Ethernet Access for Next Generation Metro and Wide Area Networks

Cisco Validated Design I

September 24, 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-14760-01

Cisco Validated Design

The Cisco Validated Design Program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit www.cisco.com/go/validateddesigns.

Ethernet Access for Next Generation Metro and Wide Area Networks

CONTENTS

Ethernet Access for Next Generation Metro and Wide Area Networks

Introduction

Scope

This document provides design recommendations, configuration examples, and scalability test results for implementing a next-generation WAN for Voice and Video Enabled IPsec VPN (V3PN) based on a service provider WAN interface handoff using Ethernet at the enterprise campus and branch locations.

Purpose

This document provides the enterprise network manager with configuration and performance guidance to successfully implement or migrate to a WAN architecture using Ethernet as an access technology to a service provider network.

The key to success is the appropriate implementation of quality-of-service (QoS) on a per-branch or per-application class per-branch technique. In traditional Frame Relay, ATM, and leased-line WANs, this QoS function is implemented at lower data rates, is limited by the number of physical interfaces or ports that can be terminated in the WAN aggregation router, or is offloaded to an interface processor. Examples of offloading per-virtual circuit (VC) shaping and queueing are the ATM PA-A3 port adapter and the virtual IP (VIP) interface processor with distributed Frame Relay traffic shaping.

With current Ethernet access to the service provider network commonly at 100 Mbps or 1 Gbps data rates, the data rate of the user-network interface (UNI) interface is no longer a gating factor.

Because this implementation relies heavily on per-branch or per-application per-branch QoS techniques, and each instance of QoS can be a heavy consumer of CPU resources, the suitability of each platform is a function of the number of peers and the total bandwidth available, as well as the target data rate on a per-peer basis.

Currently, the access and mid-range routers (the Cisco 800, 1800, 2800, 3800, and 7200 VXR Series platforms) do not offload to an interface processor, and do not have any means of hardware assistance with implementing HCBWFQ on a per-branch/peer basis.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

However, the Cisco 7600 Series implements distributed packet buffering, queueing, and scheduling on certain classes of interfaces:

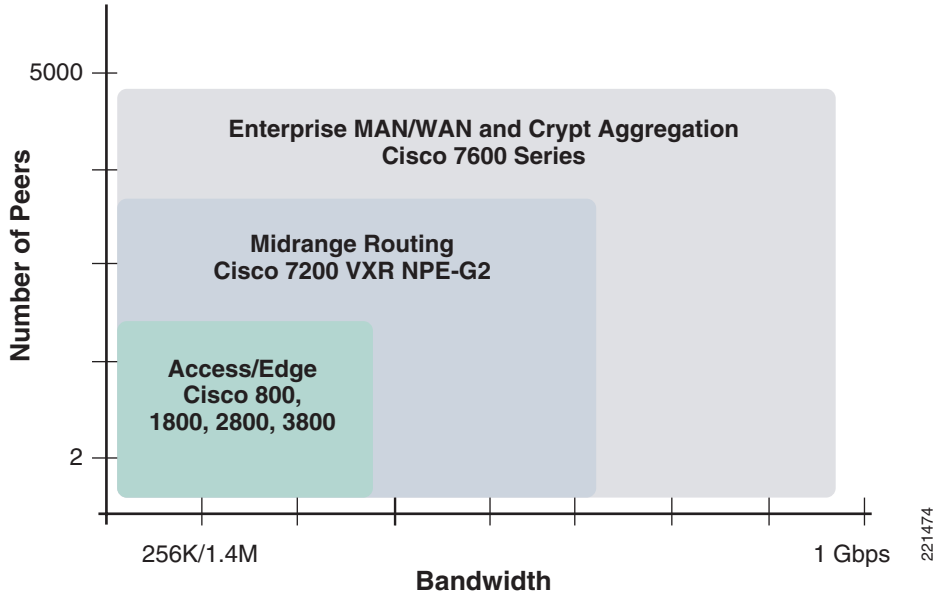
- Distributed Forwarding Card 3 (DFC3) (or integrated DFC3 on SIP600)
- Optical Services Module (OSM) WAN and SIP-600 ports

Note Regarding the OSM, check with your account team to verify end-of-sale and end-of-life announcements prior to implementation.

- FlexWAN (SIP-200, SIP-400)

The goal, therefore, is to provide sufficient scale testing to provide conservative estimates of the bounds of the three router platform categories, as shown in Figure 1.

Figure 1 Router Platform Bounds



The legends on Figure 1 range from 2–5000 peers and from less than 2 Mbps aggregate traffic to over 1 Gbps of aggregate traffic. Intermediate hash marks are void as to scale because the performance section provides specific guidance.

Finding the most cost-effective hardware platform that meets or exceeds the expected offered load with the desired features enabled is a core requirement of all network designs.

Prerequisites

The target audience is a Cisco enterprise customer deployment. It is not intended as a reference for a service provider offering Metro Ethernet services. Instead, service providers should contact their account team for access to the following documents:

- *Metro Ethernet 3.1 Design and Implementation Guide*
- *Metro Ethernet 3.1 Quality of Service*

For additional information on V3PN deployments, the following series of design guides are available at http://www.cisco.com/go/srnd:

- *IPsec VPN WAN Design Overview*
- *Multicast over IPsec VPN Design Guide*
- *Voice and Video Enabled IPsec VPN (V3PN) SRND*
- *V3PN: Redundancy and Load Sharing Design Guide*
- *Dynamic Multipoint VPN (DMVPN) Design Guide*
- *IPsec Direct Encapsulation VPN Design Guide*
- *Point-to-Point GRE over IPsec Design Guide*
- *Enterprise QoS Solution Reference Network Design Guide*
- *Business Ready Teleworker*
- *Enterprise Branch Architecture Design Overview*
- *Enterprise Branch Security Design Guide*
- *Digital Certificates/PKI for IPsec VPNs*

Key Benefits of Metro Ethernet

Metro Ethernet is one of the fastest growing transport technologies in the telecommunications industry. The market for Ethernet is extremely large compared to other access technologies such as ATM/DSL, T1/E1 Serial, or Packet over SONET (POS), making Ethernet chipsets and equipment comparatively low cost. Ethernet provides the flexibility to cost-effectively move from 10 Mbps to 100 Mbps to 1 Gbps as an access link, with full-duplex (FDX) 100 Mbps and 1 Gbps Ethernet being the norm. Carriers are more commonly using Ethernet access to their backbone network, whether via SONET/SDH, MPLS, Frame Relay, or the Internet. Broadband connectivity is provided by an Ethernet handoff to either a cable modem or DSL bridge.

Key benefits of Metro Ethernet include the following:

- Service enabling solution
  - Layering value-add advanced services (AS) on top of the network
- More flexible architecture
  - Increasing port speeds without the need for a truck roll and typically no new customer premises equipment (CPE)
  - Evolving existing services (FR/ATM inter-working) to an IP-optimized solution
- Seamless enterprise integration
  - Ease of integration with typical LAN network equipment
  - IP optimized

Challenges

One advantage of Ethernet as an access technology is that the demarcation point between the enterprise and service provider may no longer have a physical interface bandwidth constraint. Rather, the amount of offered load to the service provider WAN is now limited logically by means of a software-configured QoS-based policer configured in the service provider CPE and/or provider edge router or switch.

In this new paradigm, the QoS function has moved from congestion feedback being triggered by the hardware-based transmit (TX) ring or buffer in the physical interface to a logical software-based token bucket algorithm.

Routers that do not offload or distribute this logical QoS function to a CPU dedicated to the physical interface must use main CPU resources to manage the token bucket. When the interface processor provides congestion feedback, the main CPU needs to manage the software queues during periods of congestion. With no congestion, the interface processor can simply transmit the frame; no main CPU resources are consumed to address queueing.

Queueing packets is the process of buffering packets with the expectation that bandwidth will be available in the near future to successfully transmit them. A queue has some maximum threshold value, commonly 64 (packets), but it is configurable. When the queue contains the number of packets equal to the threshold value, subsequent packets are dropped, which is called a tail drop. Random Early Detection (RED) is a means to randomly drop packets before tail dropping. Weighted RED (WRED) uses the ToS byte to determine the relative importance of the queued packets, and randomly drops packets of less importance. For TCP-based applications, packet loss effectively decreases the arrival rate and thus eliminates the congestion rather quickly. WRED is better than tail drops at educating the TCP applications on the amount of available bandwidth between the two endpoints.

In either case, the QoS burden to the main CPU with QoS enabled on a single physical output interface is approximately 10 percent.

On routers that must manage the token bucket by counting the arrival rate of packets with the main CPU rather than a distributed CPU or interface processor, the QoS burden is substantially higher than 10 percent. One reason is that the main CPU must be involved with accumulating counters for every packet, regardless of whether congestion is present to engage queueing. There is no interface processor to provide congestion feedback.

In the past, the QoS component of Cisco IOS primarily addressed congestion feedback from an interface processor rather than from a logical shaper function. Evidence of this is that until recently, Hierarchical Class-Based Weighted Fair Queueing (HCBWFQ) configurations on logical interfaces (crypto or generic routing encapsulation tunnels) were always process-switched when the shaper is active. HCBWFQ configurations on physical interfaces such as FastEthernet also exhibit a higher amount of process switching than if the CBWFQ configuration is applied to a serial interface.

From a design standpoint, the enterprise network manager must be made aware of the performance capabilities of the entire Cisco product line from the low end teleworker router to the campus crypto and WAN aggregation to deploy a device capable of processing the expected offered data load for the configured security, management, and control plan of each device.

Starting Assumptions

This section defines the key elements of the network topology, including terminology and definitions.

Key Elements

In addition to the primary element that the branch and headend locations are connected to the WAN by means of some form of Ethernet handoff from the service provider, other elements include the following:

- All LAN-originated traffic, voice over IP (VoIP), video, and data is encrypted. Management traffic such as SSH, NTP, and PKI may traverse the WAN outside the encrypted tunnel as appropriate.
- VoIP and video are important now or will be in the future.

- QoS is required for a converged voice, video, and data network.
- Firewall and intrusion detection and prevention support is required only if the WAN infrastructure is a public network such as the Internet.
- A routing protocol is used to address load sharing and availability across multiple paths.
- IP addresses for branches may be assigned statically, dynamically, or a combination of both. Ideally, the branch should be identified by its inside LAN IP address (typically a private IP address) or for IKE authentication purposes, identified by a fully qualified domain name (FQDN).

Terminology

To communicate effectively in the descriptions and topology diagrams in this design guide, the following terms are defined and used accordingly throughout this guide:

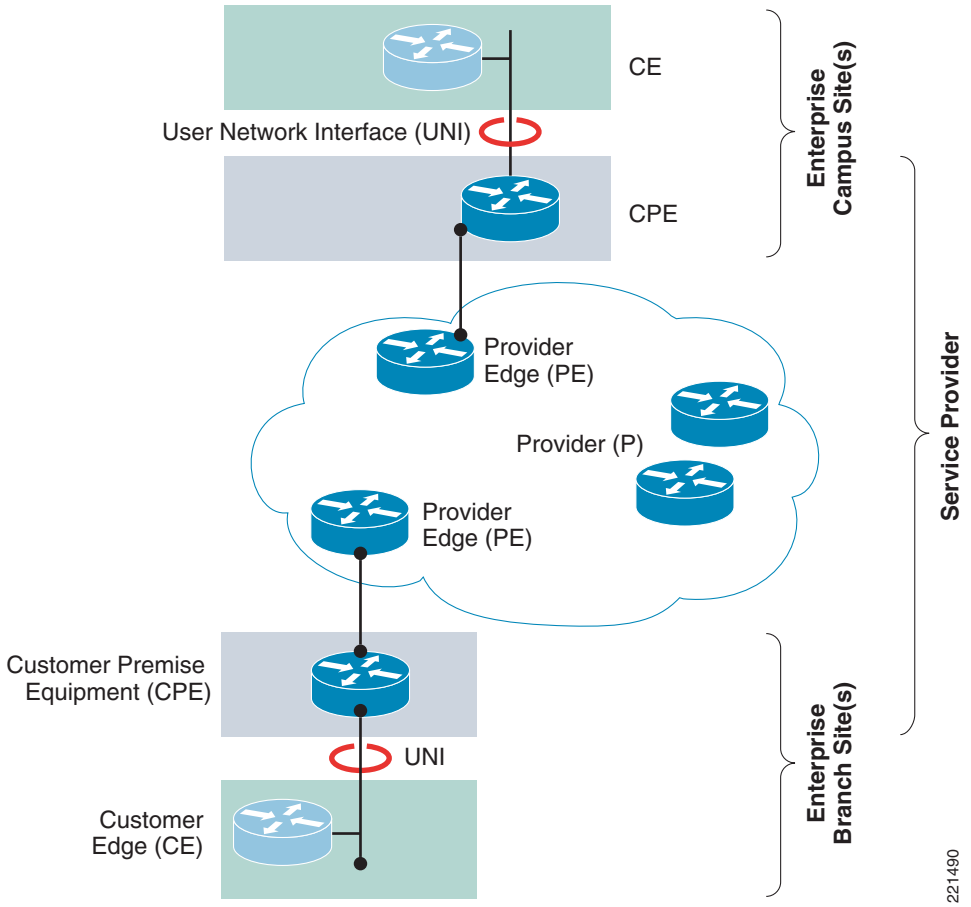
- *Subscriber* —The business or entity using a WAN to interconnect offices; also referred to as the enterprise or enterprise customer. The "C" or "customer" in the CPE and CE acronyms refers to the subscriber.

  This design guide is targeted at a deployment by a large enterprise rather than a small-to-medium business or a service provider. Examples of large enterprise entities include most Fortune 500 companies, and most federal, state, and Department of Defense agencies.
- *Provider* or *service provider*—The telecommunications company selling the network service. Examples include Verizon Communications, Sprint Nextel Corporation, AT&T Inc., and EarthLink.
- *Customer premises equipment* or *customer-provided equipment (CPE)*—This device resides at the subscriber location. It may be owned and managed by either the subscriber or provider, depending on the type of deployment. For example, in a broadband network, a cable modem or DSL bridge (modem) is the CPE device. Both these devices have an Ethernet handoff to the subscriber while their uplink is co-axial or twisted-pair. In broadband deployments, the CPE device is typically given to the subscriber free of charge or at no charge, with a contract of several months to a year. Broadband CPE equipment is not typically managed by the provider. At data rates higher than broadband, the CPE device may be a low-to-midrange router or desktop switch owned and managed by the service provider. Typically, the configuration includes the basics necessary to properly provision the service. It may not include features that would provide additional value to the subscriber (for example, firewall or access control lists) unless there is a contract for managed or enhanced services.
- *Customer edge (CE)* router or switch—The CE device connects to routers and switches at the campus or headend location as well as the branch locations. Because this device is owned and managed by the enterprise, intelligent features such as encryption, firewall, access control lists, and so on, are enabled by the network manager to provide the enterprise with these needed services.
- *Provider edge (PE)* or *PE router*—The PE functions as an aggregation point for CPE devices, or an interconnection between other service providers or other networks of the same service provider.
- *Provider (P)* router or switch—This is considered the WAN core. This can include the Internet, an MPLS network, Layer 2 Ethernet, Frame Relay switches, or a SONET/SDH infrastructure.
- *User-network interface (UNI)*—The physical demarcation point or *demarc* between the responsibility of the service provider and the responsibility of the customer or subscriber.
- *Inside LAN interface* of the CE device—Connects to other routers, switches, or workstations under the administration of the enterprise network manager. The *inside* designation implies that the LAN is protected by a combination of access control lists (ACLs), Network Address Translation (NAT)/Port Network Address Translation (pNAT), firewalls, and an encrypted tunnel to a campus location.

- *Outside WAN interface*—The CE UNI interface. The *outside* designation implies that an encrypted tunnel traverses this link.

These terms are shown in Figure 2.

Figure 2 Topology and Terms



This design guide focuses specifically on the CE device. The associated UNI is the Ethernet access link. The CE UNI Ethernet interface is typically a 10/100 Mbps interface in the case of broadband, or 100 Mbps to 1 Gbps interface for all other deployments.

Note Many CE devices have differing QoS capabilities on a per-port basis. Advanced QoS functions may be supported only on a certain subset of ports, such as the Enhanced Services GE ports on the Catalyst 3750ME. Other CE devices, such as the Cisco 871, designate an Ethernet interface as WAN and the switched Ethernet ports as LAN. In this example, the designated WAN interface is the UNI.

The CE device can be a relatively inexpensive teleworker router; for example, a Cisco 871 or 1811, supporting a single user. Small branch locations with a combination of point-of-sale devices, IP-enabled video security cameras, and workstations may be supported by the Cisco 1800, 2800, 3800, and the 7200 VXR Series. The CE device at the campus locations is typically a Cisco 7200 VXR or a 7600 Series.

Branch locations are typically implemented with a single-tier architecture; a CPE device performs QoS, security, access control and protection, encryption, and other network functions as required. A large branch office may have more than one single-tier CPE device; for example, each WAN link may terminate on a separate router. However, all the aforementioned network functions reside in the single-tier device. These devices operate in parallel.

A dual-tier model is often deployed at the campus location to better aid in scalability and isolation of function across multiple hardware platforms. As the name suggests, a dual-tier model uses more than one hardware device, separating the required network functions on one or more pieces of equipment: routers, switches, and network appliances. In the dual-tier model, the devices operate in sequence: WAN and QoS on one chassis, with security, access control, protection and encryption on one or more additional devices.

Technology Overview

For the network manager of a large enterprise, understanding the various service offerings of each service provider in a geographical market and how these relate to the Metro Ethernet service definitions and attributes of the Metro Ethernet forum can be cause for confusion.

To help simplify and clarify, this section divides the offerings into demarcation type and service type. The demarcation type is either simple or trunked. The service type is either point-to-point or multipoint. Table 1 shows this relationship and provides examples of implementations.

Table 1 Demarcation Type and Service Type Implementations

Demarcation Type/ Service Type	Point-to-point	Multipoint
Simple	Ethernet private line (EPL) (for example, Ethernet mapped to SONET/SDH frames) *or* Ethernet Internet access with IPsec encryption (no split tunnel)	Ethernet Internet access with multipoint DMVPN or MPLS Ethernet access to group encrypted transport (GET)
Trunked	Ethernet Virtual Private Line (EVPL), also called Ethernet Relay Service (ERS)	Ethernet Relay Multipoint Service (ERMS) or Ethernet Multipoint Service (EMS)

Because the performance of the CE device is heavily dependent on the QoS configuration, this section addresses the Ethernet access technologies using both the data rate and associated QoS challenges. By doing so, the performance section can be separated into the following subsections:

- Port-based
- Per-VLAN
- Per-class per-VLAN

The service type is also discussed in relation to similarities to existing WAN/LAN technologies, which allows the network manager to put the QoS challenges in perspective.

Demarcation Types

To simplify the design and configuration of the CE routers deployed in a Metro Ethernet environment, the various Metro Ethernet services are consolidated and segregated into distinct demarcation types that govern how the CE router is configured to best support a QoS-enabled IPsec-encrypted VPN transporting voice, video, and data.

This document is targeted toward, and focuses on, assisting the network manager of a large enterprise in configuring the CE router. As such, details of the service provider network topology are simplified or ignored where appropriate.

For a detailed description of the service provider functional layers, see the section on Architectural Roles in the *Metro Ethernet 3.1 Design and Implementation Guide*.

Simple Handoff

In a simple handoff, there is no trunking encapsulation on the link, either because the CPE or CE devices do not support trunking, or trunking is not required for transport across the service provider network. The UNI is a Ethernet, FastEthernet, or GigabitEthernet access link.

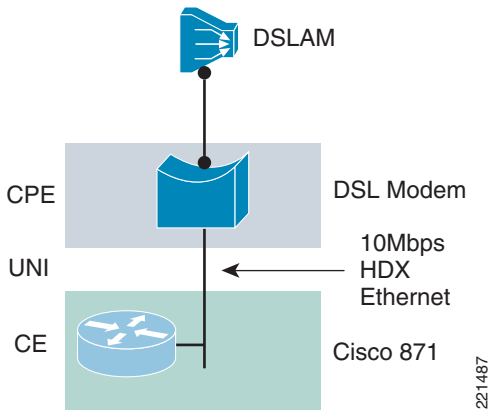
Examples

The following are common examples of a simple handoff:

- DSL broadband service
- Cable broadband service
- Ethernet Internet access
- Ethernet Private Line (EPL)—Port-based point-to-point service that maps Ethernet frames to a time division multiplexing (TDM) circuit, commonly SONET

Figure 3 shows an example of a port-based, simple handoff. This example is of a DSL broadband link to the Internet. The CPE device is a DSL modem (more correctly, an Ethernet-to-ATM bridge) that connects to the DSL Access Multiplexer (DSLAM) of the service provider by a copper twisted pair (phone line), while the UNI access link is a 10 Mbps Ethernet half-duplex link.

Figure 3 Port-based Handoff



This example is typical of a teleworker deployment. For more information on teleworker deployments, see the *Business Ready Teleworker Design Guide* at the following URL: http://www.cisco.com/go/srnd.

Data Rates

For port-based services, the data rates can range from very low, as would be the case with iDSL at 144 Kbps, to common WAN speeds of DS1(T1) at 1.544 Mbps, or even typical headend campus rates of DS3 at 44.736 Mbps, OC-3, 155.52 or above. In any case, the CE device has no awareness of the actual link speed because it accesses the WAN by way of an 10/100/1000 Ethernet link.

Caution In all port-based, simple handoff deployments, the enterprise must assume that the service provider is policing traffic into their network. Otherwise, because of the speed mismatch between the access link (UNI) and the WAN transport mechanism, packets may be dropped indiscriminately during periods of congestion. QoS techniques are therefore mandatory on the CE router to prioritize real-time traffic.

QoS

In a simple handoff, packets may be discarded in the service provider network, either because of congestion on a link without an appropriate QoS policy or because of a policer QoS configuration on the service provider network that serves to rate limit traffic accessing the WAN core. To address these issues, QoS on the CE device is applied at a per-port level. A QoS service policy is configured on the outside Ethernet interface, and this parent policy includes a shaper that then references a second or subordinate (child) policy that enables queueing within the shaped rate. This is called a hierarchical CBWFQ (HCBWFQ) configuration. If the crypto configuration consists of logical tunnel interfaces, such as GRE/IPsec, DMVPN, or IPsec VTI, the QoS service policy can alternately be configured on each tunnel interface rather than on the outside physical interface.

The reasons for attaching the service policy on the outside interface is that a split tunnel or an unencrypted spouse-and-child VLAN is present on the branch router. Split tunnel refers to where branch access to the Internet occurs at the branch router. Non-split tunnel refers to a configuration where all traffic traverses the tunnel, and Internet access is provided at the campus headend. Unencrypted spouse-and-child directly accessing the Internet is also a form of split tunnel.

In this case, not all traffic would traverse the logical (tunnel) interface, and the QoS service policy must be applied to the outside physical interface to classify both encrypted and unencrypted traffic.

One drawback to applying the QoS service policy on the outside physical interface is that queueing happens post-encryption rather than pre-encryption. With post-encryption queueing, packets may be delayed and then later dropped by the replay detection logic of the decrypting router. When queueing is pre-encryption, the packets are queued (delayed) before encryption and assignment of the IPsec sequence number. Packets are transmitted *first in first out* (FIFO) by the outside physical Ethernet interface and are therefore not subject to queueing and the potential reordering of the packet and the corresponding IPsec sequence number.

By configuring the QoS service policy on the logical interfaces, in the event there are two or more logical interfaces, the routing protocol must be configured to use one interface as the primary path and the other logical interfaces as backup interfaces. If load sharing across the two logical interfaces is permitted, the QoS service policy must be configured at a data rate half of the rate of the uplink given two logical interfaces, or there is the potential to overrun the uplink and indiscriminately drop packets.

Note Configuration examples of these QoS service policies can be found in Simple Handoff, page 53.

The service provider assumes a minimal service-level agreement (SLA) responsibility.

In a simple handoff, the enterprise implements and manages services such as VPNs, VoIP, or video-conferencing, and takes full responsibility for issues such as security and class of service (CoS)/ QoS.

Trunked Handoff

In a trunked handoff, the demarcation point is a physical Ethernet with one or more Ethernet virtual circuits (EVCs) provisioned logically. This is a trunked link that is implemented as an Inter-Switch Link (ISL) Protocol or IEEE 802.1Q trunking. Trunking is a way to carry traffic from several VLANs over a point-to-point link. ISL is a Cisco proprietary protocol that was available before the IEEE 802.1Q standard. IEEE 802.1Q trunking is preferred today because the standard provides interoperability between different vendors.

The most common trunked handoff implementation is Ethernet Relay Service (ERS), also known as Ethernet Virtual Private Line (EVPL). EVPL is a point-to-point VLAN-based service targeted at Layer 3 CE routers. It is sold as an alternative to Frame Relay or ATM offerings.

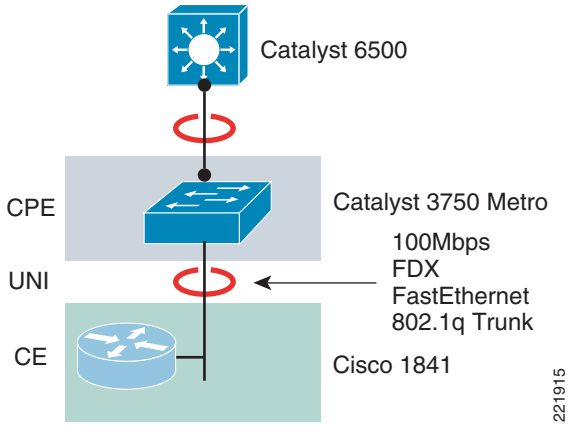
Examples

The following are common examples of where a trunked handoff might be used:

- EVPL
- EVPL access to ATM service interworking
- EVPL access to Frame Relay
- EVPL access to MPLS

Figure 4 shows a trunked handoff using IEEE 802.1Q VLANs. In this example, the service provider has provisioned a Catalyst 3750 Metro switch at the customer location, connecting the appropriate VLANs from the aggregation switch of the provider with the Cisco 1841 router owned by the enterprise customer. The Ethernet access link, or UNI, is 100 Mbps full duplex.

Figure 4 Trunked Handoff using IEEE 802.1Q VLANs



In this configuration, the service provider may choose to configure QoS shaping and/or policing on the Catalyst 3750 Metro switch, as well as policing on the Catalyst 6500.

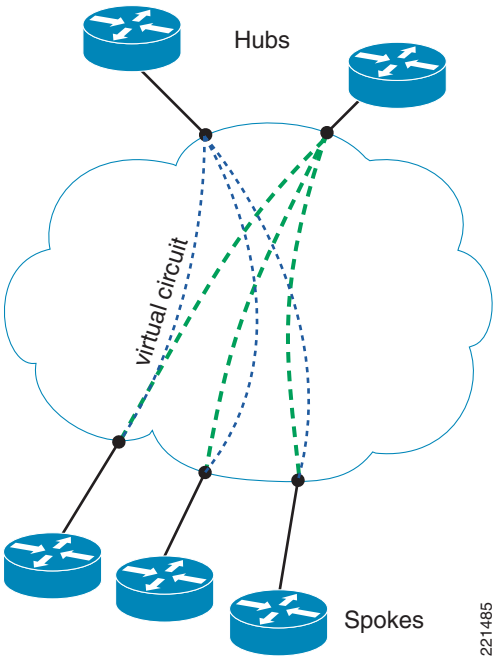
Comparison Topology

EVPL is structured similarly to Frame Relay and as such, it is useful to review the typical enterprise customer deployment of Frame Relay. Most customers implement two active hub locations, and sometimes a third standby hub at the corporate disaster recovery location. The hubs implement a point-to-point sub-interface connecting to every remote location. Each of the hubs have a sub-interface for each remote router.

The remote routers have a sub-interface corresponding to each hub location. Figure 5 shows two hubs and three remote locations, or spokes. Each hub router has three sub-interfaces. Each spoke router has two sub-interfaces, one corresponding to each hub.

Each point-to-point sub-interface is assigned its own network number. To the Layer 3 routing protocol, each sub-interface is a separate point-to-point network.

Figure 5 Two Hub Topology



In a Frame Relay deployment, the service provider offers a Layer 2 network service that includes the following advantages and limitations to the enterprise customer:

- The upper limit of available bandwidth is capped by the access port speed. Branch locations typically were 56 Kbps or T1 port speeds. Campus locations were typically T1 or T3 for end-to-end Frame Relay or DS3 or OC3 when Frame to ATM service interworking was deployed.
- Hub routers were often implemented on the Cisco 7500 platform when coupled with a VIP-offloaded Frame Relay traffic shaping to the VIP processor. The ATM PA-A3, on either the 7500 or 7200, also offloaded ATM shaping to the line card. Offloading QoS shapers to the interface rather than performing this function on the main router CPU helped scalability. QoS shaping can be very CPU-intensive.
- The committed information rate (CIR), which is the minimum bandwidth guaranteed by the PVC and the data rate guaranteed by the service provider, is the value the enterprise customers use for configuring the data rate of the Layer 3 QoS shaper. Service providers offering a zero CIR confounded customers when configuring Frame Relay traffic shaping because there was no guaranteed rate as a target for the shaper configuration.
- The service provider network was tuned to buffer rather than drop frames. Buffering frames may avoid excessive drops, but buffering increases latency, which results in jitter. By increasing the buffer size on the Frame Relay switch, voice quality has already diminished by the time queues have backed up enough to trigger Backward Explicit Congestion Notifications (BECNs).
- Appropriately configuring Frame Relay for good voice quality often causes data throughput to suffer.

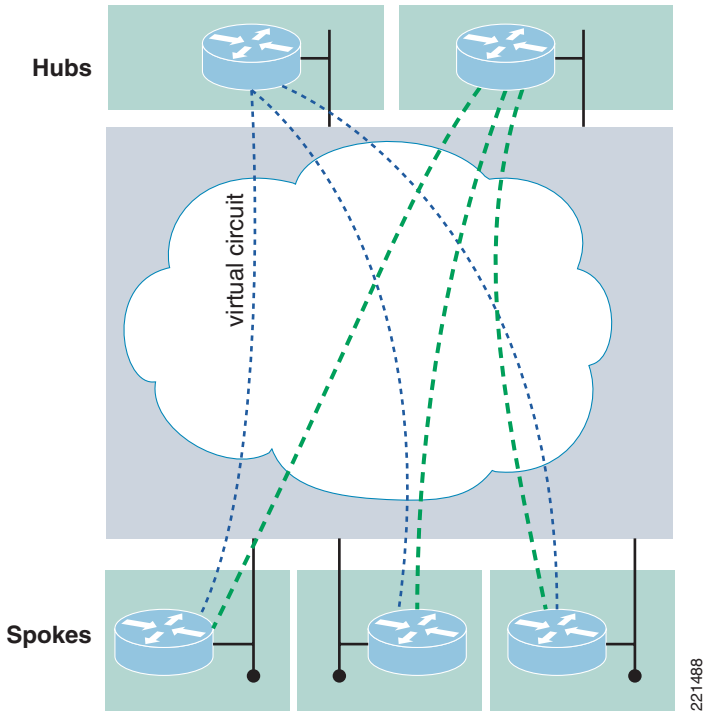
Ethernet Virtual Private Line

EVPL, like Frame Relay, provides for multiplexing multiple point-to-point connections over a single physical link. In the case of Frame Relay, the access link is a serial interface to a Frame Relay switch with individual data-link connection identifiers (DLCIs) identifying the multiple virtual circuits or connections.

In the case of EVPL, the physical link is Ethernet, typically FastEthernet or Gigabit Ethernet, and the multiple circuits are identified as VLANs by way of an 802.1q trunk.

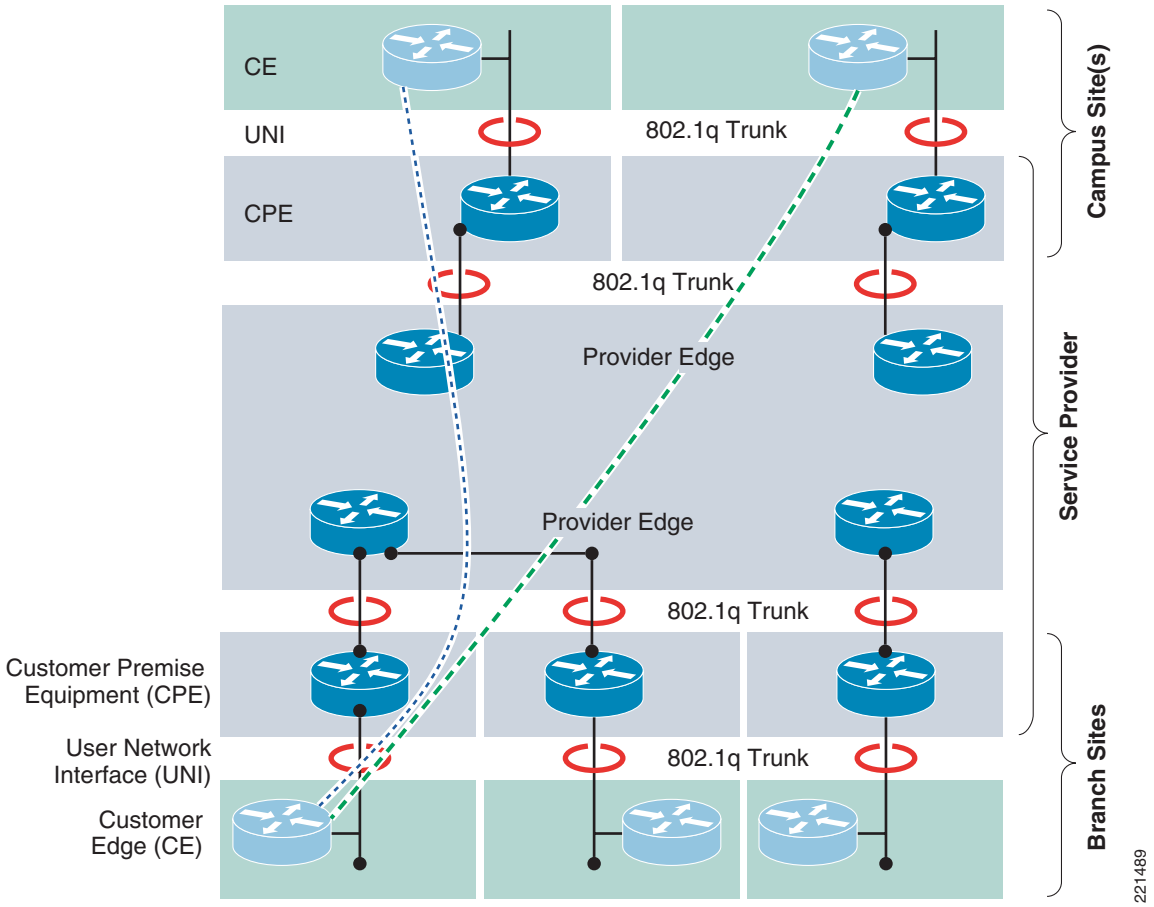
Figure 6 shows the similarities of an EVPL topology to the previous Frame Relay diagram.

Figure 6 EVPL Topology



Now that the high level topology of EVPL is shown to be similar to Frame Relay, consider the service provider logical view of the WAN topology, as shown in Figure 7,

Figure 7 Service Provider Logical View of WAN Topology



The UNI, or Ethernet handoff, between the CE router and the service provider CPE may multiplex multiple point-to-point connections by way of an 802.1q trunk. This is analogous to Frame Relay PVC.

With EVPL, branches communicate with other branches by way of the central site.

Data Rates

Data rates offered are 10 Mbps, 100 Mbps, and 1000 Mbps (Ethernet, FastEthernet, GigEthernet) provisioned by EVCs, typically in increments as 1–10 Mbps in 1 Mbps increments, then 10 Mbps increments to 100 Mbps, and 100 Mbps increments up to Gbps.

QoS

QoS by the CE device is on a per-VLAN level. Typically, the service provider assumes a more robust SLA responsibility with EVPL. Often 3–5 CoS options are available. With three classes of service, an example is basic, priority, and real time. This offering is obviously targeted for VoIP and video deployments.

Note Configuration examples of these QoS service policies can be found in Branch Configuration—Two VLANs (Per-Class Shaper), page 61.

Service Types

The Metro Ethernet Forum (MEF) has defined both point-to-point and multipoint service types for Metro Ethernet service offerings. This design guide also includes topologies that include port-based Ethernet handoff for access to an Internet service provider, a traditional Frame Relay network, or an enterprise self-provisioned WAN based on long-reach Ethernet or dark fiber. This section discusses issues related to transporting encrypted VoIP traffic on true Metro Ethernet services and other Ethernet handoff derivations.

The point-to-point service type is discussed in the context of the preceding point-to-point WAN technology of Frame Relay, as well as issues related to operations, administration, and maintenance (OAM) of these circuits.

The multipoint service section addresses issues in the context of its predecessor technology of ATM LAN Emulation (LANE), as well as the issues related to implementing QoS in a multipoint topology.

Point-to-Point Services

This section defines and discusses point -to-point services. In a point-to-point topology, QoS is a manageable deployment in configuration and provisioning within the parameters of the respective performance capabilities of the chassis. In this section, the point-to-point services are discussed in the context of OAM of a logical (or virtual) connection between a hub and spoke.

EVPL

EVPL is a VLAN-based service targeted at Layer 3 CE routers and is sold as an alternative to Frame Relay offerings.

Because the focus of this design guide is the transport of encrypted real-time applications (voice, video, and data), it is important to review the various mechanisms of verifying the end-to-end availability of the path between branch and campus headend to re-route traffic in the event of a link failure. The following section provides an overview of these components on the existing technology and how these functions are implemented in the next-generation MAN/WAN network.

EVPL Compared to Frame Relay

EVPL services are structured similarly to legacy point-to-point services such as Frame Relay permanent virtual circuits (PVCs). One key component of Frame Relay services is the Local Management Interface (LMI), which is a set of enhancements to the basic Frame Relay specification. LMI virtual circuit status messages are exchanged between the Frame Relay DCE (typically the Frame Relay switch) and the DTE devices (typically the customer router). These control messages are used to prevent data being sent to a “black hole” or PVC that no longer exists or is functional.

The enterprise customer, however, relies on a Layer 3 routing protocol hello packet (keepalive) between the router interface on the branch and headend to verify end-to-end Layer 3 connectivity. Therefore, the Frame Relay LMI provides a Layer 2 keepalive mechanism. The routing protocol (which is commonly RIP, RIPv2, OSPF or EIGRP on Frame Relay interfaces) provides an end-to-end Layer 3 keepalive mechanism. In most customer deployments, the dynamic Layer 3 routing protocol determines path selection (as opposed to static routes to a point-to-point interface), while the Layer 2 keepalive mechanism is geared toward generating link up/down SNMP traps and syslog messages for network management systems.

Ethernet OAM

Ethernet OAM (E-OAM) provides similar management functionalities to ATM OAM and Frame Relay LMI. Ethernet OAM is a general term that actually comprises several component standards implementations and capabilities that work together to provide management of a Metro Ethernet MAN/WAN.

- Ethernet Local Management Interface (E-LMI)—Similar to its counterpart in Frame Relay. This protocol was developed by the Metro Ethernet Forum. It operates on the link between the CE device and the PE device. E-LMI automates provisioning of the CE device. On-going fault notification (as detected by 802.1ag) to the CE device is most important to the enterprise customer. See Ethernet LMI, page 65 for an example of an Ethernet sub-interface state change to UP/DOWN by E-LMI. As with traditional Frame Relay WANs, the Layer 3 routing protocol also detects and routes around the failure. SNMP traps sourced from a loopback address on the branch CE router, a link up/down SNMP trap, and syslog message are available to the campus network management systems.

  The enterprise customer must configure the **ethernet lmi interface** command under the primary interface.

- IEEE 802.1ag Connectivity Fault Management (CFM)—Provides "service" management. The customer purchases end-to-end connectivity (via EVC) through the service provider network, and CFM identifies and notifies the service provider of failed connections. At the user-facing PE, the CFM and E-LMI functions interoperate (communicate) to provide a true end-to-end circuit validation.

  The enterprise customer needs to be aware only that IEEE 802.1ag CFM is an available feature to the service provider because the customer does not directly interact or require any CFM configuration in the PE device.

- Link Layer OAM (IEEE 802.3ah OAM)—Provides link-level Ethernet OAM and operates on a link-by-link basis. This protocol addresses discovery, link monitoring, remote fault detection, and remote loopback. Link Layer OAM interworks or is relayed to CFM on the same device. CFM can then notify remote devices of the localized fault, as previously described. As with CFM, no customer CE configuration is necessary.

Availability of Ethernet OAM

These features are targeted for availability in both the 6500 and 7600 platforms. See www.cisco.com or contact the appropriate sales support organization for current status. Cisco therefore recommends that enterprise deployments use Layer 3 protocols today, and in the future provide routing around link failures and routing protocol features such as *eigrp log-neighbor-changes* and *ospf log-adj-changes* to alert the network management system of neighbor adjacency changes.

Ethernet OAM is not intended to be a substitution for a Layer 3 routing protocol. E-OAM is *not* a fast convergence technology. Rather, the enterprise customer should consider routing protocol enhancements such as OSPF fast hello packets as one option for enabling rapid convergence (less than 1 second) over a normally very reliable network. In both EIGRP and OSPF, the hold and hello intervals can be configured lower than the default values. Changing the hello interval to 1 second with a hold time of 3–5 seconds is also an option.

Note Decreasing the hello interval of a routing protocol increases main CPU consumption. This is especially evident on a headend crypto aggregation router that terminates several hundred remote routing protocol neighbors. Cisco recommends that the network manager consult with an experienced networking professional familiar with large-scale aggregation or measure the impact of proposed changes in a testing environment before implementing on a production network.

Ethernet Internet Access with Point-to-Point IPsec Encryption

Another point-to-point service offering outside the scope of the Metro Ethernet Forum is the Ethernet handoff from an ISP using a hub-and-spoke IPsec encryption. Examples of this crypto configuration are point-to-point Dynamic Multipoint VPN (DMVPN), IPsec/Generic Routing Encapsulation (GRE), and direct IPsec encryption (crypto maps applied directly to the router interface).

For the purposes of supporting encrypted VoIP, QoS is required in the topology. Tier 1 ISPs currently offer QoS on existing serial access links (T1, for example), and the natural progression of this service offering should extend to Ethernet Internet access. The ISP must apply HCBWFQ from the Internet to the customer branch location, and the enterprise customer must apply HCBWFQ to the Internet core. The core routers may have some form of QoS or may be under capacity with little or no congestion.

In the case of using broadband (cable/aDSL) access to the Internet with Ethernet handoff from the cable modem or DSL bridge/router, this deployment model has been extensively tested and documented in the *Business Ready Teleworker Design Guide* (http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008074f24a.pdf). The viability of supporting near toll quality VoIP in this configuration has been demonstrated for over three years by the author working as a full-time teleworker over residential broadband.

Because Internet access is purely an IP-routed network, Internet service providers rarely if ever provide any Layer 2 keepalive mechanism between the CE and user-facing PE equipment. Serial link High-Level Data Link Control (HDLC) or Point-to-Point Protocol (PPP) keepalives would be the extent of any mechanism. These operate only on a single link basis and offer nothing similar to end-to-end “circuit” verification.

However, because IPsec is almost universally implemented in this WAN environment to provide authentication and data secrecy, end-to-end connection verification is controlled either by ISAKMP keepalive messages (either periodic or on-demand Layer 3 keepalives running parallel to the crypto tunnel), and by the Layer 3 routing protocol hello packets that are encapsulated and traverse between the two crypto peers within the logical tunnel. Even in IPsec direct encapsulation, where there is no GRE, mGRE, or VTI logical tunnel interface to transport hello packets, the Reliable Static Routing Backup Using Object Tracking feature influences routes in the IP routing table with the success or failure of IP SLA probes.

Although this topology does not offer identical functions to the OAM functions of Ethernet OAM in an EVPL deployment, it is not without a toolset to provide fault management and diagnosis of end-to-end connectivity issues.

SNMP Traps, page 66 and Crypto Logging Session, page 66 show two best practice configuration commands. Processing traps by the enterprise NMS station and network logging of the logging buffer are two key elements in building both historical data as to the reliability or physical links or logical circuits. Crypto tunnels are logical circuits that traverse a Layer 3 network while EVPL is a Layer 2 provisioned service, but they share the common characteristic that the access port may be some form of Ethernet that provides no interface congestion feedback to the branch router.

Multipoint Services

This section defines various types of multipoint services and discusses their suitability for transporting real-time traffic.

Ethernet Relay Multipoint Service

Ethernet Relay Multipoint Service (ERMS) is a VLAN-based service that would be used to connect more than two sites, in contrast to EVPL, which is a point-to-point connection between two sites. In both EVPL and ERMS, Layer 2 control traffic, such as spanning tree Bridge Protocol Data Units (BPDUs), are not passed end-to-end.

Ethernet Multipoint Service

Ethernet Multipoint Service (EMS), also known as Ethernet Private LAN Service, is an any-to-any network, emulating an Ethernet bridge environment where broadcasts and Layer 2 control plane traffic (such as spanning tree BPDU) transparently traverses the WAN. The Cisco Virtual Private LAN Services (VPLS) solution is one implementation of EMS that offers the service provider a means of creating a Layer 2 virtual switch over the MPLS infrastructure.

One reason for choosing an EMS services is to enable applications to use Layer 2 “heartbeat” mechanisms that cannot be routed, such as non-IP applications (such as Microsoft Windows for Workgroups) that use NetBIOS Extended User Interface (NetBEUI) for communications. With these applications, broadcast and multicast packets need to be flooded to all sites, presenting a scalability concern with the associated packet replication on the service provider network edge devices.

EMS Compared to ATM LANE

The multipoint services are structured similarly to other transparent LAN services such as ATM LANE, so it is useful to understand the use of ATM LANE in the enterprise network.

ATM LANE was popular in the 1990s as a means of providing emulated LANs, Ethernet or Token Ring, over an ATM WAN. In the late 1990s, ATM LANE was no longer considered advantageous or recommended for the enterprise network, for reasons including the following:

- The education and training required to become competent in diagnosing and troubleshooting LANE
- Limits on scalability; emulated LANs at some point need to be segmented by routers
- Cost of implementing LANE for the few applications that benefit from an emulated LAN
- Complexity of configuring and providing for the availability of LANE services such as LAN Emulation Service (LES), Broadcast Unknown Server (BUS), and LAN Emulation Clients (LECS)

As a WAN transport, ATM LANE was never considered ideal for connecting routers between campus and branch sites. As a best practice, soft-VCs are configured on ATM switches, and the associated routers are connected by RFC 1483 PVCs. A soft-VC is essentially a PVC between routers that can be rerouted around a failure in the ATM network. The routed interface consists of a physical interface and sub-interfaces representing one or more individual point-to-point VCs.

Note Early IOS implementations of Frame Relay configurations did not support sub-interfaces and associating a DLCI with the sub-interface using the **frame-relay interface-dlci** command. Instead, it was required to configure static maps or dynamic mapping via inverse ARP to map the next-hop protocol address to the correct DLCI. By default, Frame Relay physical interfaces are multipoint interfaces. When sub-interface support was introduced, the best practice was to migrate to point-to-point sub-interfaces and to assign a Frame Relay sub-interface number that mirrors the DLCI value of the Frame Relay PVC assigned to that sub-interface. This results in a similar configuration to ATM RFC 1483 PVCs on sub-interfaces.

This review of ATM LANE demonstrates that transparently bridging over a WAN, whether a Vitalink or Proteon bridge from the 1980s or ATM LANE in the 1990s, has never proven to be an effective means of providing high availability, scalability, and supportability in the enterprise network.

Fallacy of Latency

Most discussions of peer-to-peer networking topology claim that one advantage of the technology is to "ensure minimal latency for peer-to-peer applications such as voice and video." However, in most cases, those making this claim have never implemented, managed, or tested voice or video over the peer-to-peer technology in question, but offer this observation as fact, expecting that the audience will accept the statement.

However, latency below 80 ms is of little consequence to VoIP. The sound of the human voice travels from the front of a large lecture hall to the rear in approximately 80 ms (at sea level, 70 degrees F, sound travels approximately 1128 feet per second, or about a foot per millisecond). Few if any people experience difficulty with a conversation between a student in the rear of the hall and an instructor. In testing during pilot implementations of the teleworker deployment, Cisco documented that the largest factor contributing to latency in a hub-and-spoke IPsec VPN deployment between two phones at spoke locations was the speed of their respective broadband circuit. Traversing the Internet from spoke to spoke, by way of the respective VPN tunnels to the hub, encrypting, decrypting, encrypting, and again decrypting by the receiving VPN router in most all cases exhibited less than the ITU recommendation of 100–150 ms of one-way latency.

In fact, the Cisco team routinely observed and tested broadband access links, both cable and aDSL in the range of 256 K/1.4 M and 768 K/3 M with < 40 ms latency between the teleworker LAN and the Cisco campus lab LAN, with the Internet (three ISPs) as the transport. Only with relatively low-speed connections (between 144 K/144 K and 256 K/1.4 M) was latency (and the associated jitter) ever a concern. The serialization delay of these relatively low-speed broadband connections is the major factor contributing to latency.

Given that this document offers design guidance for Metro Ethernet services at data rates of the physical link typically at 100 Mbps to 1 Gbps, the serialization delay of the UNI is at most 1/40th of an aDSL circuit trained at 256 K/1.4 Mbps. Serialization delay of the access link is of little to no concern in comparison.

Do not assume that voice quality will be demonstratively better with a multipoint WAN service.

Some data applications, however, may actually be more influenced by WAN latency than voice. Many data applications require a series of "lock step" transactions to access file or database retrievals. They exhibit TFTP-like behavior. TFTP is a UDP-based file transfer mechanism where 512 bytes of data are sent, and before any additional packets are sent, the receiver must send an acknowledgement for each data packet. In this case, an 80 ms or more round-trip time between sender and receiver greatly influences the application performance. This issue can be addressed by attempting to reduce the latency by a multipoint configuration. However, Cisco Wide Area Application Service (WAAS) is a technology that is targeted at optimizing WAN performance, especially data applications that suffer as a result of a series of round-trip transactions. Additionally, implementing WAAS may offer other benefits in reducing WAN traffic volume, not simple optimizing applications.

Partial Mesh

A partial mesh topology is a means to address the desire to allow sites with high or constant packet flow between two or more branches (or smaller campus locations) to communicate directly while providing connectivity between branches that have casual or intermittent spoke-to-spoke flows. The partial mesh is provisioned as a set of point-to-point links, with a portion of the branches having a link or links connecting two branches.

Partial mesh topologies often are viewed in an unfavorable light because many equate them to the practice of two branches implementing a “back door” connection. The back door connection is one that generally is implemented without the advice and consent of the WAN architecture group and does not make use of a dynamic routing protocol, but rather static routes. Because of this fact, “back door” connections are often associated with poor network design.

A well-designed partial mesh, however, can be a very effective design in that it addresses traffic flow between branches that have a higher degree of branch flows, in addition to the branch to campus requirement that is a typical common requirement of most networks.

Partial mesh networks lend themselves well to forming a hierarchical network topology. The high bandwidth sites have links to two, or preferably three, other high bandwidth sites. The sites with lower bandwidth requirements have a single link to two of the high bandwidth sites. The high bandwidth sites form the distribution layer and core network to support the access circuits for the low bandwidth sites.

In partial mesh networks that are not designed to support a hierarchical core, the routing protocol is configured to either permit or deny using the branch-to-branch link as a transit network, or only for use in flows between the two branches. If it is a transit network, it can be used either as transit for traffic only from the originating branch to the headend through the second branch, or as transit for one or more additional branches with path failures.

The following key factors must be considered in using a partial mesh topology:

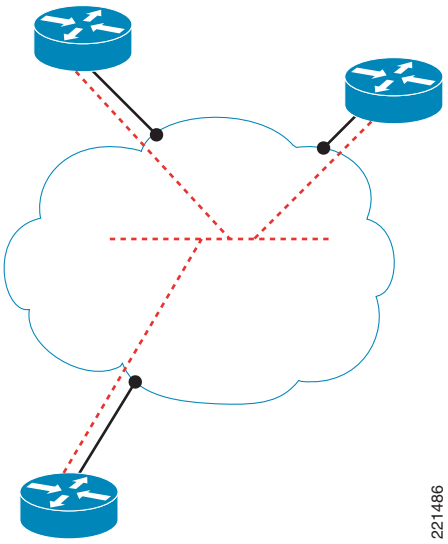
- Is the partial mesh for transit traffic, or only for flows that terminate on the two branches?
- What is the bandwidth required to support transit traffic?
- What is the likelihood of the branch-to-branch link being installed as the best or only path for transit flows?
- Are performance management tools implemented to address capacity and utilization issues in all link failure states?

For a more thorough understanding of hierarchical design principles, documents such as *Advanced IP Network Design* (Retana, et. all, ISBN 1-57870-097-3) address these concepts in more detail.

QoS in a Multipoint World

Enabling QoS between multiple hub locations and the branch routers in a multipoint WAN topology becomes problematic for the enterprise network manager. Consider the simple multipoint topology shown in Figure 8.

Figure 8 Simple Multipoint Topology

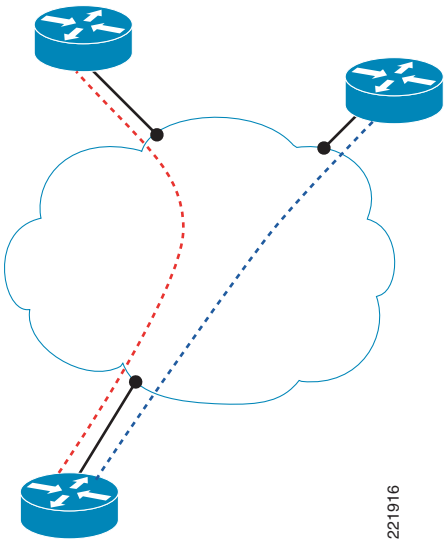


The dotted line represents a multipoint connection shared by all three routers: two hub routers at the top of the cloud with a spoke router in the lower left. The hubs are connected directly by the virtual circuit. From the perspective of the routing protocol, all three routers are peers. Assuming that both hub routers advertise the emulated LAN network address at equal cost to the campus routers, return path traffic from the campus to the branch router load shares with CEF enabled on a per-source/destination basis, and as the number of flows increase, the hub routers both switch packets to the branch location.

All routers have one physical interface (100 Mbps) and one logical interface (policed at 10 Mbps) to the emulated LAN, with both hubs as routing protocol neighbors. How should QoS be configured on the logical interface of the hub, if each hub must apply a global policy on the multipoint interface, identifying the branch by IP address or other means? Within that class, each hub must shape at no more than 10 Mbps to the branch router. If both hub routers send 10 Mbps to the branch, they may police that rate down to the 10 Mbps service as subscribed. If both hub routers shape at 5 Mbps, the branch does not exceed the 10 Mbps contract, but any one flow between hub and branch is never able to use the full 10 Mbps bandwidth at the branch.

Next consider this topology changed to a point-to-point configuration, as shown in Figure 9

Figure 9 Point-to-Point Topology



The branch now has two point-to-point EVCs, one to each hub. Assume that each EVC is contracted at 10 Mbps. Traffic from both hubs now has a QoS policy applied to a point-to-point sub-interface, rather than to a multipoint interface. From a routing protocol perspective, the branch router is only a neighbor, with one hub on their respective EVC interfaces. The branch router can be configured as an EIGRP stub router or in an OSPF totally stubby area. Either practice greatly reduces the number of routes in the routing table of the branch router. Compared to the multipoint example, adding more spoke routers does not increase the number of neighbors for each spoke. All spokes in a point-to-point configuration always have only the two hubs as neighbors.

Additionally, the hub routers can use EIGRP to advertise distribute lists on a per-logical interface basis and to advertise partial or summary routes on a per-branch basis.

QoS is also now applied on a sub-interface level. The configuration is much simpler and easier to maintain.

Although most network traffic flows from data center to workstation or between a VoIP gateway at the campus to an IP phone at the branch, sites that have a high degree of spoke-to-spoke traffic patterns can be partially meshed if required.

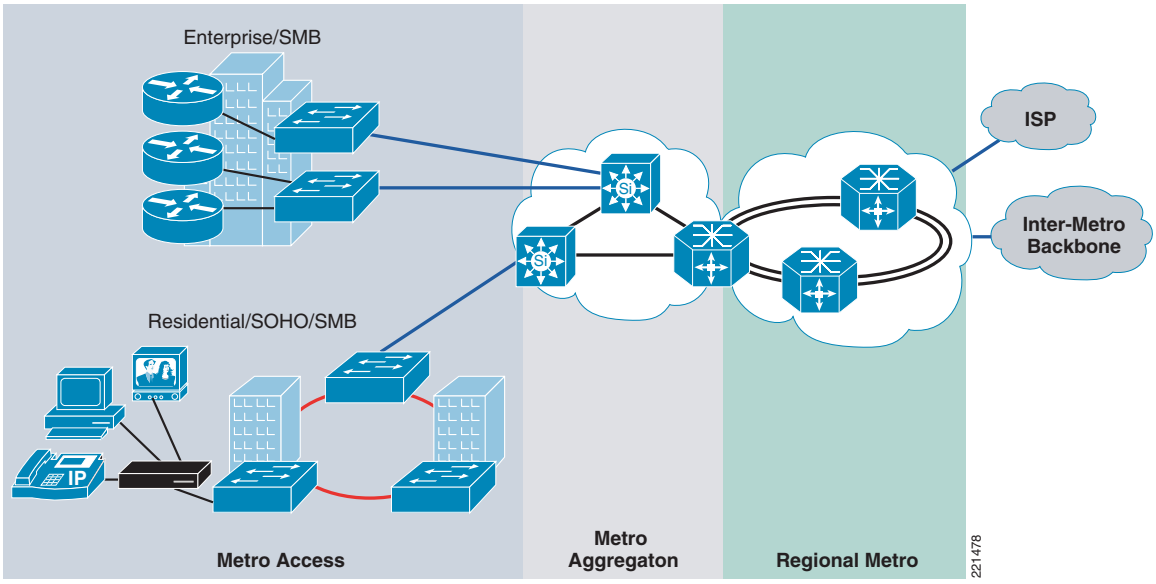
Design Requirements

This section provides a design overview of a Metro Ethernet deployment focusing on the enterprise-centric view of the CPE topologies in a next-generation MAN/WAN. The top-level design is discussed in general terms, after which various design topologies, including single-tier and dual-tier, are reviewed.

Design Overview

As Metro Ethernet services become more pervasive service offerings, enterprise networks will increasingly consider Ethernet access at both the branch office and large campus locations. This design guide is focused on the Metro access tier shown in Figure 10. The Metro aggregation and regional Metro components are the responsibility of the Metro Ethernet service provider and are the subject of the design guides referenced in the introduction of this document.

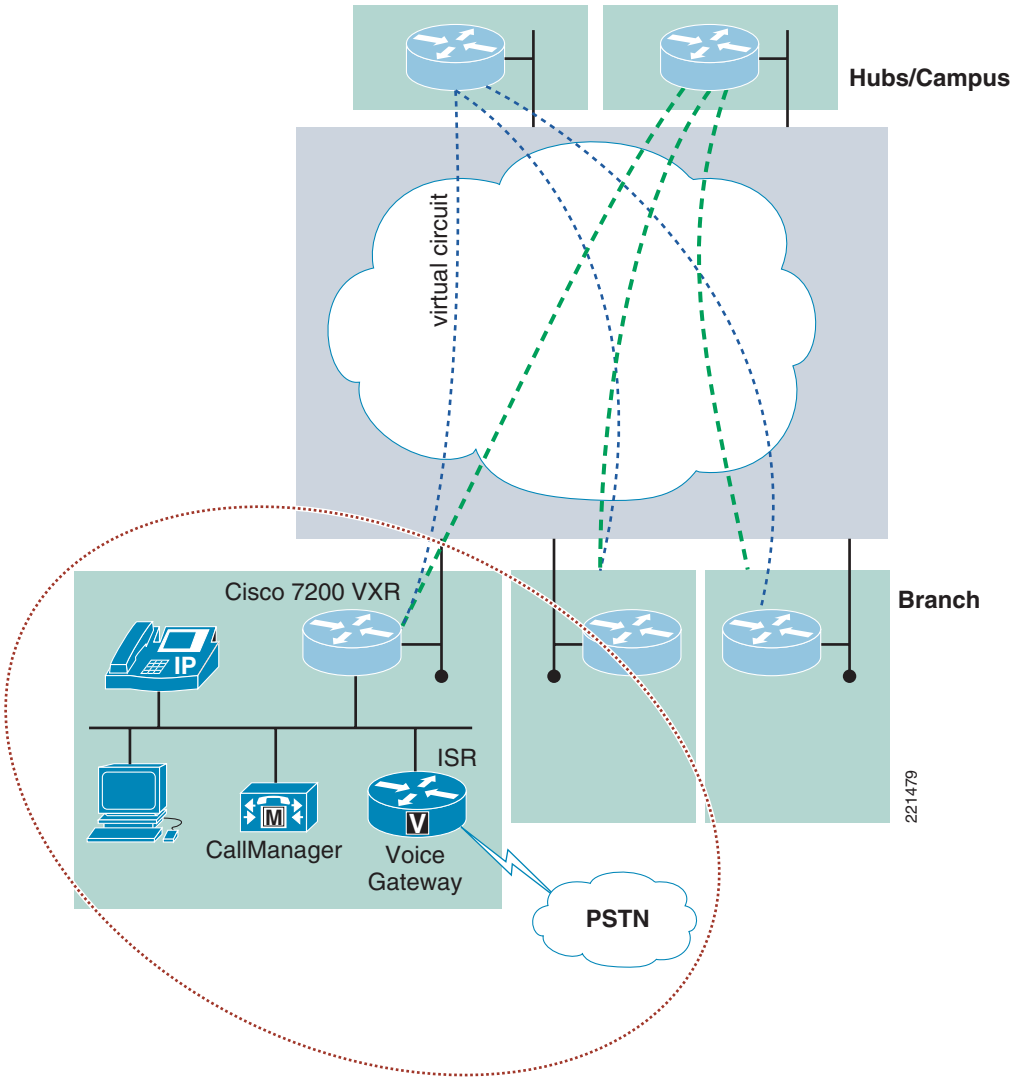
Figure 10 Metro Access Tier



The Metro access component in Figure 10, the enterprise/small and medium branch (SMB) represents the headend or large campus locations as well as the SMB locations. Additional Ethernet access may be used for a residential user (teleworker) or small office location. The handoff may be a true Metro Ethernet service, such as EVPL, or the more traditional broadband access by way of a cable modem or an aDSL bridge (modem) or router terminating the aDSL circuit. More commonly, a combination of these technologies is used at various points of the network.

Next, the focus is on how an enterprise might structure a branch office topology, in terms of services and network equipment, to support the integration of voice, video, and data service. Depending on the packet per second (pps) rate offered from the branch, various platforms may be appropriate to support QoS, firewall, and data privacy through IPsec encryption. In the example shown in Figure 11, a Cisco 7200VXR is shown as the CE router supporting these network services.

Figure 11 Sample Branch Topology Supporting Voice, Video, and Data



Depending on the size of the branch office and the number of users being supported, either a centralized call processing model is used or, as shown in Figure 11, a Cisco CallManager may also be part of the branch deployment. To provide voice gateway services to the PSTN, a Cisco ISR router is shown as the voice gateway.

In this example of a large branch office, a single link into the Metro Ethernet WAN does not provide the necessary degree of redundancy to support a highly available network infrastructure. However, with EVPL services, two or more logical connections can exist between the branch office and headend campus locations over a single Ethernet access link. To provide redundancy for the branch office access link, a second access link should be provisioned with local loop redundancy. Multiple access routers (7200VXR is shown as the CE in this example) may also be a requirement.

Another best practice to increase availability is to supplement the EVPL WAN with an alternative WAN access method. Direct Internet access through a traditional serial WAN or Internet access provisioned by way of a port-based Ethernet handoff can be provisioned. An MPLS service provider can be used as an alternative WAN. IPsec encryption is certainly a requirement for traffic traversing the Internet, but a case can also be made for encryption of voice, video, and data over the EVPL and the MPLS provider as well.

The next section explores in more detail topologies that can be used to support the central and remote offices.

Design Topologies

This section addresses design topologies the enterprise customer may have choices in implementing, or are available from service providers operating in the geographical region of the enterprise customer.

Single-Tier Model

The single-tier model is better suited for a branch location rather than a headend campus location, because of the potentially high data rates associated with an Ethernet handoff deployment.

Dual-Tier Model

The dual-tier model is typically associated with a campus headend topology. Dual tier is defined as a topology that separates network functions on physically separate chassis. This is very effective at the headend campus because it allows improved scalability, the ability to run different IOS versions or feature sets on the individual chassis, improved redundancy, and recovery from link or hardware failures. It is common to implement a dual-tier topology at the headend campus while the branch locations are single tier.

However, with an Ethernet handoff at the branch location now becoming increasingly common, there may be some advantages to implementing a dual-tier topology at the branch location as well. The following subsections discuss two models:

- Apportioned dual-tier
- Commingled dual-tier

Reasons for implementing a dual-tier model at the branch include the nature of the service provider offering and scalability given the higher data rates now available to the branch with a FastEthernet or GigabitEthernet handoff at the branch location.

Apportioned Dual-Tier

This design topology is a common deployment model of European MPLS providers. It is a dual-tier model in that the QoS function is separated from the CE router, which may terminate the enterprise IPsec VPN or may solely rely on the VPN nature of MPLS to provide isolation from other subscribers.

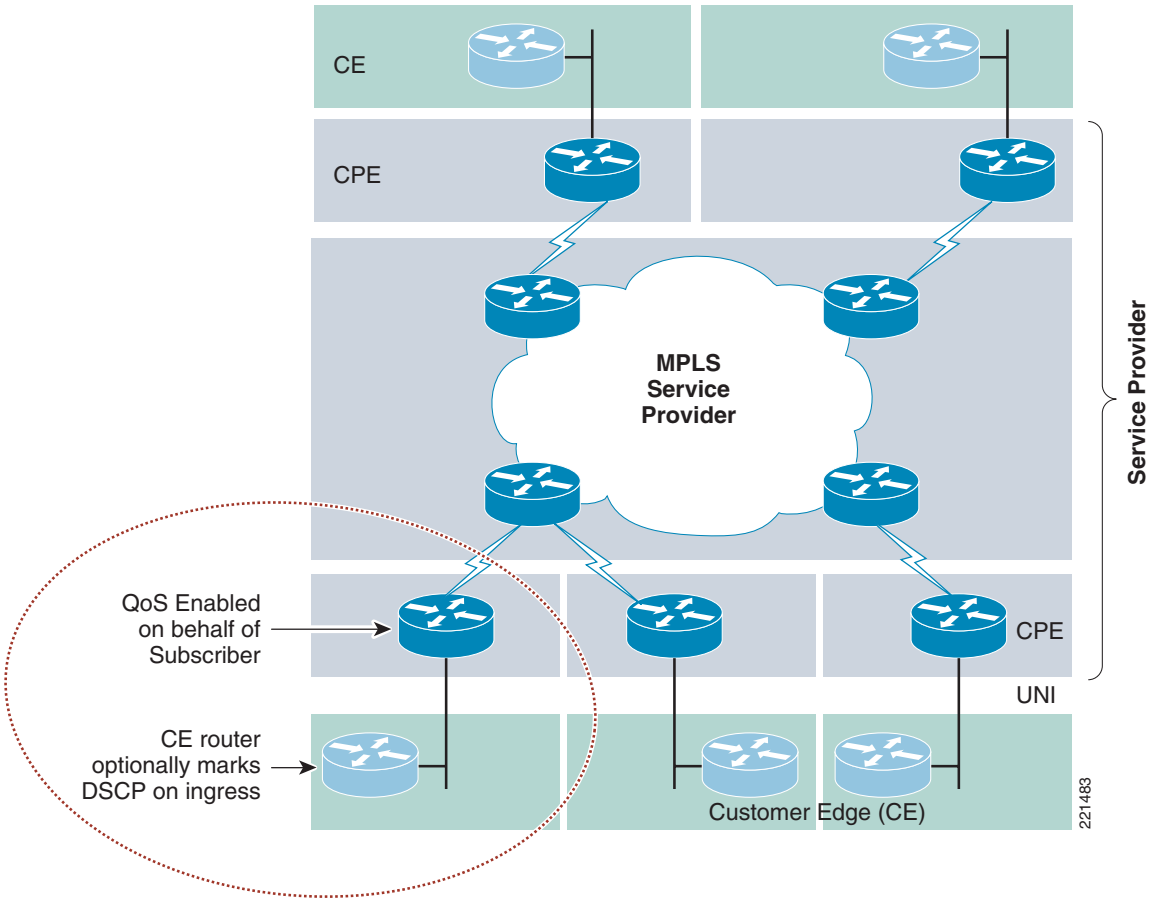
It is apportioned because these roles are divided and assigned according to a plan between the service provider and the subscriber.

The service provider implements an intelligent CPE device capable of providing advanced Layer 3 QoS functionality. The service provider QoS functions include classification based on the ToS byte or other criteria and queueing within a shaped rate, or HCBWFQ. The subscriber optionally marks (or re-marks) packets on ingress to the CE router but implements no egress QoS.

Ingress re-marking is required only if the packets are not marked by the application, or marked differently than prescribed by the service provider. An IP phone or VoIP gateway is an example of an application that marks packets. Ingress re-marking may also be appropriate if applications are considered untrusted and re-marking is appropriate to comply with the QoS policy.

Figure 12 shows an example of this apportioned dual-tier model.

Figure 12 Apportioned Dual-Tier Model



The responsibility of the service provider for implementing QoS is both an advantage as well as a disadvantage to the subscriber. The advantage is that with the service provider addressing QoS, the enterprise need not configure or consume CPU resources for outbound QoS. The disadvantage is the loss of control over the QoS policy and configuration. If there are voice quality issues, the service provider is the responsible party. The subscriber needs to contact the service provider to troubleshoot and correct any QoS configuration issues. The enterprise is responsible for implementing call admission control (CAC) to limit the number of voice calls to the available bandwidth configured in the low latency (priority) queue configured in the service provider CPE router.

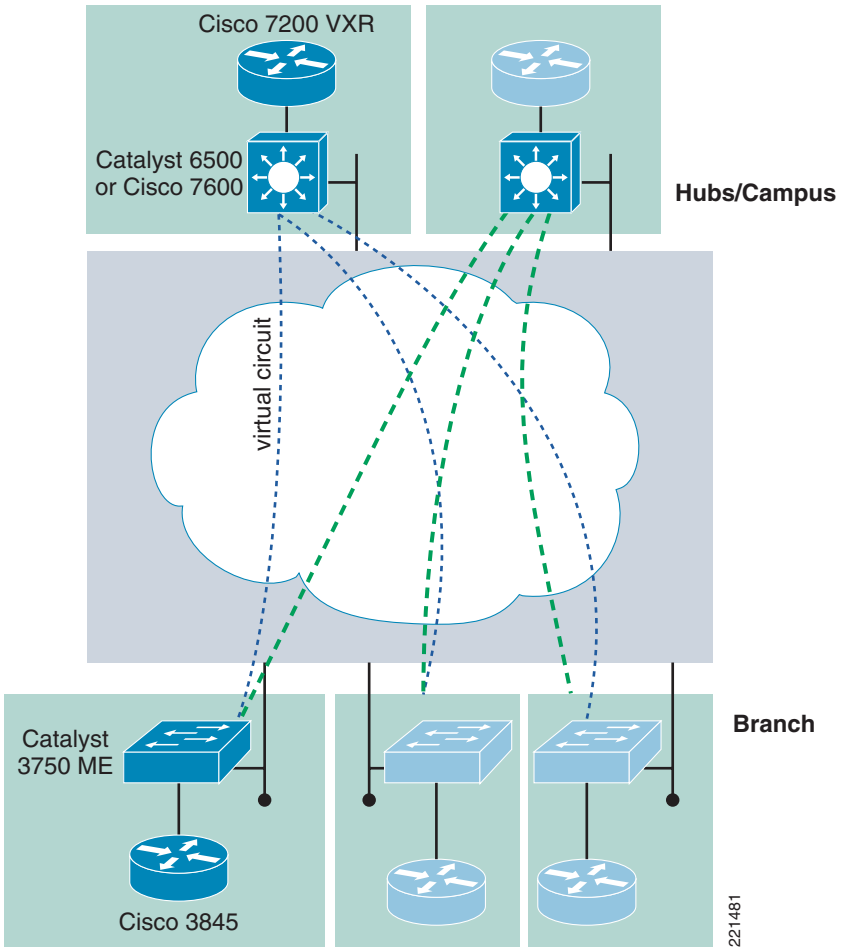
From the enterprise viewpoint, this model can be very effective in that the service provider has control over, and can implement, QoS on an end-to-end basis. The enterprise is purchasing a QoS-enabled WAN infrastructure. Given a professionally managed service, this may be of great value to the enterprise.

Commingled Dual-Tier

This topology separates the QoS function from the CE router by implementing QoS on a switch chassis at either the headend campus location, at the branch locations, or both. It is termed “commingled” to distinguish it from the apportioned dual-tier topology. In this case, two chassis are used to support the required network functions, while the devices are commingled under one administrative control. In this case, the enterprise owns and controls both devices.

Figure 13 shows an example of this topology.

Figure 13 Commingled Dual-Tier Model

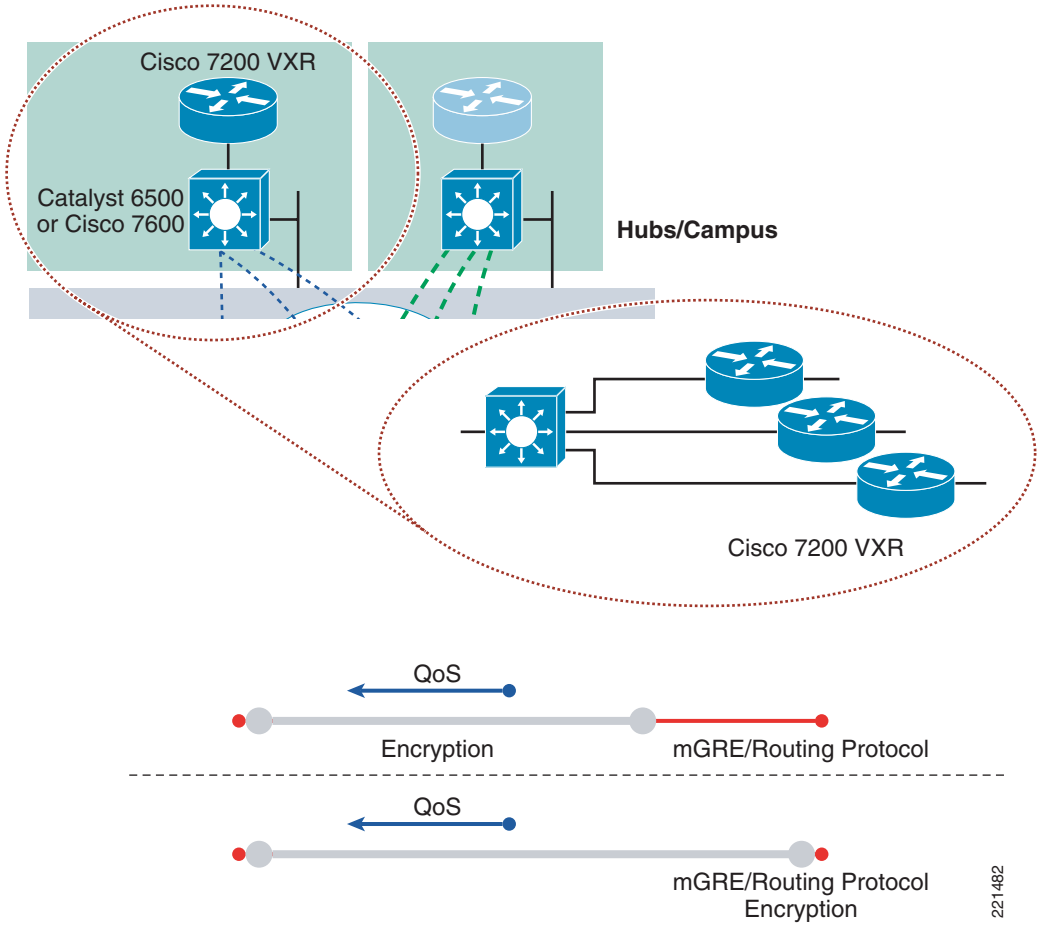


This topology can be used for any WAN type (MPLS, Internet, SONET/SDH, and so on) with or without encryption enabled on the CE router. However, it is most likely implemented when encryption is a requirement. The enterprise may require a separate switch chassis to support the location. Offloading the QoS function to the switch allows the QoS CPU resources to be used by the CE router for other functions, which can include higher packet switching performance or implementing additional network functions.

One disadvantage of implementing QoS on a separate chassis post-encryption relates to the increased likelihood of packet drops because of the replay detection logic of the decrypting router. There are means to minimize anti-replay drops, including disabling the anti-replay check, increasing the size of the anti-replay buffer, and tuning the QoS service policy to drop packets during congestion aggressively rather than buffer (causing delay to the buffered packets) and ultimately to drop because of the anti-replay logic.

Additionally, at the headend campus location, the dual-tier model can include implementing the encryption function on the headend 6500 or 7600 using a VPN shared port adapter (SPA) in addition to the QoS function. With both encryption and QoS on the switch, the backend Cisco 7200 VXR routers terminate the mGRE interfaces and have the Interior Gateway Protocol (IGP), typically EIGRP or OSPF, enabled on the tunnel interfaces, as shown in Figure 14.

Figure 14 Terminating Encryption with a VPN SPA



The advantages of the dual-tier model include the following:

- Increased scalability by dedicating a separate chassis for different network functions
- Separate chassis permits a layered approach to implementing network security policies
- Differing Cisco IOS levels or feature sets can be implemented on the separate chassis

Disadvantages include costs, both in hardware and in maintenance contracts, as well as the need to maintain spare chassis.

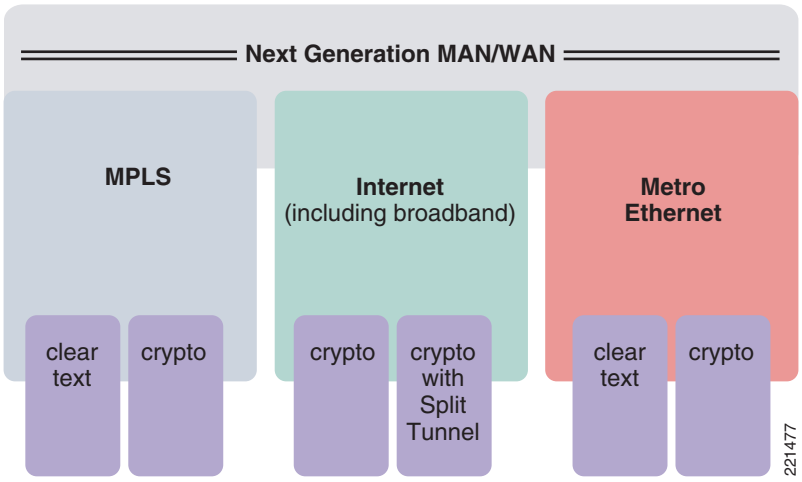
Design Considerations

This section reviews various Ethernet handoff deployment designs and implementations, and describes important considerations for the network manager during the design phase of the project. Although best practices recommendations are provided, these recommendations may not be ideal for every deployment because the requirements of each network differ.

WAN Selection

This design guide does not focus only on true Metro Ethernet services, but rather takes the more general approach that some form of Ethernet handoff may also exist for MPLS or Internet deployments, either now or in future offerings made available to the enterprise customer. For this reason, Figure 15 shows various offerings that may have some form of Ethernet handoff available.

Figure 15 Various Ethernet Handoff Designs



MPLS

For the MPLS component, the enterprise must determine whether clear text is sufficient, or the encryption features of data secrecy, authentication, and replay detection are required by regulation or the nature of the applications and data. Many enterprise customers choose to implement encryption over MPLS because it provides more control over how the network converges in the event of a network failure. One key feature of encryption with a GRE tunnel (or mGRE, as with DMVPN) is the ability to run an IGP routing protocol inside the tunnel. Because the IGP inside the tunnel determines reachability and path selection, it gives the enterprise end-to-end control over how quickly the network converges, which is not available with an MPLS network alone.

Internet

The Internet component has been using Ethernet handoff for many years with the widespread deployment of broadband services. Cable modems and DSL bridges/routers almost universally provide Ethernet handoff to the CE device. It is also increasingly popular to provide FastEthernet or

GigabitEthernet handoff instead of high-speed Packet over SONET (POS) connections. These connections typically are based on per-port shaping at a single aggregate data rate rather than the more granular per-VLAN, per-class shaping as is typical with EVPL.

Metro Ethernet

With true Metro Ethernet services, the enterprise customer can choose between offering data in clear text, much like with MPLS, or use encryption. With EVPL services that are point-to-point services at Layer 2, the IGP of the enterprise customer forms a direct neighbor relationship between the branch and campus headend. Contrast that with an MPLS service where the enterprise customer and the service provider peer at the branch, traverse multiple Layer 3 hops across the backbone, and again peer on the access link between the service provider and the enterprise at the headend. The enterprise customer has no control over the routing protocol configuration on the various Layer 3 hops in the service provider core. With EVPL service, enterprise customers do have control, and this allows the routing protocol to converge much like a crypto tunnel over the Internet.

This is a very desirable and distinguishing feature of Metro Ethernet compared to MPLS.

Services

This section discusses various network services that are applicable to WAN environments and specifically Ethernet handoff deployments.

Encryption

IPsec encryption addresses the network security problem by the application of privacy, authentication, nonrepudiation, and integrity. Privacy and authentication are the key elements in the next-generation MAN/WAN. However, network layer encryption deployed in Cisco routers, including GRE/IPsec and DMVPN, provides one element that has nothing to do with privacy of data, but rather the concept of a logical tunnel interface securing the channel between the two endpoints.

This tunnel provides a logical interface for IOS to address similarly to a physical router interface in that it is defined as a point-to-point or multipoint interface, capable of carrying multicast packets, and is enabled for IP routing including the full suite of IP routing protocols. This Layer 3 logical tunnel that spans between branch and headend across one or more IP network hops in the service provider network allows the enterprise customer the ability to control both ends of the connection, and to form IP routing protocol neighbor relationships that are configurable for hello interval and hold times. This allows the enterprise to control in what manner, and how quickly, the network converges. Payload encryption methods such Secure Socket Layer (SSL), Secure Real-Time Transfer Protocol (SRTP), or Group Encrypted Transport VPN (GETVPN) do not share that same benefit. A network brownout or soft failure is detectable by the loss of routing protocol hello packets, causing the neighbor adjacency to fail and an alternate path to be selected. Application payload encryption cannot detect these failures, they rely only on TCP retransmission and ultimately time-out.

Additionally, IPsec encryption may be required on the MAN/WAN as a due diligence, customer or business partner requirement, or by regulation.

Firewall (IOS)

Cisco IOS Firewall is enabled on the test results provided in this design guide. The firewall function is important for maintaining and protecting the integrity of the network from public networks such as the Internet. If split-tunnel is not enabled at the branch location, it is questionable whether firewall needs to

be enabled on the branch router. However, there may be instances where it is a requirement or desired by the network manager. As such, it has been configured to provide performance results that are accurate for these deployments and conservative in nature for those that do not deploy firewall in their configurations.

QoS

QoS is certainly a key component of the designs in this guide, and is the foundation for the performance test results. With Ethernet handoff, the outside interface is rarely if ever congested, and as such, cannot provide any congestion feedback to QoS. In most instances, the committed information rate (CIR) of the Metro Ethernet service is below that of the line rate. This is similar to Frame Relay and ATM WAN networks of the past.

The goal in this guide is to provide performance data on which platform is suited for a particular CIR provisioned at the CE router. QoS can be very costly in terms of CPU cycles consumed, with the need for shaping and policing to calculate the arrival and discharge rate of packets. With a serial interface, the interface transmit buffer fills if the discharge rate is less than the arrival rate, and this state is communicated to the software drivers as congestion feedback. With a shaper function in software, there is no offloading of this function on an interface driver, and it must be calculated in software.

The other key goal in this guide is to provide guidance on how the hardware-assisted shapers in the 3750ME chassis, 7600 and 6500 Sup32, and SIP-400 and SIP-600 cards allow for higher scaling.

Capacity Planning

In Metro Ethernet deployments, the enterprise customer must monitor and analyze traffic patterns on an ongoing basis to ensure the bandwidth allocated is adequate to support user requirements. This task requires more granularity in a Metro Ethernet deployment where each class of service (CoS) is purchased at an individual bandwidth level. Each class now must be monitored to ensure that increased utilization because of additional employees and application demands continue to be serviced by the deployed QoS policy and subscribed service with the service provider.

Routing Protocol

A hub-and-spoke topology similar to a typical Frame Relay network is available in deployments with the following:

- Point-to-point service, such as EVPL
- Where Ethernet Internet access is provided with point-to-point interfaces, as can be the case with IPsec encryption of GRE tunnels
- A DMVPN using point-to-multipoint interfaces (effectively a hub-and-spoke deployment)

In this hub-and-spoke topology, a distance vector routing protocol such as EIGRP has advantages over link-state protocols such as OSPF and IS-IS.

The decision to use EIGRP rather than OSPF usually involves non-technical issues, such as OSPF being an open standard and EIGRP being Cisco proprietary. However, the following key technical considerations are also important:

- EIGRP can summarize on a per-interface basis; summarization with OSPF is less granular.
- EIGRP has no concept of areas, as in OSPF, and there is no need to flood a topology database.
- OSPF forces hierarchy (areas) decisions into a hub-and-spoke topology.

- Use of EIGRP stub areas eliminates queries to spoke routers.
- OSPF must periodically synchronize router databases within an area, while EIGRP has no similar requirement.
- EIGRP is a very “quiet” protocol when configured as stub and a single default (0/0) route is advertised to all spokes.
- EIGRP by default consumes only 50 percent of the configured bandwidth of the interface for sending updates; a tunnel interface by default is 9 K. Configuring the bandwidth of the tunnel to match the actual underlying link speed generally is advisable on DMVPN (mGRE) interfaces.
- OSPF has a configurable interpacket spacing parameter to provide a means of throttling routing protocol traffic (**timers pacing flood/restans milliseconds**).

Either EIGRP or OSPF can be successfully deployed with or without encryption as an overlay to the WAN transport.

Platform Considerations

Access and Midrange Routers—ISR and 7200 VXR Series

The industry is currently experiencing a significant decline in the installation of the traditional WAN interface modules of serial E1/T1 and ATM. However, for existing deployments, and new deployments of branch (access routers), the existing ISR and 7200VXR Series are well-equipped to seamlessly support a transition from E1/T1 and ATM as the primary WAN interface to some form of Ethernet WAN interface.

For example, the Cisco 3800, 2821, and 2851 chassis have two fixed (RJ-45) LAN ports for 10/100/1000 (Ethernet, FastEthernet, and Gigabit Ethernet) connectivity. The Cisco 2801 and 2811 routers have two 10/100 fixed LAN ports. Transitioning from traditional WAN interfaces to Ethernet handoff is simply a matter of attaching cables and modifying the existing configuration.

Branches that currently use Frame Relay can be migrated to the following:

- Frame Relay access to MPLS
- Ethernet access to MPLS
- True Metro Ethernet services such as EVPL
- Ethernet attached to broadband services such as DSL or cable

The use of Metro Ethernet services or MPLS as the primary WAN connectivity option with broadband access by way of DSL or cable as a backup provides an economical means to increase both the primary and backup WAN speeds while using alternate network topologies for the primary and backup connectivity to the campus.

The following features of the access and midrange router remain unchanged in the configuration:

- Ethernet switching modules with inline power
- Wireless access points
- QoS, firewall, and web caching with IP voice gateway functions

Modular Edge Routing—Cisco 7600 Series

The Cisco 7600 architecture distributes processing across subsystems to provide scalable performance capabilities. The following are the 7600 IPsec VPN functional components:

- VPN SPA provides hardware acceleration for IPsec
- Multilayer Switch Feature Card 3 (MSFC3) does routing termination
- Policy Feature Card 3 (PCF3) on Sup720 processes GRE in hardware
- QoS is performed in hardware on the line card

The key consideration in positioning the 7600 Series in the campus or hub location for terminating and aggregating Metro Ethernet-attached branches is the ability to provide a highly scalable solution for the termination of IPsec encryption from the branches, and to also take advantage of the distributed processing of QoS in hardware on supported line cards.

With the FlexWAN, SIP-200, and SIP-400, QoS is fully distributed with no dependencies on the PFC3 on the Sup720 to provide QoS. This series of cards supports packet buffering, queueing, and scheduling by means of software-definable queues, using CBWFQ, low latency queueing (LLQ), shaping, and WRED.

The OSM WAN with the SIP-600 supports the following QoS features:

- Distributed packet buffering, queuing, scheduling
- Software-definable queues
- Shaping
- CBWFQ, LLQ, WRED (Enhanced OSMs)
- Policing, marking (done on integrated DFC3 on SIP-600)
- Policing and marking for the OSM is done on the PFC3

In testing, the 7600 Series provided exceptional performance in both crypto termination and also in the ability to shape and queue packets to effectively implement downstream QoS in a Metro Ethernet deployment.

Note The SIP-400 supports HCBWFQ while the SIP-600 does not. This is an important distinction if the customer wants to queue packets and categorize them into classes as voice, call-setup, transactional data, best effort, and so on, and then provide congestion feedback with a shaper. This is described as queueing within a shaped rate. The SIP-600 can shape each individual class within a VLAN sub-interface, but does not implement the concept of HCBWFQ.

Note When you upgrade from OSM-4GE-WAN-GBIC to an OSM-2+4GE-WAN+, the existing configuration is not saved and applied to the new OSM-2+4GE-WAN+.

Desktop Switches

The Catalyst 3750 Metro switch provides advanced QoS capabilities in an economically form factor at high data rates. The built-in dual small form-factor pluggable (SFP) enhanced services Gigabit Ethernet uplink ports are network processor-based and allow for both policing and shaping on both ingress and egress, using CBWFQ/LLQ for packet scheduling.

Note The two Enhanced Services uplink ports are solely Gigabit Ethernet, or 1 Gbps data rate; these ports are not 10/100/1000 speed ports.

Additionally, dual hot-swappable modular power supplies are available in AC and DC versions. For LAN attachments, the switch also contains two ASIC-based SFP Gigabit Ethernet ports, as well as 24 10/100 ports.

This switch provides impressive QoS performance, as shown in Scalability and Performance Results, page 40.

Scalability Considerations

This section addresses the factors that influence or constrain the scalability of the design.

Overview

In the *Voice and Video Enabled IPsec VPN (V3PN) Solution Reference Network Design Guide*, QoS is described as being applied to the branch router and also to the WAN aggregation routers in the campus to guarantee good voice quality for encrypted VoIP traffic. In this example, the WAN consists of a traditional Frame Relay network. Frame Relay traffic shaping is implemented by applying QoS on a per-DLCI (per-PVC) basis on both the branch and WAN aggregation router. The QoS shaper is configured at a percentage of the CIR (typically 95 percent), and packets matching the different classes (VoIP, call setup, and transactional data) are allocated bandwidth by either an LLQ or bandwidth value. Data packets are queued with the aggregate shaped rate.

In the *Enterprise Class Teleworker Design Guide*, QoS is described as being applied on the upstream broadband link. The QoS configuration is HCBWFQ, which is a parent QoS policy that includes a shaper providing congestion feedback and a child service policy implementing queueing within that shaped rate. This service policy is applied to the outside physical interface, which in this section is referred to as *QoS shaping per port*. In the teleworker design guide, no downstream QoS (from campus to branch) was applied because broadband service providers did not offer this feature, and it was too costly in CPU resources to enable it on the campus headend. Fortunately, the asymmetrical nature of broadband data rates, in which the downlink rate usually is 6–8 times the uplink rate, generally enables a single teleworker user to experience good VoIP quality with QoS enabled where it is needed the most: on the link with the least amount of bandwidth.

In the September 2006 performance updates to the *Dynamic Multipoint VPN (DMVPN) Design Guide* and the *Virtual Tunnel Interface (VTI) Design Guide*, per tunnel/branch HCBWFQ is implemented and the performance results reported in the respective design guide. In the *Virtual Tunnel Interface (VTI) Design Guide*, HCBWFQ is applied to the logical tunnel interface (virtual-template). In the *Dynamic Multipoint VPN (DMVPN) Design Guide*, HCBWFQ is applied to the outside physical interface with each branch identified by the inside VLAN network address (**qos pre-classify** is enabled on the mGRE interface) and the traffic for each branch is shaped accordingly.

This section addresses implementing HCBWFQ at both the branch and headend location. The performance testing is targeted at the following three general configurations:

- QoS shaping per port
- QoS shaping per Ethernet virtual circuit (per VLAN)
- QoS shaping per application class (DSCP) within each VLAN

Table 2 showing these three QoS configuration options in the context of the topology described in this design guide as well as the previously-mentioned design guides.

Table 2 QoS Configuration Options

	Shaping by Port	Shaping by Logical Interface	Shaping by Branch	Shaping by VLAN	Shaping by Class by VLAN
Deployment type	Ethernet Internet access at subscribed aggregate data rate	Any head-to-branch speed mismatch	Any head-to-branch speed mismatch	Speed mismatch—Ethernet Relay Service	Speed mismatch—Ethernet Relay Service with subscribed rate per class
Branch	Identical to teleworker QoS configuration	Widely deployed for teleworker	N/A	Two or more VLANS with one shaper for each VLAN	Two VLANS with one shaper per class See Scalability and Performance Results, page 40
Headend	Generally not relevant for hub-and-spoke deployments	Refer to *Virtual Tunnel Interface (VTI) Design Guide*	Refer to *Dynamic Multipoint VPN (DMVPN) Design Guide*	VLAN per branch with one shaper each See by class/VLAN	VLAN per branch with one shaper per class See Scalability and Performance Results, page 40

Performance results for these test cases across various hardware platforms are shown in Scalability and Performance Results, page 40.

QoS Configuration

To bound the performance results, the QoS configuration used in testing is described in this section.

Traffic Classes

Although each customer may have different traffic classes and bandwidth allocation percentages for their internal QoS configuration, when traffic is transported across a service provider network offering end-to-end QoS, both the service provider and enterprise customer must coordinate ToS byte (DSCP/IP Precedence) markings and bandwidth allocation.

The number of classes and the bandwidth allocation percentage differ from service provider to service provider. The testing in this design guide uses the following allocation:

- Real-time (VoIP, call signaling and optionally video-conferencing)—35 percent
- Gold class (transactional, mission-critical, RP, NMS)—15 percent
- Silver class (streaming video, bulk data)—25 percent
- Best Effort (scavenger data)—25 percent

This allocation represents a reasonable test case. Testing every possible deployment scenario in common use would make scale testing unnecessarily complex and repetitive.

Note It must be assumed that every service provider will be different, but four classes at these percentage allocations per class is considered a reasonable test case.

Reference Bandwidth Values

Table 3 shows sample bandwidth values based on port CIR and bandwidth allocation percentages.

Table 3 Bandwidth Values

Class	%	2 Mbps	10 Mbps	20 Mbps	100 Mbps
Real-Time	35%	717 K	3584 K	7168 K	35 M
Gold	15%	207 K	1536 K	3072 K	15 M
Silver	25%	512 K	2560 K	5120 K	25 M
Best Effort	25%	512 K	2560 K	5120 K	25 M

Class Map

The QoS class map in use is shown in the following example.

```
!
class-map match-any GOLD
 match ip dscp cs3
 match ip dscp cs6
class-map match-any TRANSACTIONAL_DATA
 match ip dscp af21
class-map match-any NETWORK_MANAGEMENT
 match ip dscp cs2
class-map match-any SILVER
 match ip dscp cs2
class-map match-any REAL_TIME
 match ip dscp cs5
 match ip dscp ef
 match ip dscp af41
class-map match-any STREAMING_VIDEO
 match ip dscp cs4
class-map match-any BEST_EFFORT
 match ip dscp default
 match ip dscp cs1
class-map match-any BULK_DATA
 match ip dscp af11
class-map match-any CALL-SETUP
 match ip dscp cs3
 match ip dscp af31
```

```
!
```

Note A DSCP value of AF41 is used by Cisco Unified Video Advantage (CUVA, formerly Cisco VT Advantage), while a voice/video call is active for both the voice and video data stream.

Remarking

Although remarking does not significantly degrade QoS performance, it is assumed that the enterprise customer and service provider may need to remark both the Layer 3 ToS Byte (DSCP) and the Layer 2 CoS value. This function is also included in the tested QoS configuration.

```
policy-map INGRESS
  class REAL_TIME
  set ip dscp cs5
  class CALL-SETUP
  set ip dscp cs5
  class STREAMING_VIDEO
  set ip dscp cs2
  class TRANSACTIONAL_DATA
  set ip dscp cs3
  class NETWORK_MANAGEMENT
  set ip dscp cs3
  class BULK_DATA
  set ip dscp af21
!
```

Note Remarking CoS is shown in the EGRESS service policy in the next section.

Per-Port Shaping

The following policy map configuration example is applicable for per-port shaping. The shaped rate is 2 Mbps (2000000) with a 10 ms interval (20000).

```
policy-map EGRESS
  description test
  class GOLD
  bandwidth percent 15
  set cos 3
  class SILVER
  bandwidth percent 25
  set cos 2
  class REAL_TIME
  priority percent 35
  set cos 5
  class class-default
  fair-queue
  random-detect
  set cos 0
policy-map SHAPER
  class class-default
  shape average 2000000 20000
  service-policy EGRESS
!
```

Per-Class Shaping

In configurations that deploy shaping on a per-class basis, the following is an example. Note that the REAL-TIME class does not apply to shaping or policing. Call Admission Control is used to limit the number of concurrent calls to adhere to the subscribed rate.

```
policy-map PER_CLASS_SHAPING
  class REAL_TIME
   estimate bandwidth
  set cos 5
  class GOLD
  shape average 307000
  set cos 3
  class SILVER
  shape average 512000
  set cos 2
  class class-default
  shape average 512000
  fair-queue
  random-detect
  set cos 0
```

Security Configuration

This section discusses the security features enabled in the performance tests.

Intrusion Protection System

The Cisco IOS Intrusion Protection System (IPS) is configured on the branch router. The IPS configuration is similar to that used in the *Enterprise Branch Security Design Guide* at the following URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a00807593b6.pdf.

IOS IPS acts inline to watch packets and sessions flowing through the branch router. Packets are scanned for matches to any IPS signatures. In testing signatures, 1107 (RFC 1918 Addresses Seen), 2000 (ICMP Echo Reply), and 2001 (ICMP Host Unreachable) are disabled.

```
!
ip ips deny-action ips-interface
ip ips notify SDEE
ip ips signature 1107 0 disable
ip ips signature 2000 0 disable
ip ips signature 2001 0 disable
ip ips name ceb
!
interface Tunnel0
 description Tunnel0
 bandwidth 2048
 ...
 ip access-group TUNNEL_ACL in
 ...
 ip ips ceb in
 ip route-cache flow
!
interface Tunnel1
 description Tunnel1
 bandwidth 2048
 ...
 ip access-group TUNNEL_ACL in
```

```
 ...
 ip ips ceb in
 ip route-cache flow

!
interface FastEthernet0/0.2200
 description Primary WAN
 encapsulation dot1Q 2200
 ip address 192.168.0.2 255.255.255.252
 ip access-group INPUT_ACL in
 ip ips ceb in
 service-policy output PER_CLASS_2mb
!
interface FastEthernet0/0.3300
 description Secondary WAN
 encapsulation dot1Q 3300
 ip address 192.168.0.146 255.255.255.252
 ip access-group INPUT_ACL in
 ip ips ceb in
 service-policy output PER_CLASS_2mb
!
```

IPS CPU Consumption

Preliminary tests were completed with and without IPS configured on a Cisco 1841 ISR router running Cisco IOS version 12.4(9)T2. The branch topology is a single physical outside trunked interface with two 802.1q VLANS. There is a DMVPN tunnel associated with each outside VLAN interface into the service provider network. Each VLAN is configured with a 2 Mbps shaper. The performance test is run first with IOS Firewall enabled and then with both IOS Firewall and IPS. The results are shown in Table 4.

Table 4 Cisco 1841 ISR

Test	VoIP Drop %	VoIP Jitter ms	VoIP Delay ms	VoIP G.729 Calls/pps	Data pps	Total CPU Busy
Baseline with QoS	0	3	6.3	12 (1200 pps)	800	68%
Add firewall	0	2.6	6.7	12 (1200 pps)	794	85%
Add firewall and IPS	0	1.4	5.2	12 (1200 pps)	261	99%

In all tests, the branch router supported 12 concurrent G.729 VoIP calls with performance results exceeding the criteria for acceptable VoIP quality for the Real-Time Protocol (RTP) streams. For the same level of data and VoIP packets per second, the average total CPU utilization increased from 85 percent to 99 percent because IPS was enabled. The main CPU busy value of 80 percent is the upper bound for a recommended deployment. A total sustained CPU busy of 99 percent is not a recommended deployment.

A 15–20 percent increase in main CPU busy can be expected in the Cisco ISR platforms when IPS is enabled.

Summary

Assuming that most customer deployments do not require IPS at the branch in this topology, the performance results in this document do not have IPS enabled in the configuration.

IOS Firewall

The Cisco ISO Firewall configuration used in performance testing is as follows:

```
ip inspect name CBAC sip
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp

interface {inside LAN}
ip inspect CBAC in

interface [Outside_Ethernet_WAN]
ip access-group INPUT_ACL in
!
interface Tunnel 0
ip access-group TUNNEL_ACL in
!
interface Tunnel 1
ip access-group TUNNEL_ACL in
!
ip access-list extended INPUT_ACL
 remark this is meant to be fairly generic
 remark you could be more specific in the source IP for IKE/ESP, NTP etc.
 permit udp any  any eq isakmp
 permit udp any  any eq non500-isakmp
 permit esp any any
 permit udp any any eq bootpc
 permit udp any eq ntp any eq ntp
 permit tcp any eq 22 any
 permit icmp any any
 deny   ip any any

ip access-list extended TUNNEL_ACL
 remark Verify this is acceptable for testing
 remark Most customers would want to open this up a bit
 permit eigrp any any
 permit udp any eq ntp any eq ntp
 permit tcp any eq 22 any
 permit icmp any any
 deny   ip any any
!
```

Encryption Algorithms

In testing, the Advanced Encryption Standard (AES) with the maximum configurable key length of 256 is used. AES offers three different key lengths: AES-128, AES-192, and AES-256. AES-128 is similar to 3DES in terms of encryption strength. AES-192 and AES-256 provide a higher level of security than 3DES.

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
!
crypto ipsec transform-set AES_SHA_TUNNEL esp-aes 256 esp-sha-hmac
```

As shown above, 256-bit AES is used for both Internet Key Exchange (IKE) and IPsec.

Scalability and Performance Results

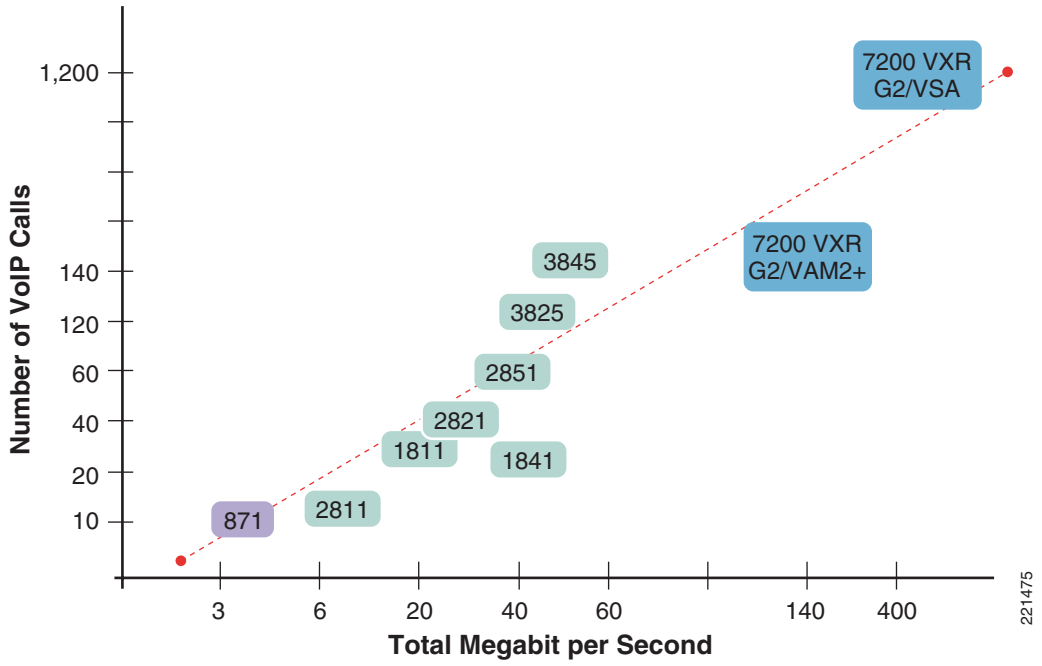
This section provides performance guidance for both branch and headend aggregation roles.

Single-Tier Branch

The single-tier branch deployment integrates all functions (QoS, firewall, ACL, and encryption) on a single chassis. This is the most commonly deployed topology in a branch environment because the single chassis reduces costs associated with deployment of hardware, support, and maintenance of the large number of branch routers in the enterprise customer network.

Figure 16 provides a high-level overview of the suitability of different Cisco routers based on the number of concurrent VoIP calls and total megabits per second of aggregate (both uplink and downlink) traffic for voice and data.

Figure 16 Cisco Router Platform Capabilities



This performance data is based on a QoS service policy applied to each outside VLAN interface (uplink) with a single DMVPN tunnel associated with each uplink. The branch configuration is therefore a DMVPN dual-hub, dual-cloud deployment (two DMVPN clouds, each having a single hub router, while the branch has a logical interface to both clouds) with a single port into the service provider network with two logical sub-interfaces. Each IPsec tunnel has an affinity to its respective sub-interface.

Each class has its own shaper configured. This is described as a “two VLANS with shaper per class” topology.

The results shown in Figure 16 are represented in tabular format in Table 5.

Table 5 Cisco Router Platform Capabilities

Platform	Number of Tunnels Shaped at (Mbps) each	VoIP Drop %–Jitter-Delay (ms)	VoIP G.729 Calls (pps)	Data (pps)	Total pps	Total Mbps	Total CPU Busy
871	2 at 2 Mbps	0.1% 3.3 12.5	12/1200	478	1,047	5.6	64%
2811	2 at 2 Mbps	0% 1 2.4	12/1200	675	1,875	7.3	65%
1841	2 at 4 Mbps	0% 0.5 1.1	24/2400	6,108	8,508	44	50%
1811	2 at 7Mbps	0% 0.2 1.2	42/4200	2,443	6,643	25	56%
2821	2 at 7 Mbps	0% 0.1 1.3	42/4200	1,303	5,503	28	43%
2851	2 at 10Mbps	0% 0.8 2.5	60/6000	2,714	8,714	41	70%
3825	2 at 20 Mbps	0% 1.5 2.2	120/12000	4,775	16,775	48	41%
3845	2 at 25 Mbps	0% 1 2.2	145/14500	5,863	20,363	55.7	43%
7200VXR NPE-G2 VAM2+	2 at 50 Mbps	0% 0.1 0.5	145/14500	28,996	43,496	139	60%
7200VXR NPE-G2 VSA	2 at 200 Mbps	0.5% 0.8 2	1159/ 115900	27,070	142,570	401	78%

Observations and Comment

In these test results, the offered traffic load was not generated at varying rates and re-tested to target a specific percent CPU busy. In previous Cisco design guides, the goal was to obtain as close to an 80–85 percent CPU busy. With the more granular QoS configuration and the per-source/per-destination load balancing of CEF switching, along with multiple uplinks to the WAN, targeting a specific CPU busy value is extremely difficult and time consuming.

The aggregate Mbps rates used in testing are intended to report test results with total CPU busy falling in a range of 40–85 percent in most cases.

The voice drops, jitter, and delay (latency) are reported but as can be seen, all represent extremely favorable values. VoIP call quality is considered toll quality in these tests. The number of concurrent VoIP calls are shown to provide some guidance into the number of employees that can be supported on these hardware platforms at a given uplink rate. Busy hour traffic (in Erlangs) is the number of hours of call traffic there are during the busiest hour of operation of a telephony system. Given that many enterprise deployments use a factor of 1:4 to 1:10 active calls per employee, a value of 90 concurrent VoIP calls can support the VoIP requirements of 360 to 900 employees at that location.

The total pps rate is shown because this value represents the most accurate sizing metric. Total Mbps is also shown, but this is for purposes of illustration and compatibility. Representing site data requirements based on Mbps is less reliable than pps because the average packet size greatly skews the results when reported in Mbps.

Summary

Based on these test results, the Cisco products tested are capable of supporting a branch of one teleworker up to a large branch office of 6000 employees. For larger branch offices, multiple WAN routers would likely be deployed to enhance redundancy, as well as VoIP gateways and potentially direct Internet connectivity, but the inter-enterprise VoIP and data requirements can be supported by an encrypted WAN deployed using Metro Ethernet handoff.

Single-Tier Headend

The test results shown in Table 6 represent a single-tier headend, where QoS is enabled on a per-branch basis and encryption is also enabled.

Table 6 Single-Tier Headend Test Results

Platform	Number of Tunnels, QoS Configuration, and Shape Rate	VoIP Drop % Jitter (ms) Delay (ms)	VoIP G.729 Calls (pps)	Data (pps)	Total PPS	Total Mbps	Total CPU Busy SIP/ MSFC
7200 VXR G2 w/ VSA	30 HCBWFQ 4Mbps	0% 1.3ms 2.7ms	454/ 45,400	12,367	57,767	124	69%
7600 SIP-400	150 HCBWFQ 4 Mbps	.03% .7 ms 3.3ms	2575/ 257,500	53,526	311,029	692	4% 15%
7600 SIP-400	240 per-class per-VLAN 4 Mbps	.22% .6ms 2.1 ms	4009/ 400,900	53,951	454,851	1,002	8% 15%
7600 SIP-600	240 Per-class per-VLAN 4 Mbps	.5% 1.3 ms 5.8 ms	4320 / 432,000	80,990	512,990	1,462	22% 12%

Note the following:

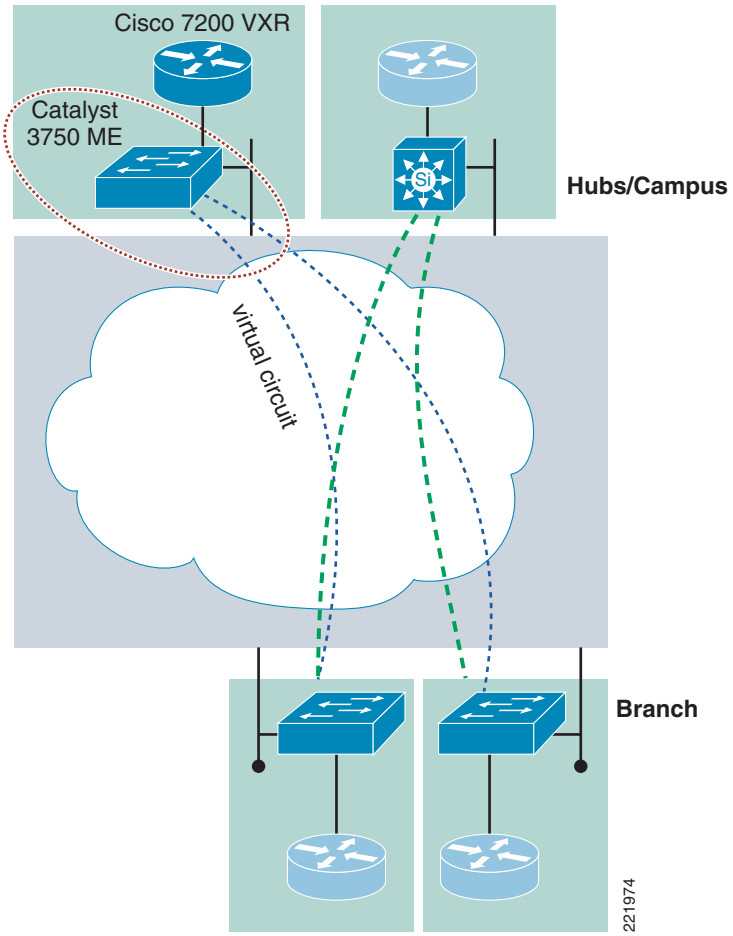
- The SIP-600 does not support HCBWFQ as does the SIP-400. For this reason, no performance results were reported.
- The criteria for testing VoIP in the Cisco lab was <8 ms jitter, <50 ms latency (delay), and <.5 percent drops given a Frame Relay WAN in the test bed, with no service provider propagation delay. Given an appreciable decrease in serialization delay by substituting a Frame Relay WAN with a Metro Ethernet WAN, the VoIP drops, latency, and jitter are considerably less than shown in previous design guides.

QoS Devices for Dual-Tier Models

In some customer deployments, using a dedicated device to offload the QoS function may be desirable. Table 7 shows how a Catalyst 3750 Metro Ethernet switch can be deployed to provide QoS functions. The results are shown for a headend campus perspective. However, the 3750ME switch can also be deployed at a branch location. Figure 17 shows the typology for the information shown in Table 7.

Figure 17 Catalyst 3750 ME Test Topology
Table 7 Using the Catalyst 3750 Metro Ethernet Switch

Platform	Number of Tunnels Shaped per class at Agg (bps)	VoIP Drop % -Jitter-Delay (ms)	VoIP G.729 Calls (pps)	Data (pps)	Total PPS	Total Mbps	Total CPU Busy
Catalyst 3750 Metro Ethernet	75 at 4 Mbps	.4% 2.6 6	1350/ 135,000	13,805	148,805	347	18%



The Catalyst 3750 Metro Ethernet switch in this example does not terminate encryption, VoIP, or any other service; it is simply inserted at the headend to provide downstream shaping. VoIP drops, jitter, and delay are reported to demonstrate that these data rates can be sustained without introducing any significant overhead to the existing VoIP stream flowing inside the encrypted DMVPN tunnel. The total CPU busy value does not increase linearly with increased packet per second rates of offered load. Do not rely on Total CPU busy as an indication of reserve capacity.

Summary

Implementing the dual-tier model to a dedicated device as a standalone QoS function may be effective in some customer deployments. However, if the packets being acted upon by the QoS function are encrypted, delaying data packets by queueing them may actually cause anti-replay drops by the decrypting router. For more information on the IPsec replay detection function and how this relates to QoS, see the *Voice and Video Enabled IPsec VPN (V3PN) SRND* at the following URL: http://www.cisco.com/go/srnd.

Additionally, implementing two chassis does incur additional costs in maintenance and management of separate chassis that should also be considered in addition to the initial purchase price of the equipment.

Case Study

This section provides a case study describing a typical enterprise deployment based on Frame Relay, and demonstrates the configuration changes required at the branch router to connect to an EVPL service at the branch location.

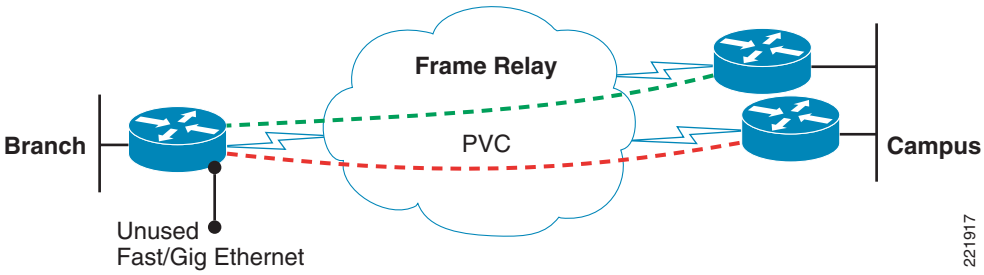
It is assumed that the existing branch router is a Cisco ISR 3825, with one of the onboard Gigabit Ethernet interfaces connecting to a Layer 2 switch in the branch office and the second onboard Gigabit Ethernet currently available for use. This available interface is connected to a switch provided by the Metro Ethernet service provider using 802.1q encapsulation.

The current network topology includes a single serial interface with two PVCs to the campus location. All traffic flows via the primary campus hub router unless a failure occurs, at which time the secondary or backup hub router is used. This is accomplished by using EIGRP as a routing protocol and the *offset-list* configuration option on the secondary router to decrement the metric on routes advertised from the secondary router. It is assumed that both PVCs have a CIR of 512 K and that QoS is applied to the Frame Relay PVC.

Existing Topology and Configuration

Figure 18 shows the existing topology. Relevant portions of the configurations are shown following the diagram.

Figure 18 Case Study—Existing Topology



Branch Router Configuration

The branch router is configured as an EIGRP stub. It has a single physical serial interface with two Frame Relay PVCs, each terminating on a separate headend router.

```
!
hostname vpn4-3800-1
!
! System image file is "flash:c3825-advipservicesk9-mz.124-15.T"

!
class-map match-all call-setup
 match ip precedence 3
class-map match-any mission-critical
 match ip precedence 2
 match ip precedence 6
class-map match-all voice
 match ip precedence 5
!
!
```

```
policy-map llq-branch
 class call-setup
  bandwidth percent 5
 class mission-critical
  bandwidth percent 22
 class voice
  priority 168
 class class-default
  fair-queue
!
!
interface GigabitEthernet0/1.228
 description Inside LAN
 encapsulation dot1Q 228
 ip address 10.0.104.1 255.255.255.0
!
!
interface Serial0/1/0
 bandwidth 2000
 no ip address
 encapsulation frame-relay
 load-interval 30
 frame-relay traffic-shaping

!
interface Serial0/1/0.100 point-to-point
 description to vpn4-3800-3
 bandwidth 512
 ip address 10.0.65.1 255.255.255.252
 frame-relay interface-dlci 100
  class ts-branch
!
interface Serial0/1/0.101 point-to-point
 description to vpn-jk2-3640-1
 bandwidth 512
 ip address 10.0.65.5 255.255.255.252
 frame-relay interface-dlci 101
  class ts-branch
!
router eigrp 50
 network 10.0.0.0
 no auto-summary
 eigrp stub connected
!
map-class frame-relay ts-branch
 frame-relay cir 486400
 frame-relay bc 4864
 frame-relay be 0
 frame-relay mincir 486400
 frame-relay fragment 640
 service-policy output llq-branch
!
end
```

Primary Frame Relay Headend Configuration

Both the primary headend and the secondary headend send a default route (0/0) to the branch routers. This is accomplished by redistributing a static route to the default network into the EIGRP process.

```
!
hostname vpn4-3800-3
!
!
class-map match-all call-setup
 match ip precedence 3
class-map match-any mission-critical
 match ip precedence 2
 match ip precedence 6
class-map match-all voice
 match ip precedence 5
!
!
policy-map llq-branch
 class call-setup
  bandwidth percent 5
 class mission-critical
  bandwidth percent 22
 class voice
  priority 168
 class class-default
  fair-queue
!
!
interface GigabitEthernet0/1.106
 encapsulation dot1Q 106
 ip address 192.168.131.99 255.255.255.224
 no snmp trap link-status
!
interface Serial0/1/0
 bandwidth 2000
 no ip address
 encapsulation frame-relay
 load-interval 30
 frame-relay traffic-shaping
!
interface Serial0/1/0.100 point-to-point
 description to vpn4-3800-1
 bandwidth 512
 ip address 10.0.65.2 255.255.255.252
 frame-relay interface-dlci 100
  class ts-branch
!
router eigrp 50
 redistribute static metric 1536 100 255 1 1500 route-map ROUTES_TO_BRANCH
 network 10.0.0.0
 network 192.168.131.96 0.0.0.31
 distribute-list ROUTES_TO_BRANCH out Serial0/1/0.100
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Null0
!
ip access-list standard ROUTES_TO_BRANCH
 permit 0.0.0.0
!
!
map-class frame-relay ts-branch
```

```
 frame-relay cir 486400
 frame-relay bc 4864
 frame-relay be 0
 frame-relay mincir 486400
 frame-relay fragment 640
 service-policy output llq-branch
!
route-map ROUTES_TO_BRANCH permit 10
 match ip address ROUTES_TO_BRANCH
!
end
```

Secondary Frame Relay Headend Configuration

The QoS configuration is not shown; for this, see Primary Frame Relay Headend Configuration, page 47.

```
!
hostname vpn-jk2-3640-1
!
!
!
interface Serial0/0
 bandwidth 2000
 no ip address
 encapsulation frame-relay
 load-interval 30
 no dce-terminal-timing-enable
 frame-relay traffic-shaping
 frame-relay lmi-type cisco
!
interface Serial0/0.101 point-to-point
 description to vpn4-3800-1
 bandwidth 512
 ip address 10.0.65.6 255.255.255.252
 frame-relay interface-dlci 101
  class ts-branch
!
!
interface FastEthernet1/0.106
 encapsulation dot1Q 106
 ip address 192.168.131.98 255.255.255.224
 no snmp trap link-status
!
!
```

Note Note that *offset-list* is included in the secondary headend configuration to increase the metric by a value of 3000, making routes learned from this headend less preferred than those received from the primary Frame Relay headend router.

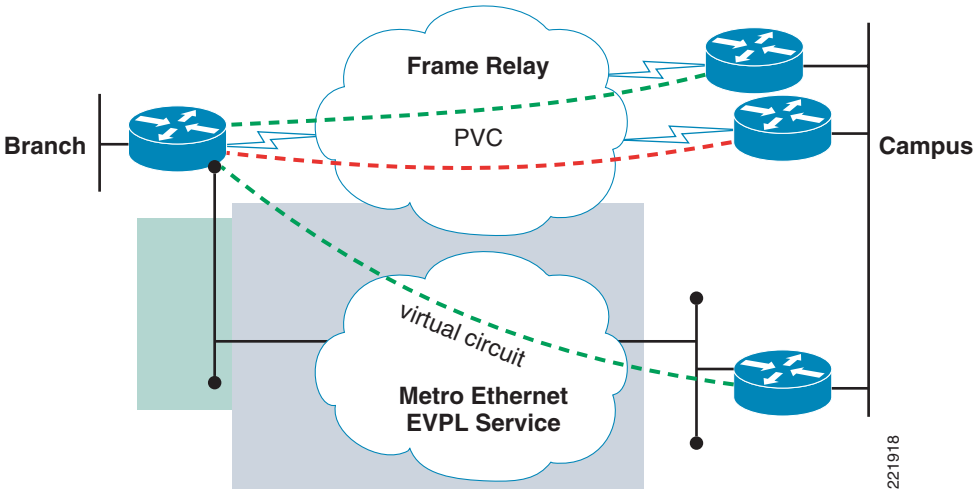
```
!
router eigrp 50
 redistribute static metric 1536 100 255 1 1500 route-map ROUTES_TO_BRANCH
 offset-list ROUTES_TO_BRANCH out 3000
 network 10.0.0.0
 distribute-list ROUTES_TO_BRANCH out Serial0/0.101
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Null0
!
ip access-list standard ROUTES_TO_BRANCH
 permit 0.0.0.0
```

```
!
!
route-map ROUTES_TO_BRANCH permit 10
 match ip address ROUTES_TO_BRANCH
!
end
```

Revised Topology and Configuration

The revised topology now includes a Metro Ethernet EVPL WAN through the available Gigabit Ethernet port on the branch router, as shown in Figure 19. A new campus router has also been implemented to terminate the Metro Ethernet service on the campus location.

Figure 19 Case Study—Revised Topology



Branch Router Configuration

The branch router is updated to include new QoS class maps and policy maps to align with the Metro Ethernet service offering. It is assumed that this location has a 2 Mbps CIR in aggregate. Of this aggregate rate, the four classes are allocated as follows:

- Real-Time—35 percent or 717 K
- Gold—15 percent or 207 K
- Silver—24 percent or 512 K
- Best Effort—25 percent or 512 K

The addition to the existing configuration is as follows:

```
!
hostname vpn4-3800-1
!
class-map match-any GOLD
 match ip dscp cs3
 match ip dscp cs6
 match ip dscp af21
class-map match-any SILVER
```

```
 match ip dscp cs2
class-map match-any REAL_TIME
 match ip dscp cs5
 match ip dscp ef
 match ip dscp af41
!
policy-map PER_CLASS_2mb
 class REAL_TIME
    police 716500 conform-action transmit  exceed-action transmit  violate-action transmit
  set cos 5
 class GOLD
  shape average 307200
  set cos 3
 class SILVER
  shape average 512000
  set cos 2
 class class-default
  shape average 512000
  set cos 0
!
interface GigabitEthernet0/0.229
 description EVPL VLAN;WAN Interface 229
 encapsulation dot1Q 229
 ip address 10.0.65.14 255.255.255.252
 service-policy output PER_CLASS_2mb
!
```

A portion of the IP routing table following the enabling of the Metro Ethernet services and configuration changes is as follows:

```
vpn4-3800-1# show ip route | beg 10.0.0.0/8
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.0.65.12/30 is directly connected, GigabitEthernet0/0.229
C       10.0.65.0/30 is directly connected, Serial0/1/0.100
C       10.0.65.4/30 is directly connected, Serial0/1/0.101
C       10.0.104.0/24 is directly connected, GigabitEthernet0/1.228
D*EX 0.0.0.0/0 [170/1694720] via 10.0.65.13, 00:52:02, GigabitEthernet0/0.229
```

The default route (0/0) is now in the IP routing table with the new Metro Ethernet service being the preferred path. There have been no changes on the branch router to accomplish this. The derived EIGRP metric over the Gigabit Ethernet interfaces is preferred over the existing Frame Relay service, making it the preferred choice for use for traffic from branch to headend and also the return path, from headend to branch.

If the Metro Ethernet service is disabled for any reason or the associated headend router fails or is taken offline, the Frame Relay service is again used. This can be seen by looking at the EIGRP topology table for the default route:

```
vpn4-3800-1#show ip eigrp topology detail-links
IP-EIGRP Topology Table for AS(50)/ID(172.26.156.100)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 0.0.0.0/0, 1 successors, FD is 1694720, serno 12
        via 10.0.65.13 (1694720/1692160), GigabitEthernet0/0.229
        via 10.0.65.2 (5537536/1692160), Serial0/1/0.100
        via 10.0.65.6 (5540536/1695160), Serial0/1/0.101
```

From the above display, all three paths are in the EIGRP topology table. The Metro Ethernet service is preferred, with the lowest metric, then the primary Frame Relay hub, followed by the backup Frame Relay hub.

Sizing the Metro Ethernet Headend

As discussed in Scalability and Performance Results, page 40, data is provided to assist the network designer in selecting the appropriate type of headend to support the expected data rate and number of branch routers.The most important data points for sizing a headend are:

- Number of branch locations
- Data rate in packets per second by branch.

Simply sizing the headend based on the port speed or CIR of the branch locations will likely give an unrealistic requirement for sizing the headend campus location.

Because the performance testing represented in this document included VoIP using a G.729 CODEC, the results, in terms of total Mbps, are highly conservative estimates. the G.729 CODEC generates a relative small packet (60 bytes at Layer 3) and therefore the performance results in Mbps are much lower than performance data where the test traffic is all TCP-based flows. File Transfer (FTP) or web sessions (HTTP) are TCP flows which often have an average packet size of 300-500 bytes or more.

The packet per second rate offered by the branch routers is the most critical factor in sizing a headend capable supporting the branch offices. In most deployments with more than 30 to 50 branches requiring more than 1,000 to 2,000 pps each, the appropriate headend is a Cisco 7600 series with either a SIP-400 or SIP-600. This assumption is based on a requirement to implement QoS from headend to branch and also provide encryption.

If the branch locations are services by bandwidth purchased on a per-class, per VLAN (per branch location), the SIP-600 offers the highest performance characteristics. If the branch locations are connected by a service that is based on an aggregate rate for all classes, then Hierarchial CBWFQ, which entails queueing within a shaped rate, is most appropriate. The SIP-400 supports this configuration.

As the specific requirements and traffic profiles of each customer deployment differ, the performance results represented in this document can only be used as a guide. More specific testing in a customer lab environment, pilot deployment, or a Cisco customer proof-of-concept (CPOC) engagement may be appropriate for a successful deployment.

Metro Ethernet Headend Configuration

This headend is installed to support the headend campus termination of the Metro Ethernet sub-interfaces. The QoS configuration is similar to the branch configuration, and the EIGRP configuration is similar to the primary Frame Relay router.

Note This configuration is based on a Cisco 3825 as an example. The Configuration Examples section provides sample configuration for other platforms, including the Cisco 7600 series.

```
!
hostname vpn4-3800-4
!
!
class-map match-any GOLD
```

```
 match ip dscp cs3
 match ip dscp cs6
 match ip dscp af21
class-map match-any SILVER
 match ip dscp cs2
class-map match-any REAL_TIME
 match ip dscp cs5
 match ip dscp ef
 match ip dscp af41
!
!
policy-map PER_CLASS_2mb
 class REAL_TIME
    police 716500 conform-action transmit  exceed-action transmit  violate-action transmit
  set cos 5
 class GOLD
  shape average 307200
  set cos 3
 class SILVER
  shape average 512000
  set cos 2
 class class-default
  shape average 512000
  set cos 0
!
!
interface GigabitEthernet0/1.229
 encapsulation dot1Q 229
 ip address 10.0.65.13 255.255.255.252
 service-policy output PER_CLASS_2mb
!
router eigrp 50
 redistribute static metric 1536 100 255 1 1500 route-map ROUTES_TO_BRANCH
 network 10.0.0.0
 network 192.168.131.96 0.0.0.31
 distribute-list ROUTES_TO_BRANCH out GigabitEthernet0/1.229
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Null0
!
!
ip access-list standard ROUTES_TO_BRANCH
 permit 0.0.0.0
!
!
route-map ROUTES_TO_BRANCH permit 10
 match ip address ROUTES_TO_BRANCH
!
end
```

Summary

This case study illustrates one of the strengths of deploying Metro Ethernet service to support increased bandwidth requirements for branch locations. The case study demonstrates how a 2 Mbps Metro Ethernet service can be easily provisioned using an unused Gigabit Ethernet interface on the branch router. Furthermore, with the addition of a QoS configuration and a few simple interface configuration commands, the branch location is easily upgraded, while the existing WAN links remain deployed as ready backup if needed. In this example, the Frame Relay WAN could be eliminated entirely, or replaced

with a DSL or cable modem deployment to provide backup over broadband services. Because of the embedded encryption adapter support on the ISR series, encryption of both the Metro Ethernet service and the backup links using DSL or cable over the Internet can also easily be deployed.

Configuration Examples

This section includes sample configurations used in performance and other testing.

Simple Handoff

This example represents a simple handoff configuration as is common with an aDSL connection using a DSL bridge (modem) or a cable modem.

```
!
hostname aebright-vpn
!
class-map match-any VOICE_and_VT_Advantage
 match ip dscp ef
 match ip dscp af41
class-map match-any VOICE
 match ip dscp ef
 match ip precedence 5
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
 match ip dscp cs6
class-map match-any VIDEO-surveillance
 match ip dscp cs4
 match access-group name IPmc
!
!
policy-map V3PN-teleworker
 description Note LLQ for ATM/DSL G.729=64K, G.711=128K
 class CALL-SETUP
  bandwidth percent 2
 class INTERNETWORK-CONTROL
  bandwidth percent 5
 class VOICE
  priority 128
 class class-default
  fair-queue
  random-detect
!
policy-map Shaper
 class class-default
  shape average 365000 36500
  service-policy V3PN-teleworker
!
!
interface FastEthernet4
 description Outside
 ip address dhcp
 ip access-group INPUT_ACL_29Mar07 in
 ip nat outside
 ip inspect CBAC out
 ip virtual-reassembly
 ip route-cache flow
```

```
 ip tcp adjust-mss 542
 duplex auto
 speed auto
 no cdp enable
 service-policy output Shaper
!
end
```

For additional information on teleworker configurations, see the *Business Ready Teleworker Design Guide* at the following URL: http://www.cisco.com/go/srnd.

Headend Configuration—7600 SIP-400 - HCBWFQ per VLAN

This configuration sample is for the performance testing using a SIP-400 configured with 150 VLANs and using HCBWFQ.

```
!
hostname he3-7600-1
!
boot-start-marker
boot system flash disk0:c7600s72033-adventerprisek9-mz.122-33.SRB1.bin
boot-end-marker
!
class-map match-all r6-9-0158-2358
  match vlan  2358
class-map match-all r7-8-0187-2387
  match vlan  2387
class-map match-all r8-3-0212-2412
  match vlan  2412
class-map match-all r9-2-0241-2441
  match vlan  2441
... [and so on] ...
!
policy-map branch-traffic
  class REAL_TIME
    priority percent 35
   set cos 5
  class GOLD
    bandwidth percent 15
   set cos 3
  class SILVER
    bandwidth percent 25
   set cos 2
  class class-default
    bandwidth percent 25
   set cos 0
!
policy-map hqos-policy
  class r2-1-0030-2230
    shape average 4096000
   service-policy branch-traffic
  class r2-2-0031-2231
    shape average 4096000
   service-policy branch-traffic
  class r2-19-0048-2248
    shape average 4096000
   service-policy branch-traffic
... [and so on] ...
!
vlan 100
 name Outside
```

```
!
vlan 101,161,163,171,173,181,183,191,193,201,203,211,213
!
vlan 1100
 name r1-1-LAN
!
vlan 1101
 name r1-2-LAN
!
vlan 1102
 name r1-3-LAN
!
... [and so on] ...
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set AES_SHA_TUNNEL esp-aes 256 esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto ipsec profile vpn-dmvpn
 set transform-set AES_SHA_TUNNEL
!
!
crypto identity aeisha
 !
 !
!
!
interface Tunnel0
 description Tunnel0
 bandwidth 100000
 ip address 10.56.0.1 255.255.248.0
 no ip redirects
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105600
 ip nhrp holdtime 1800
 ip nhrp registration timeout 120
 ip summary-address eigrp 1 10.204.0.0 255.252.0.0 5
 load-interval 30
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel protection ipsec profile vpn-dmvpn
 crypto engine slot 2/0 inside
!
!
interface GigabitEthernet4/0/0
 description GigabitEthernet4/0/0 Outside Interface
 no ip address
 load-interval 30
 negotiation auto
 service-policy output hqos-policy
 hold-queue 4096 in
 hold-queue 4096 out
!
interface GigabitEthernet4/0/0.2200
 description r1-1
```

```
 encapsulation dot1Q 2200
 ip address 192.168.0.1 255.255.255.252
 crypto engine slot 2/0 outside
!
interface GigabitEthernet4/0/0.2201
 description r1-2
 encapsulation dot1Q 2201
 ip address 192.168.1.1 255.255.255.252
 crypto engine slot 2/0 outside
!
interface GigabitEthernet4/0/0.2202
 description r1-3
 encapsulation dot1Q 2202
 ip address 192.168.2.1 255.255.255.252
 crypto engine slot 2/0 outside
!
... [and so on] ...
!
interface GigabitEthernet4/0/1
 description GigabitEthernet4/0/1-Inside
 ip address 10.204.0.1 255.252.0.0
 no ip redirects
 load-interval 30
 negotiation auto
 service-policy input INGRESS
!
end
```

Headend Configuration—7600 SIP-400 - Per-Class Shaper per VLAN

This configuration sample is used for the 7600 SIP-400 using a per-class shaper per VLAN in performance testing.

```
!
hostname he3-7600-1
!
boot-start-marker
boot system flash disk0:c7600s72033-adventerprisek9-mz.122-33.SRB1.bin
boot-end-marker
!
class-map match-all r6-9-0158-2358
  match vlan  2358
class-map match-all r7-8-0187-2387
  match vlan  2387
class-map match-all r8-3-0212-2412
  match vlan  2412
class-map match-all r9-2-0241-2441
  match vlan  2441
... [and so on] ...
!
!
policy-map branch
  class REAL_TIME
   police 3072000    conform-action transmit     exceed-action drop     violate-action
drop
    priority
   set cos 5
  class GOLD
    shape average 460800
```

```
   set cos 3
  class SILVER
    shape average 768000
   set cos 2
  class class-default
    shape average 2480000
   set cos 0
!
policy-map INGRESS
  class REAL_TIME
   set dscp cs5
  class CALL-SETUP
   set dscp cs5
  class STREAMING_VIDEO
   set dscp cs2
  class TRANSACTIONAL_DATA
   set dscp cs3
  class NETWORK_MANAGEMENT
   set dscp cs3
  class BULK_DATA
   set dscp af21
!
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 100
 name Outside
!
vlan 101,161,163,171,173,181,183,191,193,201,203,211,213
!
vlan 1100
 name r1-1-LAN
!
vlan 1101
 name r1-2-LAN
!
vlan 1102
 name r1-3-LAN
!
vlan 1103
 name r1-4-LAN
!
... [and so on] ...
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set AES_SHA_TUNNEL esp-aes 256 esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto ipsec profile vpn-dmvpn
 set transform-set AES_SHA_TUNNEL
!
!
crypto identity aeisha
 !
 !
```

```
 crypto dynamic-map dmap-vlan100 10
 set transform-set AES_SHA_TUNNEL
!
!
!
interface Tunnel0
 description Tunnel0
 bandwidth 100000
 ip address 10.56.0.1 255.255.248.0
 no ip redirects
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105600
 ip nhrp holdtime 1800
 ip nhrp registration timeout 120
 load-interval 30
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel protection ipsec profile vpn-dmvpn
 crypto engine slot 2/0 inside
!
!
interface GigabitEthernet4/0/0
 description GigabitEthernet4/0/0 Outside Interface
 no ip address
 load-interval 30
 negotiation auto
 hold-queue 4096 in
 hold-queue 4096 out
!
interface GigabitEthernet4/0/0.2200
 description r1-1
 encapsulation dot1Q 2200
 ip address 192.168.0.1 255.255.255.252
 crypto engine slot 2/0 outside
 service-policy output branch
!
interface GigabitEthernet4/0/0.2201
 description r1-2
 encapsulation dot1Q 2201
 ip address 192.168.1.1 255.255.255.252
 crypto engine slot 2/0 outside
 service-policy output branch
!
... [and so on] ...
!
interface GigabitEthernet4/0/1
 description GigabitEthernet4/0/1-Inside
 ip address 10.204.0.1 255.252.0.0
 no ip redirects
 load-interval 30
 negotiation auto
 service-policy input INGRESS
!
...
end
```

Headend Configuration—7600 SIP-600 - Per-Class Shaper per VLAN

The following configuration sample is for a Cisco 7600 SIP-600 with each VLAN having a per-class shaper configured.

```
!
hostname he3-7600-1
!
boot-start-marker
boot system flash disk0:c7600s72033-adventerprisek9-mz.122-33.SRB1.bin
boot-end-marker
!
class-map match-all r6-9-0158-2358
  match vlan  2358
class-map match-all r7-8-0187-2387
  match vlan  2387
class-map match-all r8-3-0212-2412
  match vlan  2412
class-map match-all r9-2-0241-2441
  match vlan  2441
!
... [and so on] ...
!
policy-map INGRESS
  class REAL_TIME
   set dscp cs5
  class CALL-SETUP
   set dscp cs5
  class STREAMING_VIDEO
   set dscp cs2
  class TRANSACTIONAL_DATA
   set dscp cs3
  class NETWORK_MANAGEMENT
   set dscp cs3
  class BULK_DATA
   set dscp af21
!
policy-map branch-noset
  class REAL_TIME
   police 3072000    conform-action transmit     exceed-action drop     violate-action
drop
    priority
  class GOLD
    shape average 460800
  class SILVER
    shape average 768000
  class class-default
    shape average 2480000
!
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 100
 name Outside
!
vlan 101,161,163,171,173,181,183,191,193,201,203,211,213
!
vlan 1100
 name r1-1-LAN
!
vlan 1101
 name r1-2-LAN
```

```
!
vlan 1102
 name r1-3-LAN
!
... [and so on] ...

!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set AES_SHA_TUNNEL esp-aes 256 esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto ipsec profile vpn-dmvpn
 set transform-set AES_SHA_TUNNEL
!
!
!
interface Tunnel0
 description Tunnel0
 bandwidth 100000
 ip address 10.56.0.1 255.255.248.0
 no ip redirects
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 105600
 ip nhrp holdtime 1800
 ip nhrp registration timeout 120
 load-interval 30
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel protection ipsec profile vpn-dmvpn
 crypto engine slot 2/0 inside
!
!
interface GigabitEthernet4/0/0
 description GigabitEthernet4/0/0 Outside Interface
 no ip address
 load-interval 30
 mls qos trust dscp
!
interface GigabitEthernet4/0/0.2200
 description r1-1
 encapsulation dot1Q 2200
 ip address 192.168.0.1 255.255.255.252
 crypto engine slot 2/0 outside
 service-policy output branch-noset
!
interface GigabitEthernet4/0/0.2201
 description r1-2
 encapsulation dot1Q 2201
 ip address 192.168.1.1 255.255.255.252
 crypto engine slot 2/0 outside
 service-policy output branch-noset
!
... [and so on] ...
!
interface GigabitEthernet5/1
 description GigabitEthernet5/1-Inside
```

```
 ip address 10.204.0.1 255.252.0.0
 no ip redirects
 load-interval 30
 mls qos trust dscp
 service-policy input INGRESS
!

end
```

Branch Configuration—Two VLANs (Per-Class Shaper)

The following sample configuration is for a Cisco 3845 using a 25 Mbps aggregate rate on each of two VLANs, supporting two DMVPN tunnels.

```
version 12.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service compress-config
!
hostname he1-3800-2
!
boot-start-marker
boot-end-marker
!
logging snmp-authfail
logging buffered 65535 debugging
!
spd headroom 4000
no aaa new-model
!
resource policy
!
clock timezone EST -5
clock summer-time EDT recurring
clock calendar-valid
!
!
ip cef
ip tcp path-mtu-discovery
!
!
class-map match-any GOLD
 match ip dscp cs3
 match ip dscp cs6
class-map match-any TRANSACTIONAL_DATA
 match ip dscp af21
class-map match-any NETWORK_MANAGEMENT
 match ip dscp cs2
class-map match-any SILVER
 match ip dscp cs2
class-map match-any REAL_TIME
 match ip dscp cs5
 match ip dscp ef
 match ip dscp af41
class-map match-any STREAMING_VIDEO
 match ip dscp cs4
class-map match-any BEST_EFFORT
 match ip dscp default
 match ip dscp cs1
class-map match-any BULK_DATA
```

```
 match ip dscp af11
class-map match-any CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
!
!
policy-map PER_CLASS_25mb
 class REAL_TIME
   police 8960000 conform-action transmit  exceed-action transmit  violate-action transmit
  set cos 5
 class GOLD
  shape average 3840000
  set cos 3
 class SILVER
  shape average 6400000
  set cos 2
 class class-default
  shape average 6400000
  set cos 0
!
policy-map INGRESS
 class REAL_TIME
  set ip dscp cs5
 class CALL-SETUP
  set ip dscp cs5
 class STREAMING_VIDEO
  set ip dscp cs2
 class TRANSACTIONAL_DATA
  set ip dscp cs3
 class NETWORK_MANAGEMENT
  set ip dscp cs3
 class BULK_DATA
  set ip dscp af21
!
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key bigsecret address 192.168.31.254
crypto isakmp key bigsecret address 192.168.31.253
crypto isakmp key bigsecret address 192.168.31.252
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set AES_SHA_TUNNEL esp-aes 256 esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto ipsec profile vpn-dmvpn
 set transform-set AES_SHA_TUNNEL
!
!
buffers small permanent 1500
buffers small max-free 2000
buffers small min-free 450
buffers middle permanent 1000
buffers middle max-free 1500
buffers middle min-free 300
buffers big permanent 1000
buffers big max-free 1500
buffers big min-free 300
!
!
```

```
!
!
interface Tunnel0
 description Tunnel0
 bandwidth 10240
 ip address 10.56.1.0 255.255.252.0
 ip hold-time eigrp 1 35
 ip nhrp authentication test
 ip nhrp map 10.56.0.1 192.168.31.253
 ip nhrp map multicast 192.168.31.253
 ip nhrp network-id 105600
 ip nhrp holdtime 600
 ip nhrp nhs 10.56.0.1
 ip nhrp cache non-authoritative
 ip route-cache flow
 ip summary-address eigrp 1 10.192.0.0 255.255.255.0 5
 load-interval 30
 tunnel source 192.168.0.2
 tunnel destination 192.168.31.253
 tunnel protection ipsec profile vpn-dmvpn
!
interface Tunnel1
 description Tunnel1
 bandwidth 10240
 ip address 10.56.5.0 255.255.252.0
 ip hold-time eigrp 1 35
 ip nhrp authentication test
 ip nhrp map 10.56.4.1 192.168.31.254
 ip nhrp map multicast 192.168.31.254
 ip nhrp network-id 105640
 ip nhrp holdtime 600
 ip nhrp nhs 10.56.4.1
 ip nhrp cache non-authoritative
 ip route-cache flow
 ip summary-address eigrp 1 10.192.0.0 255.255.255.0 5
 load-interval 30
 tunnel source 192.168.0.146
 tunnel destination 192.168.31.254
 tunnel key 105640
 tunnel protection ipsec profile vpn-dmvpn
!
interface GigabitEthernet0/0
 description GigabitEthernet0/0
 no ip address
 ip mtu 1400
 load-interval 30
 duplex auto
 speed 100
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/0.2200
 description Primary WAN
 encapsulation dot1Q 2200
 ip address 192.168.0.2 255.255.255.252
 service-policy output PER_CLASS_25mb
!
interface GigabitEthernet0/0.3300
 description Secondary WAN
 encapsulation dot1Q 3300
 ip address 192.168.0.146 255.255.255.252
 service-policy output PER_CLASS_25mb
!
interface GigabitEthernet0/1
```

```
 description GigabitEthernet0/1
 ip address 10.192.0.129 255.255.255.192 secondary
 ip address 10.192.0.1 255.255.255.128
 load-interval 30
 duplex full
 speed 100
 media-type rj45
 no keepalive
 service-policy input INGRESS
!
!
router eigrp 1
 passive-interface GigabitEthernet0/1
 network 10.0.0.0
 no auto-summary
!
ip route 172.26.0.0 255.255.0.0 172.26.180.1
ip route 192.168.0.0 255.255.0.0 192.168.0.1
ip route 192.168.0.0 255.255.0.0 192.168.0.145
ip route 192.168.31.252 255.255.255.255 192.168.0.1
ip route 192.168.31.253 255.255.255.255 192.168.0.1
ip route 192.168.31.254 255.255.255.255 192.168.0.145
!
control-plane
!
call admission limit 70
!
!
end
```

Dual-Tier—3750 Metro Ethernet Configuration

The following sample configuration is for the performance test results in QoS Devices for Dual-Tier Models, page 43.

```
!
!
hostname he1-3750-1
!
! System image file is
"flash:c3750me-i5-mz.122-25.SEG1/c3750me-i5-mz.122-25.SEG1.bin"
!
class-map match-all r1-1-0000-2200
  match vlan  2200
class-map match-all r2-2-0031-2231
  match vlan  2231
class-map match-all r5-5-0124-2324
  match vlan  2324
! ...and so on ...
!
! Note: class-map configurations same as other tests
!
policy-map branch-traffic
  class REAL_TIME
   set cos 5
    priority
  class GOLD
    bandwidth percent 15
   set cos 3
  class SILVER
    bandwidth percent 25
   set cos 2
```

```
  class class-default
    bandwidth percent 5
   set cos 0
!
policy-map hqos-policy
  class r1-1-0000-2200
   shape average 1280000
   service-policy branch-traffic
  class r1-2-0001-2201
   shape average 1280000
   service-policy branch-traffic
  class r1-3-0002-2202
   shape average 1280000
   service-policy branch-traffic
  class r1-4-0003-2203
   shape average 1280000
   service-policy branch-traffic
! ..... and so on ...
!
interface GigabitEthernet1/1/2
 switchport mode trunk
 service-policy output hqos-policy
 load-interval 30
 mls qos trust dscp
!
end
```

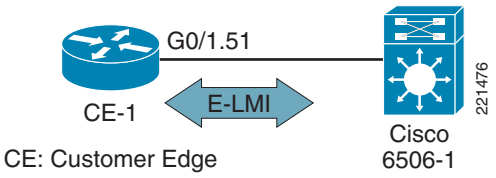
Troubleshooting

This section includes various examples and notes on useful troubleshooting tools and methods.

Ethernet LMI

The example in this section demonstrates the concept of Ethernet LMI. Figure 20 shows the test case.

Figure 20 Ethernet LMI



The following is the output from a **show interface** command from a E-LMI active interface before a link failure:

```
CE-1#show int g0/1.51
GigabitEthernet0/1.51 is up, line protocol is up
  Hardware is MV96340 Ethernet, address is 0017.94e8.1af1 (bia 0017.94e8.1af1)
  Internet address is 20.20.20.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  EVC Id: EVC51
  E-LMI EVC Status: Active
  Encapsulation 802.1Q Virtual LAN, Vlan ID  51.
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interface" counters never
```

A cable break is simulated between the CE-1 and 6506-1 devices:

```
6506-1#
*Apr 12 15:36:02 %ETHER_SERVICE-6-EVC_STATUS_CHANGED: status of EVC51 changed to InActive

CE-1#show int g0/1.51
GigabitEthernet0/1.51 is down, line protocol is down
  Hardware is MV96340 Ethernet, address is 0017.94e8.1af1 (bia 0017.94e8.1af1)
  Internet address is 20.20.20.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  EVC Id: EVC51
  E-LMI EVC Status: Inactive
  Encapsulation 802.1Q Virtual LAN, Vlan ID  51.
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interface" counters never
```

SNMP Traps

When encryption is enabled on WAN links, regardless of the type of WAN, configuring the appropriate SNMP traps and processing them on the enterprise NMS station is a useful tool to help in fault determination and isolation. EIGRP traps can also be enabled. Analysis of the frequency and duration of failures can help determine whether remedial action must be taken on either the enterprise owned and managed equipment, or trouble reports must be sent to the service provider to address issues proactively.

The following list of traps is recommended:

```
!
! System image file is "flash:c2600-advipservicesk9-mz.124-9.T2"
!
! By enabling in configuration mode
!
snmp-server enable traps
!
!
! All SNMP traps suppored are enabled.
!
!
snmp-server enable traps eigrp
!
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
!
end
```

Crypto Logging Session

In addition to enabling crypto-related SNMP traps, enabling crypto logging provides a useful audit trail in the syslog subsystem.

```
!
crypto logging session
!
end
```

Appendix

Reference Material

- Ethernet service provision requires the right demarcation— http://lw.pennnet.com/Articles/Article_Display.cfm?Section=ARTCL&ARTICLE_ID=229356&VERSION_NUM=3&p=13
- The long-term architecture for OPT-E-MAN uses Multiprotocol Label Switching/Hierarchical Virtual Private LAN Service (MPLS/H-VPLS)— http://www.att.com/gen/network-disclosure?pid=1803
- Ethernet Services Stage 2— http://www.lightreading.com/document.asp?doc_id=88144&print=true
- Cisco Shared Port Adapters/SPA Interface Processors Introduction— http://www.cisco.com/en/US/products/ps6267/prod_module_series_home.html
- Cisco 7600 Series/Catalyst 6500 Series IPsec VPN Shared Port Adapter (IPsec VPN Services SPA)— http://www.cisco.com/en/US/products/ps6267/products_data_sheet0900aecd8027cbb2.html
- Cisco 7600 Series SPA Interface Processor-400 (Cisco 7600 SIP-400)— http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet0900aecd8027c9e6.html
- Cisco 7600 Series/ Catalyst 6500 Series SPA Interface Processor 600 (Cisco 7600 SIP-600)— http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheet0900aecd8033998f.html
- Overview of Ethernet Operations, Administration, and Management (E-OAM)— http://www.cisco.com/en/US/products/hw/routers/ps368/products_white_paper0900aecd804a0266.shtml
- Metro Ethernet Forum (MEF)—
  - http://www.metroethernetforum.org
  - http://www.metroethernetforum.org/presentations/Supercomm2003UNI.ppt
- Verizon— http://www22.verizon.com/wholesale/solutions/solution/Transparent+LAN+Service+.html