Lawful Interception of Telecom Networks

You can track any phone number from any country and anywhere in the world.

TACS

www.tacs.eu

Lawful interception (LI)

- LI is obtaining communications network data pursuant to lawful authority for the purpose of analysis or evidence. Such data generally consist of signalling or network management information or, in fewer instances, the content of the communications.
- The operator of public/private network infrastructure can undertake LI activities for infrastructure protection and cybersecurity.
- One of the important bases for LI is the interception of telecommunications by law enforcement agencies (LEAs), regulatory or administrative agencies, and intelligence services, in accordance with local law.

LAWFUL INTERCEPTION FOR IP NETWORKS

TACS

www.tacs.eu

Simplified view of lawful interception architecture

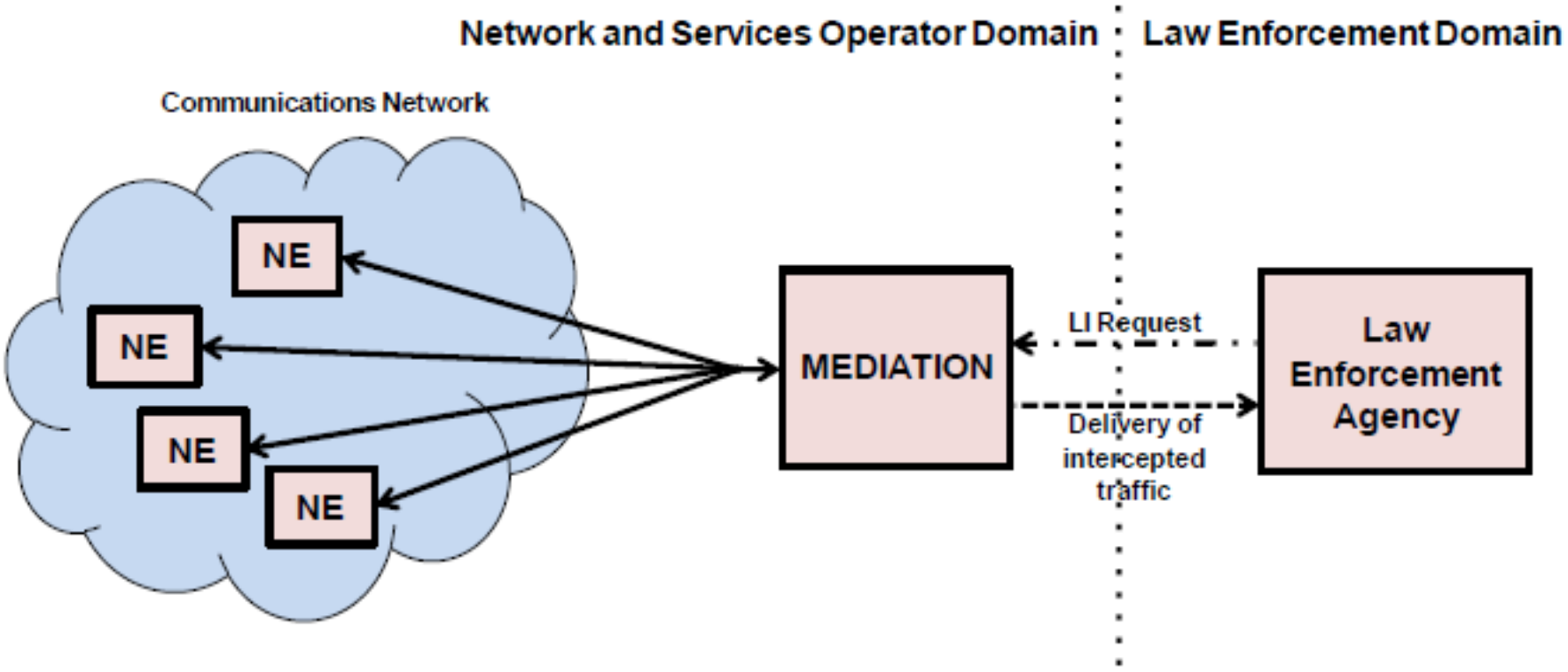
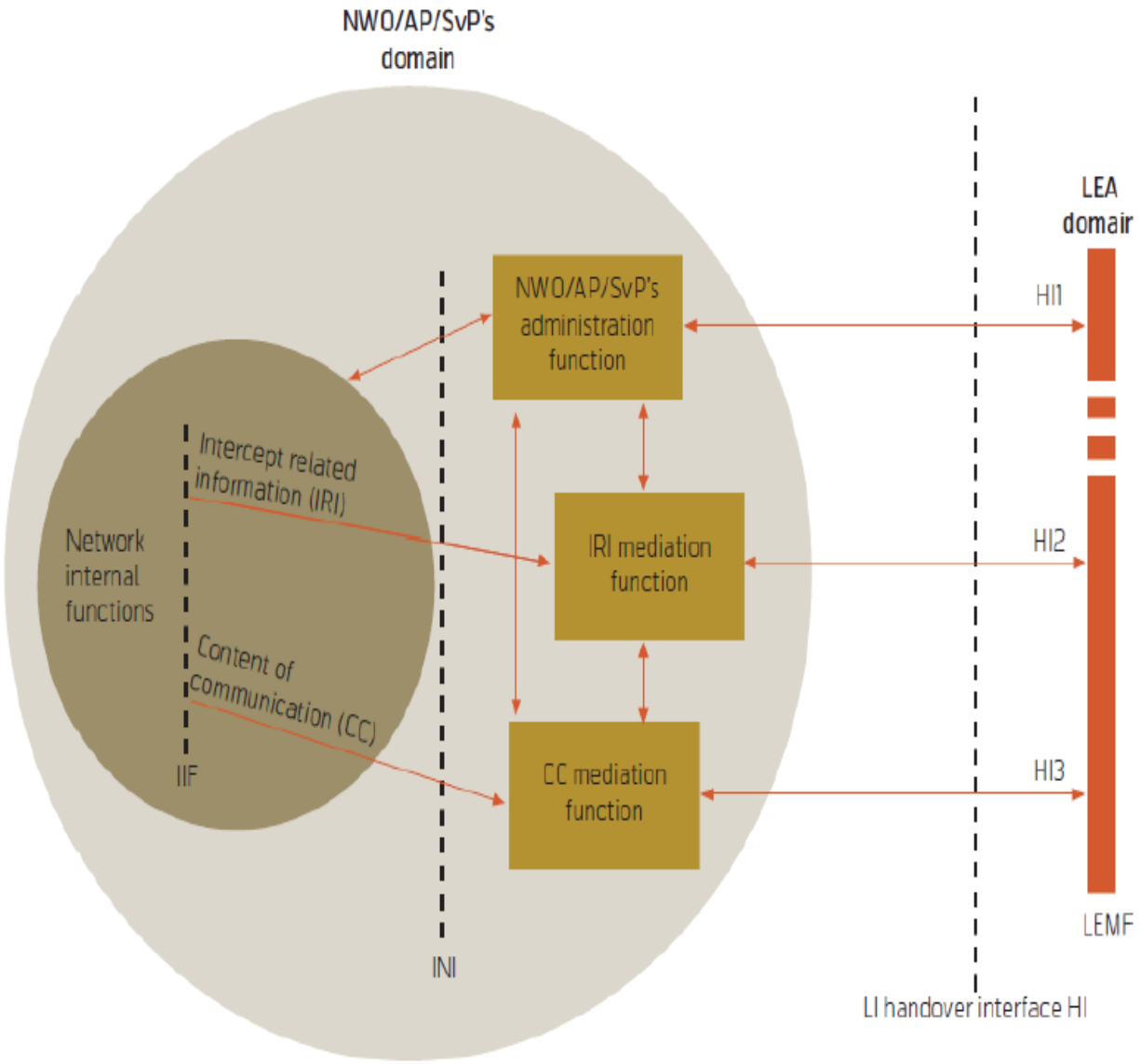


Figure 2-1. Simplified view of lawful interception architecture. Of primary interest is the use of a Mediation Platform to convey intercepted data from the network to the LEA.

General architecture for lawful interception-ETSI



ETSI has been a major driver behind the specification of hand-over interfaces and of the flow that intercepted data should follow. It specifies a general architecture for lawful inter-ception that allows systematic and extensible communication between network operators and LEAs over defined interfaces and in compliance with national legislation.

This general architecture applies to any kind of circuit- or packet-switched voice and data net-work.

ETSI-developed architecture for lawful interception

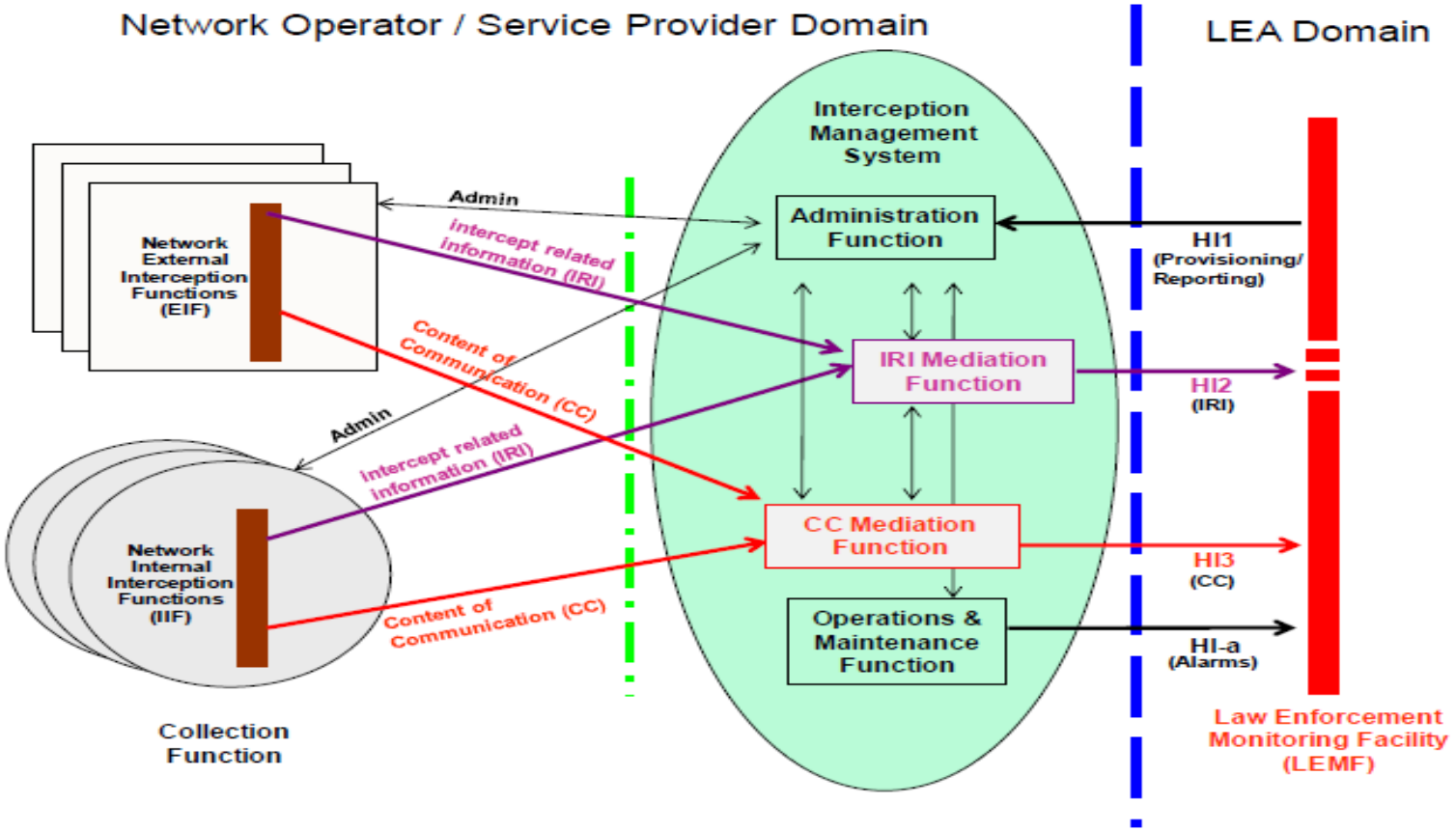


Figure 2-2. ETSI-developed architecture for lawful interception. Note the separation of lawful interception management functions (HI1), call-related data (HI2), and call content (HI3) in the interaction between the LEA and communication service provider (based on [1]; also see [2]). Call Data Channel and Call Content Channel are terminology used in the J-STD-025 A and B standards [3], and correspond to IRI and CC in this figure.

OSI 7-Layer model for packet-based communications & Typical devices that support each layer

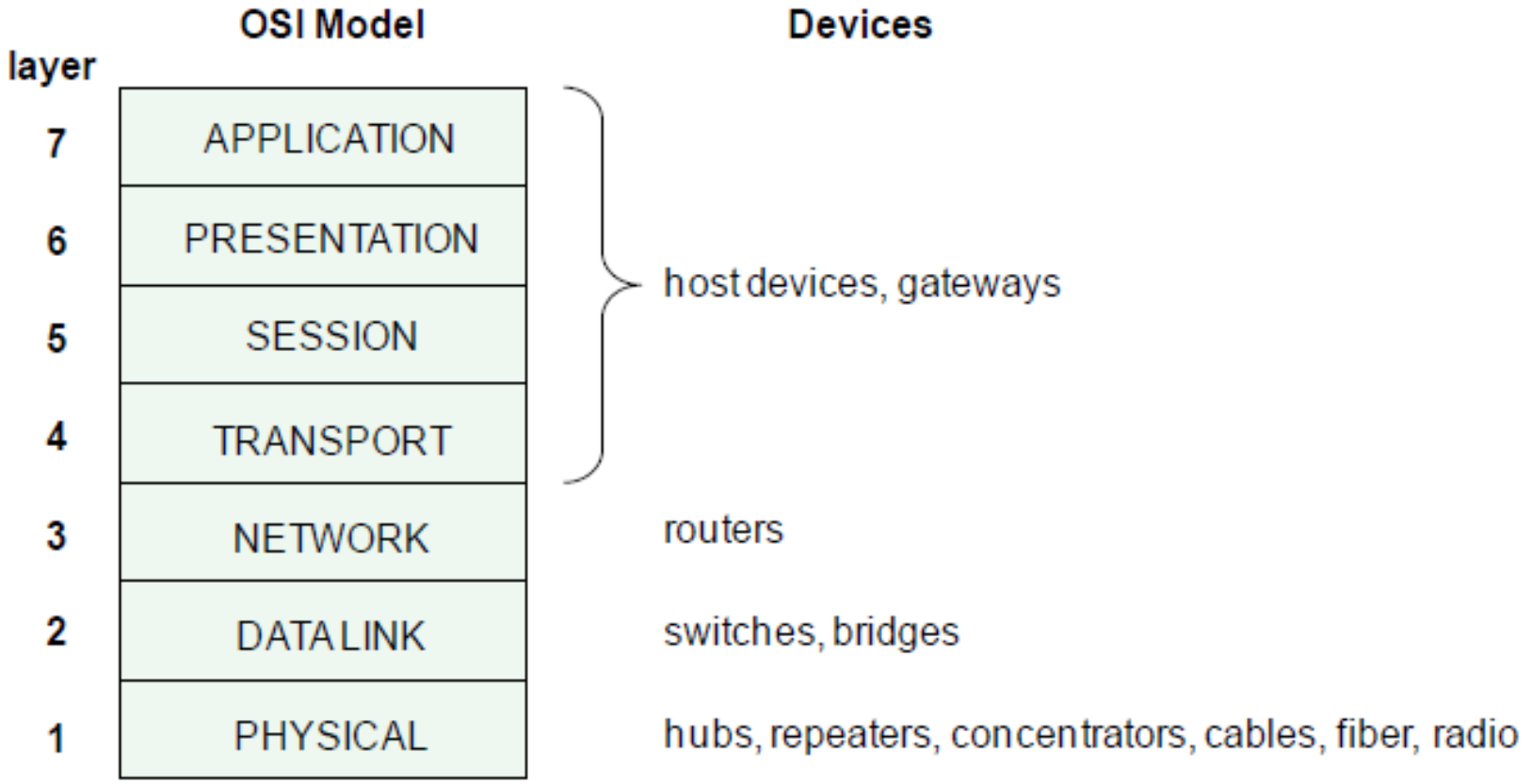


Figure 3-1. OSI 7-Layer model for packet-based communications. Typical devices that support each layer are indicated on the right.

Reduction of 7-Layer OSI model into 4-layer TCP/IP Model

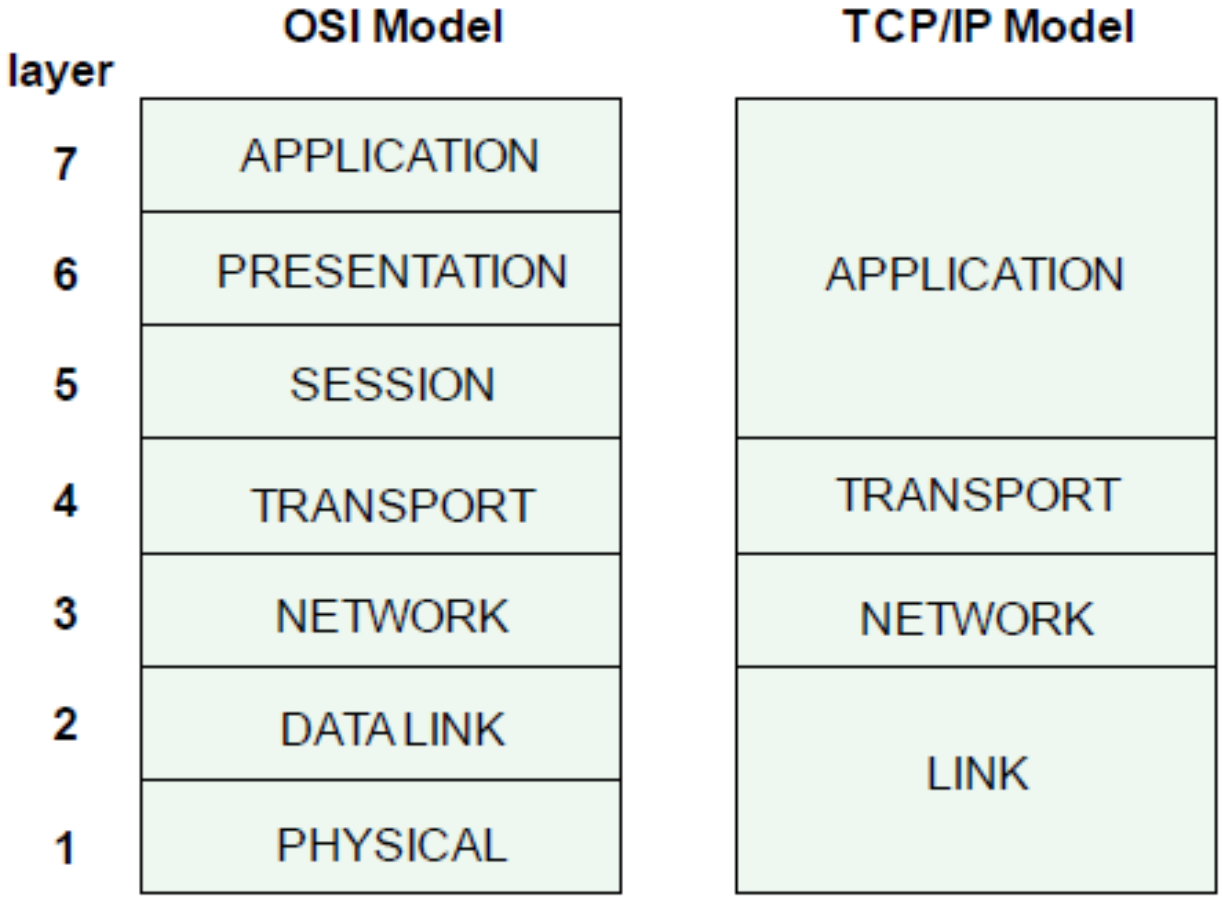


Figure 3-2. Reduction of 7-Layer OSI model into 4-layer TCP/IP Model.

Relationship of OSI layers with Lawful Interception information and data extraction

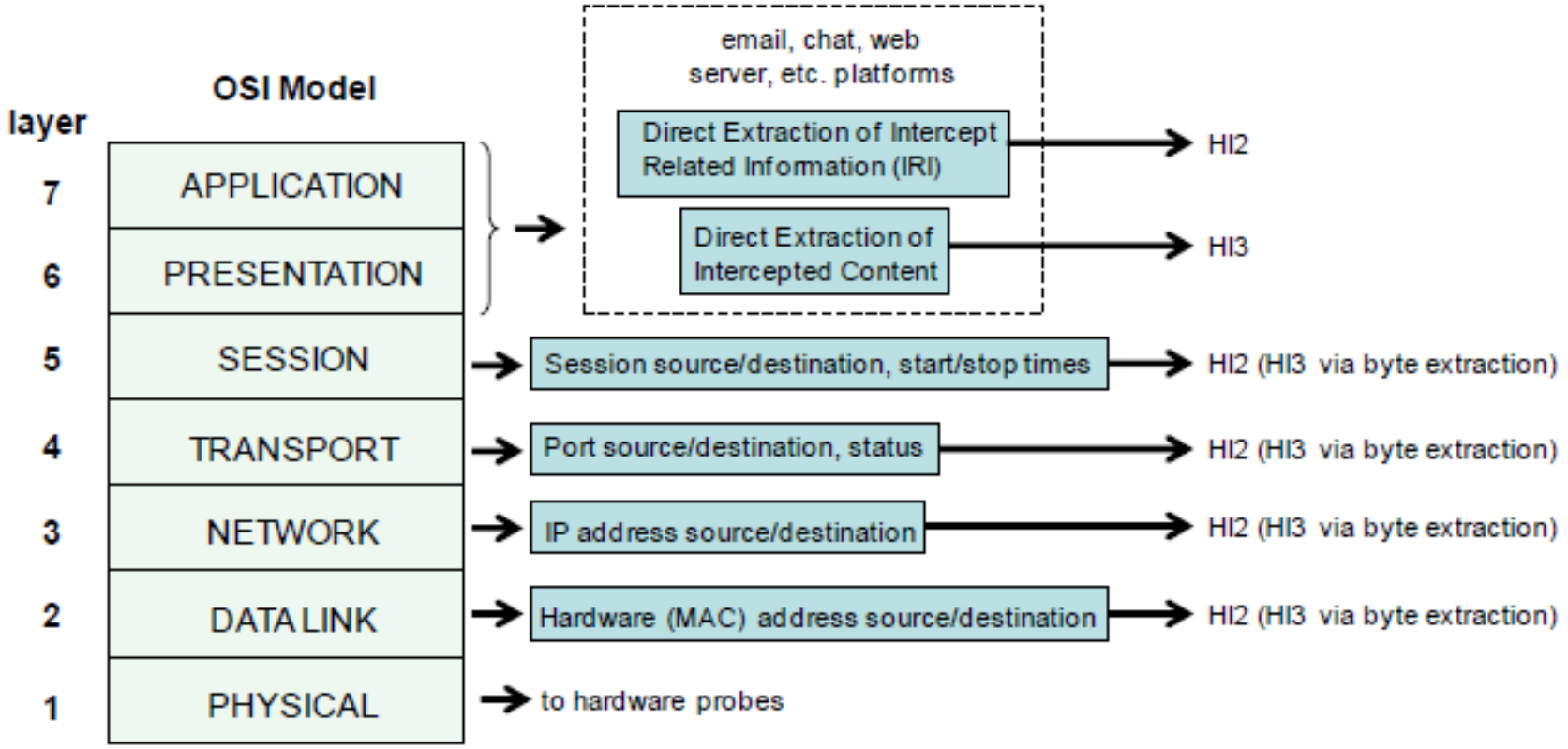


Figure 3-3. Relationship of OSI layers with Lawful Interception information and data extraction. In practice for interception, Layer 6 is combined with Layer 7. Layer 3 (IP) serves as the basis of intercepted communications in lieu of Layer 4. Layers 2 and 1 can yield useful results when network elements are available.

Separation of network access, core network, and service provider functions

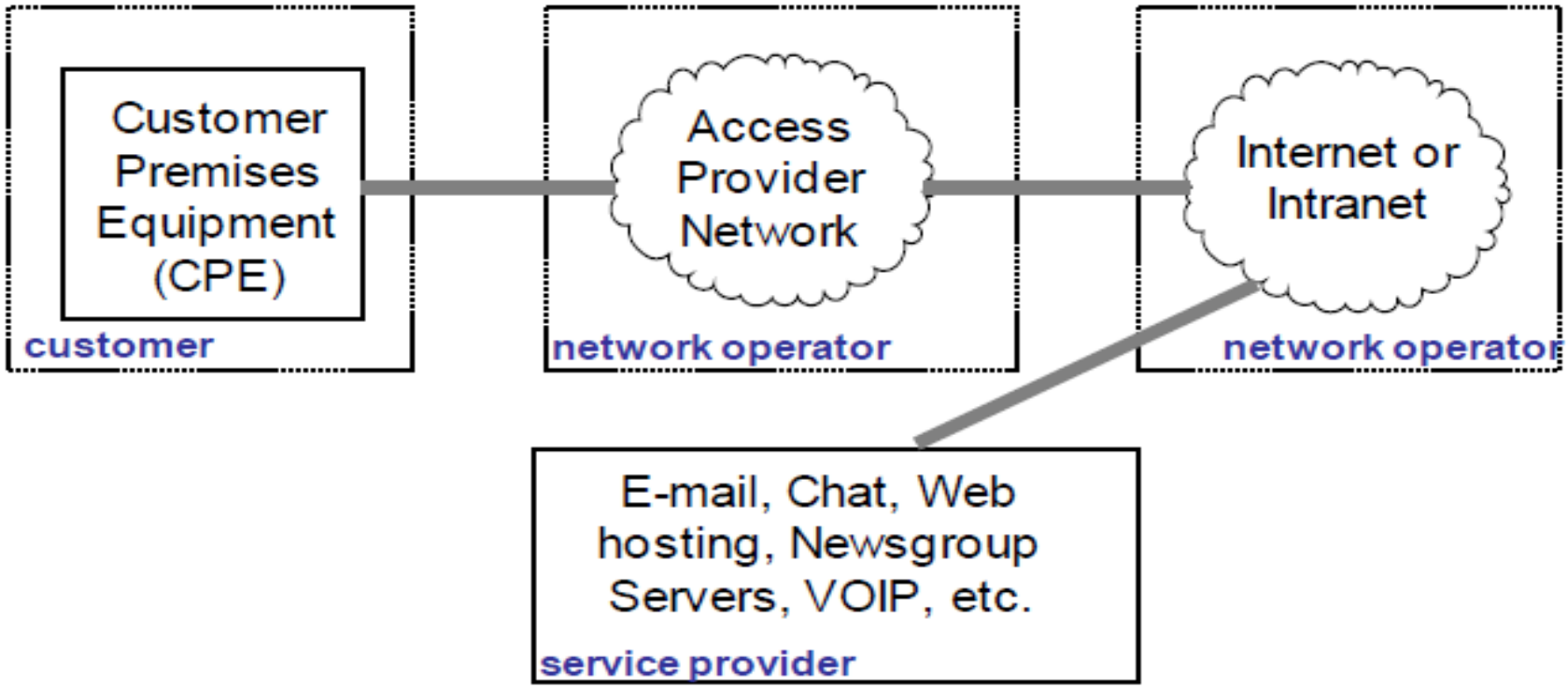
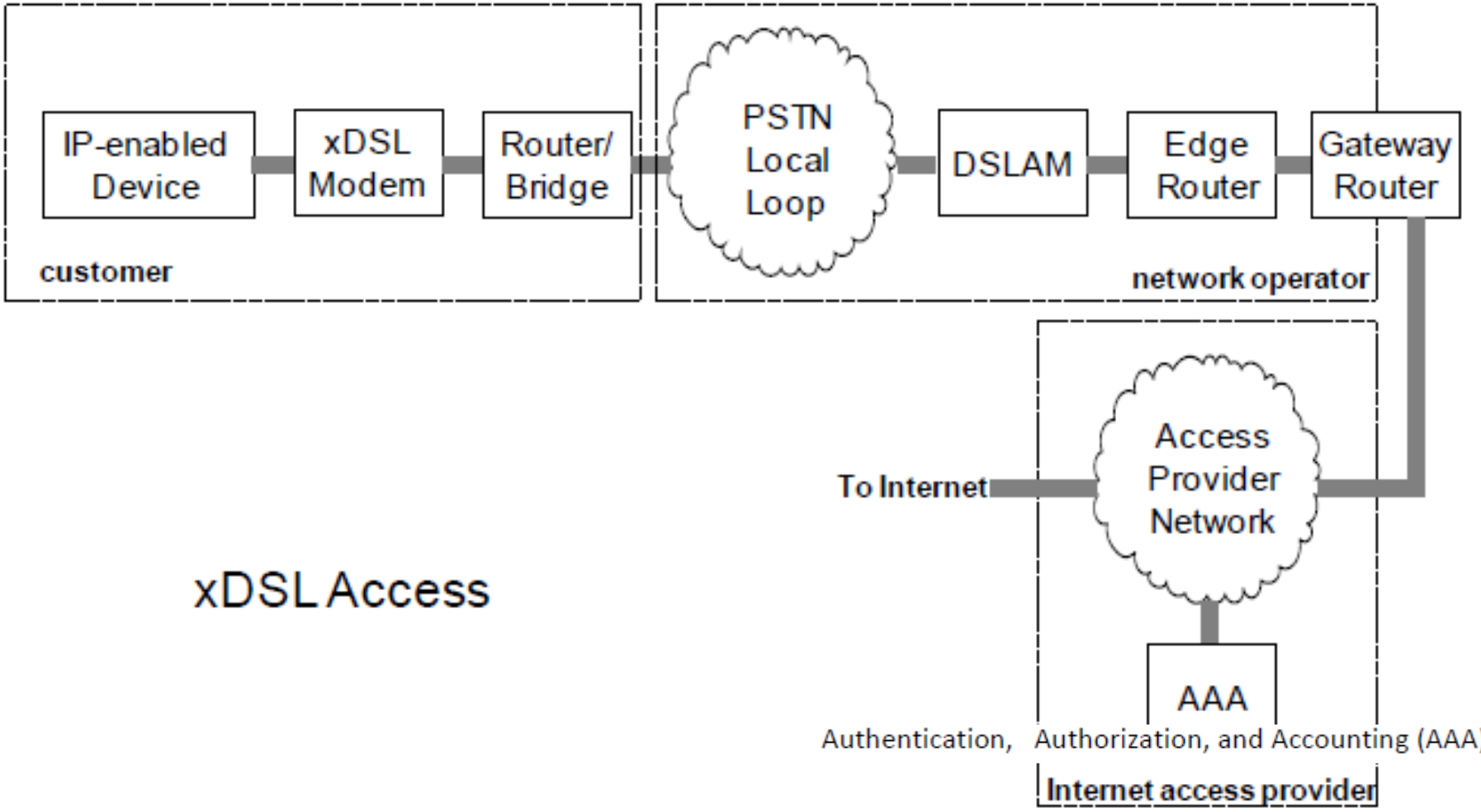


Figure 4-1. Separation of network access, core network, and service provider functions. The Network Operator can be an incumbent telecom operator (e.g., supplying DSL services over existing local loop copper), cable TV operator, etc. The core Internet or managed Intranet is operated by a Network Operator that may or may not also provide network access. (Based on [7].)

IP Interception Examples

Typical access configurations for xDSL, dial-up, cable modem, and Wi-Fi



xDSL Access

Typical access configurations for xDSL, dial-up, cable modem, and Wi-Fi

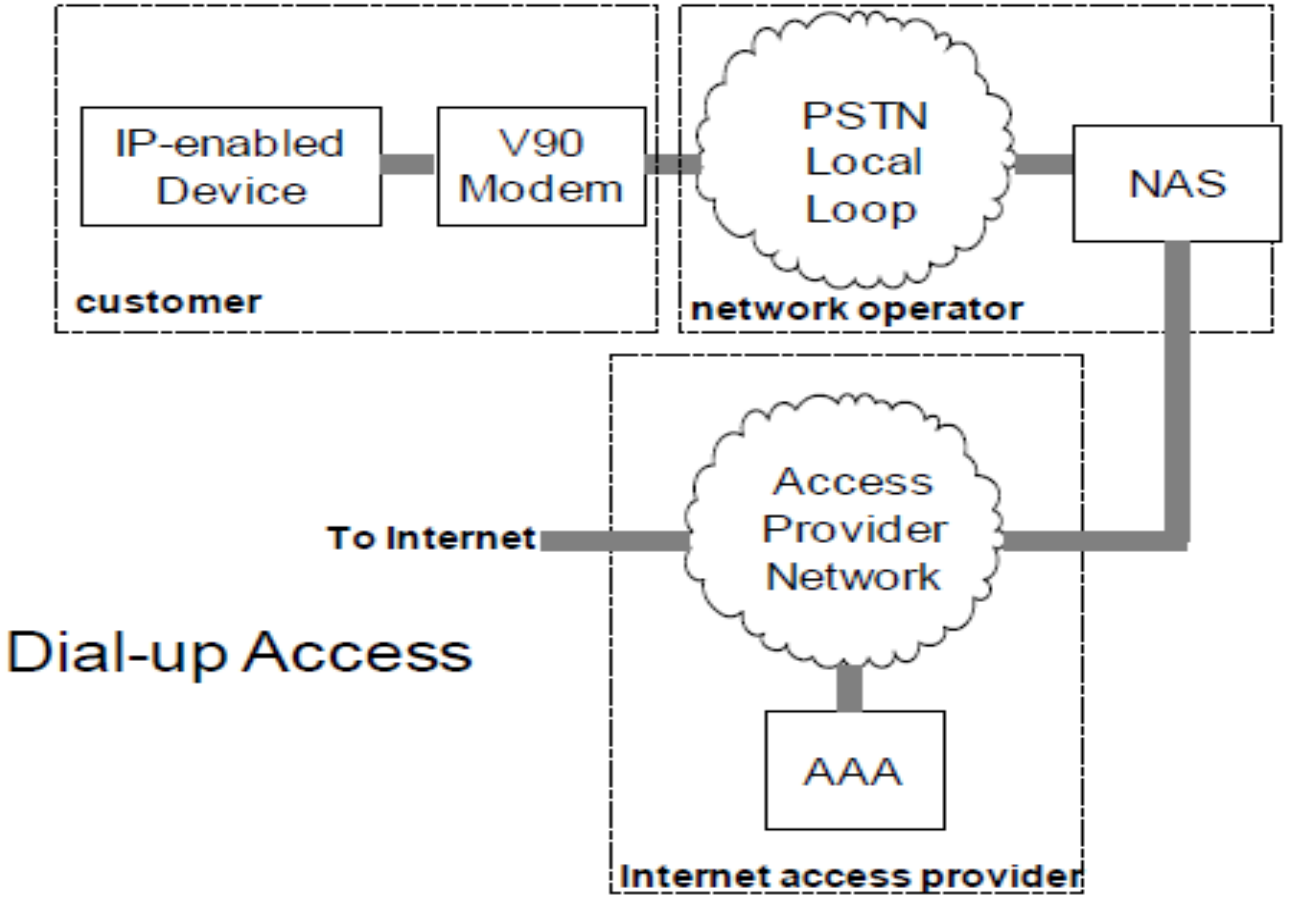
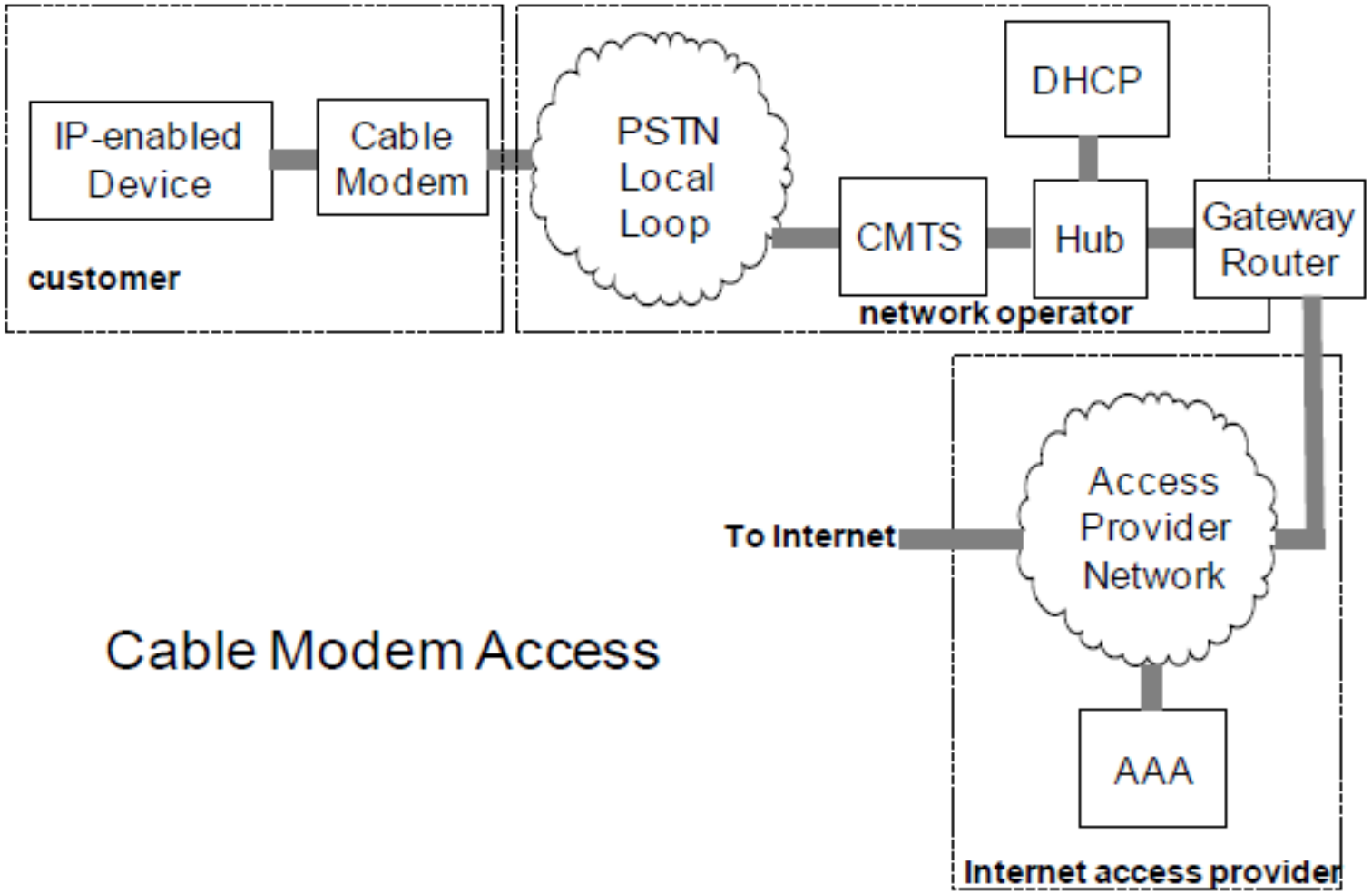


Figure 5-1 (carried to next page). Typical configurations for xDSL, Dial-up, and Cable Modem, Wi-Fi Internet access (derived from [7]).

Typical access configurations for xDSL, dial-up, cable modem, and Wi-Fi



Cable Modem Access

Typical access configurations for xDSL, dial-up, cable modem, and Wi-Fi

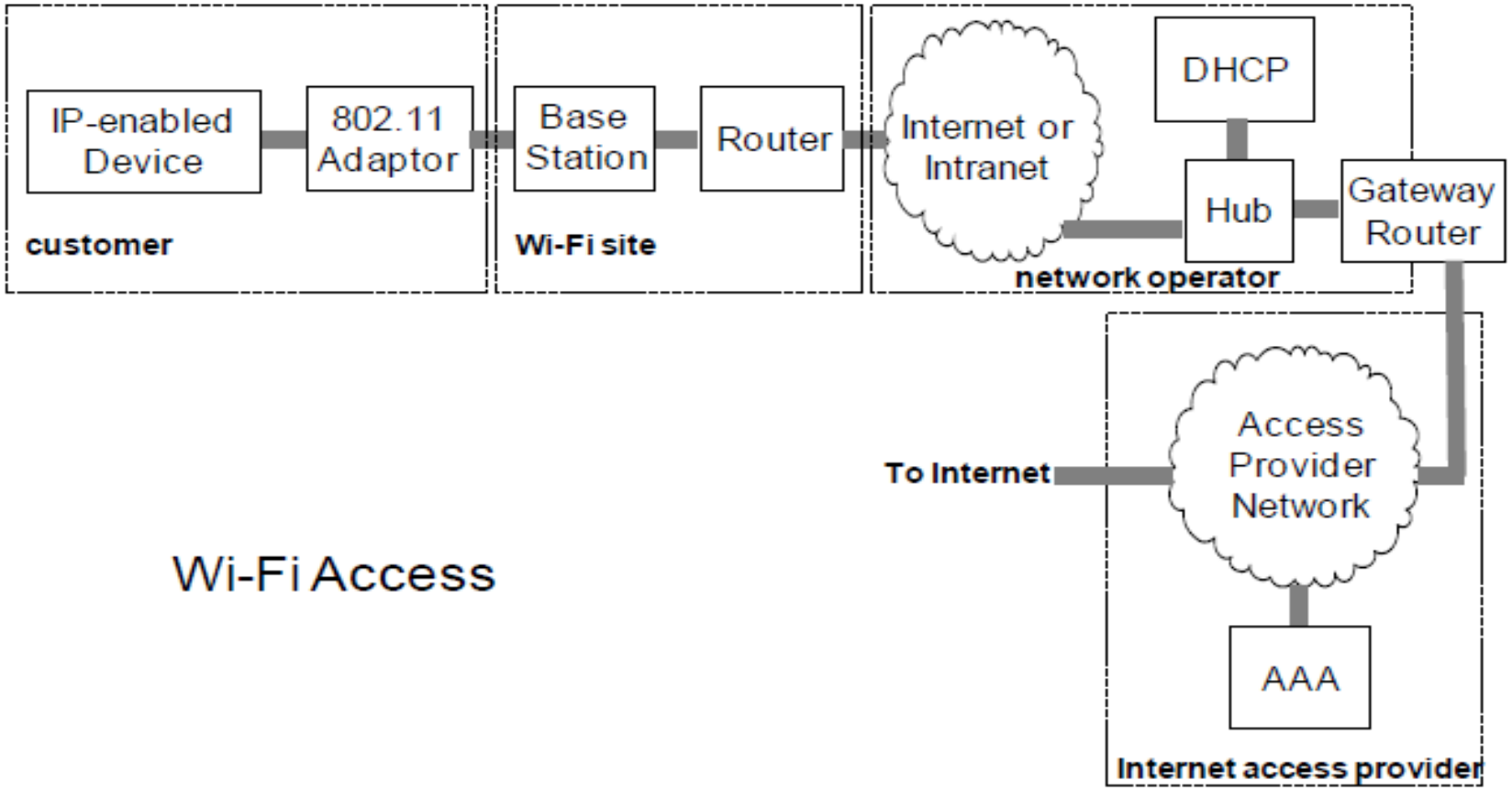
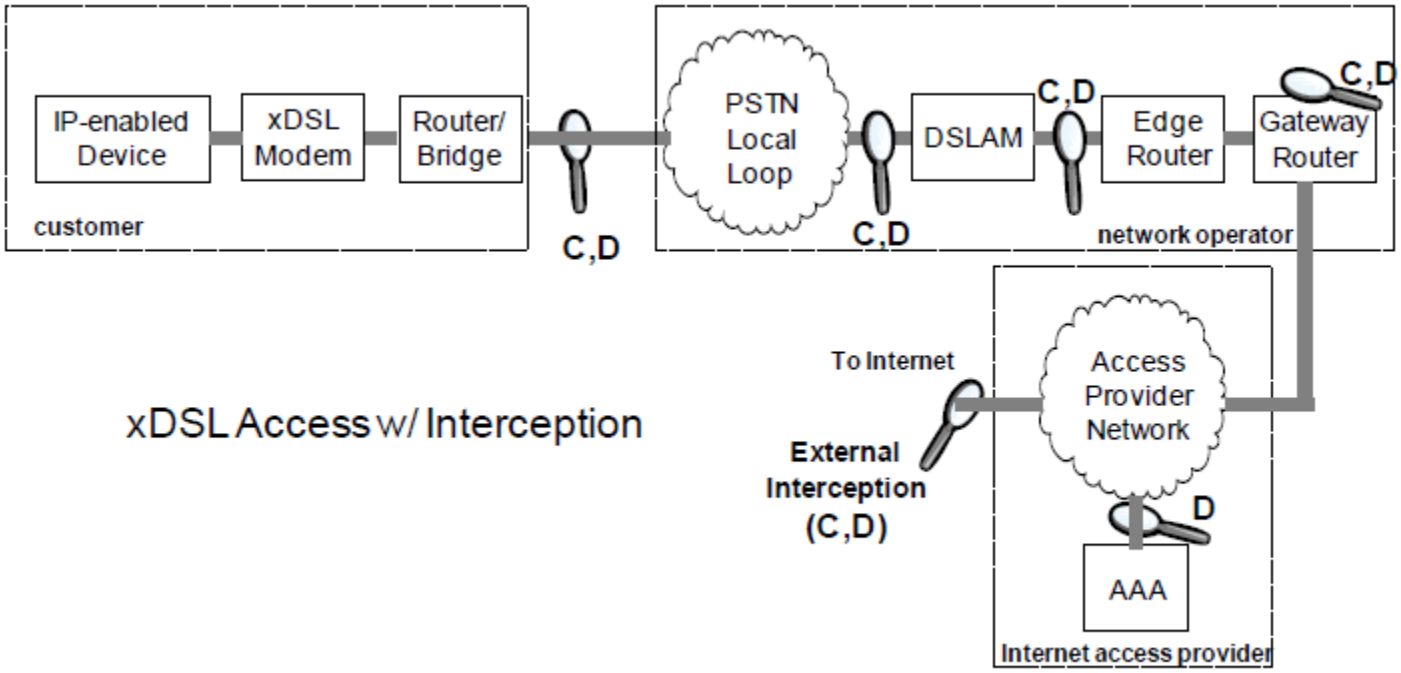


Figure 5-1 (continued). Typical configurations for xDSL, Dial-up, and Cable Modem, Wi-Fi Internet access (derived from [7]).

Typical access configurations for xDSL, dial-up, cable modem, and Wi-Fi



xDSL Access w/ Interception

Typical access configurations for xDSL, dial-up, cable modem, and Wi-Fi

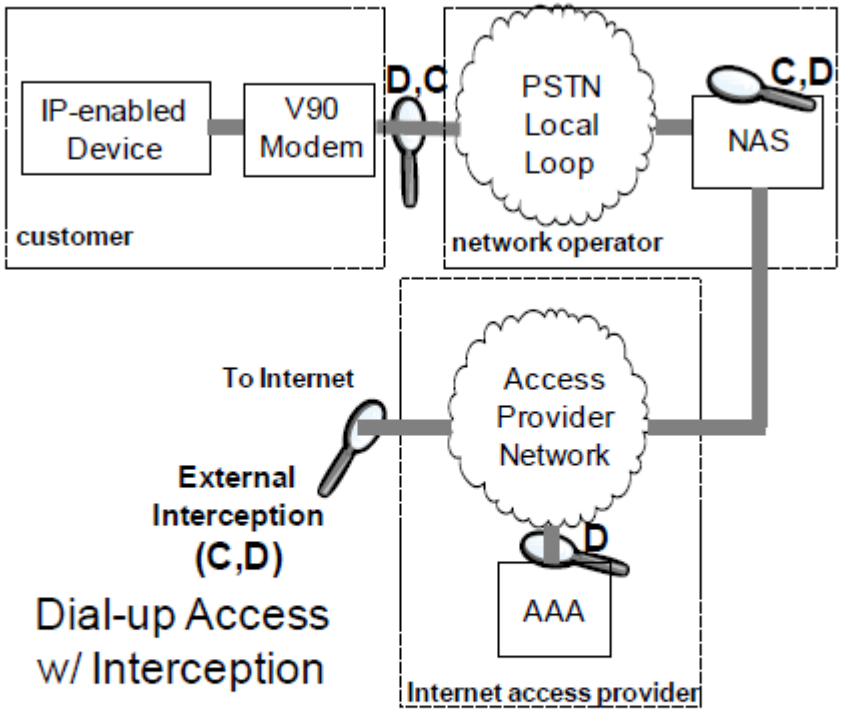
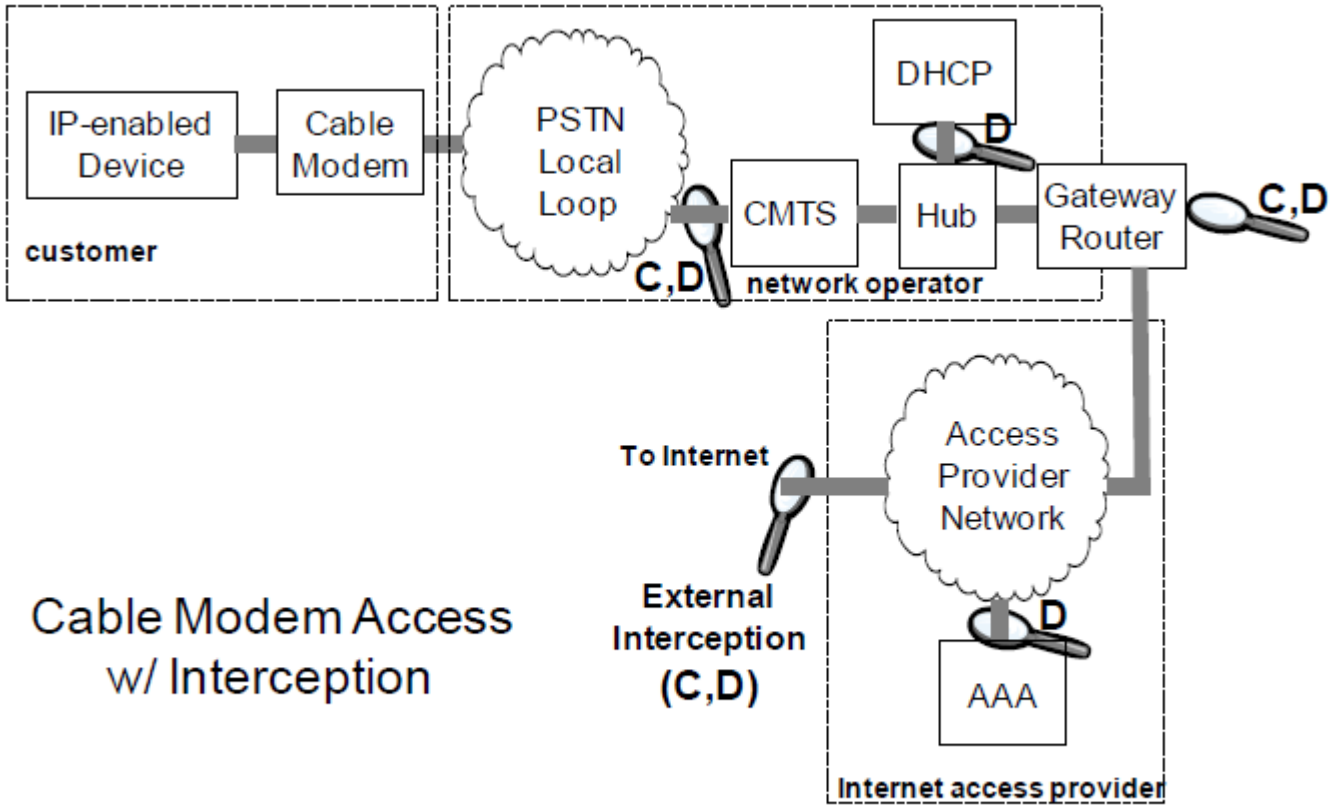


Figure 5-2. Internet access interception points. **C** and **D** denote intercepted content and session-related data, respectively.

Typical access configurations for xDSL, dial-up, cable modem, and Wi-Fi



Cable Modem Access
w/ Interception

Interception of E-mail: The process of sending an E-mail message via SMTP

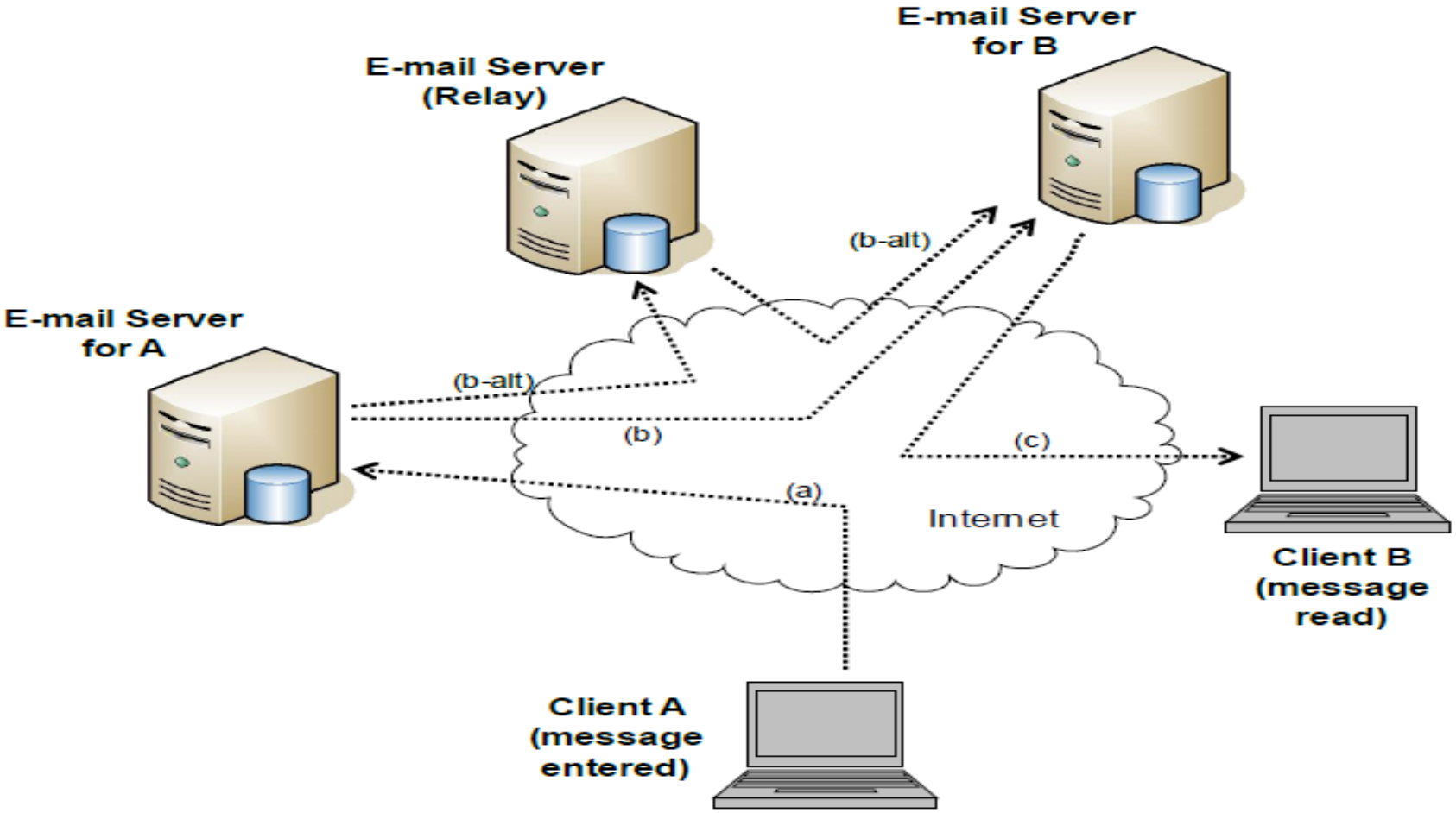


Figure 5-3. The process of sending an E-mail message via SMTP (and similar other) protocol. See text for details of each step.

Interception of E-mail

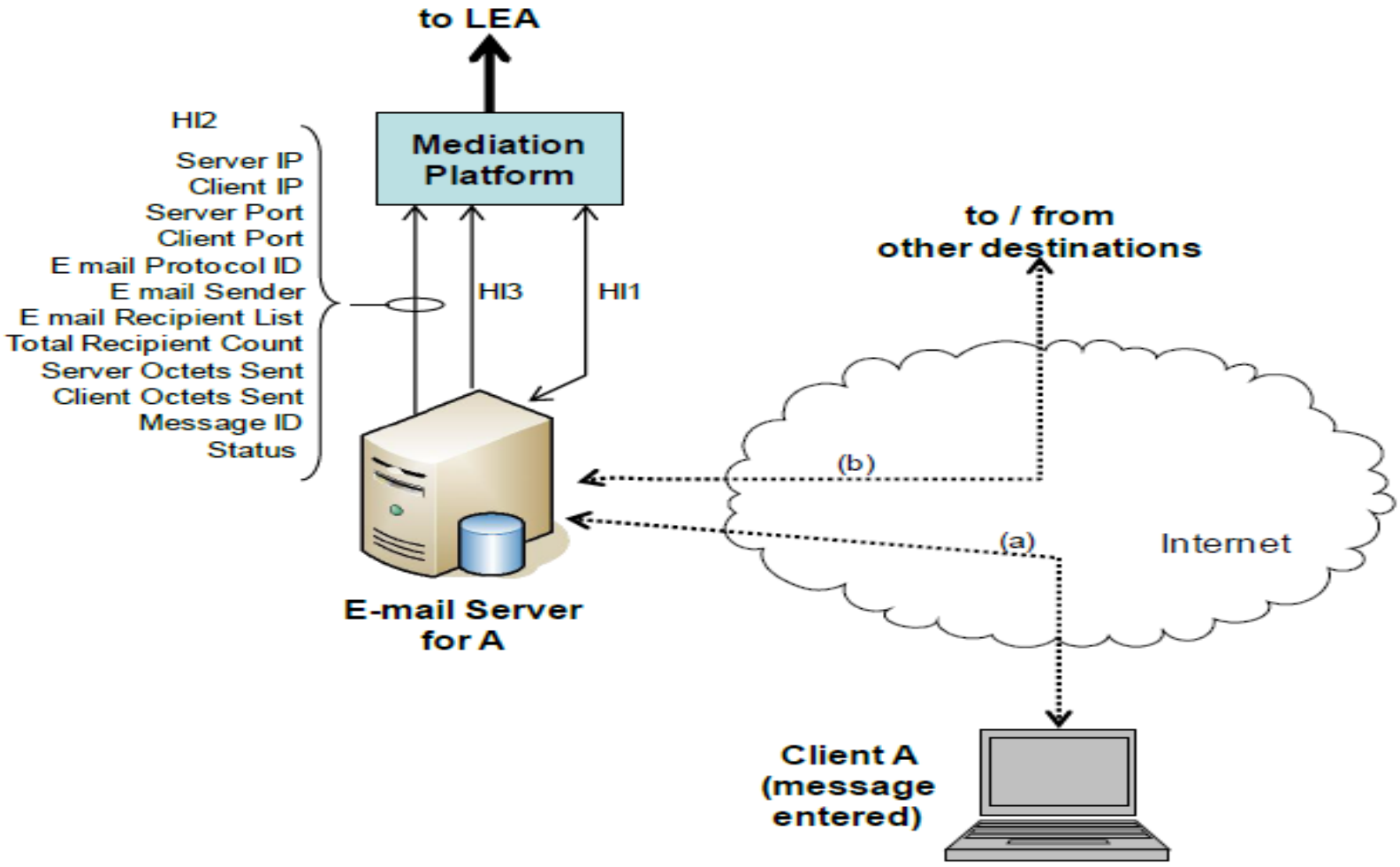


Figure 5-4. Interception of E-mail. Here an Internal or External Interception Function is illustrated since all action is at the level of the E-mail server operating on behalf of target A.

Voice-over-IP (VoIP): VoIP Interception

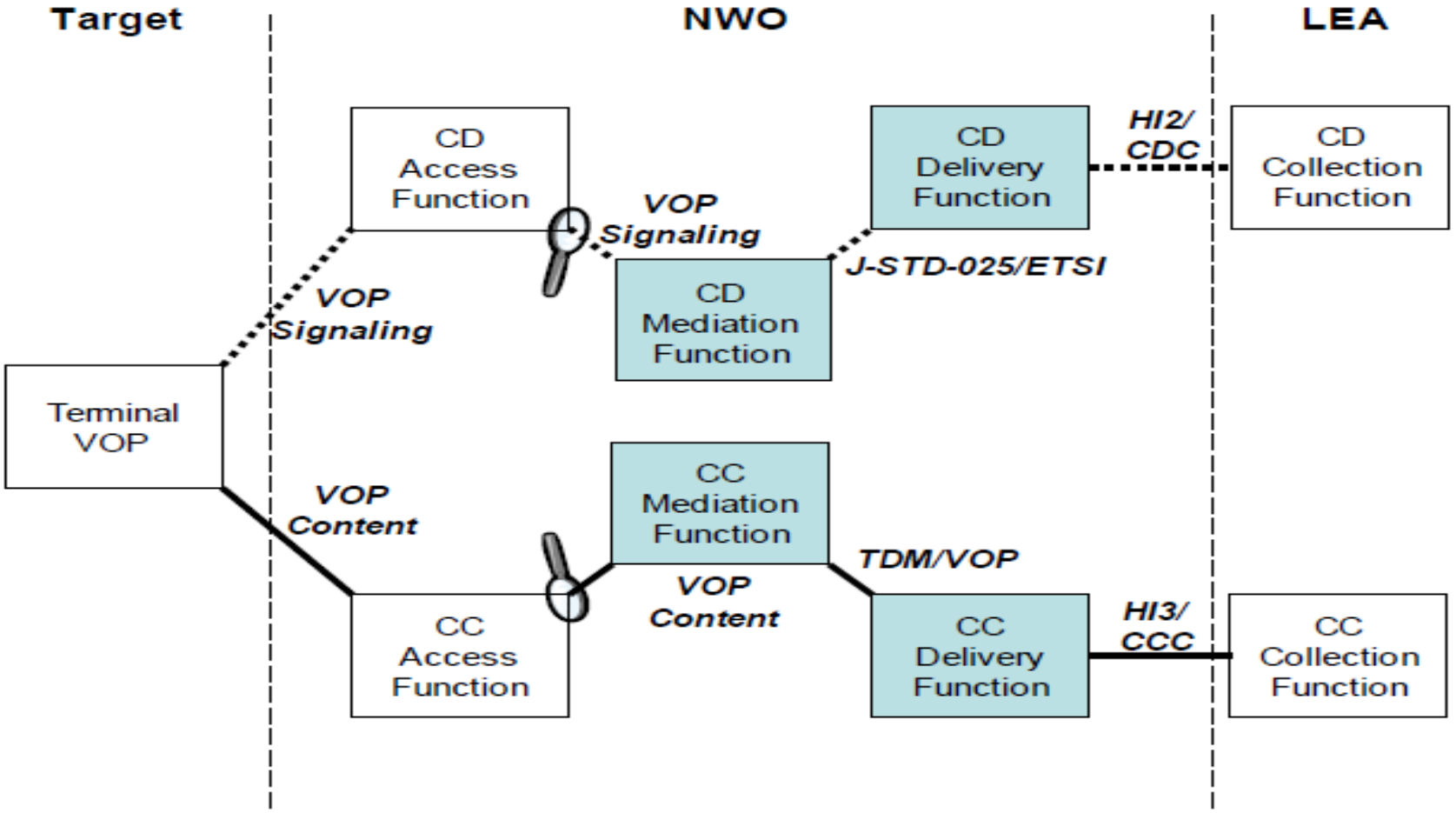


Figure 5-5. Conceptual view of interception for packet networks. Note each box can comprise single or distributed network elements. Shaded boxes correspond to functions performed by the Aqsacom ALIS mediation platform (derived from [13]).

VoIP Interception: PacketCable description for Electronic Surveillance

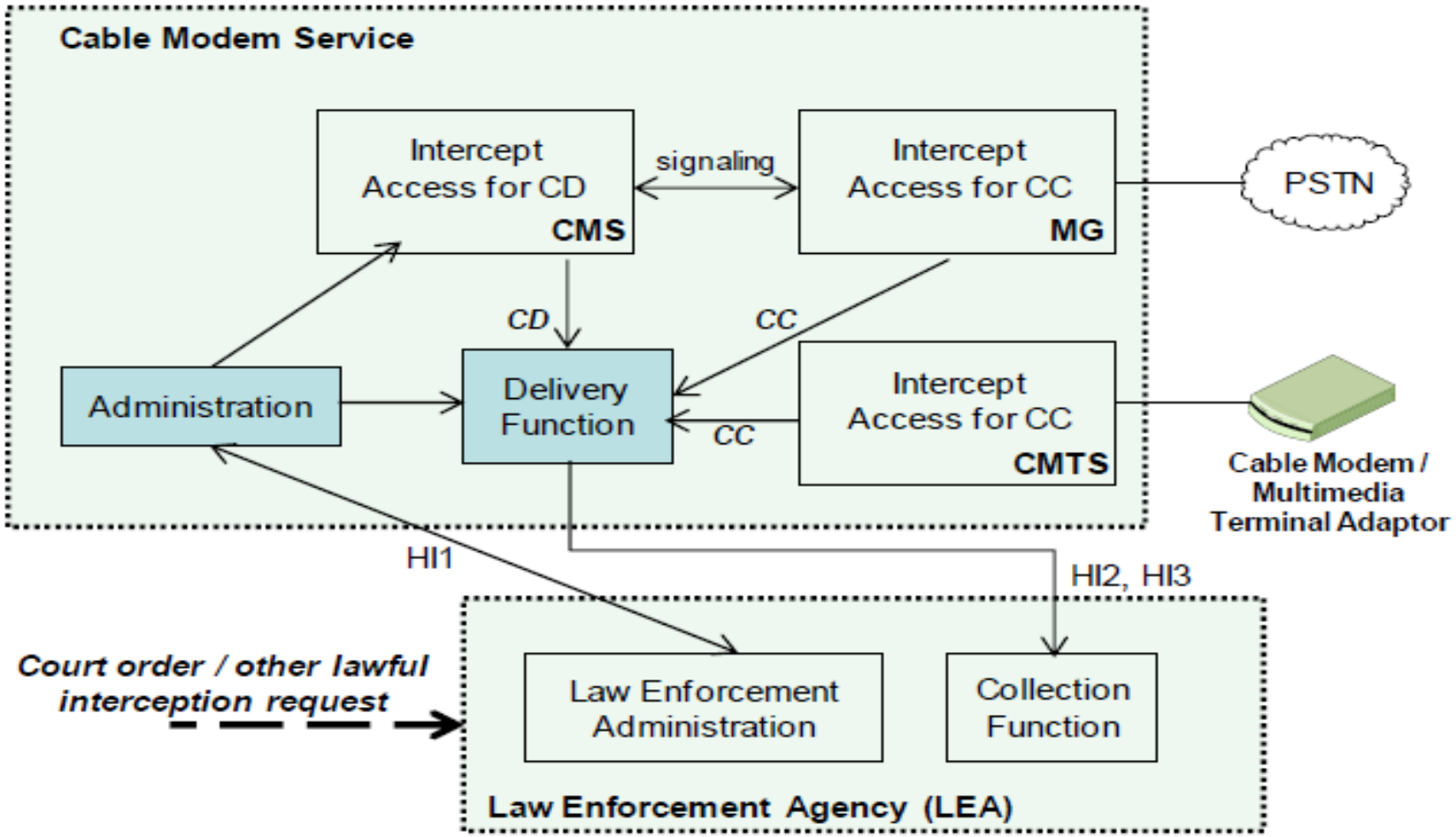


Figure 5-6. PacketCable description for Electronic Surveillance (adapted from [14, 15]). The shaded Administration and Delivery Function boxes are covered by ALIS (Section 6).

Architecture of the Aqsacom ALIS (Aqsacom real time Lawful Interception System) platform

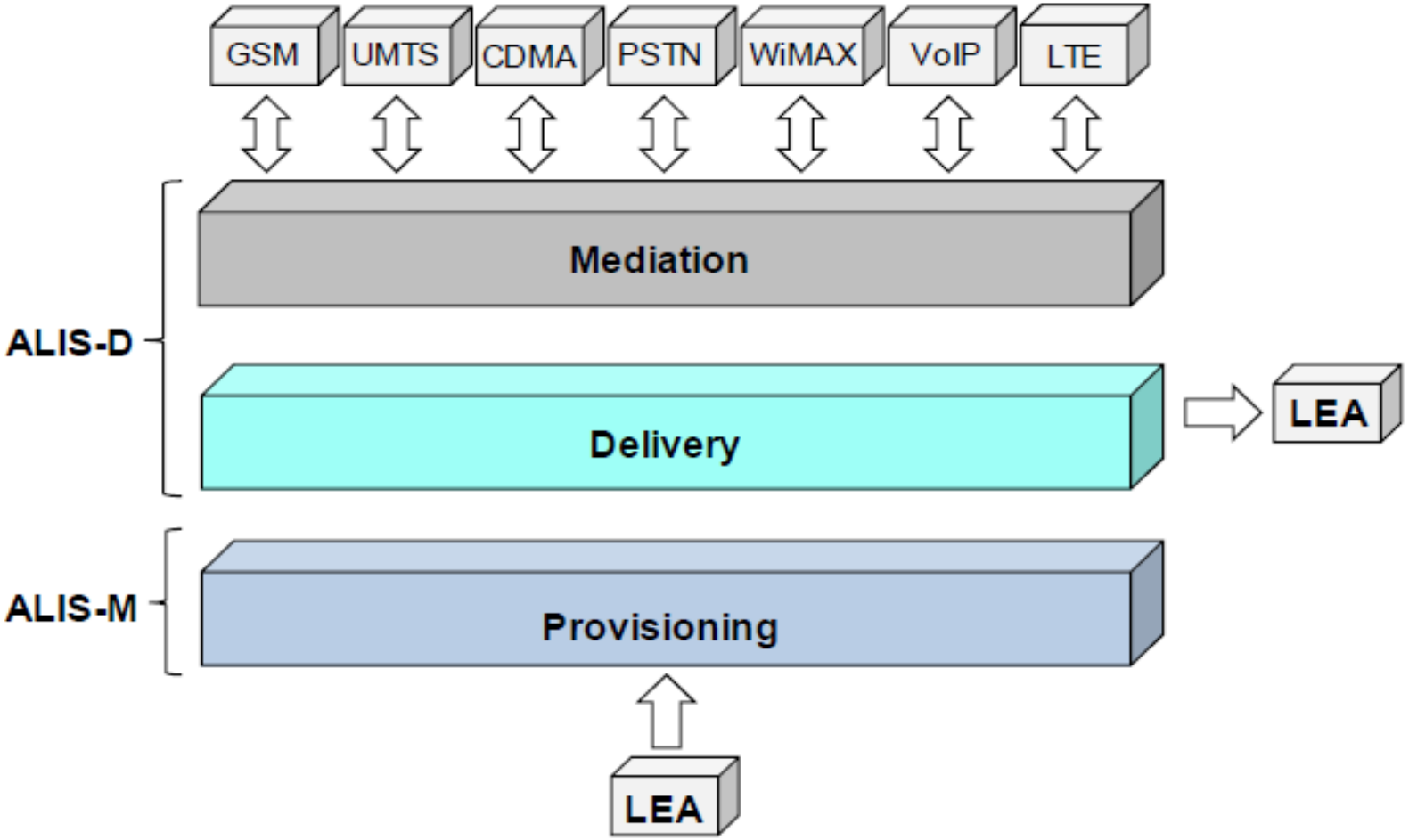


Figure 6-1. Architecture of the Aqsacom ALIS platform.

Application of the ALIS platform in the interception of a target's access to a network

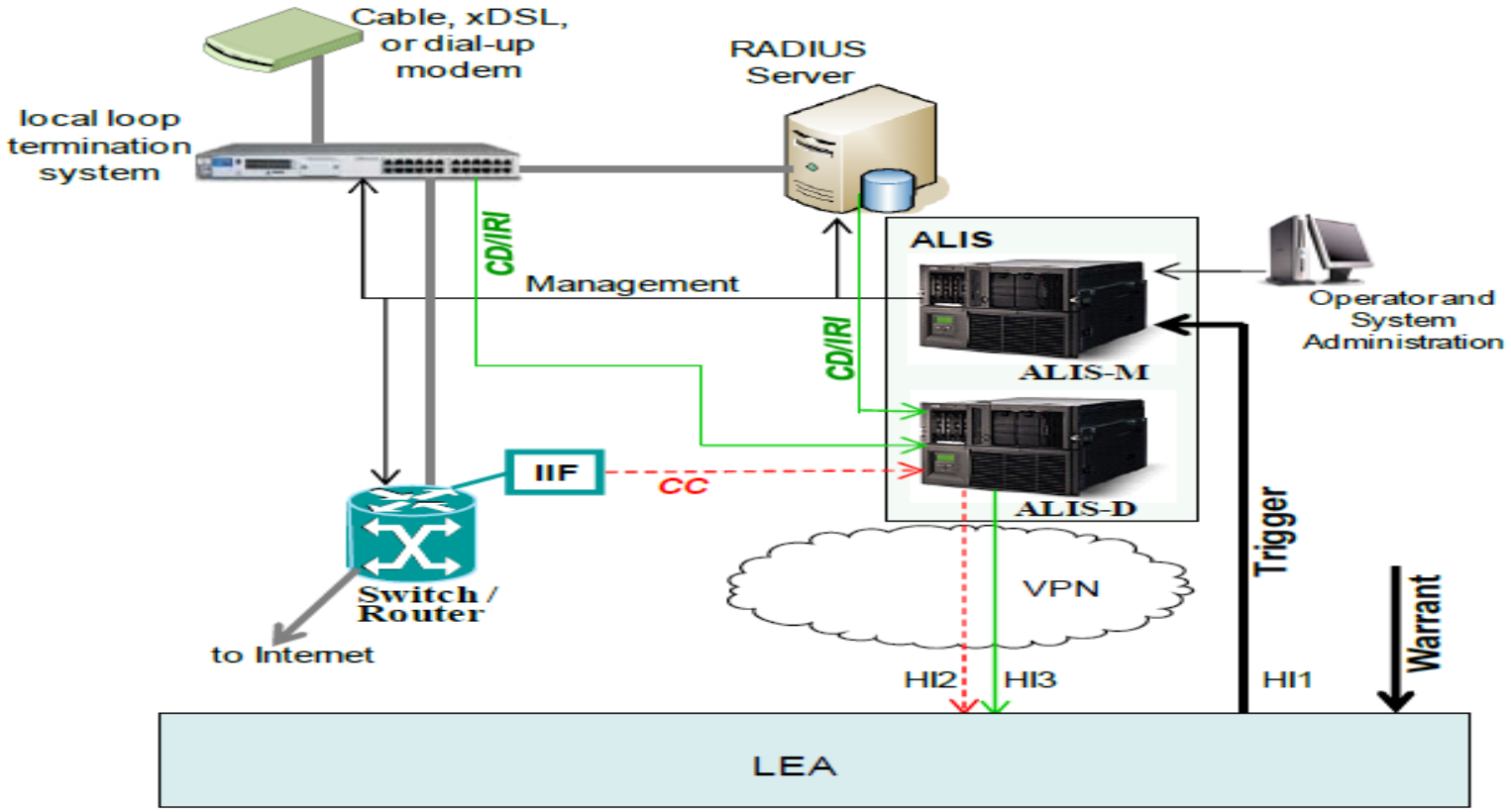


Figure 6-2. Application of the ALIS platform in the interception of a target's access to a network. For generality, the indicated access method could be cable modem, xDSL, or dial-up. The customer termination system and RADIUS server supply Call Data (IRI) to ALIS-D. The Internal Interception Function (IIF) in the router replicates and routes content to ALIS-D as well. ALIS-M handles network device management for the interception session. Call Data and Call Content are delivered to the LEA via a VPN in this example.

Example of E-mail interception

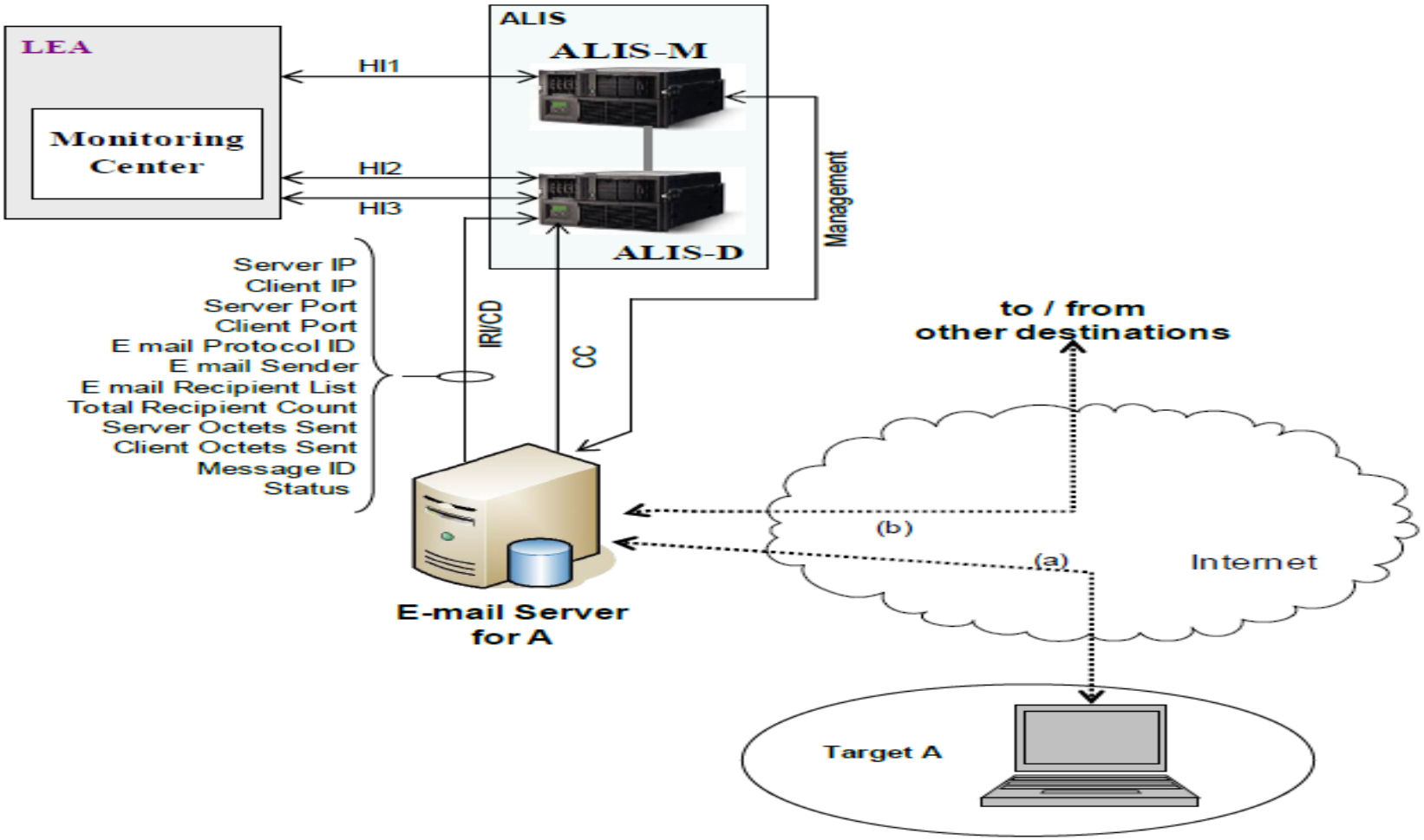


Figure 6-3. Example of E-mail interception. Here an Internal Interception Function operates within the E-mail server(s) handling outgoing and incoming messages to/from the target. Further interception can be carried out through External Interception (probes) at network points away from the E-mail server.

Application of the ALIS platform in the interception of VOIP

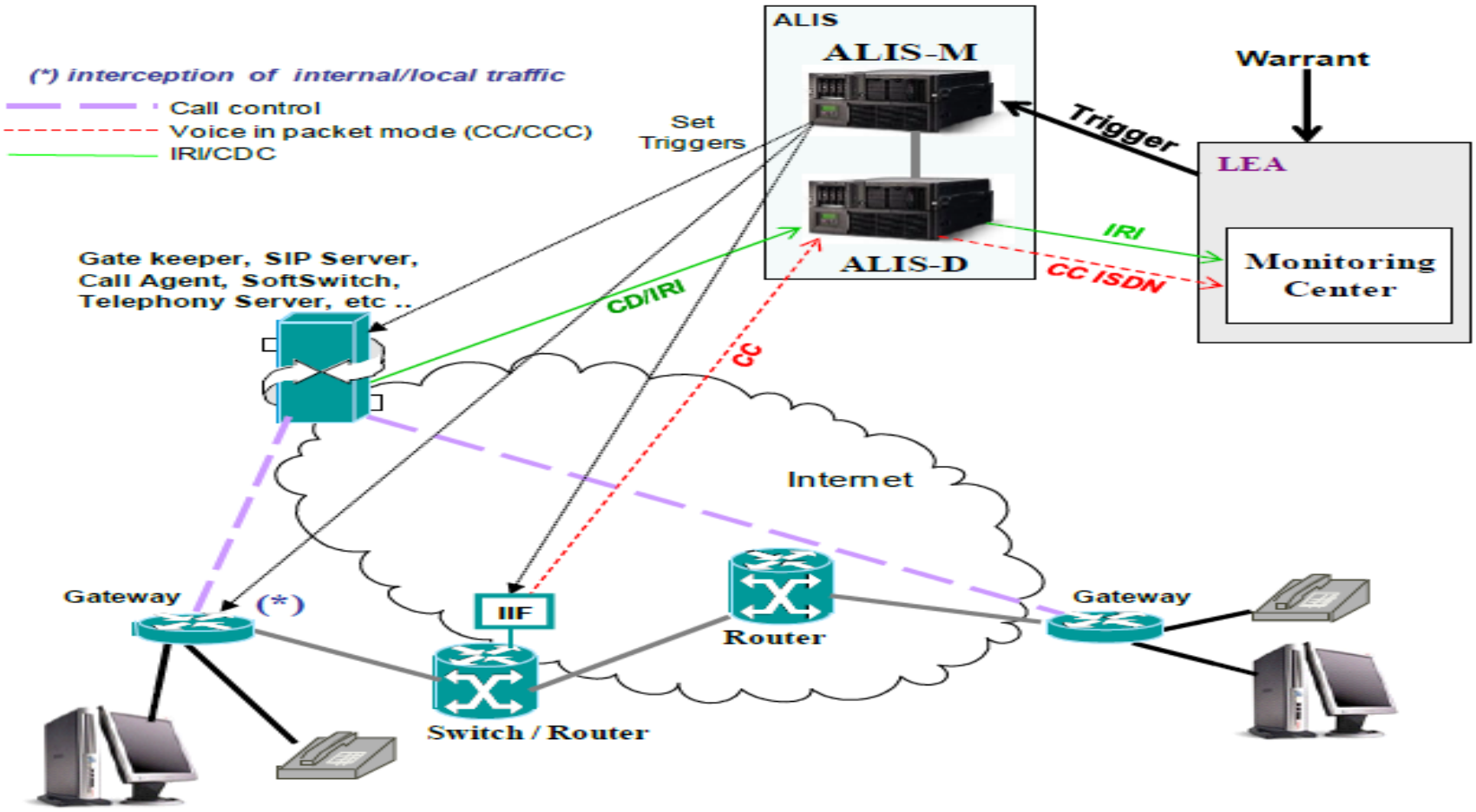
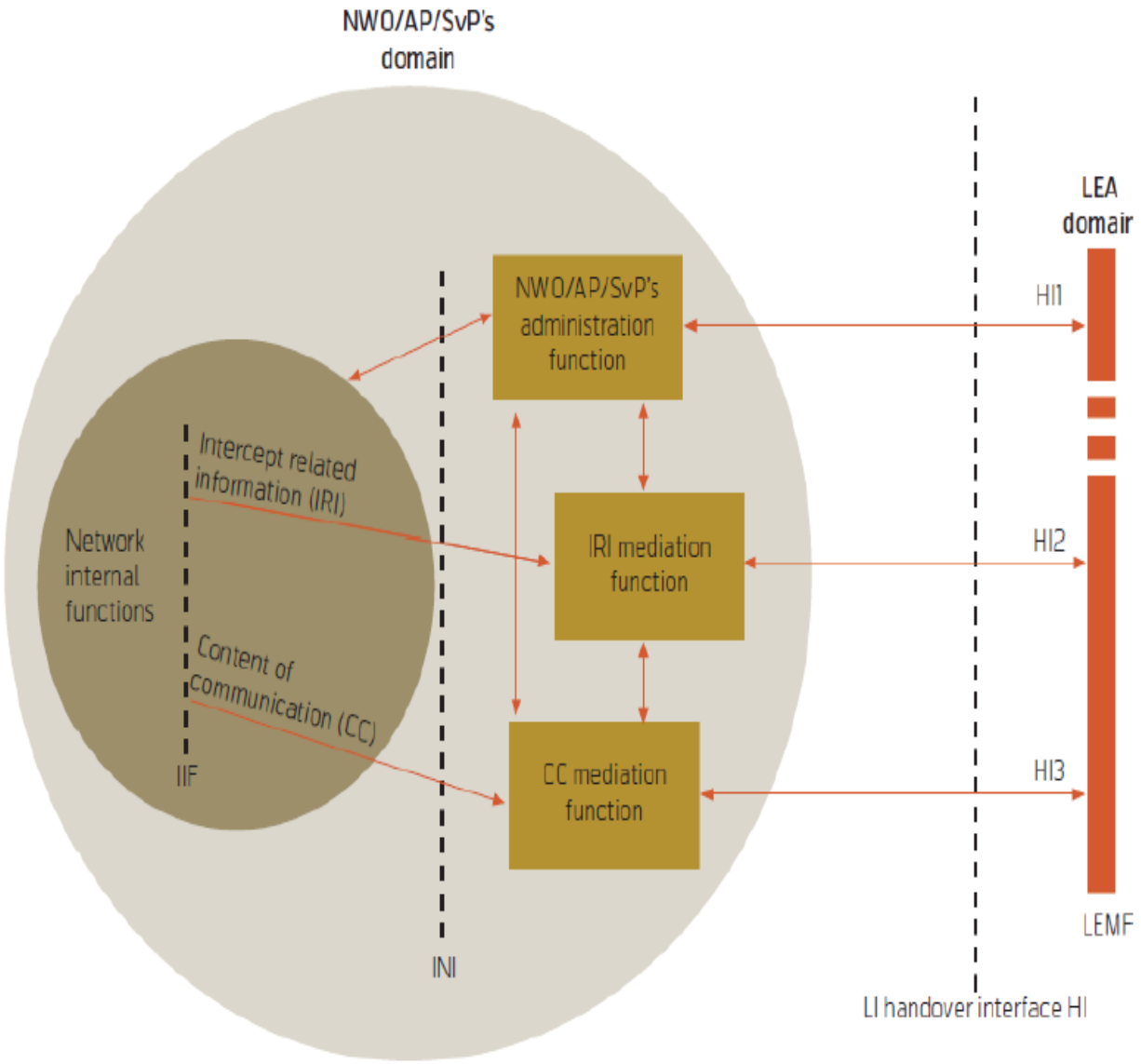


Figure 6-4. Application of the ALIS platform in the interception of VOIP. Call Data information is extracted from the Gatekeeper (or similar) device via Internal Interception and sent to ALIS-D for processing. Provisioning of pertinent network elements is carried out by ALIS-M. An Internal Interception Function (IIF) within a router replicates call content to be intercepted according to the IP address of the originating and/or destination target.

General architecture for lawful interception-ETSI

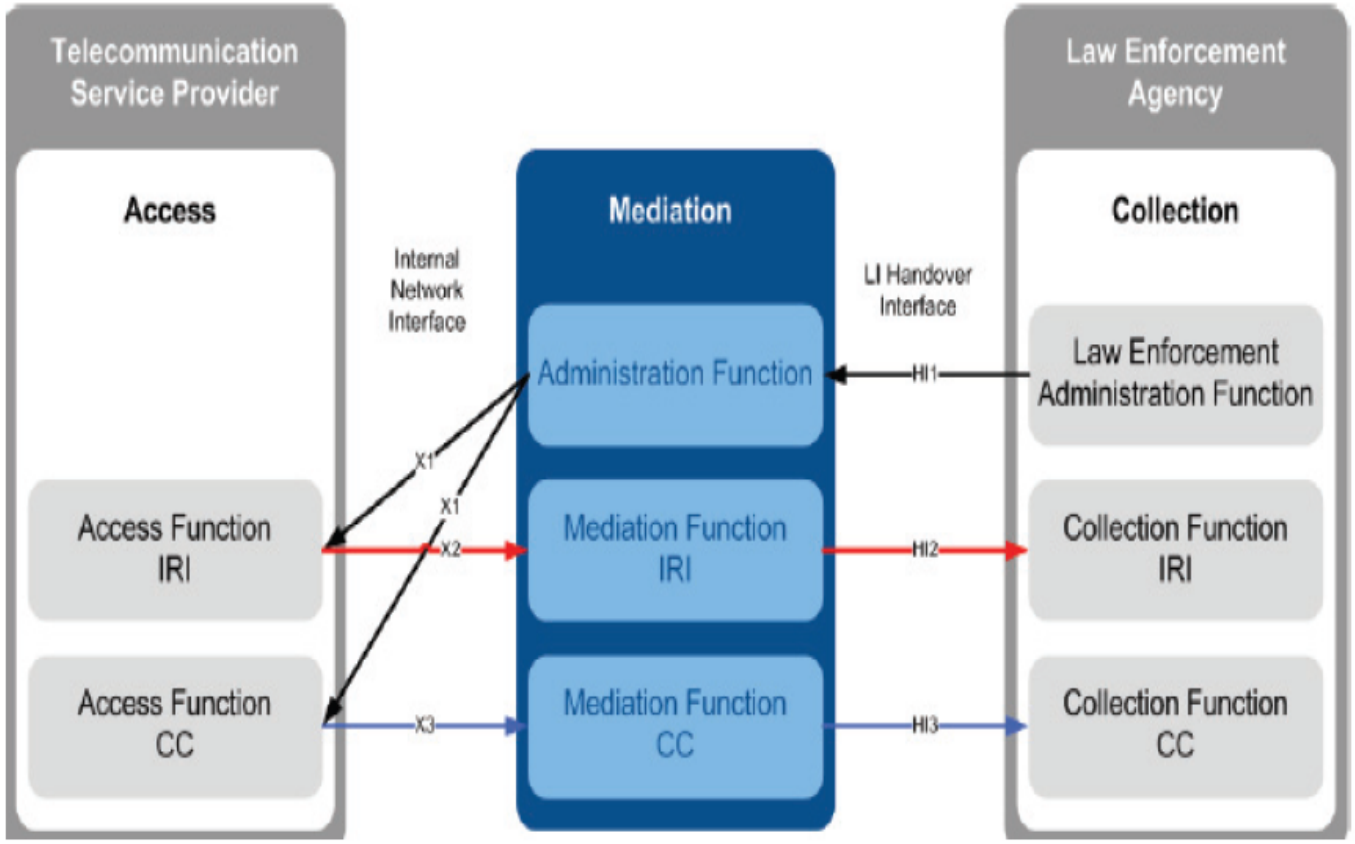


ETSI has been a major driver behind the specification of hand-over interfaces and of the flow that intercepted data should follow. It specifies a general architecture for lawful inter-ception that allows systematic and extensible communication between network operators and LEAs over defined interfaces and in compliance with national legislation.

This general architecture applies to any kind of circuit- or packet-switched voice and data net-work.

Key Components of a Dedicated Lawful Interception Solution

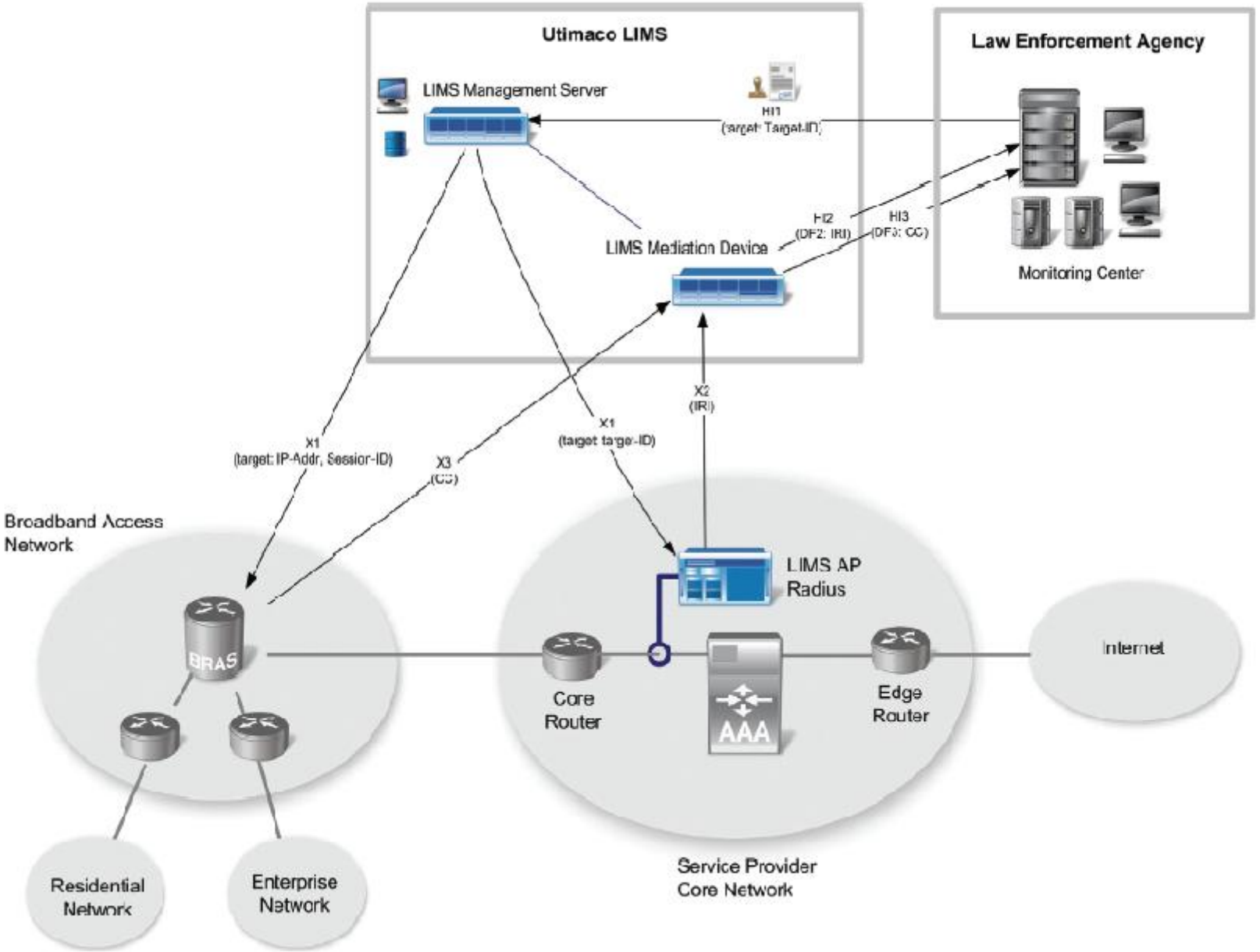
Most dedicated solutions on the market today are similar in architecture and functionality. The main difference lies in the ability to interface with network elements and in the business model proposed by the solution vendor.



The figure shows the typical functional flow of lawful interception on which the dedicated LI solutions are built.

A monitoring centre, staffed by LEA personnel, relies on standardised interfaces (e.g. ETSI or ANSI) to gain access to communications provided over fixed networks, mobile networks, and IP-related channels. The monitoring interface handles interception warrants, IRI and communications content separately.

Hybrid Interception



Multiple LI Access Points for Mobile Radio

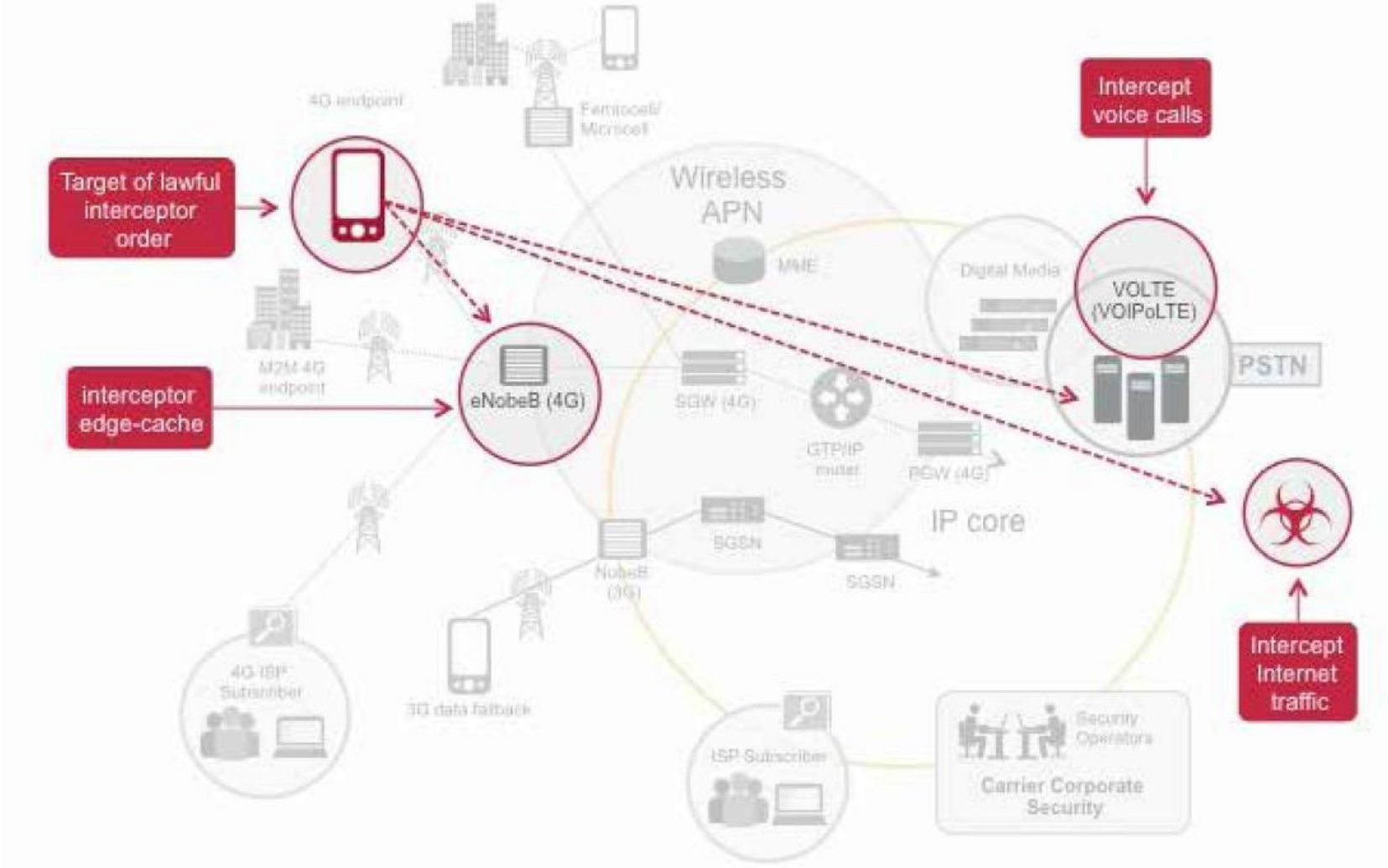
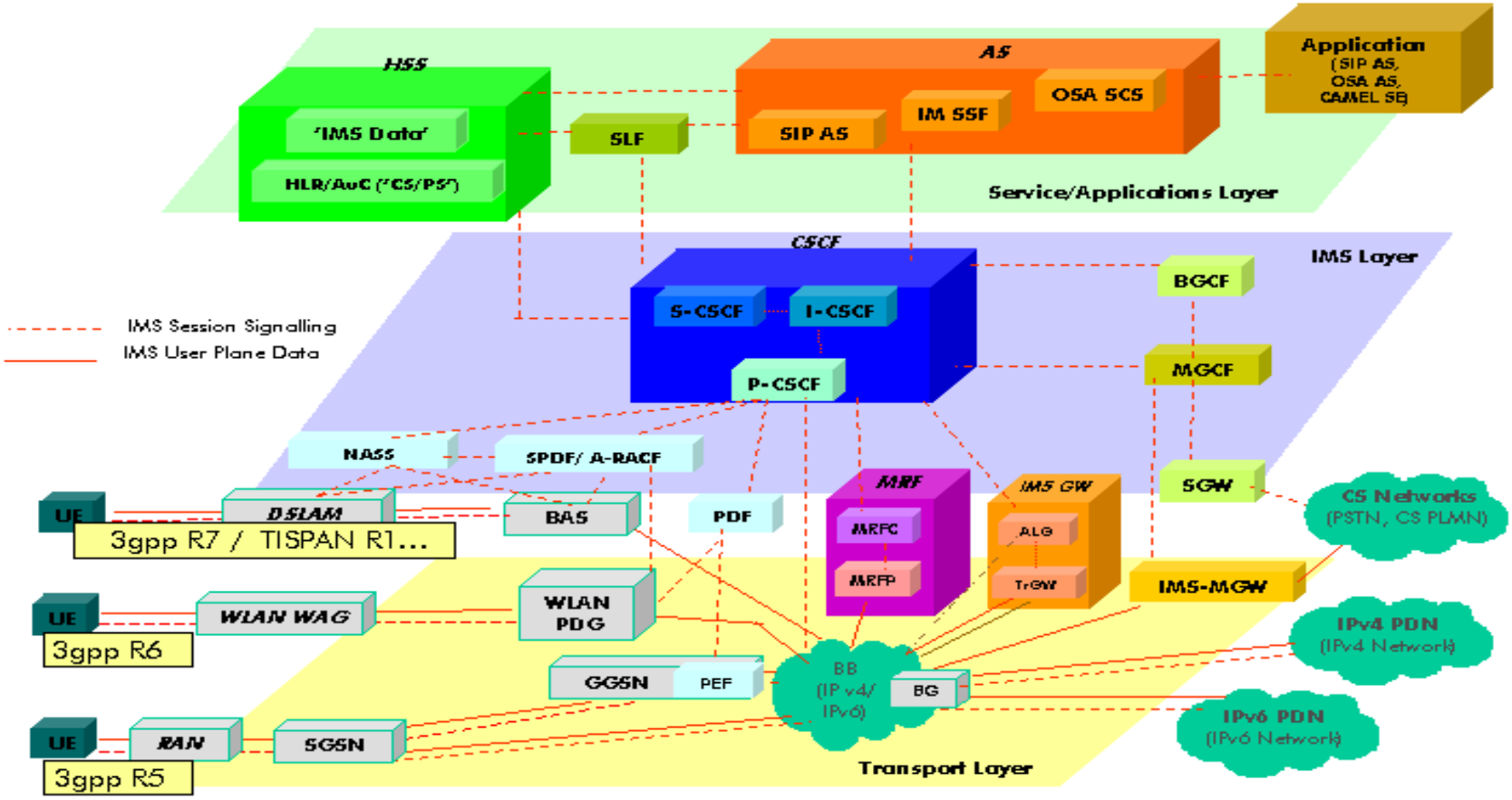
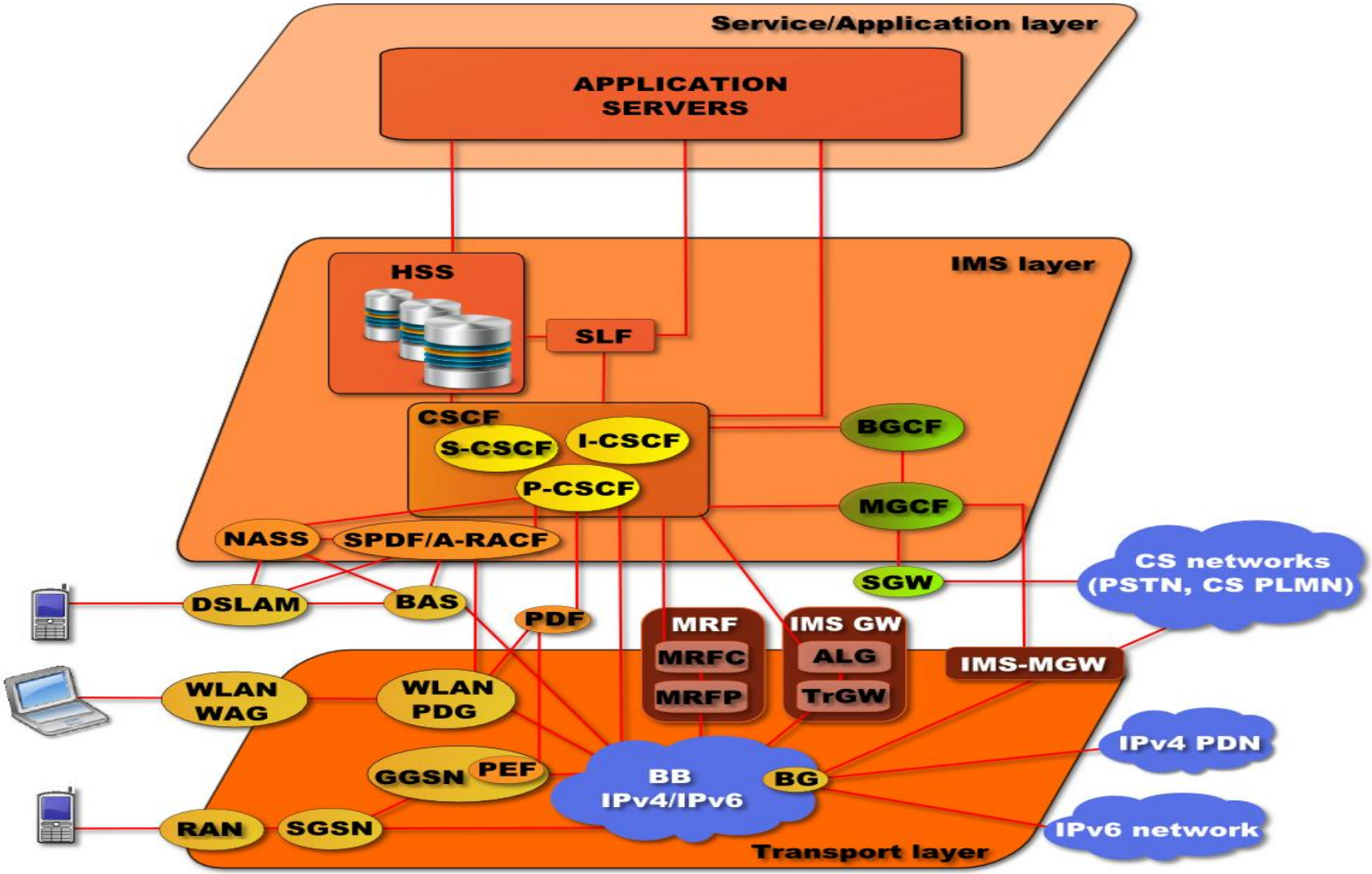


Figure 5. Compliance requires support for multiple lawful access intercept points.

IP Media System (IMS) Overwiew

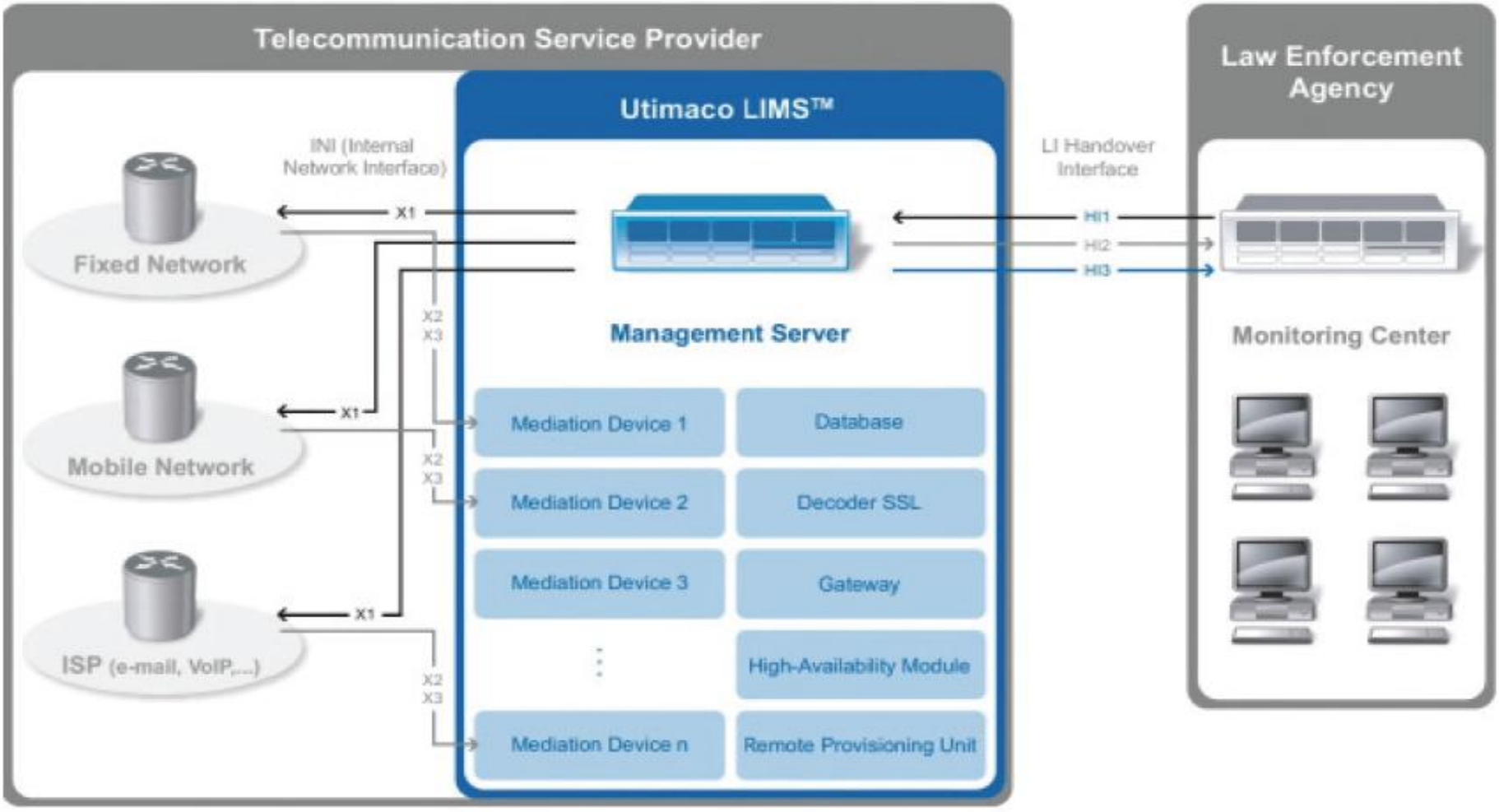


IP Media System (IMS) Overwiew



Utimaco LIMS™, a Leading-edge Solution

Utimaco LIMS™ is a central management system for all tasks related to the lawful interception of telecommunication services in mobile and fixed networks. It is a software-based solution consisting of the elements shown in the figure below.



INI: *Internal Network Interface*
IRI: *Interception Related Information*
CC: *Content of Communication*

x1, x2, x3: *Internal Network Interfaces for LI Provisioning, IRI and CC exchange*
H1, H2, H3: *Standard handover interface to the Law Enforcement Agency for LI Provisioning, IRI and CC exchange*

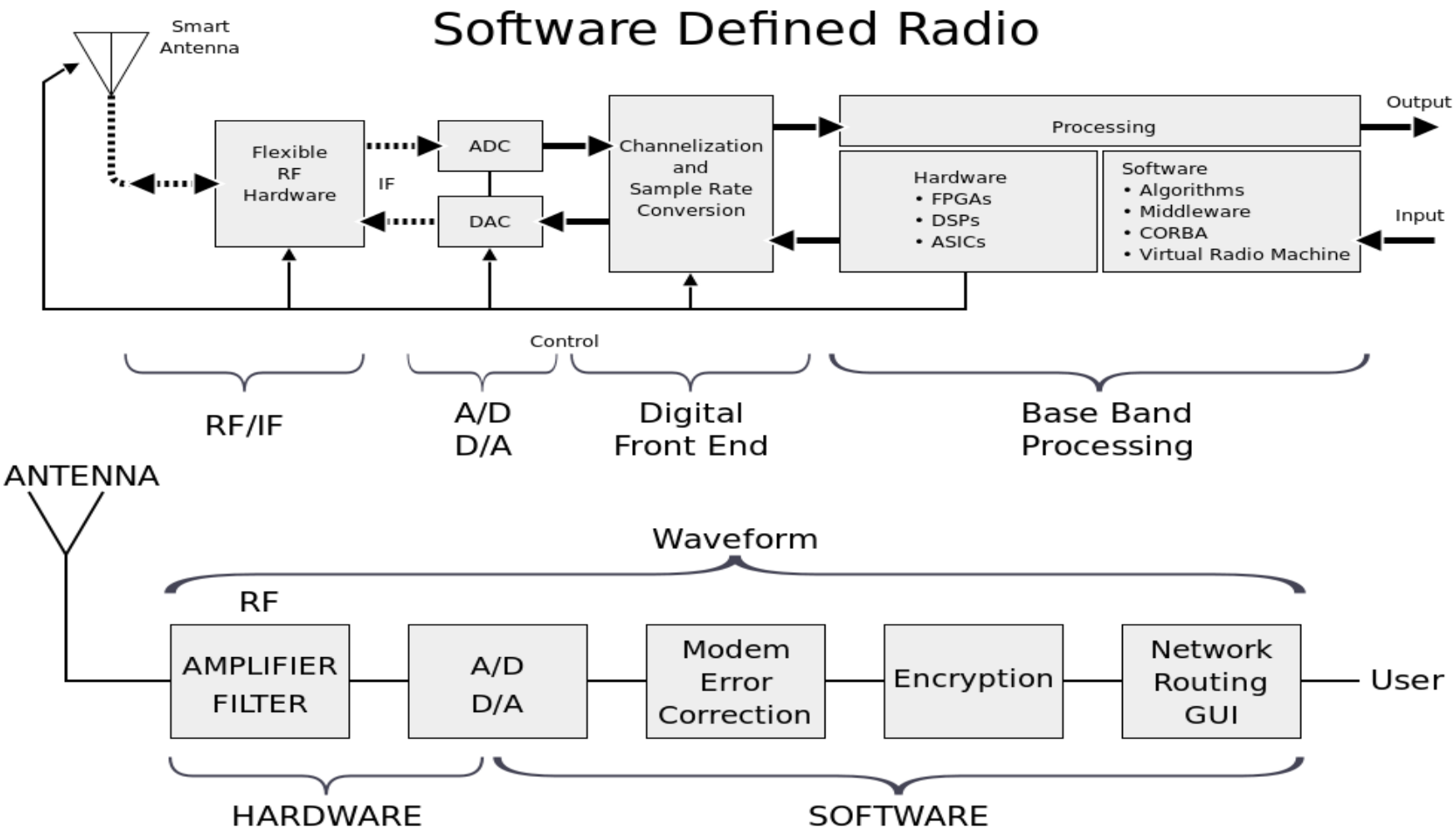
IMSI Catchers

IMSI Catchers

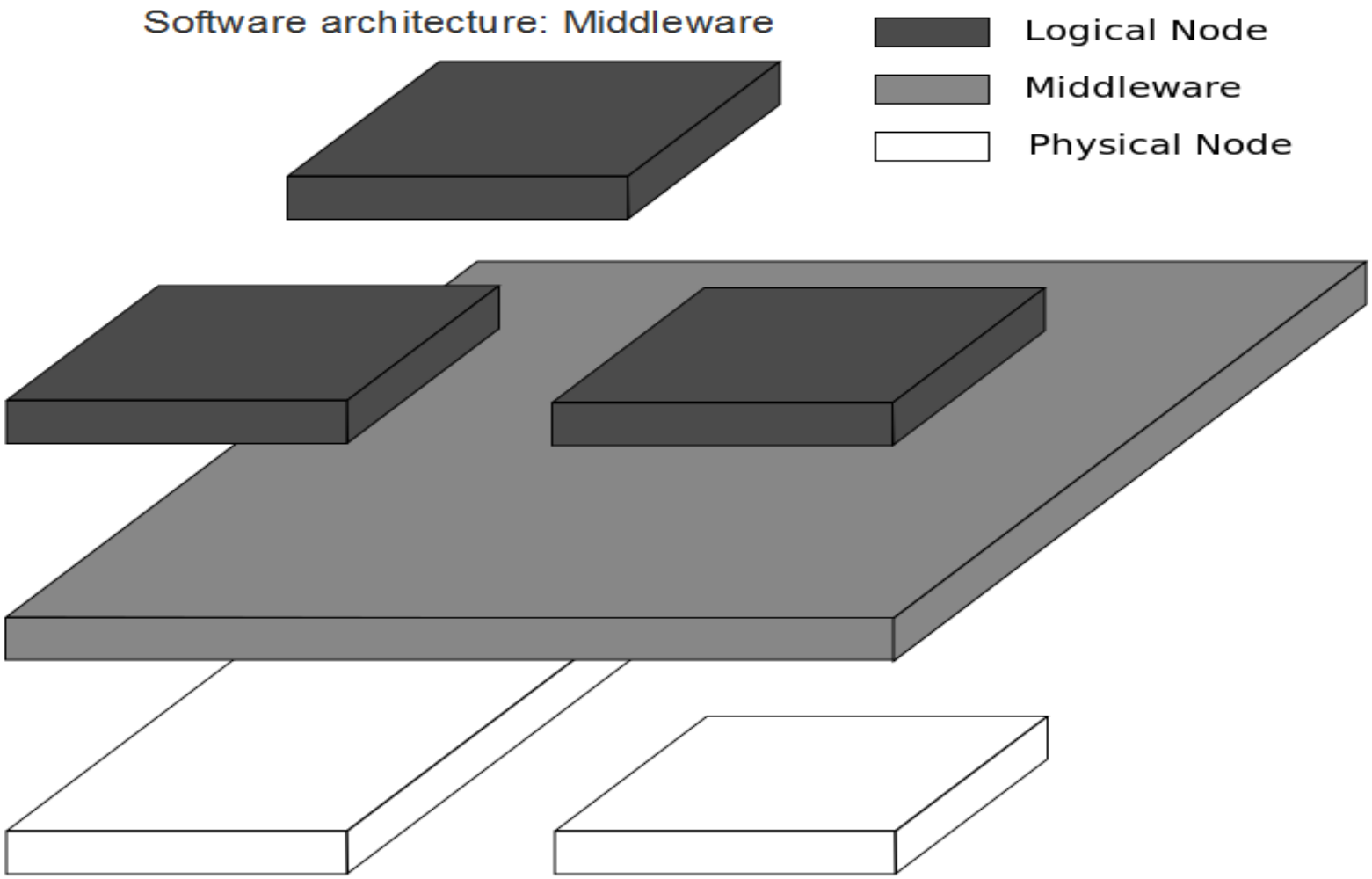
- Used for
  - Tracking users
  - Eavesdropping calls, data, texts
  - Man-in-the-Middle
  - Attack phone using operator system messages (e.g. Management Interface, reprogram APN, HTTP-Proxy, SMS/WAP-Server...)
  - Attack SIM (c.f. SIM card rooting, otherwise filtered by most mobile carriers), Attack Baseband
  - Geotargeting ads (e.g. SMS)
  - Intercept TAN, mobile phone authentication, ...

Adrian Dabrowski, adabrowski@sba-research.org

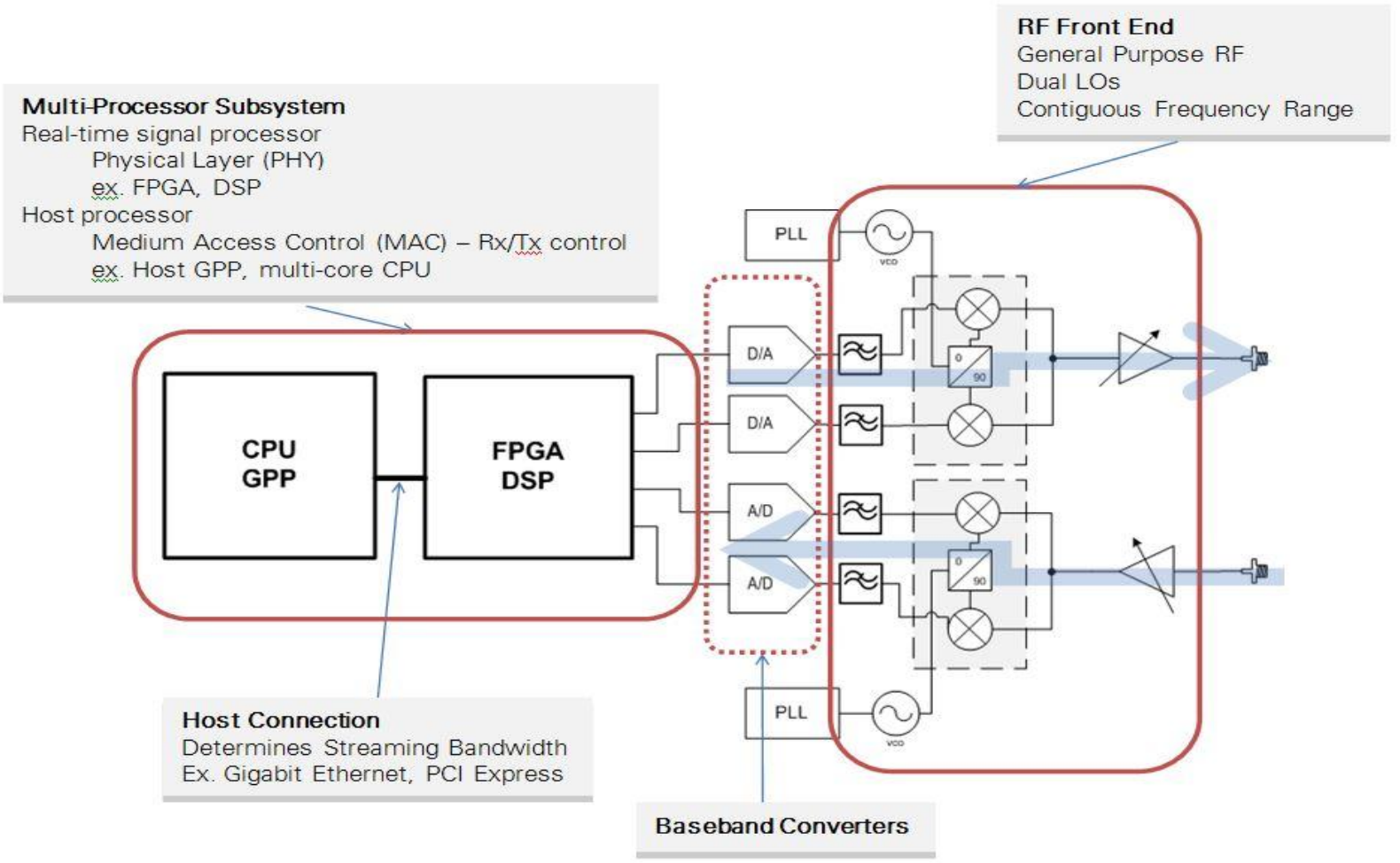
Software Defined Radio (SDR)



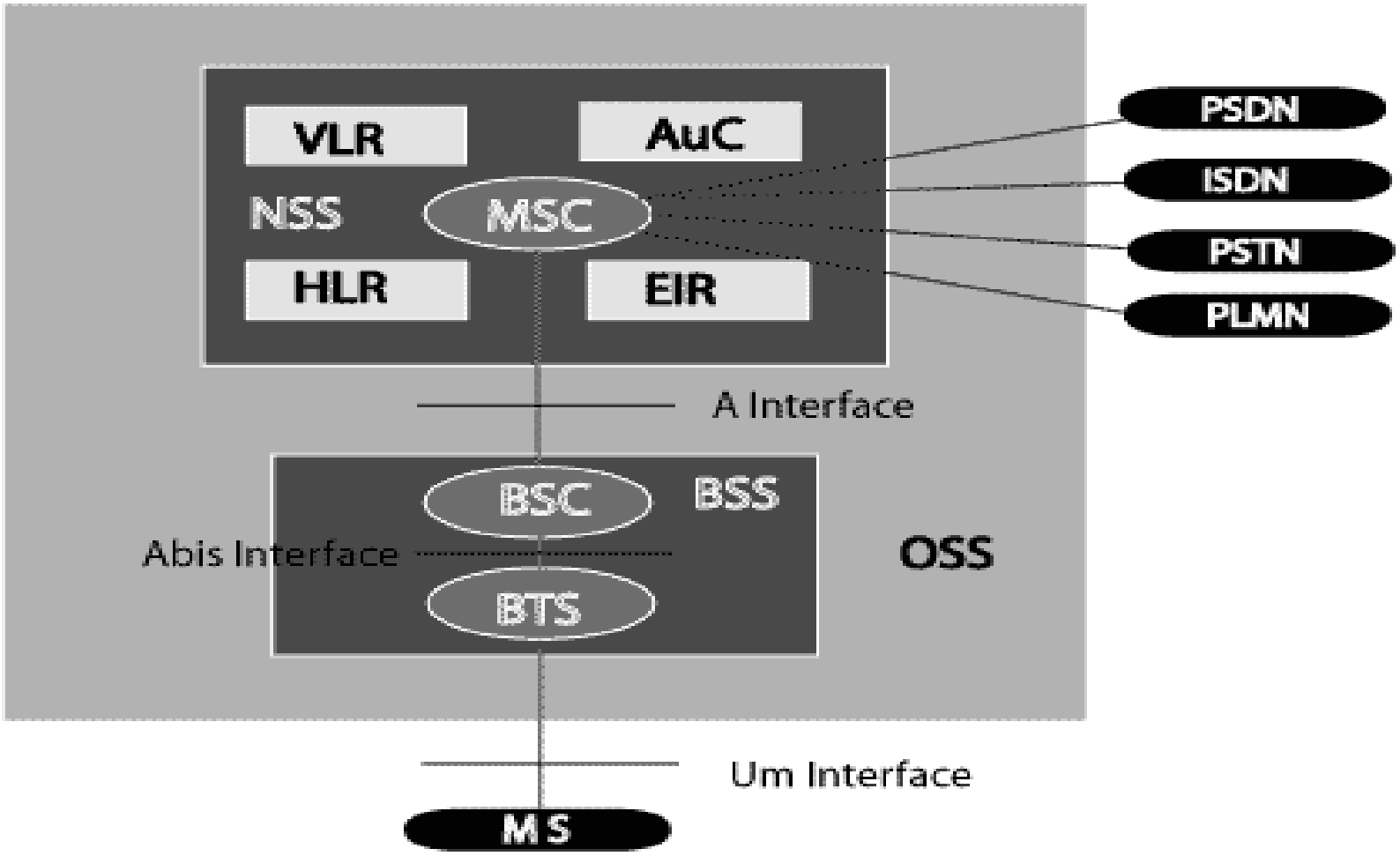
Software Defined Radio (SDR)



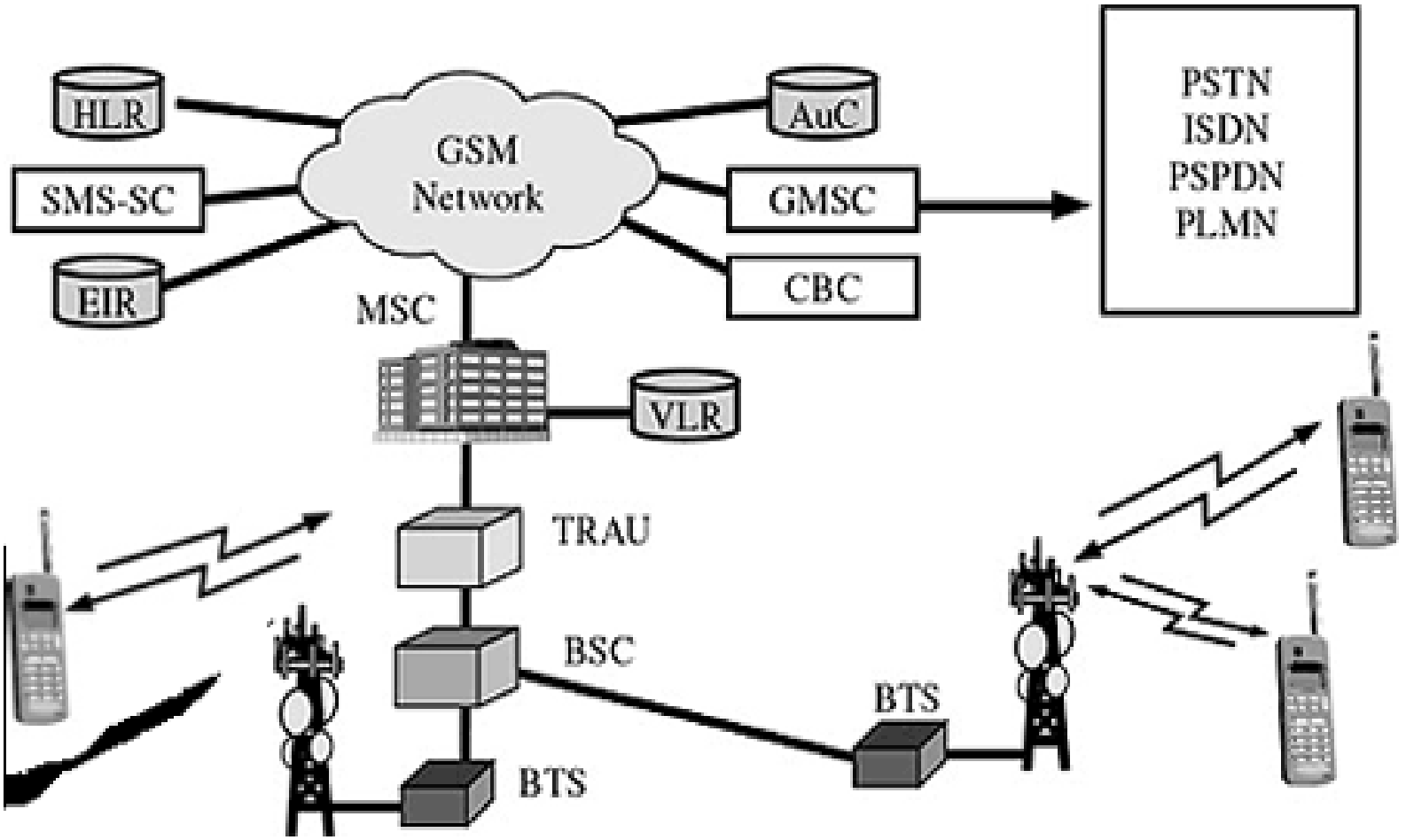
Software Defined Radio (SDR)



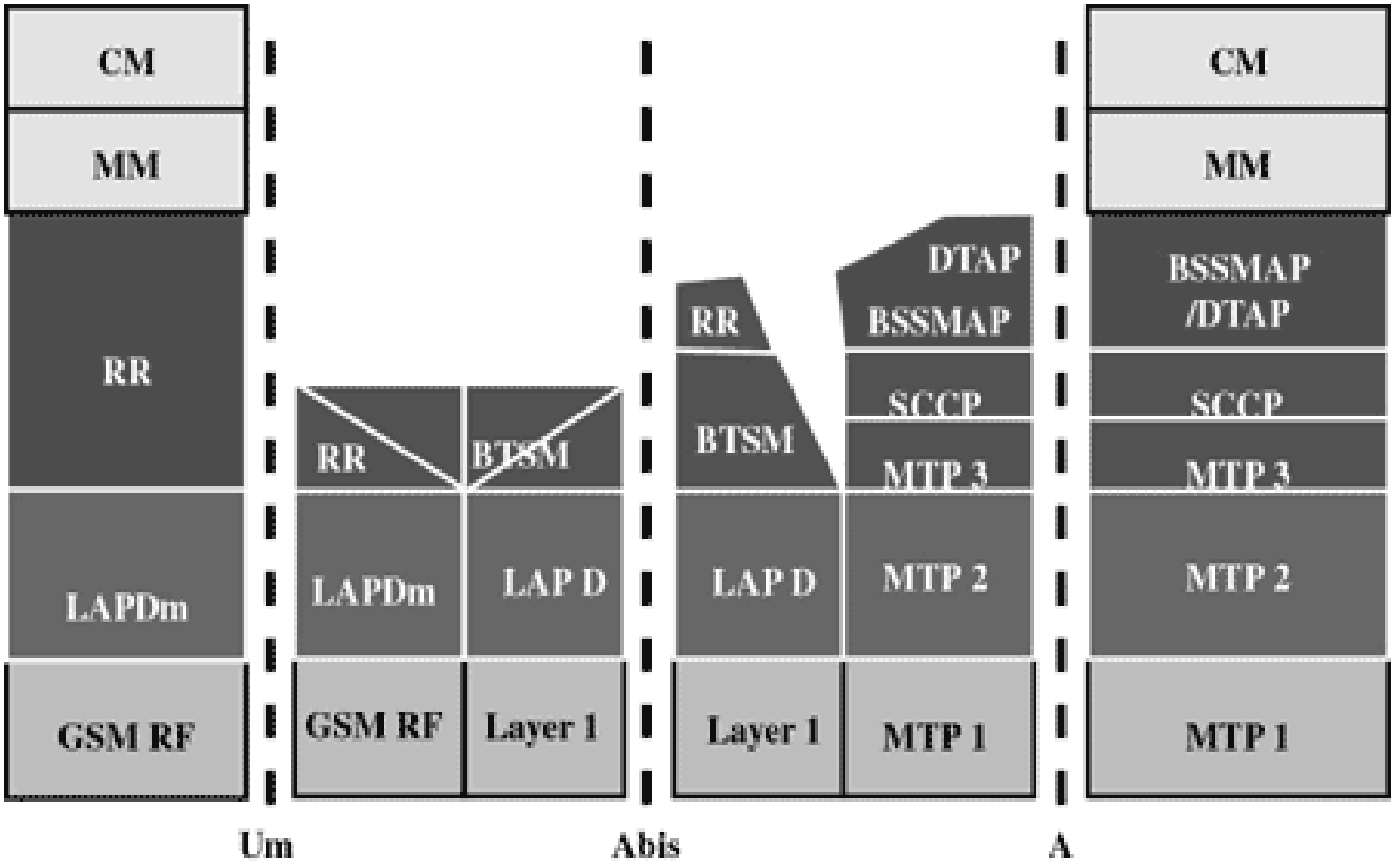
GSM Architecture



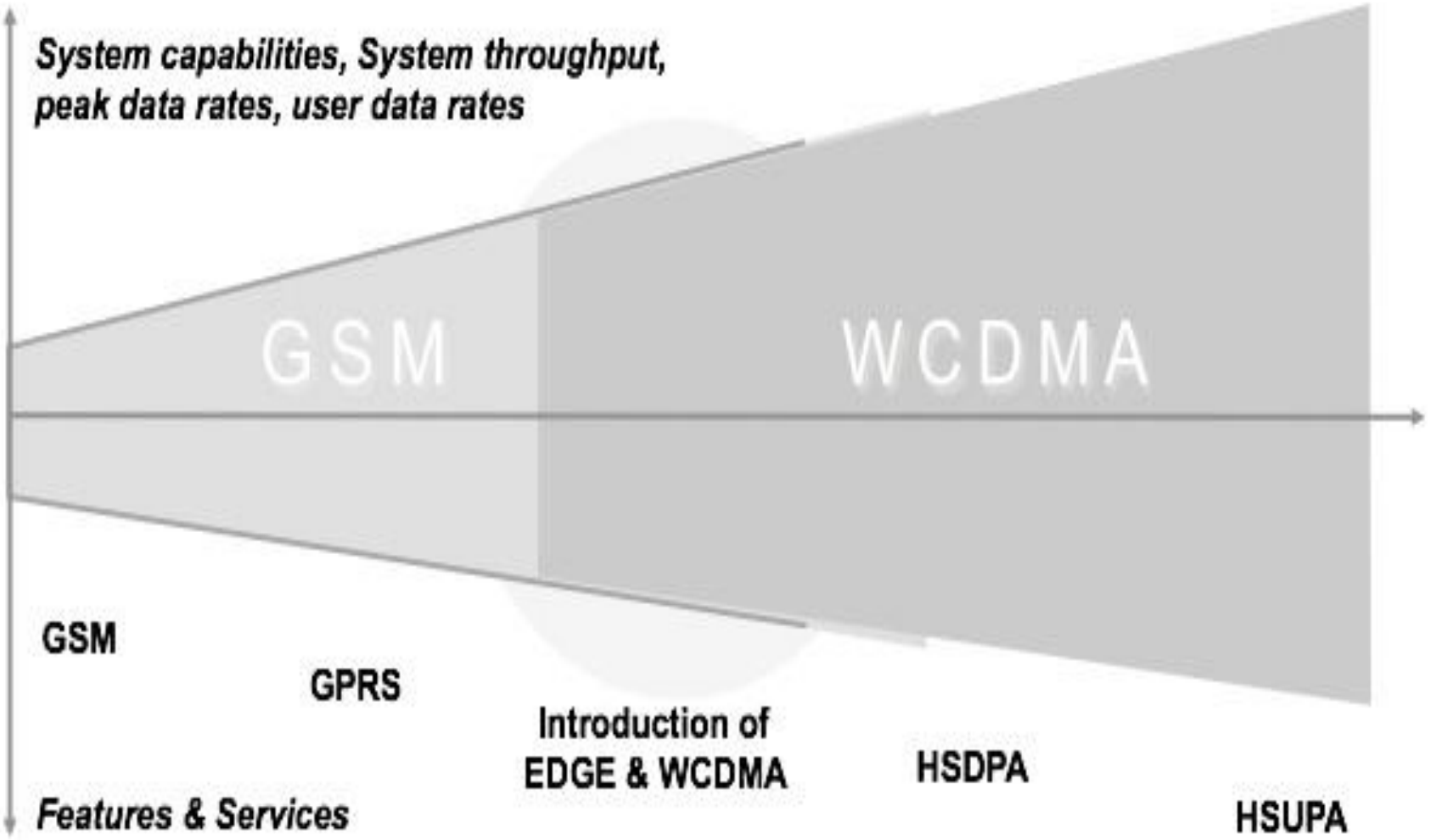
GSM Architecture: Network Elements



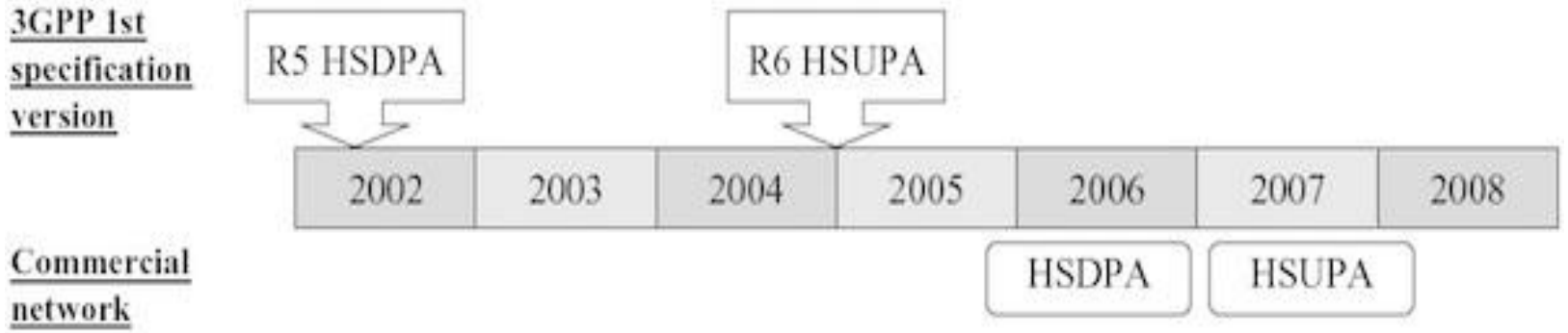
GSM Architecture: Protocol Stack



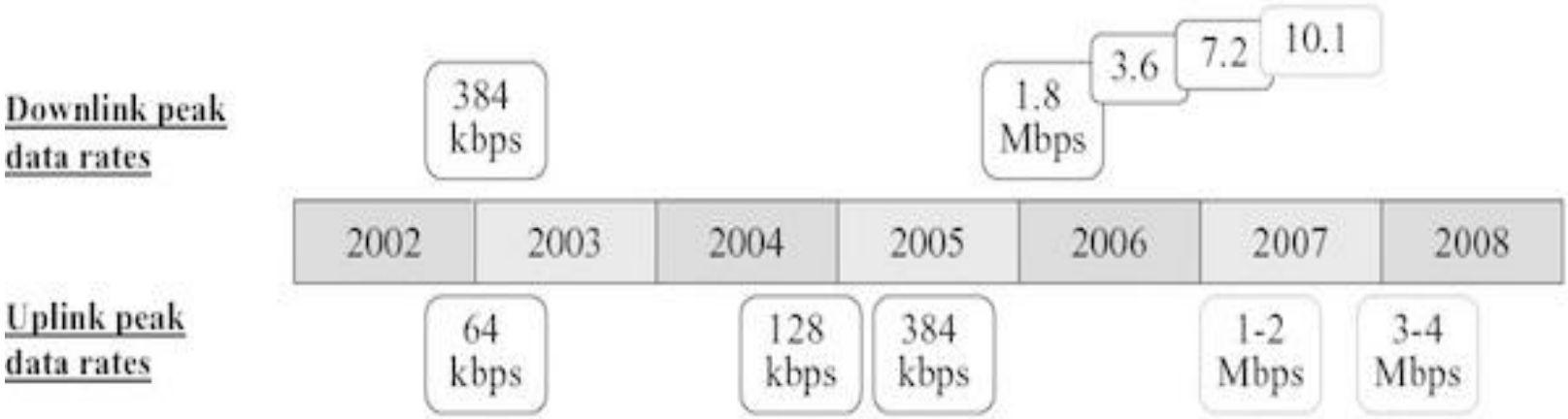
Evolution of GSM



Evolution of GSM

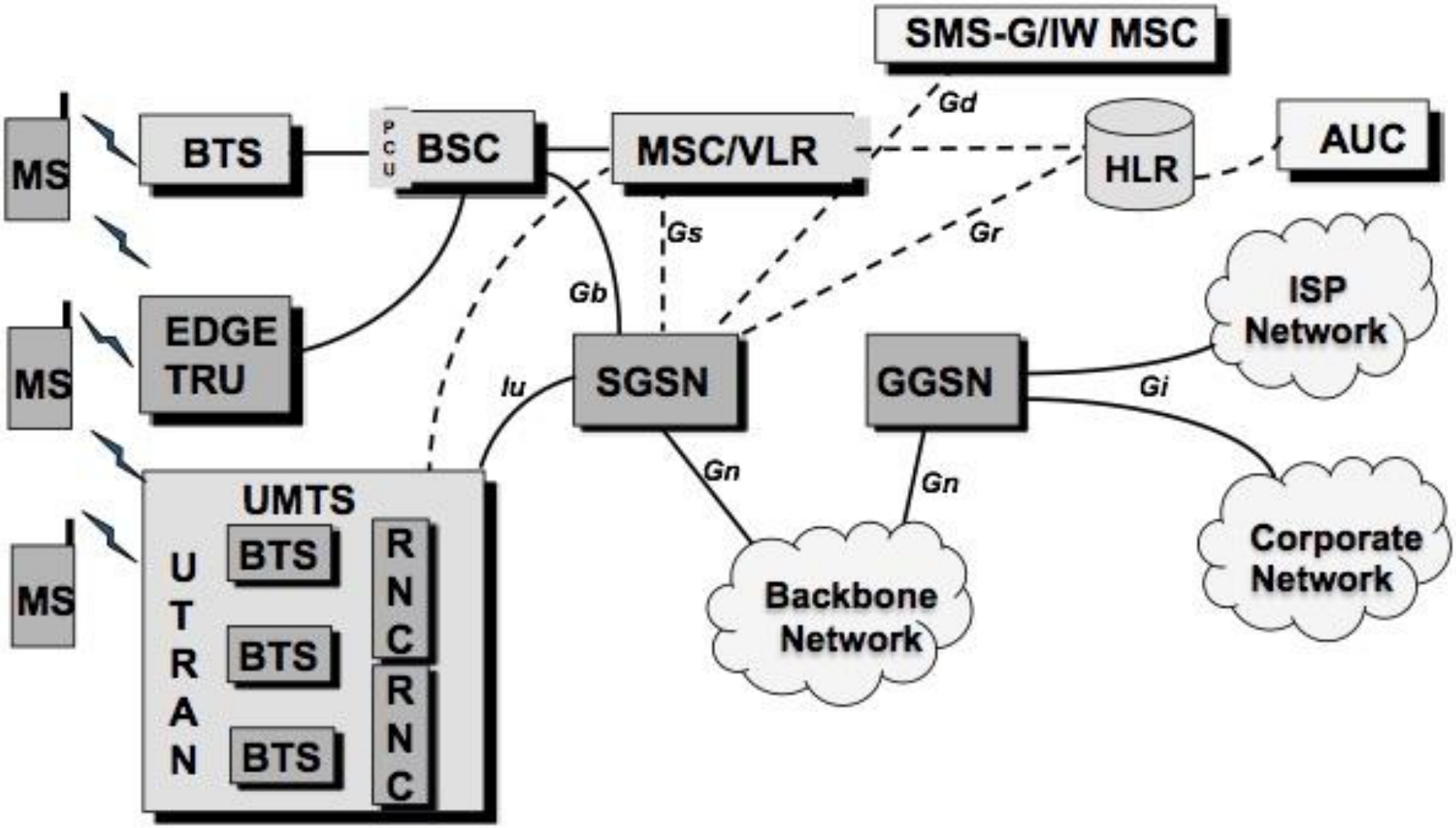


HSPA standardization and deployment schedule.



Data rate evolution in WCDMA and HSPA.

UMTS Architecture



Lawful Interception Configurations for 3G Networks

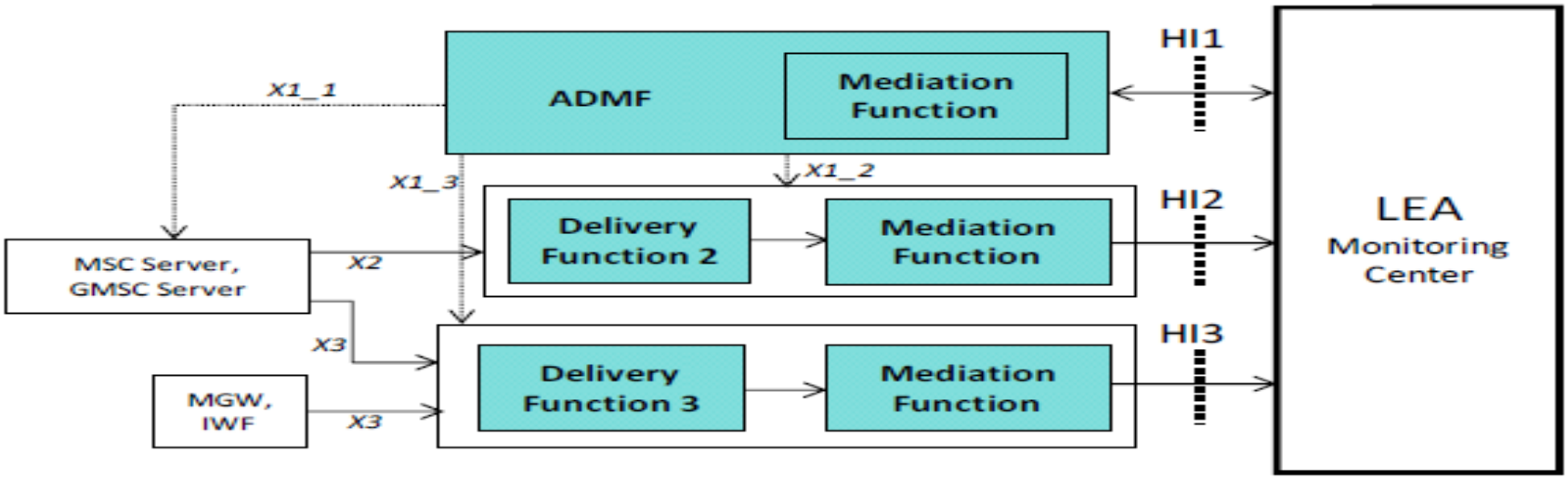


Figure 5-1. Interception model for circuit-switched services within a 3G mobile network (generalized for CDMA2000 and UMTS) (based on [10]). Functions in shaded boxes are implemented in the Aqsacom ALIS mediation platform (described in Sections 6 and 7).

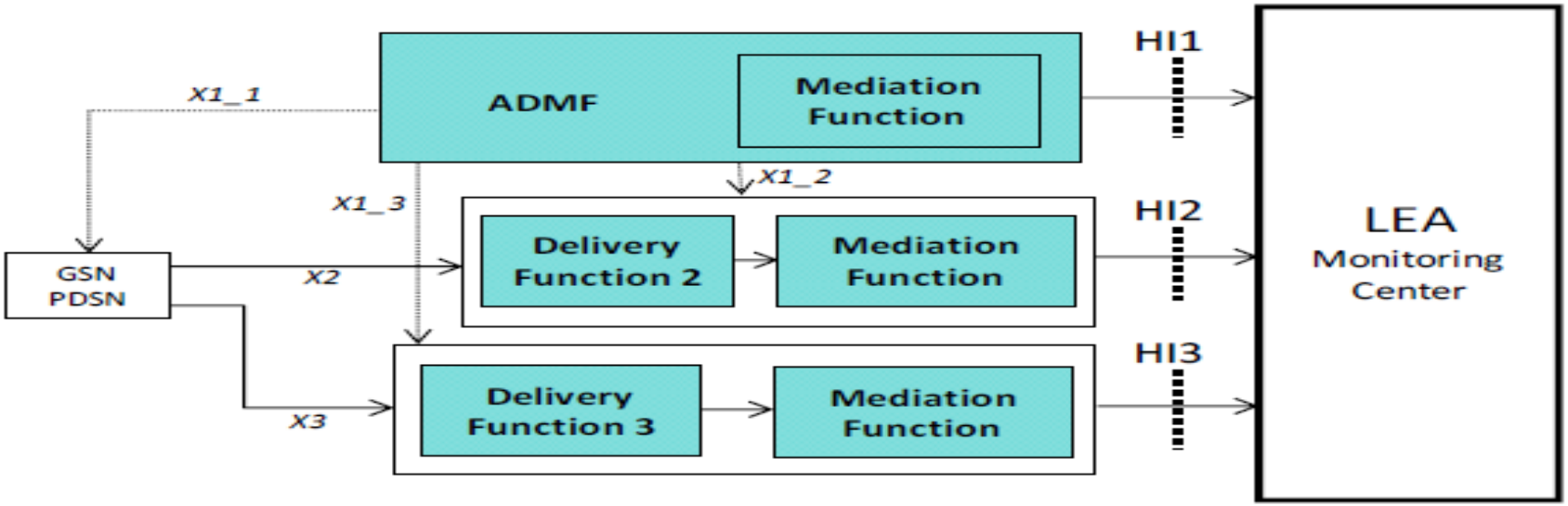
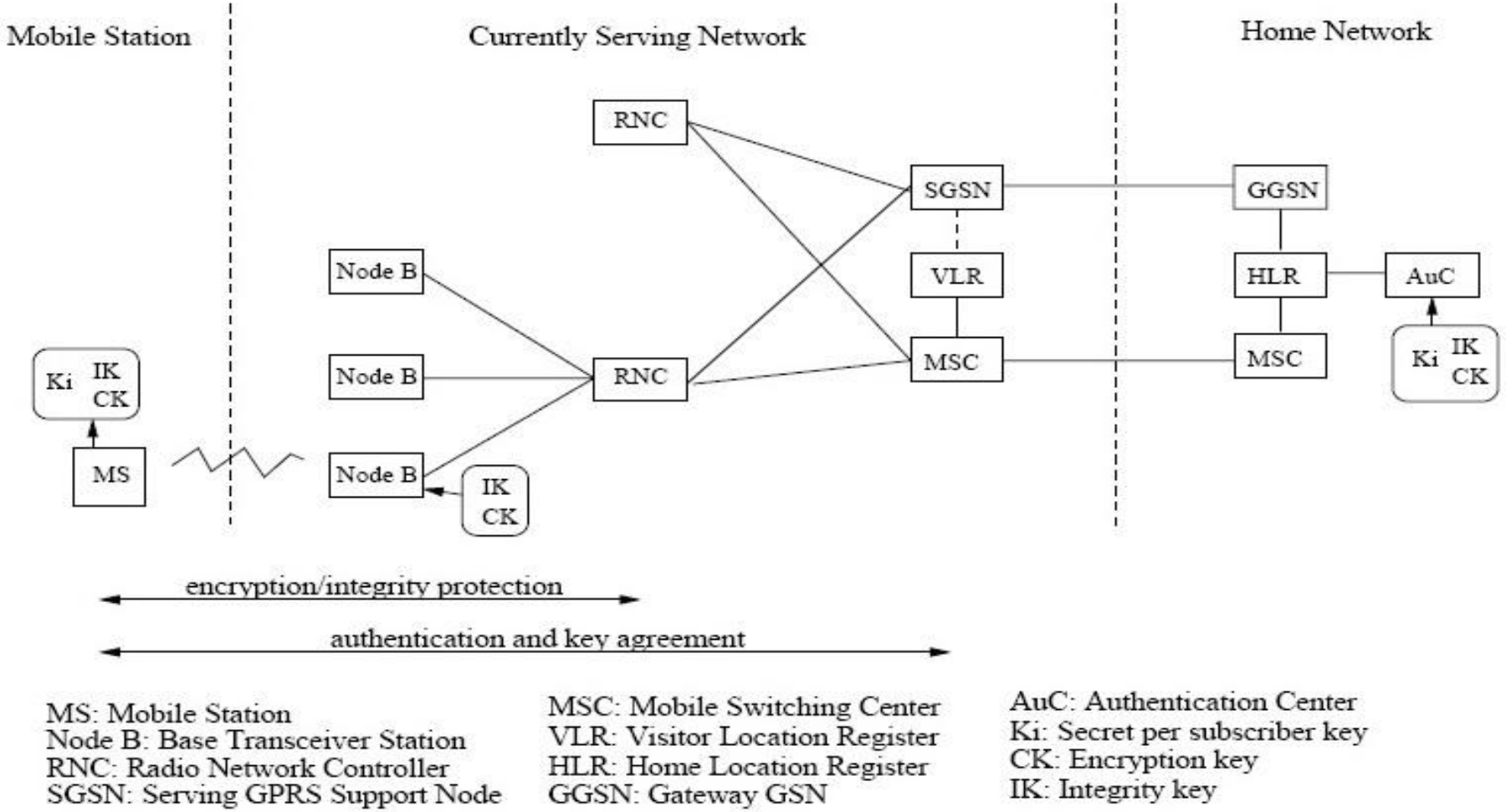


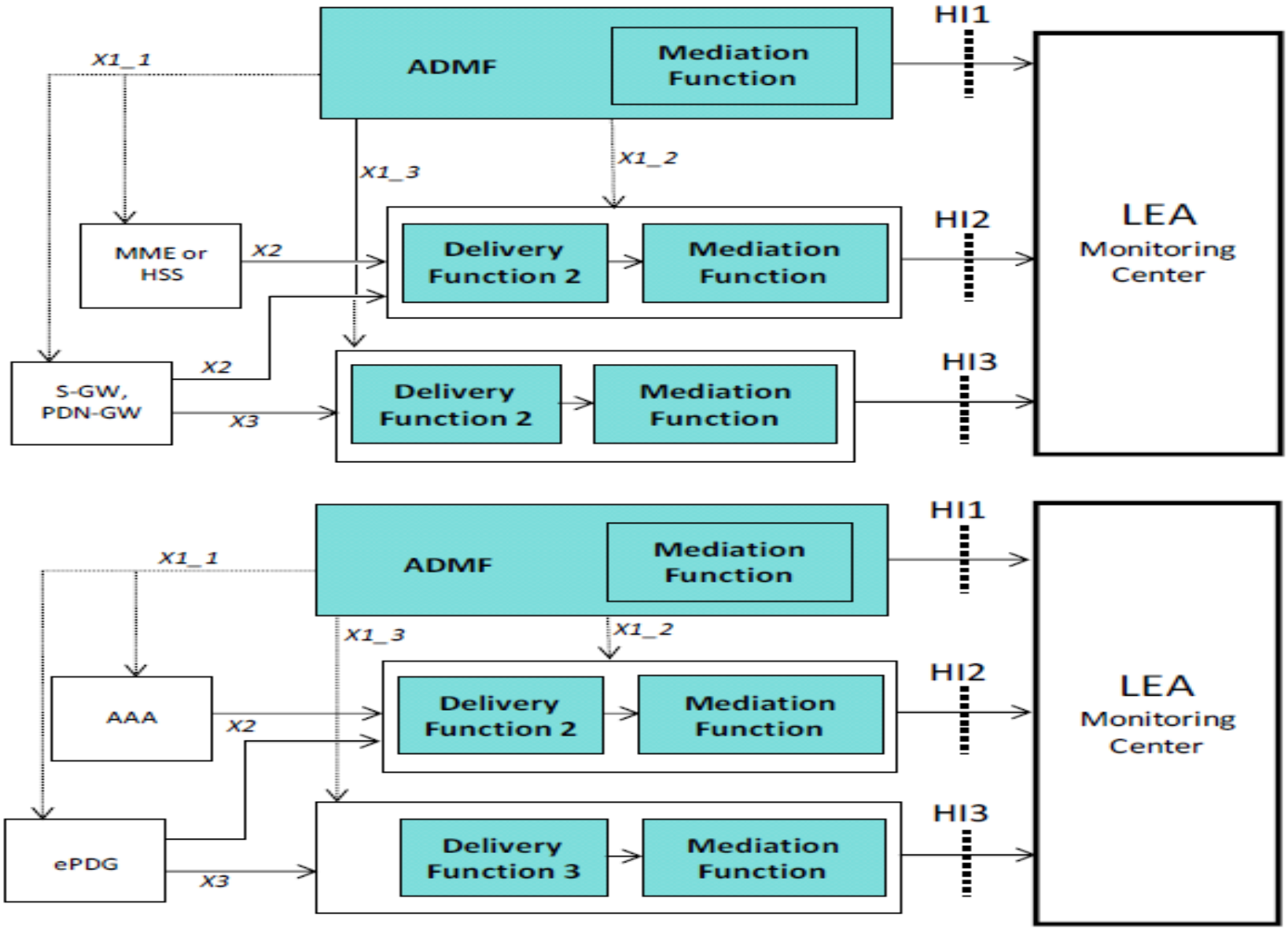
Figure 5-2. Interception model for packet data services (including IP) within a 3G mobile network (generalized for CDMA2000 and UMTS) (based on [10]). Functions in the shaded boxes are implemented in the Aqsacom mediation platform (described in Sections 6 and 7).

UMTS Architecture & Storage of Secret Keys



UMTS architecture and storage of secret keys

Lawful Interception Configurations for 4G Networks



Figures 5-3. (5-3a – *top*): Interception model for LTE networks. (5-3b- *bottom*): Interception model for the support of non-3GPP subscribers (both figures based on [11]). Functions in the shaded boxes are implemented in the Aqsacom ALIS mediation platform (see Sections 6 and 7).

Lawful Interception of Telecom Networks

You can track any phone number from any country and anywhere in the world.

TACS

www.tacs.eu