reports).
- NMS/OSS (that have to process network element collected data about defects, availability and performance management).
- The definition of HRXs (and suitable end-to-end and apportioned availability and performance management objectives).
- The definitions of consistent network services with measurable SLAs.

6.5.1 OAM, performance management and availability of co-ps layer networks

NOTE – If a co-ps service is being guaranteed by the transport stratum then by implication the transport stratum has a "call admission policy" to prevent over subscription and the consequent performance degradation. So it may be necessary to describe a "blocked call" parameter, which could become important under network failure conditions.

NOTE – Note: A p-t-mp trail can be considered as a set of p-t-p connection instances between a source and a specific sink. From the perspective of a given client instance, the only thing of concern is whether that client's source/sink p-t-p connection is working or not. Therefore, p-t-mp connectivity can be discussed in terms of p-t-p connectivity behaviour.

A layer network requires some mechanism (or mechanisms) to enable it to differentiate the up state from the down state for a given p-t-p connection, which in turn allows that layer network to measure against any performance SLAs that have been agreed for a given connection in that layer network. There is a requirement for the up and down states to have been clearly identified before we can consider performance management because performance SLAs are only meaningful when the connection they refer to is in the up state.

NOTE – In general the server layer network's protection or restoration is designed such that it can recover the connection in the event of a failure before the connection is declared to be unavailable.

NOTE – In general a transport network is monitoring a transit connection i.e. the service trail terminations are not within the scope of the transport network.

The minimum set of possible defects within a co-ps layer network that proactive co-ps OAM should be capable of detecting is as follows.

Loss of connectivity – This defect occurs when traffic originating from the co-ps trail termination source does not arrive at the corresponding co-ps trail termination sink. For example, for a co-ps trail between TT_SoA (Trail Termination Source A) and TT_SkA (Trail Termination Sink A), traffic originating from TT_SoA does not arrive at TT_SkA.

NOTE – Due to congestion or packet loss a certain degree of lost connectivity may be deemed acceptable within a co-ps layer trail. Consequently a loss of connectivity defect should only be raised once connectivity has been lost for a sustained period of time as defined in the entry and exit criteria for the loss of connectivity defect.

Mis-connected connection – This defect occurs when, for whatever reason (for example, failures or accidental operator mis-configuration), a given trail termination source is connected to the wrong trail termination sink. For example, a trail that should exist between TT_SoA and TT_SkA is misconnected to TT_SkB.

Mis-merged connections – This defect occurs when, for whatever reason (for example, failures or accidental operator mis-configuration), traffic in one trail is 'leaking' into another trail. For example, for a co-ps trail between TT_SoA and TT_SkA, traffic arriving at TT_SkA is originating from both TT_SoA and TT_SoB.

Entry and exit criteria for the above defects are not defined in the FPBN architecture. However, definitions for defect entry and exit criteria along with definitions for when a connection is considered available or unavailable must be defined in order to allow HRXs with performance apportionments to be specified.

Y.1710 [7] specifies requirements for OAM functionality in MPLS networks and Y.1711 [8] specifies an operation and maintenance mechanism for MPLS networks. Although specific to MPLS networks, the principles contained in Y.1710 and Y.1711 can be generalised and applied to any co-ps layer network and co-ps OAM mechanisms in an FPBN should reuse the general principles of Y.1710 and Y.1711 as appropriate to the specific co-ps layer network technology used.

For services that provide bi-directional connectivity between two communicating entities, if one direction enters the down state then the service (i.e. both directions) should enter the down state (i.e. the service should be considered unavailable). Therefore, the collection of performance management measurements for a bi-directional connection must be suspended in both directions even if only one direction of the connection is defective (i.e. in the down state).

The availability of a given connection is essentially a measure of the capability of that connection (or more precisely the layer network that that connection belongs to) to maintain connectivity (with the associated performance criteria that that connection has guaranteed) in spite of one (or more) defects or failures.

6.5.2 OAM, performance management and availability of cl-ps layer networks

In general it is not feasible to individually monitor the state of all flows within an FPBN cl-ps layer network. In addition, it is also not feasible for an FPBN to individually monitor the state of all service stratum sessions. This is in part due to the large number of flows that may exist at any one time and the short lived nature of many of those flows.

It is however feasible to monitor the connectivity (i.e. the ability to transfer packets between two points) in a cl-ps layer network. A cl-ps layer network therefore requires some mechanism (or mechanisms) to enable it to differentiate whether or not connectivity exists between two points within that cl-ps layer network. This in turn allows a cl-ps layer network to measure any guarantees that have been agreed for connectivity between two points in that cl-ps layer network. Additionally, an FPBN should be able to detect when traffic is delivered to an unintended destination(s)/egress(es).

The minimum set of possible defects within a cl-ps layer network that proactive cl-ps OAM should be capable of detecting is as follows.

Loss of connectivity – This defect occurs when traffic originating from a cl-ps flow termination source does not arrive at the corresponding cl-ps flow termination sink. For example, for a cl-ps flow between FT_SoA (Flow Termination Source A) and FT_SkA (Flow Termination Sink A), traffic originating from FT_SoA does not arrive at FT_SkA.

NOTE – Due to congestion or packet loss a certain degree of lost connectivity may be deemed acceptable within a cl-ps layer flow. Consequently a loss of connectivity defect should only be raised once connectivity has been lost for a sustained period of time as defined in the entry and exit criteria for the loss of connectivity defect.

Packets within a cl-ps layer network always contain a unique (within the context of that layer network) source address and therefore cl-ps layer network packets are always self-identifying with respect to their source. This means that cl-ps layer networks only multiplex, and never merge, flows and therefore a cl-ps layer network cannot experience mis-connected flow defects or mis-merged flow defects.

Entry and exit criteria for the above loss of connectivity defect are not defined in the FPBN architecture. However, definitions for defect entry and exit criteria along with definitions for when a flow is considered available or unavailable must be defined in order to allow HRXs with performance apportionments to be specified.

Flows are always uni-directional, however many services requires bi-directional connectivity and therefore it is often necessary to monitor the connectivity of both directions between two points in a cl-ps layer network. For services that provide bi-directional connectivity between two communicating entities, if one direction loses connectivity then the service (i.e. both directions) should enter the down state (i.e. the service should be considered unavailable). Therefore the collection of performance management measurements between two points in a cl-ps layer network must be suspended in both directions even if the loss of connectivity is only in one of the directions.

The availability between two points in a cl-ps layer network is essentially a measure of the capability of that layer network to maintain connectivity with the associated performance criteria that have been guaranteed.

7 Relationship between layer networks and the ISO BRM

The X.200 model and the G.805/G.809 model are useful in describing different aspects of the transport stratum. In general the X.200 model is most useful when describing the horizontal relationships (between peered layers) and functions between layers within a single stack. The G.805/G.809 model is most useful when describing the recursive interlayer relationships in multilayer transport networks. The term *layer* is used when applying the X.200 model and the term *layer network* is used when applying the G.805/G.809 model. The definition of 'layer network' used in G.805/G.809 is not the same as the definition of 'layer' used

in X.200. Both X.200 and G.805/G.809 are widely used within the industry to describe networks. A brief overview of the X.200 model and the G.805/G.809 model is provided in appendix A.

8 Relationship with other strata

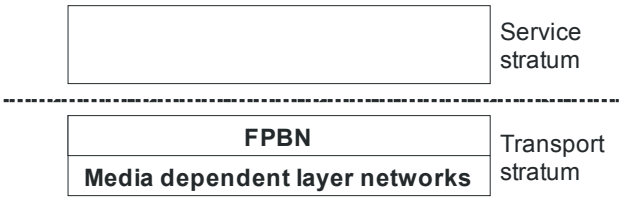


Figure 3 – Relationship between an FPBN and the transport and service strata

An FPBN is located between the service stratum and the lower part of the transport stratum from a interlayer point of view (as defined in G.805 and G.809). An FPBN may provide co-ps and/or cl-ps transport stratum services. The FPBN may be implemented with multiple layer networks as described in clause 6.

For transparency, an FPBN is independent of any lower (server) layer networking (media dependent) technologies. The lower (server) layer network provides the necessary adaptation functions and transport services required in order to interconnect FPBN nodes.

FPBN packets may be adapted onto (i.e. encapsulated in) both present and future server layer networking technologies.

8.1 Relationship between an FPBN and its client (service or layer network)

As required in Y.2001 [9] an FPBN should act as a server layer and therefore must be independent of its client layers. The client layer packets, whether they are user packets, management packets or signalling packets, are all treated as the payload of an FPBN user plane.

Client layers can be carried over cl-ps, co-ps or both transport modes as long as the service requirements of the client layers are satisfied.

One service can be mapped into one or more than one service class.

8.2 Relationship between an FPBN and its server layer network

An FPBN should act as a client of its underlying server layer and therefore the server layer must be independent of the FPBN.

9 Interfaces in an FPBN

An FPBN can serve as a core network and/or an access network, which may belong to different operators. An FPBN can interconnect remotely with another FPBN and/or connect with other heterogeneous transport networks.

The NGN architecture overview is provided in TR-FRA [10]. This illustrates the functional groups and the network interfaces which an FPBN may have.

Consider the network interconnection scenarios depicted in Figure 4, clause 0, below, in which the reference points of an FPBN are defined. In this figure, the core transport network may be connected to one or more access transport networks, and each access transport network may be connected to one or more user networks.

FPBN A is interconnected with the adjacent FPBN B, at the same time it is also interconnected with FPBN C. FPBN D belongs to a different operator to the operator that owns FPBNs A, B and C. FPBN D is connected with FPBN A but is not trusted by it. Another transport network (marked 'Other TN' in Figure 4) is heterogeneous but connected with FPBN A and it is also not trusted by FPBN A.

10 Reference points in an FPBN

The reference points for a layer network within an FPBN are classified as type a, b, c, d, e, or f. The network interfaces include UNI, I-NNI (Interior NNI of an FPBN), and E-NNI (Exterior NNI of an FPBN).

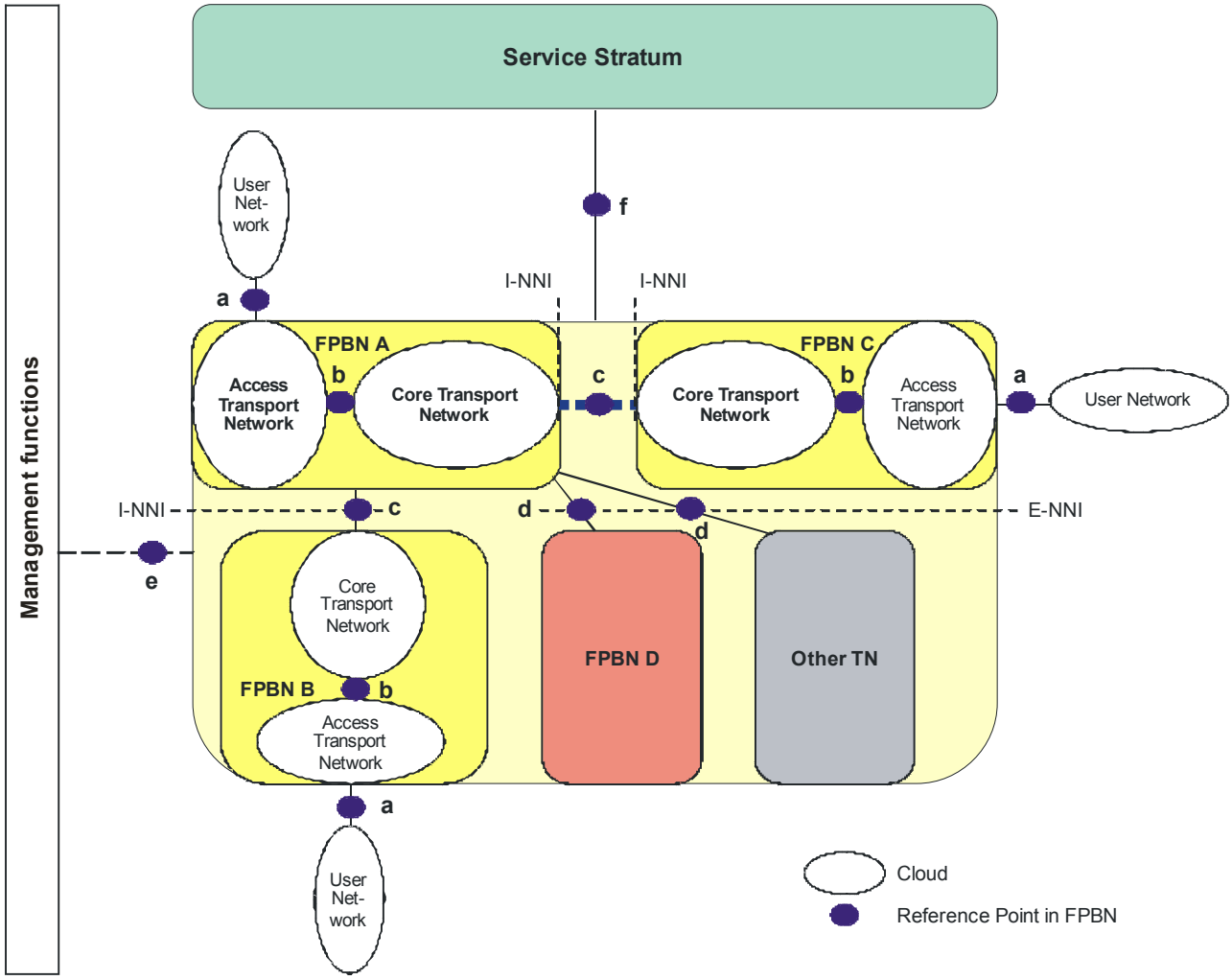


Figure 4 – Reference points in an FPBN

In Figure 4 above each FPBN shown consists of an access transport network and a core transport network. However, the access transport network or the core transport network may be null. In other words an FPBN may only support an access transport network or a core transport network but not both.

A user network could be a home network, an enterprise network, or some other network.

Reference point type (RPT) a exists between a user network and an FPBN access transport network. It allows the user to transfer and receive user data, OAM and signalling information.

RPT a may support more than one service instance within an NGN.

RPT b is located between an FPBN access transport network and an FPBN core transport network. It acts as an aggregation point for the FPBN core transport network.

RPT c represents an FPBN I-NNI and is located between two adjacent FPBN core transport networks. A single FPBN I-NNI may support more than one service instance destined to different destinations.

RPT d represents an FPBN E-NNI and is located between two FPBNs that belong to different operators, or an FPBN and a heterogeneous transport network. A single FPBN E-NNI may support more than one FPBN service instance destined to different destinations in either operator's network.

RPT e represents the management interface between the management plane of a layer network that belongs to the transport stratum and any network management functions which are outside of that layer network's management plane.

RPT f represents the interconnection point between the transport and service strata within an NGN.

11 Naming and addressing in an FPBN

An FPBN needs an addressing mechanism to identify a node, a link, an interface or other entities.

Identification is required in each layer network of the NGN transport stratum. A given entity will be assigned one or more identifiers depending on the function of that entity. FPBN layer network identifiers are independent of any client (and any server) layer network identifiers even if they share the same syntax or structure. At the boundary of a layer network mapping and/or translation mechanisms are required in order to set up relationships between the identifier used by the client layer network and the identifier used by the server layer network.

NOTE – Identifiers could be determined from multiple discontiguous fields. The global uniqueness of an identifier may be provided by the context as well as the identifier itself.

Whether a given identifier is considered to be a name or an address is dependent on several factors including the perspective (and location) of the entity that is using (or mapping to) that identifier. The same identifier can be considered an address to one entity and a name to a different entity because their perspective is different.

An FPBN may require multiple identifier spaces, for example user, management and control plane identifier spaces. Each identifier space may be independent of the other identifier spaces (even if they use the same syntax or structure). Additional identifier spaces may also be used, for example to allow independent identification of the components that implement control plane functions.

Each resource at a network boundary of the user plane of each layer network will have a name (from the user plane name space of that layer network) which is visible to the exterior of the network. These names may need to be translated into topologically significant addresses (from the user plane address space of that layer network) on the interior of the layer network boundary. In other words, resources on the interior of a given layer network use addresses. When these resources are made visible to entities on the exterior of that layer network a name may be provided instead of the interior address.

Identifiers within a layer network are administered by the owner of that layer network and must be unique within that context. Any identifiers that are made externally visible are administered within the boundaries of the enclosing network to ensure that they are unique within that context.

12 Security considerations

An FPBN requires mechanisms to make it safe or "trusted" by its client layer.

An entity can be said to 'trust' a second entity if the first entity assumes that the second entity will behave as expected by the first entity. Such an assumption of trust relies on the identity of the second entity being authenticated.

Appendix A

Relationship between layer networks and the OSI BRM

This appendix highlights and clarifies the key differences between the G.805/G.809 model and the X.200 model in order to assist a practitioner of one model to achieve an appreciation of the other model. This section is not intended to be a comprehensive tutorial on either the G.805/G.809 or X.200 models.

A.1 The X.200 model

The X.200 model is normally applied to describe a single 'network stack' from the application layer to the physical transport layer. X.200 describes a single network in terms of the logical functions that form the network and the hierarchy that exists between those logical functions at different levels within the network.

When describing a network, X.200 assumes that there is only a single 'network stack' (a single open system), and that this contains a hierarchy of (up to seven) different layers that are named and organised according to their functions: Applications, Presentation, Session, Transport, Network, Data Link and Physical. Generally the transport stratum in the NGN architecture could be represented by the lower three layers in the OSI BRM, i.e. the Network, Data Link and Physical layers.

The Network layer plays an important role in providing the interface between the service stratum and the transport stratum. The core function in the Network layer is routing and relay. It provides the service stratum with connection-oriented mode (co-ps) or connectionless mode (cl-ps) layer network services. The layering of the transport stratum based on the X.200 model is shown in Figure A-1.

A.2 The G.805/G.809 model

The G.805/G.809 model is used to describe "layer networks" within the transport stratum. Thus the G.805/G.809 model includes the concept of recursion, i.e. one layer network can be the client of another layer network. This is known as a client/server interworking relationship. G.805/G.809 provide a set of tools and rules that allows us to visualize complex transport networks that are multi-operator and multi-technology.

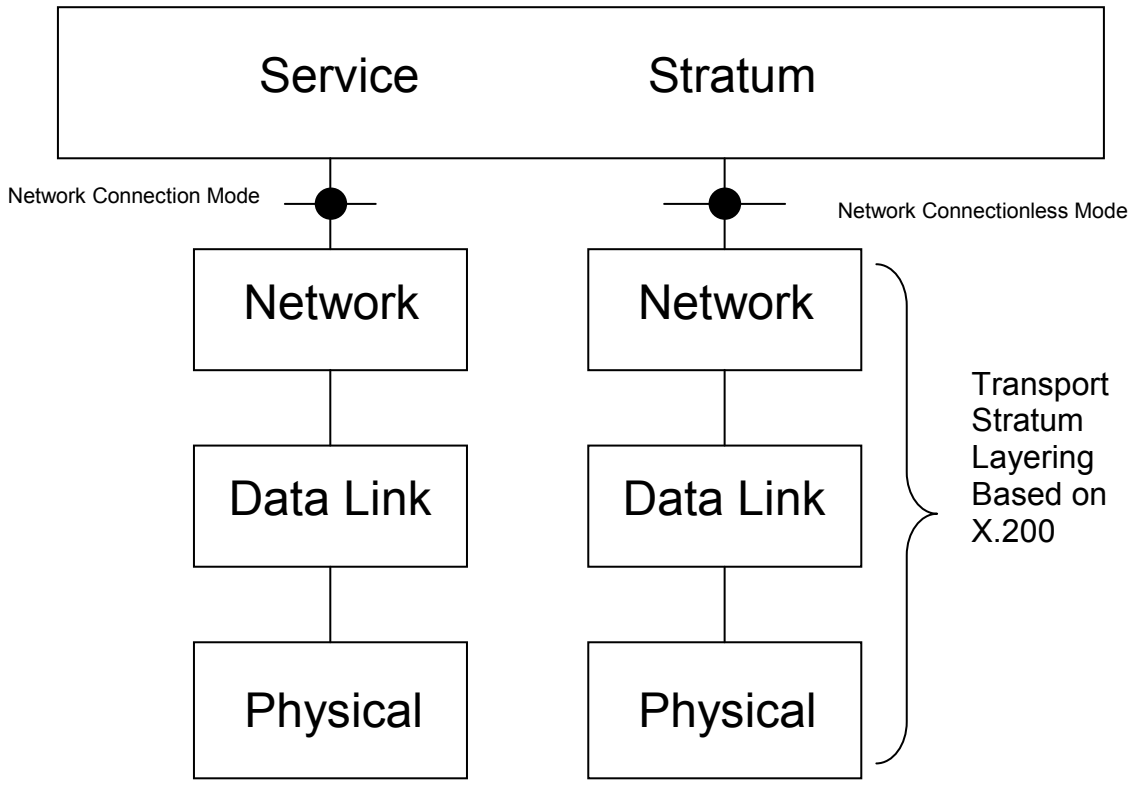


Figure A.1 – Transport stratum layering based on the X.200 model

A.3 Comparing the two models

In contrast to X.200, G.805/G.809 assumes that a single layer network may contain all of the functions described in X.200. In G.805/G.809, a layer network may be one of many that co-exist in parallel (either completely independently of each other or nested in a client/server relationship), each of which have their own set of functions that map to the functions that are described by the OSI BRM (termed "layers" in X.200). G.805/G.809 does not restrict the functions that can exist within a layer network, which allows the G.805/G.809 model to describe a layer network (or stack of layer networks) to whatever level of abstraction is most appropriate. Similarly, G.805/G.809 does not restrict the number of layer networks that can exist within a 'network stack', which allows G.805/G.809 models to describe a possibly infinite number of client/server relationships between layer networks in the 'network stack'.

A single layer network as described by G.805/G.809 does not map directly to a single layer as described in X.200. In fact, client/server relationships between G.805/G.809 layer networks allow for them to function independently, and each layer network has its own instantiation of the OSI BRM which is distinct from any instantiation of the OSI BRM in any parallel layer network. This includes both horizontally and vertically parallel layer networks. However, layer networks (as described by G.805/G.809) need not instantiate all seven layers of the OSI BRM.

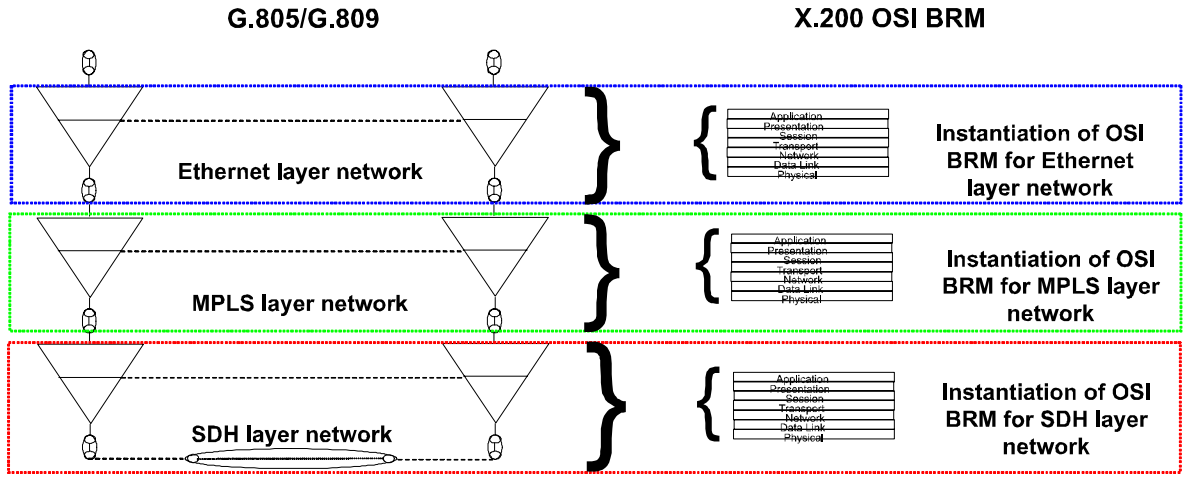
This is not to say that the functionality resembling that described in the OSI BRM is not present in layer networks (as defined by G.805/G.809), but rather that the functionality may be distributed quite differently, say across a fewer or greater number of functions, or just simply distributed differently, and not 'layered' in the same rigid hierarchical fashion as that specified in the OSI BRM.

NGN architectures require a greater amount of flexibility than was envisaged when X.200 was developed. Further details can be found in section 6 of Y.2011 where the relationship between NGNs and X.200/OSI BRM is discussed in more detail. Annex A of Y.2011 identifies some areas of X.200 which are either too restrictive and/or insufficient to accommodate recent, emerging or expected future technologies.

Additionally, Annex B of Y.2011 contains a detailed list of items retained from X.200 (since they are applicable to NGN) and a list of items not retained (since they are not applicable to NGN) from X.200.

The diagram below shows how each layer network (as described by G.805/G.809) has its own instantiation of the OSI BRM which is distinct from any other instantiation of the OSI BRM that exists in any parallel layer networks. The diagram shows a scenario in which an Ethernet layer network is supported by an MPLS layer network that is, in turn, supported by a SDH layer network. Each layer network is depicted using the diagrammatic conventions described in G.805/G.809. Alongside each layer network, an instantiation of the X.200/OSI BRM is shown to highlight that each of the three layer networks (Ethernet, MPLS and SDH) co-exist (nested in client/server relationships) and each of them has their own set of functions that map to the functions that are described by X.200/OSI BRM.

Note that a layer network does not necessarily instantiate all seven layers of the OSI BRM (for example MPLS would not instantiate the OSI BRM physical layer). It is also worth noting that the diagram shows a hierarchy of layer networks at a given level of abstraction. The G.805/G.809 model allows a layer network to be described at any level of abstraction, so for example the diagram could be expanded in order to decompose the SDH network into its constituent layer networks (VC-4, Multiplex Section, Regenerator Section etc.).



In addition to providing a model for describing layer networks (and their layering and interactions), the G.805/G.809 model can also be mapped into detailed equipment specifications (for example I.732 provides an ATM equipment specification and G.783 provides an SDH equipment specification) as well as management information models (for example TMF MTNM[8] specifications TMF 513 [11], TMF 608 [12], TMF 814 [13] and TMF MTOSI[9] TMF 517 [14] and TMF 608 [15]).

Detailed equipment specifications are considered important by equipment manufacturers as they provide a detailed formal specification of what components a piece of transport equipment should contain, how those components should interact and how the piece of equipment itself should behave. Management information models are considered important by network operators (and management standardisation organisations such as the TMF) because they formally define and describe the reference points that the operator's OSS system must interact with in order to manage a piece of transport equipment (and ultimately the transport network itself).

The diagram below shows a single SDH path layer network (e.g. VC-4) at the most abstract level (the highest level of partitioning), i.e. it is depicted as a single subnetwork bounded by its access points. This SDH path layer network is used to support various "network stacks". Note that the SDH network is itself

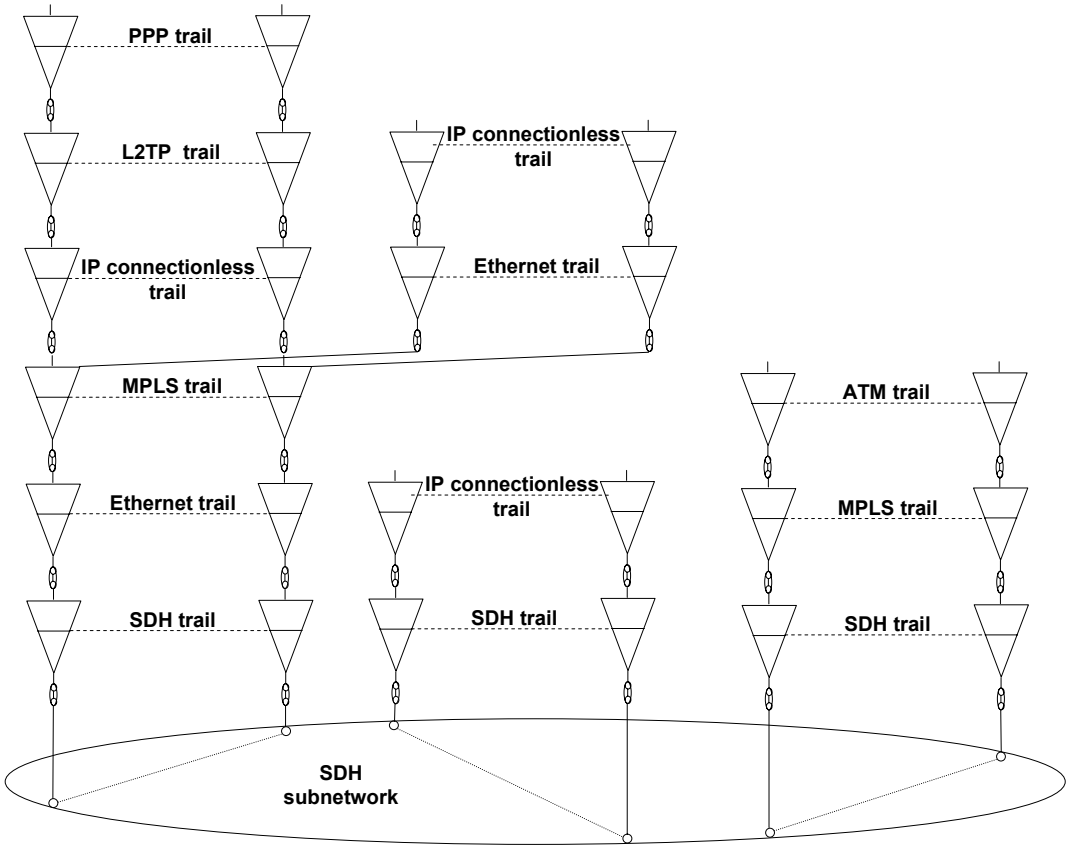
[8] Multi-Technology Network Management.

[9] Multi-Technology Operations System Interface.

decomposed into multiple layer networks (e.g. VC-4, Multiplex Section, Regenerator Section, Wavelength etc. down to the duct level). The diagram illustrates that G.805/G.809 allows us to describe a single server layer network that may support multiple (different) client layer networks (it is not possible to do the same with the OSI BRM because the OSI BRM assumes a single 'network stack'). The diagram also shows how G.805/G.809 supports recursion (through client/server relationships) and demonstrates that layer networks are not always stacked according to the rigid model provided by X.200/OSI BRM. A wide variety of network stacks may be modelled using G.805/G.809. This is illustrated in the diagram below.

Working from left to right, the network stacks shown in the diagram are:

- PPP over L2TP over IP over MPLS over Ethernet over SDH
- IP over Ethernet over MPLS over Ethernet over SDH
- IP over SDH
- ATM over MPLS over SDH



3.6 – FPBN candidate technologies*

Introduction

This document specifies the candidate technologies for the FPBN.

Table of Contents

* Status D: The FGNGN considers that this deliverable is not yet mature, requiring discussion and technical input to complete development.

3.6 – FPBN candidate technologies

1 Scope

The scope of this work item is the evaluation of packet based 'candidate technologies' against the FPBN requirements and architecture documents. The evaluation shall take the form of an analysis that details how a given candidate technology supports (or fails to support) the FPBN requirements and architecture, as well as an analysis identifying which (if any) functions or features of the candidate technology may need to be added, deprecated, modified, enhanced etc. in order for the candidate technology to support the FPBN requirements and architecture.

It is not in scope for this work item to recommend any technology as the mandated 'solution' for providing packet based transport services in a NGN.

2 References

–

3 Terms and Definitions

–

4 Abbreviations

–

Appendix A

Template for evaluation of candidate technologies against the FPBN requirements and architecture

Template for the Evaluation of Candidate Technologies

This template is based on the WG7 requirements, FGNGN-OD-00153.doc.

Name of candidate architecture:

Mode being evaluated:

If a requirement is not considered applicable for the mode being evaluated, indicate this under the requirement.

FPBN requirements

i) *General requirements*

This section specifies general requirements for the FPBN. More detailed requirements are specified in the other sections below.

The FPBN:

1. Shall provide both connectionless and connection-oriented services for multiple client types.
2. Shall efficiently support p-t-p and p-t-mp services.
3. Should efficiently support mp-t-mp services.
4. Shall support at least absolute QoS in the co-ps mode (if a co-ps mode is provided).
5. Should allow a smooth migration from current cl-ps and co-ps packet networks. (Detailed requirements should be provided by FGNGN WG6.)
6. Shall interwork and co-exist with current cl-ps and co-ps packet networks. (Detailed requirements should be provided by Q7/13.)
7. Shall support arbitrary network topologies and be able to expand bandwidth, topology, number-of-customers and number-of-services incrementally.
8. Shall secure, protect and transport user traffic as appropriate to the requirements of the service.
9. Shall detect, and recover from, facility and equipment failures and performance degradation as appropriate to the requirements of the service.
10. Shall offer the appropriate OAM functions for each plane.
11. Shall completely secure the internal control and management plane traffic from external attack and shall ensure that it remains secure and stable under situations of extreme stress.
12. Shall secure the management plane to prevent access to control and management functions by unauthorized users.
13. Shall strive to be able to accommodate unforeseen traffic types/vectors.
14. Shall allow statistical multiplexing for efficiency.

15. Shall support lawful intercept as required.
16. Shall support accounting functions by being able to monitor at least network utilization and performance parameters.
17. Shall provide the ability to distinguish between urgency (delay) and importance (survivability).
18. Shall support services that require in-order delivery of packets.
19. Should support off-path control and management planes.
20. Shall provide harmonized and consistent means of referring to user plane access points.
21. Shall provide traffic user plane defect detection and handling (OAM) that is not reliant on the control and/or management planes and is not a function of the nature of the client being transported.
22. Shall harmonize trail or connection setup and teardown with OAM activation & deactivation.
23. Shall support mechanisms to avoid traffic impact during reconfiguration.
24. Shall attempt to keep traffic flowing while recovering from failures.
25. Shall only deliver traffic from the intended source to the intended destination(s) except under extremely rare multiple failure conditions.
26. Shall support emergency services.

ii) *Detailed requirements*

This section specifies requirements that are more detailed than the general requirements specified above.

iii) *Addressing related requirements*

This section specifies addressing related requirements for the FPBN. These requirements apply to the network, not necessarily to the user packet itself.

The FPBN:

27. Shall support the identification of a packet's source and its destination within the FPBN in the cl-ps mode.
28. Shall support the identification of a connection's source within the FPBN in the co-ps mode at the connection's destination.
29. Should support FPBN addressing that is disjoint from any client addressing.

iv) *Control related requirements*

This section specifies control related requirements for the FPBN.

The FPBN:

30. Shall support mechanisms to safe guard against persistent (i.e. looping) traffic units in the cl-ps mode.
31. Shall support mechanisms to safe guard against co-ps connections containing forwarding loops.
32. Shall facilitate the in-order delivery of the traffic unit as required.
33. Shall ensure the integrity of the control information (e.g. header checksum).

v) *QoS related requirements*

This section specifies QoS related requirements for the FPBN.

The FPBN:

34. May support queuing priority, which can be implicit or explicit.
35. May support discard priority, which can be implicit or explicit.

vi) *Network performance management (PM) related requirements*

This section specifies PM related requirements for the FPBN.

The FPBN:

36. May provide utilization information on links and nodes.
37. Shall support performance monitoring (PM) including availability considerations.
38. Shall suspend any network performance measurements (for both directions of the trail or connection) if either direction of a bi-directional trail or connection enters the unavailable state.

vii) *Protection related requirements*

This section specifies protection related requirements for the FPBN.

The FPBN may support mechanism to recover from equipment or facility failures. For example:

39. inside a subnetwork
40. inside a flow domain
41. between subnetworks
42. between flow domains
43. between a subnetwork and a flow domain
44. between an access group and a flow domain

viii) *Payload related requirements*

This section specifies payload related requirements for the FPBN.

The FPBN:

45. May support mechanisms for identifying the payload type of a FPBN packet or connection at the adaptation function if used.
46. May support mechanisms for dynamically discovering the maximum transmission unit (MTU) of a path or connection across an FPBN.
47. Shall deliver packets in-sequence for the connection-oriented mode of operation.
48. May support mechanisms to enable the in-sequence delivery of packets for the connectionless mode of operation.
49. May support mechanisms to ensure the integrity of the adapted information.

ix) *OAM related requirements*

This section specifies OAM related requirements for the FPBN.

The FPBN:

50. Shall support simple OAM mechanisms to detect and handle defects.
51. Shall support OAM mechanisms that are agnostic about the client layer that the FPBN is carrying (i.e. it shall be possible to manage the server layer using the same mechanisms independent of the client that is being transported).
52. Shall support OAM defect detection and handling in the traffic user plane.

53. Shall support OAM defect detection and handling (e.g. defect indication to the trail termination) on an uni-directional basis in the traffic user plane in the co-ps mode.

54. Shall support the appropriate consequent actions (after defect detection) at a trail termination sink (e.g. suppression of client traffic, defect indication to the client and defect indication to the trail termination source) (for co-ps and co-cs clients).

x) *Security related requirements*

This section specifies security related requirements for the FPBN. The intent is to protect against and detect unauthorized end stations and not unauthorized users on authorized end stations. WG5 (security) should provide input towards clarifying this text.

The FPBN:

55. Shall provide mechanisms to protect the control plane or processes that support the delivery of packets to the control plane from malicious attacks.

56. Shall provide mechanisms to protect the management plane or processes that support the delivery of packets to the management plane from malicious attacks.

57. Shall provide mechanisms to detect malicious attacks targeted at the control plane or processes that support the delivery of packets to the control plane.

58. Shall provide mechanisms to detect malicious attacks targeted at the management plane or processes that support the delivery of packets to the management plane.

xi) *Control plane requirements*

This section specifies control plane related requirements for the FPBN.

The FPBN:

59. Shall support a control plane that is independent of any particular client layer control plane.

60. Shall have an unambiguous and reliable means of distinguishing control packets from user plane packets and management plane packets.

61. Shall allocate resources to control plane packets such that no amount of user plane traffic can cause control functions to become inoperative.

xii) *Management plane requirements*

This section specifies management plane related requirements for the FPBN.

The FPBN:

62. Shall support a management plane that is independent of any particular client layer management plane.

63. Shall have an unambiguous and reliable means of distinguishing management packets from user plane packets and control plane packets.

64. Shall allocate resources to the management plane packets such that no amount of user plane traffic can cause management functions to become inoperative.

xiii) *Transport stratum service requirements*

This section specifies transport stratum service requirements for the FPBN. The services in the transport stratum are divided into two groups; basic service and enhanced services

xiii-1) *Basic transport stratum service requirements*

This section specifies basic transport stratum service requirements for the FPBN.

The FPBN:

65. Shall provide a point to point transport stratum service without adaptation.
66. Shall support point to point transport stratum service including adaptation functions.
67. Shall support point to multi-point transport stratum service including adaptation functions.

xiii-2) *Enhanced transport stratum service requirements*

This section specifies enhanced transport stratum service requirements for the FPBN.

The FPBN:

68. Should support multi-point to multi-point transport stratum service including adaptation functions.
69. Shall support connection-oriented transport stratum services with absolute QoS assurance.
70. Shall support transport stratum services with relative QoS.

Printed in Switzerland
Geneva, 2005