LAWFUL INTERCEPTION FOR IP NETWORKS

White Paper

March 2010

Aqsacom Document No. 040451

Table of Contents

Aqsacom SA (Europe)
Les Conquerants, Bât B Everest
1 avenue de l'Atlantique
Les Ulis Courtabeouf Cedex
F-91976 France
Tel.+ 33 1 69 29 36 00
Fax +33 1 69 29 84 01

Aqsacom pty (Southeast Asia)
Suite 1009
530 Little Collins Street
Melbourne VIC 3000
Australia
Tel. +61 399 097 280
Fax +61 399 097 275

Aqsacom Inc. (Americas)
Washington, DC
Tel/fax +1 202 315 3943
New York +1 917 750 8614

Aqsacom (EMEA)
PO Box 125 139
Dubai, United Arab Emirates
Tel. +971 (0) 4 3990048
Fax +971 (0) 4 3990228

sales@aqsacom.com
www.aqsacom.com

Lawful Interception for Internet Protocol (IP) Networks

Aqsacom SA and Aqsacom Inc.

ABSTRACT

The proliferation of communications over networks based on Internet Protocol (IP) technology imposes ever growing challenges for Law Enforcement Agencies. This Aqsacom White Paper provides an introductory background on the issues behind lawful interception (LI) as applied to IP networks and their overlying applications, with emphasis on the dominant applications of E-mail and Voice-over-IP (VoIP).

1. Introduction

No amount of hyperbole can overestimate the overwhelming growth of traffic carried by the Internet during the last ten years. Perhaps more significant is the impact that IP networking has had on the behaviors of individuals and businesses, who now take E-mail, chat, social networking, Web-based information services, E-commerce, broadband film and video streaming, and even the making of telephone calls over the Internet as mundane tools of daily communications and information consumption. But given the popular acceptance of the Internet as a communications medium, there also comes a dark side to the Internet's power – namely the Internet's exploitation by criminals and terrorists. Here, illicit Internet activity can take the form of simple E-mail communications between criminal parties to invoke, for example, insider stock trading, drug deals, or terrorist acts. The widespread broadcast of spam and viruses is another form of criminal E-mail activity whose perpetrators can be held accountable through IP interception. Voice-Over-IP calls and audio/video streaming over the Internet could also carry criminal traffic that must be intercepted and analyzed to be of any value to the authorities.

Traditional lawful interception of telephone calls is relatively systematic, thanks to distinct network components handling signaling and content traffic within the telecom network infrastructure. Well-developed laws and procedures for the request and implementation of wiretaps in most countries of the developed world have also made lawful interception almost routine, in theory, for fixed line networks, perhaps with the added complication of location dependencies in mobile networks.

By contrast, intercepting Internet traffic has many added complications because:

- Target source and destination identities of the information flow are embedded within the overall flow of data, and must be carefully extracted to avoid detection by the target.

- Target and Non-target data are tightly intermingled in the bit flows at numerous points throughout the Internet. In addition, the circuits making up the Internet are not always well designed, rarely regulated, and often deployed in an ad hoc man-

ner. Therefore, privacy concerns arise since non-target data can erroneously become captured.

- Many parties are typically involved in transporting data over the Internet, including access providers on each end of the communications, transport operators, core network operators, and providers of services (e.g., E-mail). Furthermore, and unlike traditional telephony, these parties are unregulated and subject to their own business practices.

- In many countries, current laws on how to handle Internet interception are not clear. Interception efforts are often blocked by Internet Service Providers (ISPs) in the interest of protecting their customers[1], or just because it is easier to not provide interception.

- The separation of applications and relevant data from the overall data stream is not a trivial matter and requires significant software development and computing power, along with considerable trial and error.

- Encryption can make the extraction of application-level data extremely difficult, if not impossible for practical purposes.

- Lack of standards implementations. Most attempts at IP interception are carried out by esoteric organizations within government agencies. Although efforts are now beginning to make more routine the data interception and delivery process to LEAs, tools to analyze IP data still remain a cottage, R&D-like industry.

This White Paper attempts to discuss the above challenges in more detail, while presenting potential solutions to them through the use of new interception standards and methods to *mediate* the functions of interception and delivery of the resulting data to the LEAs. Many of the concepts discussed are based on the ETSI-recommended architecture for lawful interception, which is described in the next section. We then show how this architecture, combined with the classic OSI communications layer model, lay out fundamental approaches to lawful interception. Finally, we conclude with a discussion of representative IP interception examples and how these examples are addressed by Aqsacom.

[1] A good example is the recent case of the Recording Industry Association of America (RIAA) vs. Verizon (2003), where Verizon refused to hand over to the RIAA customer records of subscribers suspected of using file sharing software to exchange copyrighted music. See the Electronic Frontier Foundation's story at http://www.eff.org/Cases/RIAA_v_Verizon/. In France, subscribers were given somewhat of a protection against rights holding agencies through the "Haute Autorité pour la Diffusion des OEuvres et la Protection des Droits sur Internet (HADOPI)", which was passed in May of 2009. This law includes a "three strikes" provision that allows the ISP to cut off Internet access to persistent copyright infringers.

2. ETSI Model

Figure 2-1 depicts a highly general view of lawful interception architecture, as reflected in emerging standards that separate the functions of interception at network elements (NE) from delivery of the interception information to the LEAs [1]. This separation denotes a marked contrast to past lawful interception practices, where the monitoring tools used by the LEA were tightly coupled to proprietary switching platforms as provided by the switch vendors. Through the use of a mediation platform, LEAs can monitor traffic from different applications running on different networks built upon a diversity of equipment supplied by a diversity of vendors. The main advantage to the LEA is that they can make use of preferred interception analysis tools, independent of what switching equipment, underlying network technology, or application are running on a given network to be intercepted.

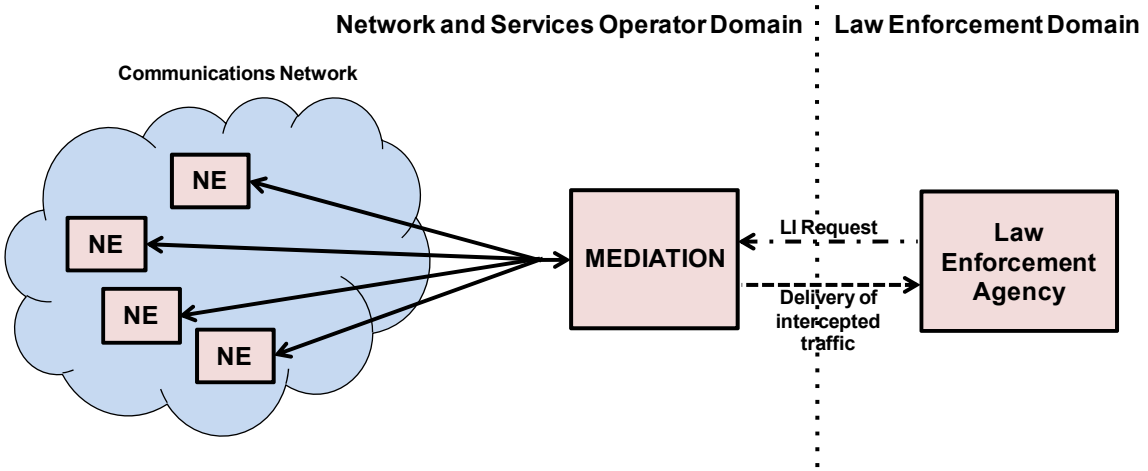


Figure 2-1. Simplified view of lawful interception architecture. Of primary interest is the use of a Mediation Platform to convey intercepted data from the network to the LEA.

A more detailed, yet still generalized architecture has been proposed by ETSI (European Telecommunications Standards Institute), as shown in Figure 2-2 [1]. Slight variations of this architecture, mainly in terminology, have been adapted by the Telecommunications Industry Association (TIA) as the basis of a safe-harbor approach to CALEA[2]. Standards setting bodies in numerous countries have also proposed similar, if not identical, models for recommended lawful interception architecture. This architecture attempts to define a systematic and extensible means by which network operators and LEAs can interact, especially as networks grow in sophistication and scope of services. Although originally

[2] Communications Assistance for Law Enforcement Act. CALEA was an act of US Congress, passed in 1994, in response to the proliferation of wireless networks and growing sophistication of wireline networks. It has attempted to define measures that carriers must take to convey lawful intercept information to LEAs. All telephone service operators, wireline and wireless, are to have complied with this law by the middle 2003. Standards for technical implementation of CALEA-directives were established by the TIA and presented as the J-STD-025A (and now B) standard (see [3] for the updated standard). FCC interpretations of the law have been published in Oct 2005 to include facilities-based broadband networks and VOIP networks interconnected to public switched telephone networks.

oriented towards telecom voice traffic, the architecture has equal practicality for the interception of IP data. Nevertheless, for consistency, much of the legacy terminology associated with switched voice calling remain.

Of particular note in this architecture is the separation of:

a) lawful interception management functions (mainly session set-up and tear down, as demanded from the courts and in some cases the LEA),
b) extraction of intercepted data from network elements, and
c) the interception-related data (e.g., destination of data, source of data, time of the transmission, duration, etc.) from the content contained in the data when conveying the overall interception data from the network operator to the LEA.

Communications between the network operator and LEA are via the Handover Interfaces (designated **HI**). **Handover Interface 1** (**HI1**) supports the provisioning of the interception order via the **Administration Function**. **Handover Interface 2** (**HI2**) supports the delivery of **Intercept Related Information** (**IRI;** e.g., destination of call, source of a call, time of the call, duration, etc.) from the network to the LEA. **Handover Interface 3** (**HI3**) supports the delivery of the **Content of Communications** (**CC**) from the network to the LEA.

The core element of Figure 2-2 is the "Interception Mediation" which carries out the following functions and safeguards:

- Collection of intercepted data from various switches, routers, probes, etc. in the network.
- Formats the data into standardized representations.
- Delivers of the data to one or more LEAs.
- Ensures that a given LEA is authorized to accept the delivered data.
- Protects of all delivered information against unauthorized access and modification through rigorous network security.
- Prevents access to all network elements through "backdoor" attacks.
- Delivers of the interception information in a timely manner, with appropriate time stamps to synchronize network events against content delivered

Aqsacom addresses the functions of the Interception Mediation through its ALIS mediation platform (discussed in Section 6). The Interception Mediation carries out the functions of what is often known as the *delivery function*.

Figure 2-2 also indicates that traffic can be collected through an **Internal Interception Function** (IIF) or **External Interception Function** (EIF). The IIF makes use of internal collection capabilities of the network elements. Sometimes these are adequate to meet the LEA requirements. When the IIF is substandard or not available, the NWO/SP needs to make use of the EIF, which is implemented through a probe. Aqsacom supports both types of collection functions.

Finally, Figure 2-2 shows an additional handover interface called **HI-a**. Although this is not formally part of the ETSI architecture, it is included here because of the importance of alarms and other feedback to the LEA concerning the progress of the interception.

The ETSI model has direct relevance to the interception of data flows through IP and other types of packet networks. This relevance can be viewed through the OSI model, which will be discussed in the next section.

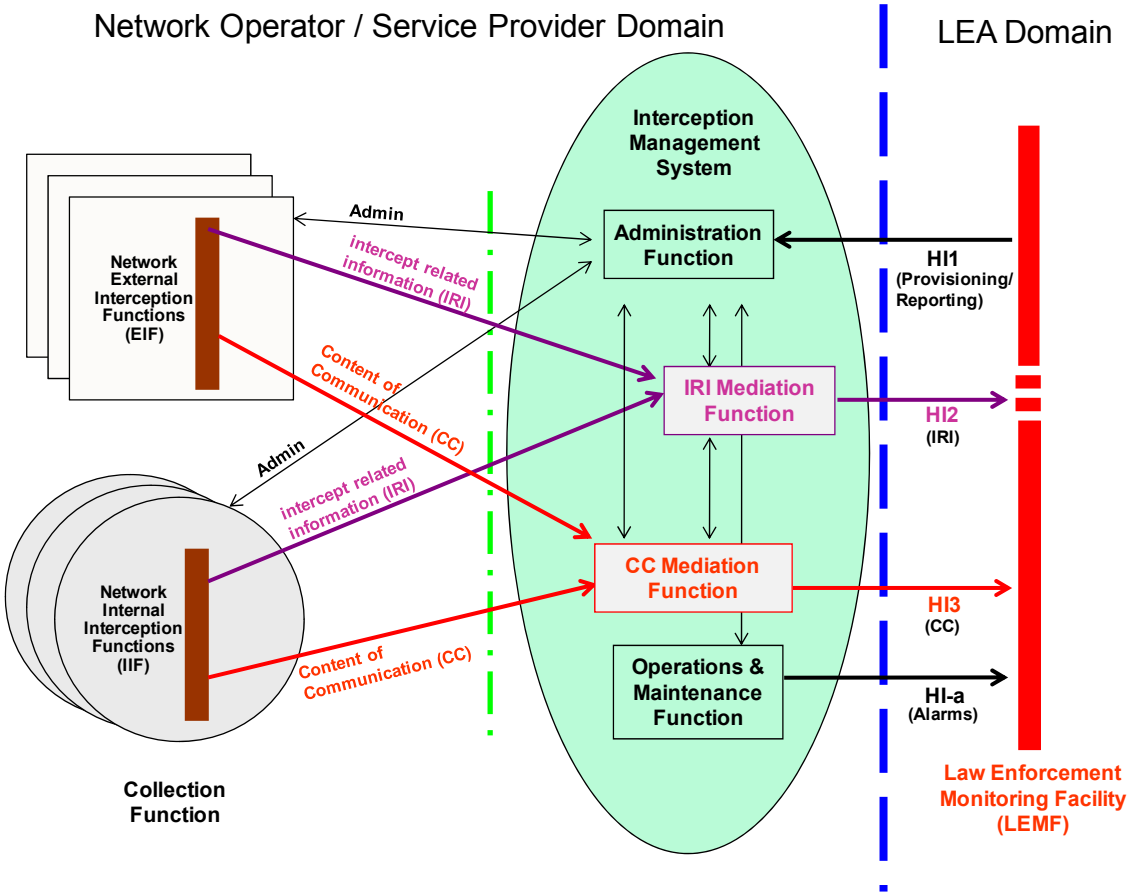


Figure 2-2. ETSI-developed architecture for lawful interception. Note the separation of lawful interception management functions (HI1), call-related data (HI2), and call content (HI3) in the interaction between the LEA and communication service provider (based on [1]; also see [2]). Call Data Channel 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.

3. Open Systems Interconnection (OSI) Model

The OSI model was proposed during the 1970s by the International Standards Organization (ISO) as a means for facilitating the intercommunications of packet network equipment from diverse manufacturers. This model also supports the interaction between applications riding on the network infrastructure supported by such equipment. Because the model calls for the independent operation of its layers, application developers and equipment vendors can separately address each layer in their respective product offers. As we shall see in this section, the concepts behind the OSI model are highly relevant to lawful interception and the ETSI model previously discussed.

Seven layers compose the OSI model (Figure 3-1). These layers are briefly described as follows [4]:

Layer 7: Application

This layer defines how applications communicate with each other over the network. Typical applications include E-mail, file transfer, remote database queries, and remote terminal access. Common protocols operating at Layer 7 include FTP, Telnet, POP3, SNMP, DHCP, HTTP, NFS, and X Windows. As we shall discuss, lawful interception at the application level can reveal information exchanged by targets running such applications; however, the application data may not necessarily be readily available from applications servers responsible for managing such applications.

Layer 6: Presentation

Layer 6 mainly concerns the format of the data exchanged. These formats include text (e.g., ASCII), graphic (GIF, TIFF, JPEG), and audio-visual (MPEG). Layer 6 interception is closely aligned with Layer 7 Application interception; i.e., intercepted data formats from specific applications are defined through Layer 6.

Layer 5: Session

This layer controls the setup and termination of communications sessions, as well as the transfer mode of the data (simplex, half duplex, full duplex). When content is extracted from a communications link, it is necessary to determine the transfer mode for lower level interceptions.

Layer 4: Transport

The Transport layer establishes the connection between two hosts, in effect creating a virtual circuit. The most common protocol supporting this layer is Transport Control Protocol (TCP), which assures a solid connection between hosts through data flow control, error detection, and packet reception acknowledgment. Another popular transport layer protocol is the Universal Datagram Protocol (UDP). UDP is much lighter than TCP and does not have transport acknowledgement, thus it moves packets while "hoping for the best" in their delivery to the destination. Nevertheless, UDP is useful for supporting applications such as streamed voice and video, where point-to-point (or multipoint) data transfer must occur fast and with a minimum of latency. TCP and UDP protocols present important IRI data to the LEAs, including source and destination port addresses, as will be discussed below.

Layer 3: Network

This layer defines how data between hosts are to be routed to each other over one or several networks. The most common protocol operating at this layer is Internet Protocol (IP). The IP header contains critical information for lawful interception, such as the source and destination IP addresses.

Layer 2: Data Link

This layer moves the IP packets (known as "datagrams") between hosts. It is described by a number of protocols, including Ethernet, ATM, frame relay, Token Ring, etc.

Layer 1: Physical

Layer 1 represents the electrical signaling characteristics, modulation schemes, connector pin layouts, etc. making up the networking infrastructure. Note that traditional voice interception had operated at this layer through physical wiretaps.

Figure 3-1 also indicates what types of devices are responsible for supporting a given layer.

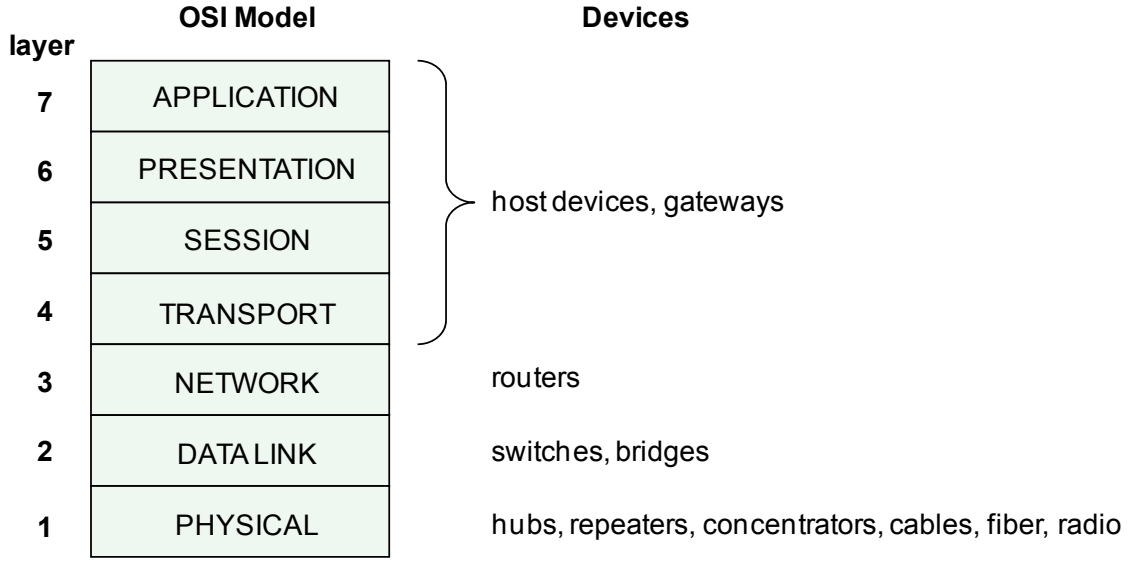


Figure 3-1. OSI 7-Layer model for packet-based communications. Typical devices that support each layer are indicated on the right.

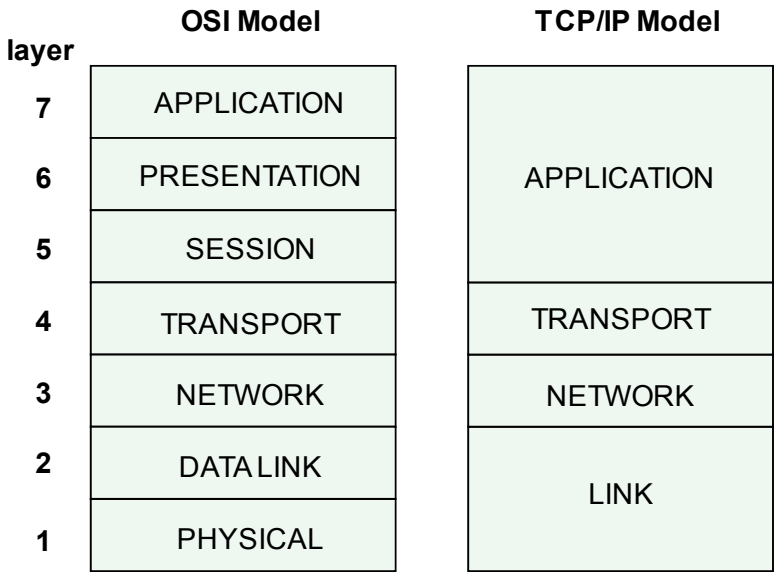


Figure 3-2. Reduction of 7-Layer OSI model into 4-layer TCP/IP Model.

The TCP/IP network representation reduces the OSI model to 4 layers. Here, Layers 5, 6, and 7 of the OSI model are condensed into a single "Application" layer, while the Data Link and Physical layers are condensed into a single "Link" layer (see Figure 3-2). From a conceptual point of view, this layer reduction might make the operation of packet interception less clear. This is because the OSI layers can provide some indication of what type of information can be extracted from Internet traffic. More specifically (Figure 3-3):

Layer 7:

Applications can be designed to hand over Intercept Related Information and content directly to the HI2 and HI3 handover interfaces, respectively. In effect, this is the process behind voice interception on TDM networks. Unfortunately for the LEAs, this is often not the case; either the platforms do not have capabilities to output intercepted data and/or the service providers are reluctant to cooperate with the LEAs for privacy and/or financial reasons.

Layer 6:

Given that this layer represents application data, this layer would feed content to the LEA via the HI3 handover interface.

Layer 5:

Session control data are routed through HI2. Extraction can occur from the host computer or device initiating, terminating, and managing the session. In a typical interception configuration, the host manages Internet access in conjunction with a RADIUS server [5].

Layer 4:

Transport information in TCP or UDP datagrams can in theory be extracted from the communicating host or device managing the virtual circuit. Pertinent information would include port numbers of the originating and receiving hosts in the target's data exchange. However, appropriate interfaces to directly extract such information from the hosts cannot be, and in practice usually are not, assured.

Layer 3:

Direct IP packet interception occurs at this level. Such a function is usually performed by a router with a port dedicated to replicating packets having the target's source and destination IP addresses. The packet flow from this port is then sent to a mediation device, where content and intercept information are separated, formatted, and sent to the LEA for further analysis.

Layer 2:

Interception, in theory, can take place at devices supporting ATM switching, frame relay routing, Ethernet, etc. where the target's identifying information is related to packets possessing designated origination or destination hardware addresses. However, considerable effort remains in reassembling higher layer packets to gain target-specific content and intercept related information.

Layer 1:

This calls for the direct "tapping" of network infrastructure at the media level, whether the medium is wire, fiber, or radio wave. Appropriate hardware interfaces are necessary to extract the information while minimizing interference with network performance. Once extracted, the signals must be converted back to bit streams. The analysis process carried out by the LEA must reconstruct higher layer packets from the bitstreams, which is not a trivial process especially when packet reconstruction must occur in real time and / or when any of the higher layers undergo encryption.

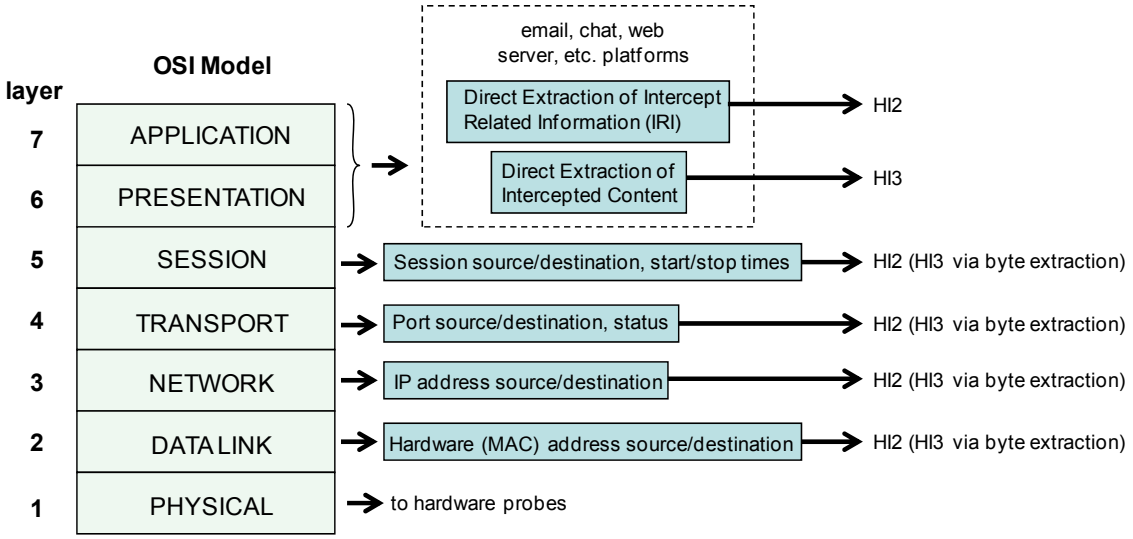


Figure 3-3. Relationship of OSI layers with Lawful Interception information and data extraction. In practice for interception, Layer 6 is combined with Layer 7. Layer 3 (IP) serves as the basis of intercepted communications in lieu of Layer 4. Layers 2 and 1 can yield useful results when network elements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

4. Other Issues in IP Interception

4.1 Network Services vs. Network Access

In the discipline of Lawful Interception, it is important to distinguish between *Network Access* and *Network Services*. For the purposes of this document, Network Access is typically managed by the Network Access Provider (AP), who's infrastructure often (but now always) relies on that of the Network Operator (NWO), such as the incumbent telecom operator, local cable TV service, or wireless services operator. Access operates at all levels of the OSI model, from access authorization to session transport to the overall public Internet [6]. In contrast, Network Services (such as E-mail, chat, VOIP, etc.) may be provided by the Network Operator or a third party service organization (designated Service Provider or SP). For example, popular E-mail services such as Hotmail and Gmail, as well as instant messaging services such as Microsoft Windows Messenger and AOL Instant Messenger, are offered by service organizations – not Network Operators / Access Providers. Network services are mainly focused at Layers 6 and 7, although lower levels can also be implicated (as in commercial or private VPN implementations based on IPSec). Figure 4-1 attempts to illustrate the distinction between Service Providers and Network Access Provider / Network Operators. In the context of lawful interception, LEAs often must interact with both the providers of Network Access and Network Services to intercept target data.

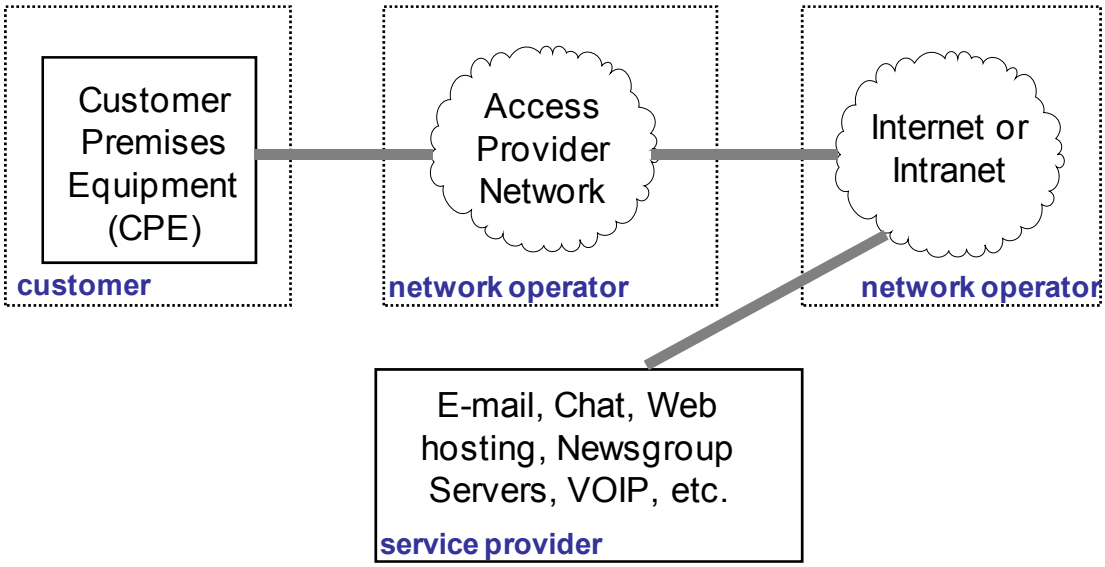


Figure 4-1. Separation of network access, core network, and service provider functions. The Network Operator can be an incumbent telecom operator (e.g., supplying DSL services over existing local loop copper), cable TV operator, etc. The core Internet or managed Intranet is operated by a Network Operator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

4.2 Delivery of Intercepted Information to the LEA

The transport of information between the NWO/SP and the LEA must ensure secure data flow that encompasses:

- *Authentication:* The LEA is who they say they are when attempting to gain access to the interception network and data. This prevents a rogue organization from performing interceptions while disguising itself as a LEA. Two-way authentication would also ensure that the intercepts are coming from the NWO/SP that is specified in the interception order.

- *Confidentiality:* This assures that no third party can eavesdrop on the transmitted data.

- *Integrity:* This assures that the data were not corrupted through deliberate modification or by transmission error.

- *Non-repudiation:* The NWO or SP cannot deny having sent the interception request to the LEA.

Of course, protective measures on the side of the NWO and SP must be in place at the edge of, and within, their respective networks and systems. In addition, the data flow cannot be interrupted and dropped, and must have sufficient buffering in the event of a transmission disruption between the LEA and network/service.

Interception data are delivered from the NWO and/or SP provider to the LEA via a number of means, including:

- *Private, dedicated circuits.* This is the most secure method of delivery, but has the drawback of higher cost on the part of the LEA who usually must pay for the dedicated line. On the other hand, this type of service can in some configurations bring revenue to the NWO, and thereby helps to offset the cost of the interception.

- *Secure circuits over a public network.* These networks include VPNs (Virtual Private Networks) running over the public Internet but with the necessary encryption and authentication control to ensure confidential data delivery. Other networks in this class are X.25 packet networks.

- *Public Networks, no security.* Here, interception information is delivered via an Internet connection. There is no inherent protection of the data. If the data traffic is light, stand-alone encryption can be applied for a semi-secure solution.

- *ISDN.* ISDN remains a reliable and secure means of delivering intercepted IP traffic to the LEA.

4.3 Internal vs. External Interception

Depending on accessibility to network system components, LEAs request IP interception through processes internal or external to the networks that carry the traffic and applications of a target under surveillance. Internal interception generally requires the cooperation of the NWO/SP and LEA, whereas the LEA may resort to external interception when direct physical or legal access to the NWO/SP's networking is not possible.

Internal interception enables the LEA, via the mediation platform and handover interfaces described in Sections 2 and 6, to extract Intercept Related Information (IRI – otherwise known as Call Data) and the target's Content Data *directly from* application servers (e.g., E-mail, Web, chat), network access systems (e.g., RADIUS server system), DSL/Cable modem termination points, routers, switches, etc. that are all part of the NWO's or SP's infrastructure. Internal interception of application platforms has the obvious advantage of *directly* delivering target data to the mediation platform because the application is inherently known, and the interception data are explicitly provided. Interception of internal network transport elements also narrows the network traffic originating from or going to specific targets.

Internal interception typically makes use of the Internal Interception Function (IIF) described in Section 2, when the IIFs of the network equipment and application servers are available or adequate to satisfy the LI requirements. Likewise, internal interception can make use of the External Interception Function (EIF) if the IIF is not available or deemed inadequate to support the volume of traffic to be intercepted. Use of an EIF would imply the application of a network probe within the NWO's or SP's network.

Note internal interception carries two strong assumptions that might not be valid. First, we assume that targeted IRI and content data from selected network and applications systems are available to the LEA, perhaps as mandated by local/national regulations. Second, the network and applications systems must support secure data paths to the mediation platform (e.g., mail servers must output targeted header and content information directly to the interception mediation platform). However, such assumptions may not hold. In many developed countries, ISPs are often reluctant to open their networks to LEAs without considerable legal fighting; hence, the ISP operations are not readily adaptable to systematic lawful interception. Perhaps even more problematic are the current applications systems in place, which by their design and implementation are not readily conducive to interception. For example, most E-mail servers handling large volumes of E-mail still must be modified if they are to provide systematic delivery of targeted IRI and content through purpose-built ports dedicated to secure interception data conveyance. This is not a trivial undertaking, especially when interception ports have to also accommodate requisite network security to protect the transport of interception data and prevent "back door" attacks into the system. Finally, mechanisms must be in place to prevent potential targets from detecting that their data flows are being intercepted; this implies the need for secure application design.

When the availability of internal interception fails, or when LEAs desire to conduct clandestine surveillance, interception needs to take place at network levels outside the realm

of the target's immediate application service or network provider. In other words, *external interception* must be performed. Such interception is performed on Internet circuits outside the target's immediate network, typically at adjacent networks or major public network concentration points. The core equipment typically includes a router with filtering capabilities, or custom hardware. In the case of a router, its Internal Interception Function capability might be used. Alternatively, External Interception Function methods involving probes are applied to collect the targeted traffic. Such probes can be constructed with PCs containing network interface cards, or they can be derived from wireless base stations for the external interception of wireless data networks (e.g., Wi-Fi). Probes typically replicate traffic flow through a network point at the physical layer; the filter targets packets containing specified IP addresses or IP address ranges and routes them to a port dedicated to interception purposes. From there, packets are routed to the mediation platform and ultimately to the LEA for analysis of datagram headers and content.

Systems that perform external interception tend to be sophisticated and not officially publicized. Where traffic is light, open source protocol analysis programs such as *Wireshark* [8] can assist in analyzing the protocols and content of data traversing a given path.

Targets must not be able to know that they are the subject of surveillance. Minimally sophisticated targets could at least suspect interception of some kind is underway through:

- *Trace route commands.* These display the router hops that a subject's Internet traffic traverses to/from a given destination. Any change from the ordinary could imply the introduction of an interception router or other device. However, the proper use of interception probes can avoid the introduction of new router hops.

- *Unusual signaling activity* in their modem, Voice-Over-IP interface box, or other hardware. These devices carry important identification and traffic information associated with the user, but can reveal interception activity to the interception target. Therefore it is not recommended that the LI process probe customer premises equipment (CPE); this process poses risks for the LEAs especially when the devices are tampered with by the users.

- *Degradation or interruptions of service*. These are obvious factors in arousing suspicion by the targets that surveillance might be taking place.

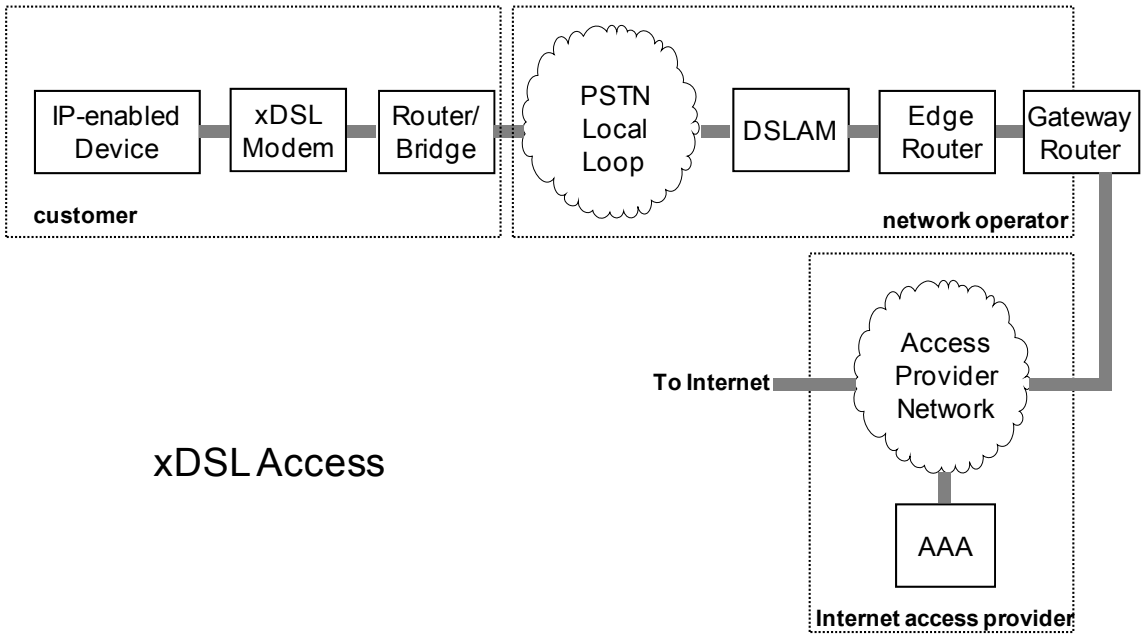
5. IP Interception Examples

5.1 Internet Access

Figure 5-1 depicts typical access configurations for xDSL, dial-up, cable modem, and Wi-Fi[3]. All access methods perform the overall function of network access, which connects the subscriber-user to the public Internet, various network-based services (e.g., E-mail, chat), or to private networks that are based on IP or other network technologies. Access to the network is typically performed along with the sequence of Authentication, Authorization, and Accounting (AAA). Authentication confirms that the user is who they say they are (such as through a password, a physical token device such as a smart card, or biometric data). Authorization controls what the user can do once they are authenticated; this includes connecting to the network, accessing E-mail, etc. Accounting refers to the process of looking up the user's subscriber records to ensure that his/her account is paid up and billed for services rendered. Likewise, Accounting can debit prepaid accounts as network services are consumed (e.g., in Voice over IP calling). AAA functions are typically managed by the network operator through a RADIUS server and associated protocol [5].

Not shown are wireless services offered by the public wireless carriers. *Interception of these networks is discussed in the Aqsacom White Paper Lawful Interception for 3G and 4G Networks*.

[3] The term Wi-Fi is a trademark of the Wi-Fi Alliance, a group of industry players advancing the deployment of 802.11 systems and their compatibility.



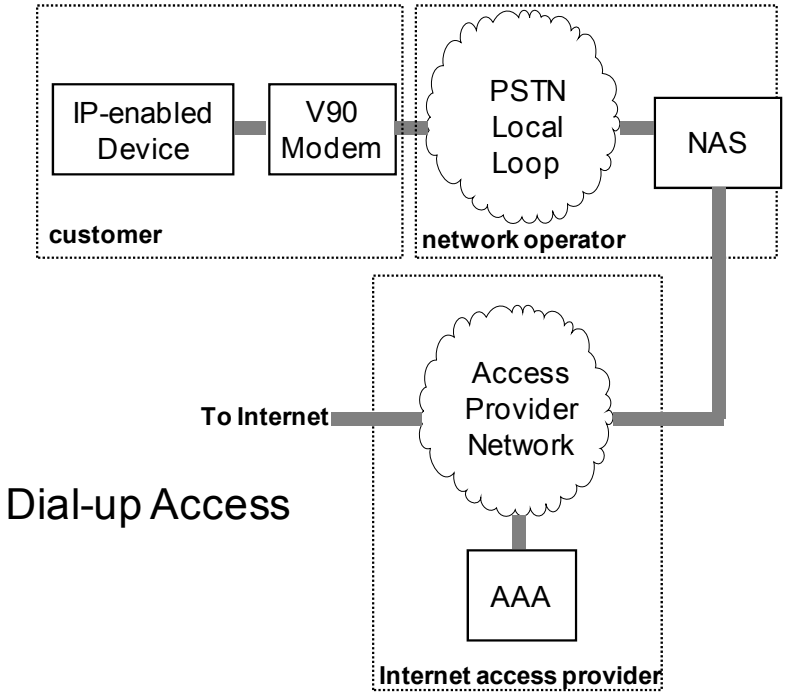
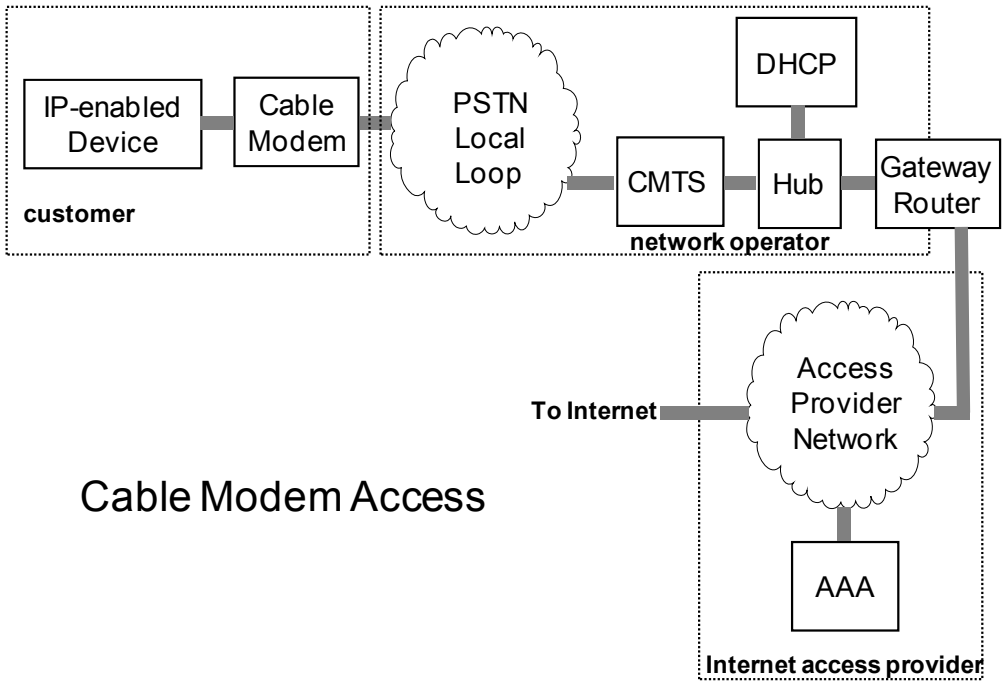


Figure 5-1 (carried to next page). Typical configurations for xDSL, Dial-up, and Cable Modem, Wi-Fi Internet access (derived from [7]).



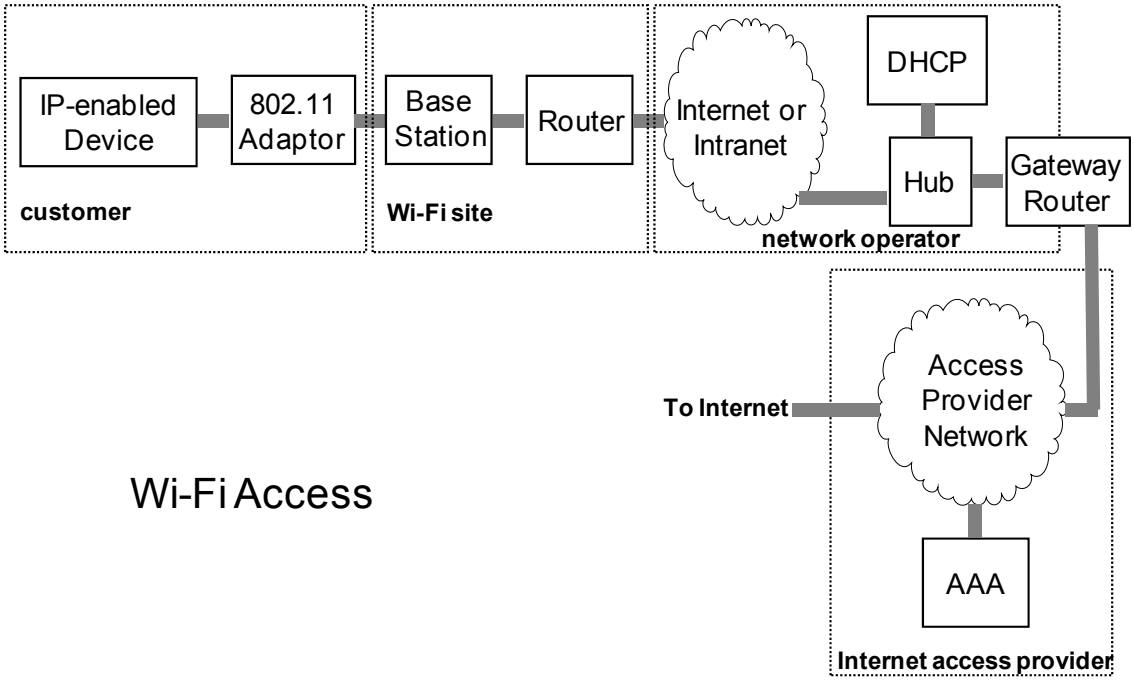


Figure 5-1 (continued). Typical configurations for xDSL, Dial-up, and Cable Modem, Wi-Fi Internet access (derived from [7]).

5.1.1 Internet Access Target Identification

The lawful interception of packet-based data flows begin by specifying the target of the interception session. However, unlike traditional voice interception where the target can be identified by a telephone number, a process needs to be invoked that matches the target's assigned IP address or other unique identifier to the target's identity. The IP address assignment may be dynamic as in dial-up, as well as in consumer/small business-oriented xDSL, cable modem , and Wi-Fi access services; therefore, the LEA must conduct coordinated interception in conjunction with the network operator. IP addresses are typically assigned through the use of DHCP [9], in conjunction with the AAA functions of the RADIUS server. Here, the RADIUS aids the LEA in identifying the target, while the DHCP process provides the LEA with the target's corresponding IP address. Interception occurs between the moments of assignment and de-assignment of the targeted user IP address. In addition, the interception of AAA packets is typically performed using a probe.

Public Internet access services oriented towards business customers usually make use of fixed IP addresses assigned to customers. The access technologies are typically dedicated T1 or fractional T1 line, xDSL, and to a growing extent, cable modem and direct fiber links. In these cases, the LEA relies on a set of permanent IP addresses as provided by the network operator.

Other target identifiers include [7]:

- Username and Network Access identifier [10]
- Ethernet address (Layer 2)
- Dial-in calling number identity
- Cable modem identifier
- MAC addresses (for other modem and wireless devices)
- Other unique identifiers agreed upon between network provider and LEA

Note that the Ethernet and cable modem identifier are related to the physical devices of the user, which must be linked to an authorization process to remain effective as spoof-free identifiers to LEAs – in other words, a target should not be allowed to hide their connection to the network by using a stolen or tampered cable modem that is connected to their usual cable TV wiring.

5.1.2 Collected Data

Call Data (or Intercept Related Information) sent to the LEA over the HI2 Handover Interface include the following [7]:

- Identity of target (using, for example, one or more of the above target identifiers)
- Services and access privileges of the target
- Time of network access attempt by target
- Time network access is successfully made or denied
- Change in network status
- Change in network access location

As for the Content of Communication (CC; conveyed via the Content Communication Channel or CCC under CALEA), relevant interception data delivered to the LEA via the HI3 Handover Interface contain the datagrams of the targeted data, including source and destination IP addresses (even though these addresses, technically, are also considered Call Data).

It is important that the LEA not become the victim of IP address spoofing, such as when the target's IP address replaces another party's source or destination address. This tricks the LEA into believing that they are intercepting data to or from the target, when the data is really associated with a non-targeted party. Such spoofing can be reasonably easy to prevent for packets originating from the target by probing the appropriate internal network points, which in theory should not allow for IP datagram modification. However, packets falsely destined towards the target from outside the target's immediate network are more difficult to validate. Here, the LEA may have to resort to route tracing, gateway analysis, and possibly lower level OSI layer analysis to ascertain the origin of such packets. The same holds for determining the origination of parties who attempt to spoof their origination addresses and send IP data to the target.

5.1.3 Lawful Interception Configurations for Network Access

The previous diagrams of Figure 5-1 are updated in Figure 5-2 to indicate the many interception points available to the network operator and LEA. The given interception points are represented only for suggestion, with only one or a couple to be put to needed use depending on network element availability, cost, and other factors. All interception points route their Call Data (**D**) and Content Data (**C**) to a mediation platform which, in turn, routes this data to the LEA via the HI2 and HI3 Handover Interfaces. Specific implementations of the Aqsacom ALIS mediation platform for these networks are discussed in Section 6. Not shown are management functions (discussed in Section 6). All indicated interception points implement internal interception by applying probes and/or networking interfaces to local networks, access loops, routers, gateways, AAA functions, etc. External interception is indicated at the level of the public Internet, beyond the immediate access network.

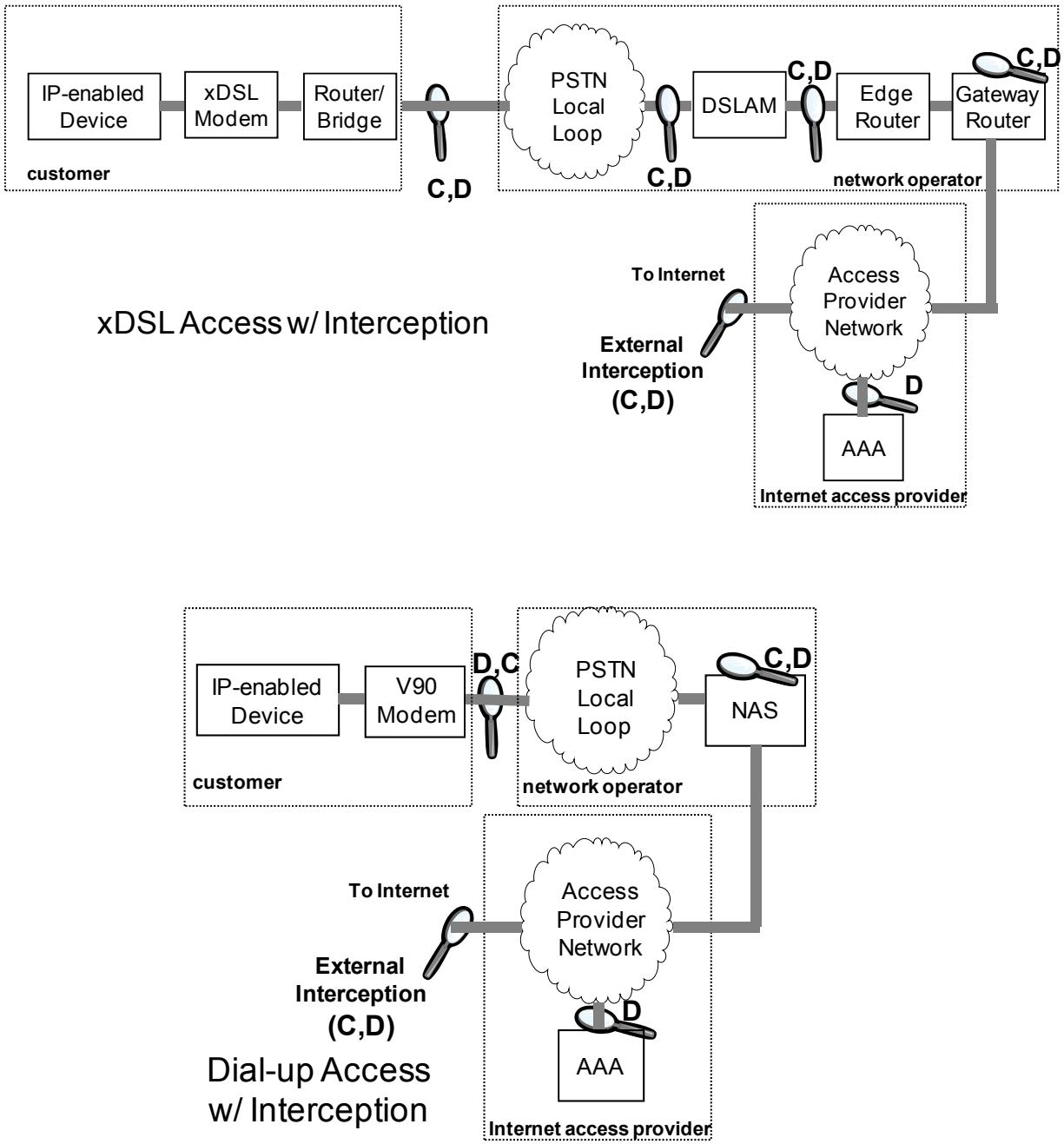
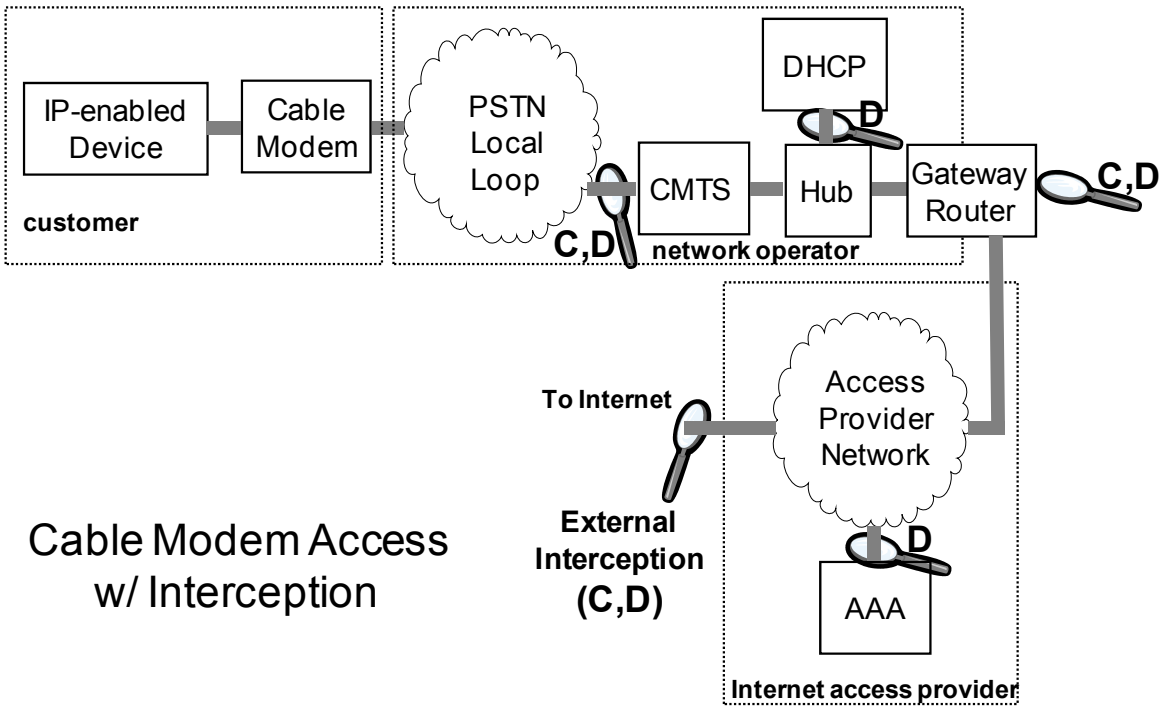


Figure 5-2. Internet access interception points. **C** and **D** denote intercepted content and session-related data, respectively.



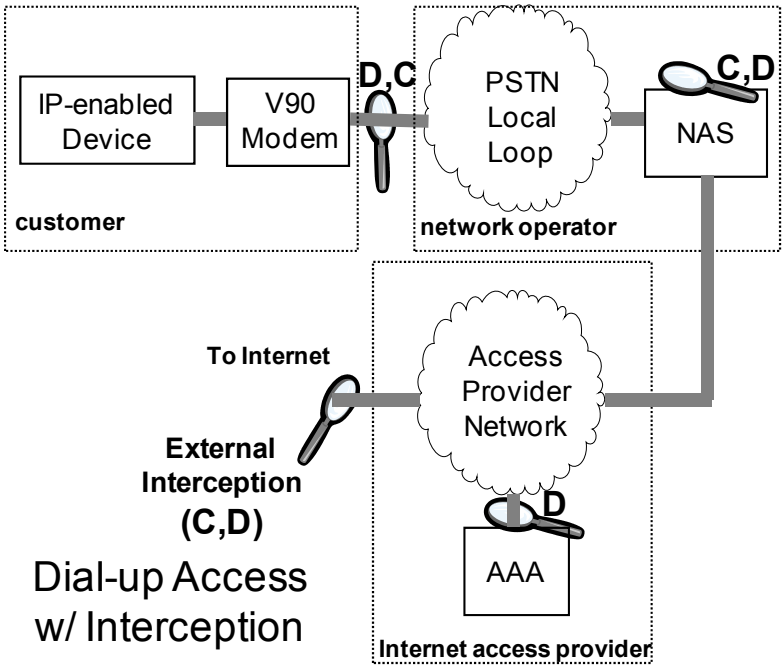


Figure 5-2 (continued). Internet access interception points. **C** and **D** denote intercepted content and session-related data, respectively.

5.2 E-Mail

Given E-mail's role as an essential mode of communications, it is only logical that LEAs and Internet Service Providers be given the tools to carry out lawful interception of E-mail traffic. Of equal interest is the growing problem of unwanted bulk E-mails ("spam"), which now constitute over half of all E-mail messages. Here, lawful interception can play a crucial role in the detection, tracking, and reduction of this menace. E-mail interception for lawful purposes can be understood by first looking the typical steps undertaken by the Simple Mail Transfer Protocol (SMTP) to convey an E-mail message (other E-mail protocols follow a similar process). Note the description to follow is highly simplified, and omits the detail of message exchanges within the protocol. Figure 5-3 shows the process.

(a) User **A** enters a message for User **B** via his/her E-mail client on a personal computer, portable device, or within a Web site. The E-mail client then forwards the message via SMTP to a designated server (known as a Mail Transfer Agent or MTA) which handles all outgoing E-mail from that user.

(b) Client **A**'s server routes the E-mail to the destination server which handles User **B**'s incoming E-mail. The routing is determined through a DNS lookup that matches the destination's E-mail domain name to an IP address. Alternatively, the message can be routed through one or more intermediate "relay" servers (see path "b-alt") for the purposes of network traffic routing (e.g., gateways), or in attempts to hide the identity and location of User **A**.

(c) Client **B** typically extracts the incoming E-mail from its assigned server via POP3 or IMAP protocol. POP3 and IMAP manage the process of downloading the E-mail into Client **B** for access by its user.

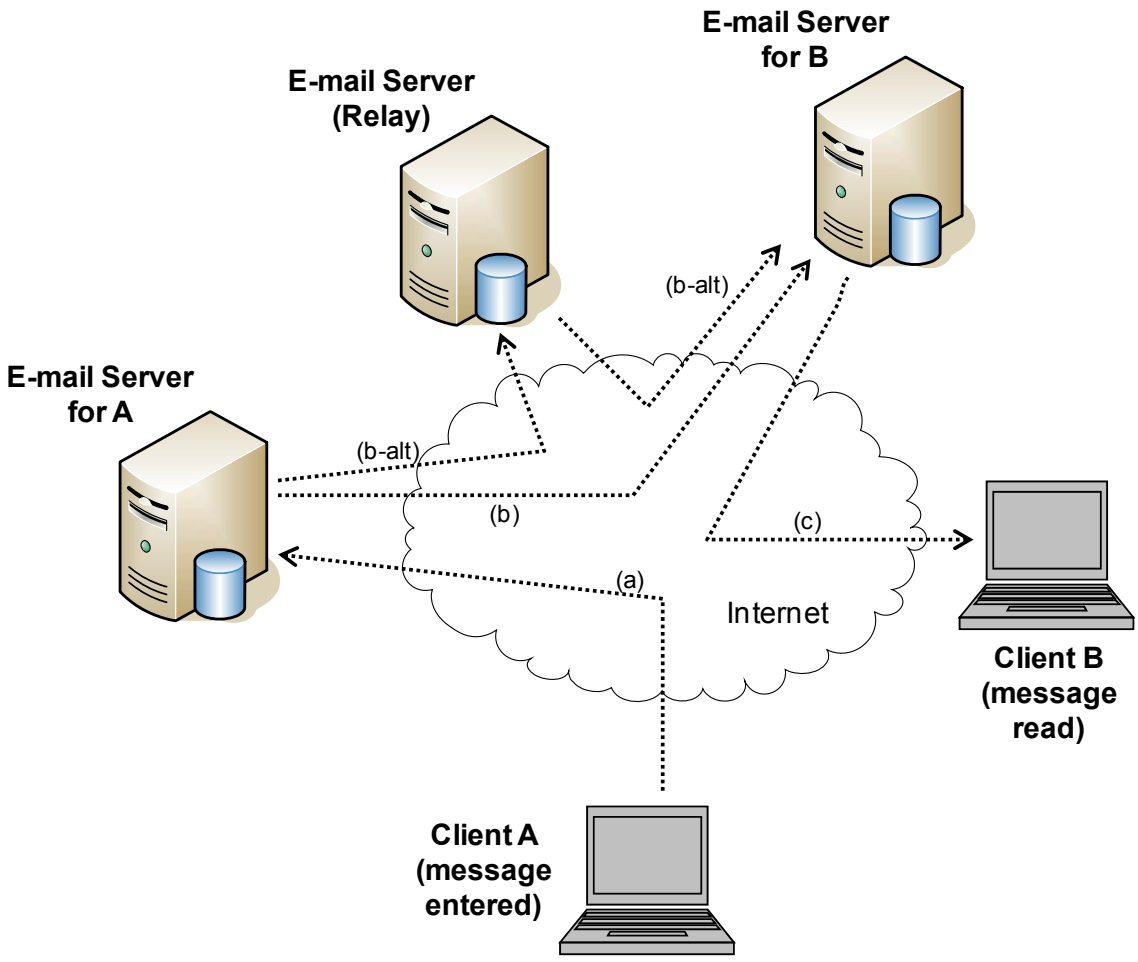


Figure 5-3. The process of sending an E-mail message via SMTP (and similar other) protocol. See text for details of each step.

Without going into the details of SMTP, IMAP, or POP3, suffice it to say that there is considerable information embedded within the headers of E-mail messages based on these protocols. This information includes:

- Server IP
- Client IP
- Server Port
- Client Port
- E mail Protocol ID
- E mail Sender
- E mail Recipient List
- Total Recipient Count
- Server Octets Sent
- Client Octets Sent
- Message ID
- Status

All of the above constitutes IRI data to be made available to the LEA [11].

An Internal Interception Function, in theory, can be applied within any E-mail server in the above described paths to identify targeted E-mail traffic and route the corresponding IRI/CD information to the mediation platform (Figure 5-4). Through appropriate parsing outside of the E-mail servers by use of a probe (External Interception Function), E-mail content can also be directly extracted from the E-mail servers. Of course, if the content is encrypted by the user or E-mail service, added efforts to decrypt the message need to be considered. Generally, ETSI and other standards require that:

- When a network operator or a service provider encrypts the E-mail data, it is the responsibility of the network operator or service provider to decipher the data before sending the information to the LEA.

- When the subscriber encrypts the E-mail data, the network operator or service provider shall send to the LEA the ciphered data. It is then the responsibility of the LEA to decipher the data.

Many E-mail servers do not allow for separate interception ports. Thus we have the issue of relying on the service provider to equip their operation with updated servers that support LEAs. Such service providers will also have to maintain the servers and ensure their security against intrusion.

One might ask: why not simply augment E-mail messages with a blind copy (bcc) to the LEA? This is not recommended because a) this method only acts on the server originating the E-mail (when multiple servers in the E-mail chain might be intercepted), b) this method is prone to operator error whereas LI methods that are well engineered are more resistant to operator error, c) the bcc would not necessarily be secure in reaching the LEA, and d) the addition of a bcc constitutes tampering of the E-mail message by the authorities, resulting in risk of exposure or violation of law. Thus, interception should be performed in a manner detached from manipulation of the E-mail message.

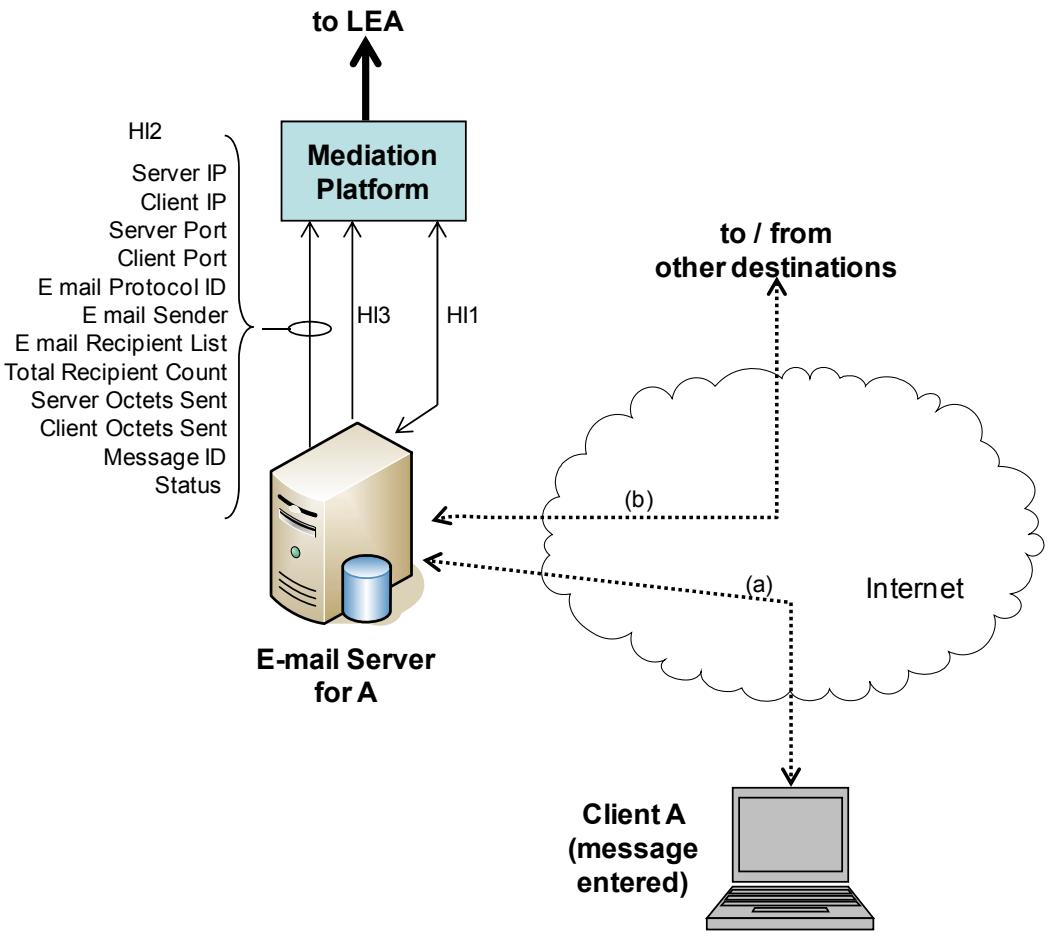


Figure 5-4. Interception of E-mail. Here an Internal or External Interception Function is illustrated since all action is at the level of the E-mail server operating on behalf of target **A**.

5.2.1 Spam

Unsolicited E-mail, otherwise known as "spam," impacts the LEA in two ways. First, the LEAs must ensure that their own interception operations are not misguided by modifications to headers in the target E-mail information that they receive. Second, LEAs can play a role in detecting spam, and in seeking spam's perpetrators.

The first problem relates to weaknesses in the SMTP and other common E-mail protocols. Users often can easily modify "From" mailbox addresses and "Reply To" addresses at the E-mail client level. Therefore, reliance on "From" and "Reply-To" fields is hardly a good practice for identifying the sender of a targeted E-mail; the interception target could falsely be specified as the source, or the target may attempt to hide themselves as the source. A more rigorous approach is to make use of the target's assigned IP address as an identifier of the E-mail, while performing interception at the level of the target E-mail server, which is confirmed to be free of defect from viruses. Nevertheless, even this latter approach is not failsafe in that rogue E-mail servers (including those hijacked by viruses) can create false message origination IP addresses.

At present, there are a number of initiatives underway to block spam that is sent with falsified headers. One group of methods attempt to authenticate the origination of the E-mail by matching the "From" domain name with the originating IP address range through a reverse DNS look-up (e.g., the Sender Policy Framework – now IETF RFC 4408). Reverse DNS look-up practices should be employed by the LEAs now, while leveraging the standardized approaches as they become available. Another means for confirming the authenticity of E-mail origination is through the use of consistency checks in header information corresponding to E-mail threads. Unfortunately, headers are not always preserved in message threads, thus making this method of limited value. Finally, LEAs should subscribe to E-mail blacklists that are compiled and disseminated regularly by nonprofit and commercial spam-prevention services (e.g., www.senderbase.com). These lists maintain updated lists of spam origination addresses, subject headings, and other information that are broadcasted to E-mail servers and filtering appliances. Such lists provide an added defense of the LEA against spam. Note that fighting spam cannot be won by any single method; it is best controlled through a mix of measures.

5.3 Voice-over-IP (VoIP)

Voice-over-IP (VoIP) represents a specific technology falling under the broader *Voice-over-Packet* (VOP) category of technology. However, given the popularity of the term VoIP, it is perhaps recognized more as a type of telephone service than a facilitating technology. VoIP originally drew interest as a means of bypassing traditional telephone networks for the placement of international calls, especially between Western nations and developing countries, the latter known to impose high long distance and international tariffs. However, the deployment of broadband access, improvements in codec technology, converging standards, and increased enterprise interest in the technology have made VoIP a mainstream technology for placing both local and long distance voice calls. VoIP calling can take place over a variety of network topologies and among a variety of user groups. We describe representative examples of these topologies and users as follows:

Phone-to-Phone for Consumer and Small Business

This group consists of services that for a fee (and sometimes free) enable customers to place calls over IP networks. These networks employ "softswitches," account management platforms (i.e., gatekeepers), and gateways that control the placement of voice calls between the traditional telephone network and IP networks. Phone-to-Phone dialing may occur with the traditional PSTN (Public Switched Telecommunications Network) acting as transport between the user telephones and gateways to the IP networking. Likewise, Phone-to-Phone can be supported via direct IP access, where the users have at their premises a VoIP interface that connects to their broadband Internet access service (typically xDSL, cable modem, dedicated line, or Wi-Fi service). Such a device allows the user to bypass the PSTN, at least on their end. Companies such as Vonage and notably cable TV operators are offering this form of VoIP service (in some cases, the VoIP interface is built into the cable modem box). The IP networking may consist of a) privately managed IP networks to ensure quality of service (as implemented by the cable operators), b) the public Internet, where quality is difficult to assure but reach is ubiquitous, or c) a combination of the two.

PC-to-PC

This is perhaps the original form of VoIP. Here PC users connect their PCs to well functioning higher speed dial-up modems, wired or wireless broadband internet connections, or fixed LANs. The calls are then placed through the PC to a distant PC. All codec transformations are performed within the software operating on the users' PCs. Connections are typically managed from a central server that maps the user names to current IP address locations. Perhaps the most visible service in this category is Skype, although Microsoft's NetMeeting and systems from VocalTek have had this capability for years. Skype gained ubiquitous acceptance thanks to its ability to traverse most firewalls, its excellent voice quality, ease of use, and ease of installation – all compelling factors that have driven the uptake of PC-based VoIP to a commonplace service. PC-to-PC VoIP services have also been interconnected to the PSTN to enable calls to wireline and mobile phones from PCs or to enable PCs to receive incoming calls via an assigned telephone number. Examples of such services include SkypeOut and SkypeIn, respectively. Note the FCC mandates that VoIP services that are interconnected to the PSTN be subject to CALEA requirements.

Corporate

VoIP enables corporations to leverage existing IP networking which typically rides over lower layer Ethernet, ATM, frame relay, or other technologies. Connectivity to traditional corporate voice networks or the PSTN occurs through gateways managed by the company. VoIP is recognized, at least in theory, as a means of consolidating the enterprise's voice and data networks into a single network, thereby creating cost savings. VoIP system vendors also claim that configuring the features and locations of terminals is much simpler than with traditional PBX-based systems.

5.3.1 VoIP Protocols

Traditionally, the H323 specification had been the driving force behind how voice calls are transported and managed over IP networks. In more recent years, the competing protocol Session Initiation Protocol (SIP) has gained favor among operators of VoIP services and equipment vendors, with further support through the IETF [12]. SIP has the added advantage of managing "presence" of a user throughout a network. Presence enables one user to readily know if a distant user is on-line, how he/she is connected, and in some cases where. Of course, all of this information would be of considerable interest to the LEAs in the context of targeted interception.

VOP IRI/CD messaging does not correspond exactly to TIA / CALEA J-STD-025. For example, there is no definition for the "SIP INVITE" message under J-STD-025. This is overcome by mapping of VOP IRI messages to those recognized by the standard, or through Direct Signal Response [13]. The latter is useful for the implementation of LI in newly built VOP systems not dependent on legacy voice LI installations. SIP Message Bodies are treated as Call Content with headers and other information describing these bodies as Call Data.

5.3.2 VoIP Interception

Figure 5-5 provides a generalized, conceptual framework for interception. Note the network functions represented by each box may physically be combined or carried out by various pieces of equipment.

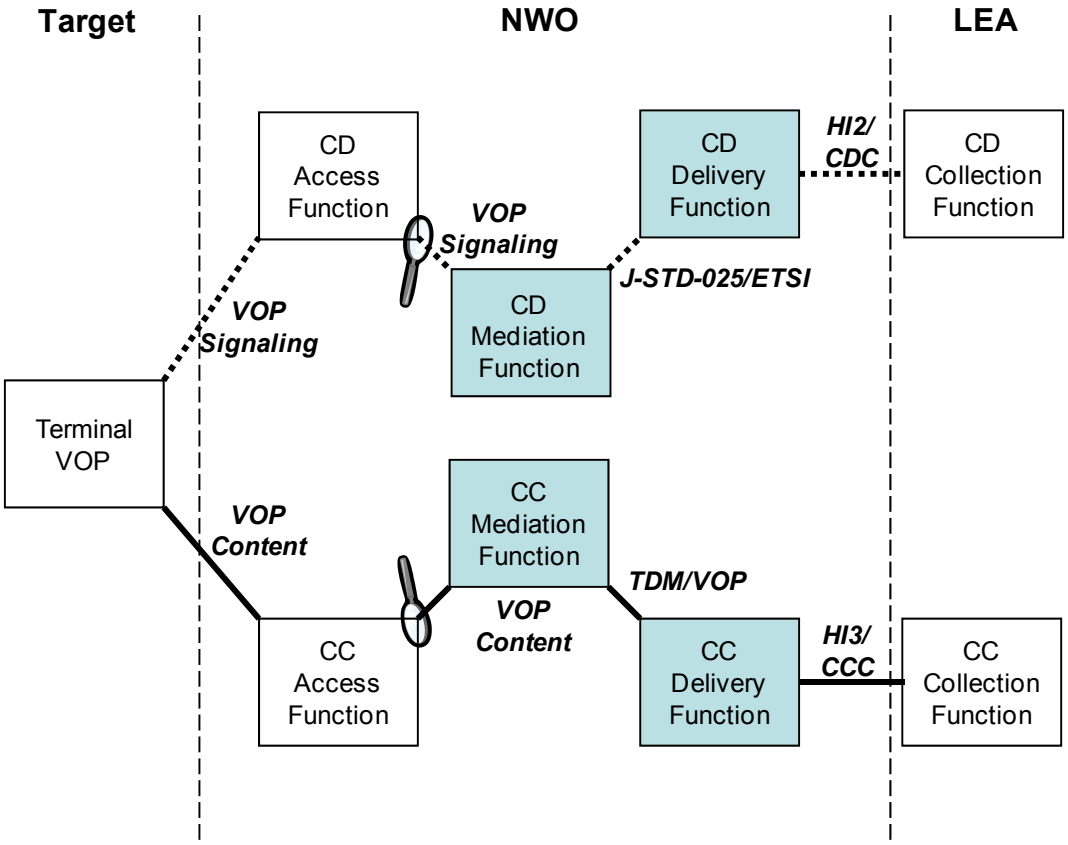


Figure 5-5. Conceptual view of interception for packet networks. Note each box can comprise single or distributed network elements. Shaded boxes correspond to functions performed by the Aqsacom ALIS mediation platform (derived from [13]).

Call Data are associated with *Surveillance Events* [13] related to the placement and dropping of a VOP call. Many of the parameters are similar to those found in traditional voice interception. The first group of Surveillance Events are *Call Control Events*, which include:

- *Answer:* the target answers an incoming VOP call or the distant party answers a call placed by the target.
- *Origination:* the target originated the call.
- *Release:* a completed or attempted VOP call has been released.
- *Termination Attempt:* a VOP call session termination attempt by the target has been detected.

Signaling Events are another form of Call Data associated with diverse network functions during the placement or manipulation of a call:

- *Dialed Digit Extraction (DDE)*: This is the capture of the extra digits that a target dials after the call is connected, such as the entry of a calling card number, line extension, or destination phone number to be dialed from an intermediate gateway. DDE remains a point of contention in the standards community. Some advocate that it be considered as part of Call Content and therefore under the responsibility of the LEA for interception; others claim that the network operator should furnish DDE digits to the LEA.
- *Direct Signal Reporting:* A signaling message is sent between the subject and VOP network, or the VOP network sends/receives a signal on behalf of the subject.
- *Network Signal:* Activity on the network that produces call identifying information (e.g., busy, ringing, alerting, etc.) is initiated or sent by a network element to the network facilities under surveillance that are serving the target.
- *Subject Signal:* Facilities under surveillance are used by the interception subject to initiate control features such as call forwarding, call waiting, call hold, etc.

Feature Use Events involves the signaling associated with conference calling, call transfer, and other call features. *Registration Events* occur when the target, or target's network facilities and equipment, provide address information to the VOP network, such as contact information, street address, etc. upon sign-up for a service or termination.

As in the case of traditional telephony interception, all Call Data must be presented to the LEA with a time stamp to ensure synchronization with the Call Content.

Note current VOP standards at present to not attempt to identify the physical location of targets. This contrasts to traditional wireline telephony, where target location is usually implied by virtue of the target's telephone number. But even traditional voice line identification can be obliterated through attempts to call through a gateway (such as with prepaid calling cards), and mobile telephony is fraught with technical challenges for determining location. Of course, and by default, locations of cable modem and xDSL services can be locked down by tying equipment ID numbers to specific CMTS or DSLAM circuits. The termination location of these circuits would be known; hence, the location of the user – unless the equipment is tampered with, which is not a trivial feat. *VoIP services that make use of gateways and switches may lose call originating information depending on the system design. In fact, the preservation of call data and the ability of service providers to furnish these to LEAs upon interception order is a controversial topic among VoIP operators and government agencies.*

To provide a basis toward the understanding of lawful interception for VoIP services, our discussion on LI will now focus on cable modem-based VoIP services.

5.3.3 Cable Labs / SCTE model

In view of the potentially large importance of Multiple Systems Operators (MSOs) in the offering of public telephony services, CableLabs published a specification on lawful surveillance for voice services operating over PacketCable networks[4][14]. This specification serves as the basis of the IPCablecom standard, as submitted by the Society of Cable Television Engineers (SCTE) to ANSI for formal standardization [15]. The goal of this specification is to make cable-based voice telephony CALEA compliant through CALEA's safe harbor provisions[5].

VoIP over cable, as well as over other access technologies, poses an interesting problem for lawful interception because in some cases part of the intelligence used to control the call sessions is placed at the edge of the network, within equipment at the customer premises. This equipment is usually a cable modem with a built-in or detached VoIP interface adaptor that connects to a typical telephone through an RJ-11 connector. Because this equipment is within the reach of the customer, and in some cases owned by them, the devices are subject to user tampering, especially when users attempt to obtain free services. In addition, it is highly unlikely that users would facilitate any LI session that requires physical or even remote access to their premises. Therefore, LI must proceed within the network that supports these edge devices.

The model proposed by CableLabs clearly has implications for cable-based VoIP services and even xDSL VoIP worldwide. Figure 5-6 describes the model's configuration for LI over cable-based VoIP services. The model's components are described as follows:

> **Cable Modem Termination System (CMTS)**: This system aggregates the physical connections and data flows from a distribution of subscriber cable modems and other customer premises terminal equipment (e.g., VOIP adaptors). Here Call Content (CC) packet streams are captured and replicated, typically via a router, and sent to the delivery function. CC includes embedded IP header information associated with the calling and called party.
>
> **Call Management System (CMS):** This supports the specific service provided to the subscriber, in this case telephony. In effect, this system captures call routing information to set up the call with the distant party for outgoing and incoming calls. This system is an important source of Call Data information, such as the originating telephone number, other ID parameters, time a call was placed, time a call was attempted, destination of call forwarding, third-party conference call identifiers, etc. Call Data delivered to the mediation system also includes the

[4] PacketCable is a set of specifications issued by CableLabs defining how IP data services are to be implemented over cable networks; among these services is voice telephony. PacketCable "rides" over CableLab's underlying DOCSIS (Data Over Cable Service Interface Specifications).

[5] The need for a PacketCable-based surveillance standard arose because the TIA CALEA standard (STD-0275), which focused mainly on traditional telephony, did not address the inherent technologies behind PacketCable.

media stream encryption key and an identifier for the encryption algorithm, both of which must be conveyed to the LEA for eventual processing. The key information can be issued from the RADIUS server. The CMTS communicates with the CMS via Common Open Policy Service Protocol. This is a client/server protocol that exchanges Quality of Service signaling and resource management [14].

Media Gateway (MG): serves as the bridge between the PSTN and IP network of the cable operator, thereby enabling the user to accept calls from parties connected to the PSTN or dial out to such parties. This can provide call content conforming to standardized fixed-line lawful interception. Also note the cable operators may situate the gateways at large distances from the immediate cable infrastructure affecting the interception target, and rely on such remotely placed gateways to provide dial-tone for long distance and even local calling. Thus, interception may have to take place at remotely located PSTN facilities far removed from the local calling area of the target. *The ubiquity of IP networking removes geographic barriers to the location of network functions. With VoIP, gone are the days of traditional telephony interception which historically has taken place within the physical facilities of the telecom network operator.*

Media Gateway Controller (MGC): Captures signaling information on the SS7 network to set up calls between the cable VOIP user and a PSTN party. This device can also perform subscriber dialing authorization and usage metering. Call Data information is supplied by this device.

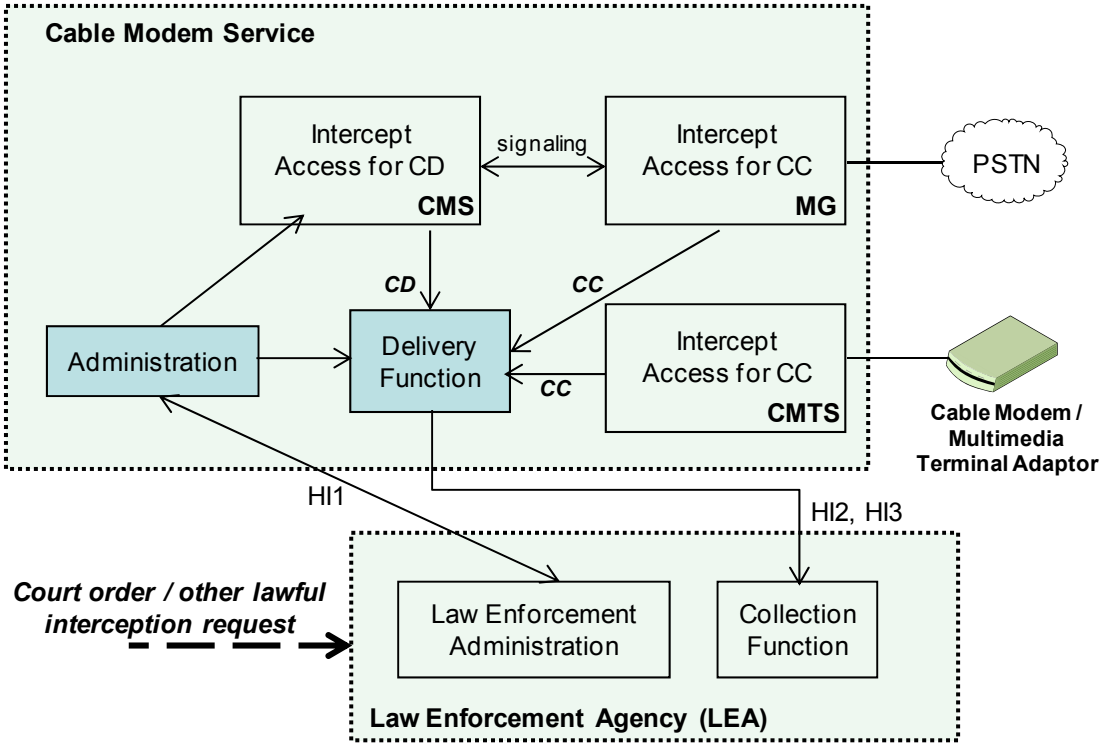


Figure 5-6. PacketCable description for Electronic Surveillance (adapted from [14, 15]). The shaded Administration and Delivery Function boxes are covered by ALIS (Section 6).

Call Data are sent to the LEA through PacketCable Electronic Surveillance Protocol, which is described through ASN.1 notation (as is CALEA/TIA J-STD-025 for traditional voice calling) [16].

Complications can occur when the cable VoIP subscriber forwards their calls to a distant phone number, the latter either within the cable network or a distant network (cable or PSTN). In these cases the intercept access points may also have to change. Another complication arises from the secure communications that takes place between the CMTS and the customer terminal equipment, especially for the exchanged data associated with access control. Security measures employed include Kerberos, IPSec, or other methods. Thus, the LEAs must receive this Call Data information decrypted by the cable operator, or the necessary keys and algorithm identifiers to enable the LEA to decrypt the information.

6. Aqsacom's ALIS Mediation Function Platform

6.1 Description

The Aqsacom real time Lawful Interception System, known as **ALIS,** reflects AQSACOM's ongoing philosophy of meeting the challenges of lawful interception in a highly systematic, low cost manner over networks supporting a diversity of services. The platform makes the deployment of lawful interception systems easier for the communications operator, while simplifying the processes of data collection and analysis by the law enforcement agency (LEA). It also addresses the growing lawful interception needs and requirements of newly emerging services, including those based on wireless 4G, broadband IP, Voice-over-IP, and other technologies.

The system's client/server layered architecture comprises two functional entities: ALIS-M for target provisioning and ALIS-D for the mediation and delivery of interception Call Content and Call Data (or IRI). Central Management facilities are also available. The overall architecture of the ALIS system is shown in Figure 6-1. ALIS-D and ALIS-M may reside on a common platform (comprised of a computing system and data interface cards – more on this below), or separate platforms. In addition, and depending on the networking topology, interception traffic load, services mix, and other factors, ALIS-D can be distributed over multiple platforms.

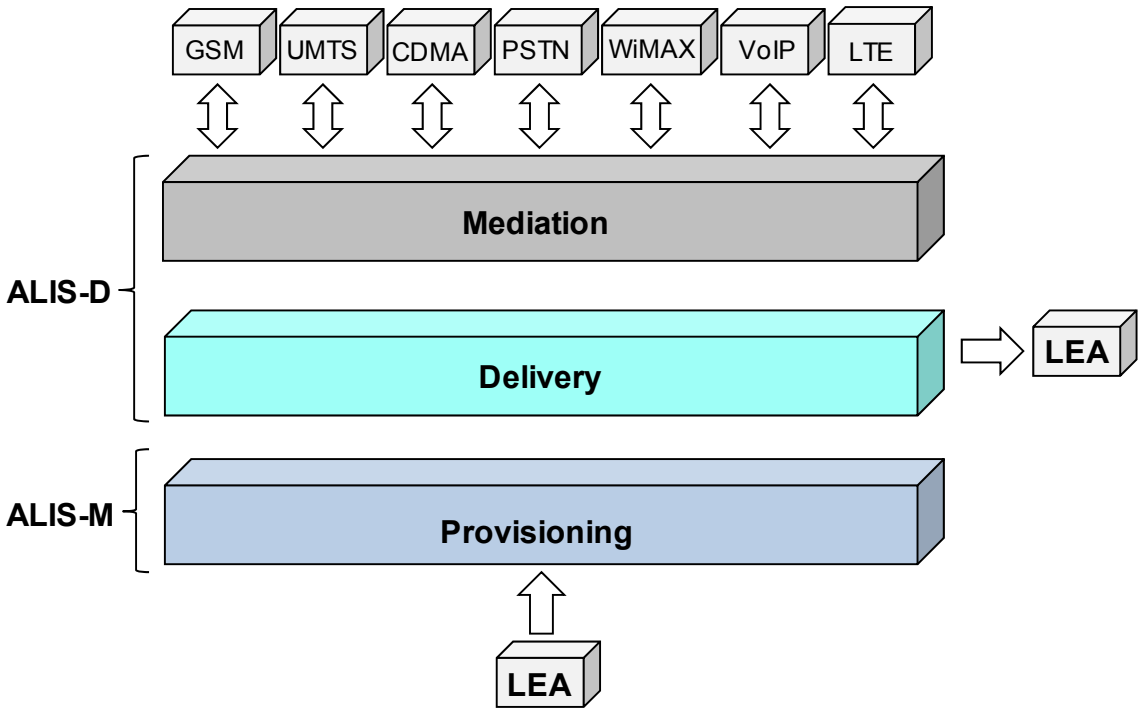


Figure 6-1. Architecture of the Aqsacom ALIS platform.

Features and functions of ALIS include:

Provisioning

ALIS-M is responsible for provisioning a lawful interception session. Provisioning falls under the Administrative Function, discussed in Figures 2-2. Specific tasks of provisioning include start, stop, query and modification of lawful interception operations, audit, consistency checking, etc. These tasks are generally invoked by the LEA (including courts), and securely communicated to ALIS, which typically resides within the network operator's premises. ALIS' friendly graphical user interface allows for the easy automation of many operational interception tasks, such as the automatic triggering or stopping of an interception operation at predefined dates and times.

Mediation and Delivery Management

Mediation is carried out by the ALIS-D platform, which gathers data from diverse intercept points within the network, formats the data, and delivers the information to the LEA over a secure network – typically a VPN, but also ISDN and a form of secured FTP. As discussed in Section 2, intercept data takes the form of Call Data (otherwise known as Intercept Related Information) and Call Content. Both types of data are delivered via separate channels. The data are also formatted by ALIS to conform to national standards such as CALEA. To ensure reliable real time delivery of interception information to the LEA, ALIS implements adequate buffering to account for nominal transmission outages or other unforeseen interruptions between the network operator and LEA.

Secure Access

Clearly ALIS, as any lawful interception system, must have highly controlled and secure access allowing for operation only by cleared personnel. Aqsacom takes this point very seriously, and has incorporated a number of safeguard technologies to assure secure access to system operation and interception data. These technologies include smart tokens and biometrics.

Billing

ALIS can be adapted to a variety of billing plans where the network operator invoices the LEA. These plans include billing on a per-LI session basis, per LI change basis, flat rate, per special service, and other plans. Likewise, billing can be configured to facilitate the operation of a LI service bureau, where several network operators share a common LI infrastructure. This configuration is attractive to those operators that are too small to invest in LI equipment and who claim that the frequency of LI requests from LEAs is not sufficient to justify the investment. In this case, billing can be addressed to the subscribing network operator, or one of many LEAs ordering the interception request.

Alarms, Statistics, Logging

ALIS provides a wide array of alarms (e.g., notification when a session is interrupted, hardware failures, security weaknesses, etc.) statistics (number of active interceptions in a given interval in time, utilization of LI system resources), and logs for tracking of past LI events.

Hardware / Operating System

ALIS makes use of off-the-shelf industrial strength PC hardware. This allows for easy parts replacement and reduced cost. All software runs under the Windows, UNIX, and Linux operating systems.

ALIS enables new network services, including those based on IP, to readily incorporate requisite lawful interception capabilities, as mandated by governments and industry standards. With the ALIS mediation platform, a diversity of network components provided by a diversity of vendors can all be readily interconnected into a common lawful interception schema without the need for customized LI installations between the LEA and network operator. Thus, the very costly and awkward LI practices of the past can finally be eliminated to make LI an essential, and even a value-added service, by network and service operators.

6.2 Deployment Examples of ALIS

We now illustrate the use of ALIS as a mediation system towards the facilitation of lawful interception in Internet Access, E-mail, and VoIP networks. Figure 6-2 illustrates Internet access (cable modem, xDSL, or dial-up). Target Call Data information is extracted from the RADIUS server and access termination point (a CMTS, DSLAM, or modem pool). An Internal Intercept Function (IIF) in a router replicates Call Content to/from the target and sends these data to ALIS-D.

Figure 6-3 elaborates upon Figure 5-4 to illustrate the application of ALIS as the mediation platform for the lawful interception of E-mail. Relevant E-mail header and other protocol information are captured directly from the E-mail server as "Call Data" and routed to ALIS-D for reformatting and delivery to the LEA. The content of the E-mail messages are routed to ALIS-D as "Call Content."

VOIP calling is illustrated in Figure 6-4. ALIS-M sets triggering events within relevant network equipment, including the call agent (such as a gatekeeper, SIP server, gateway, etc.) and routers assigned to capturing the data flow. Call Data and Call Content are then extracted from the network elements through use of their Internal Interception Functions. External Interception Functions could also be applied at points within the Internet cloud, but outside of the network elements shown.

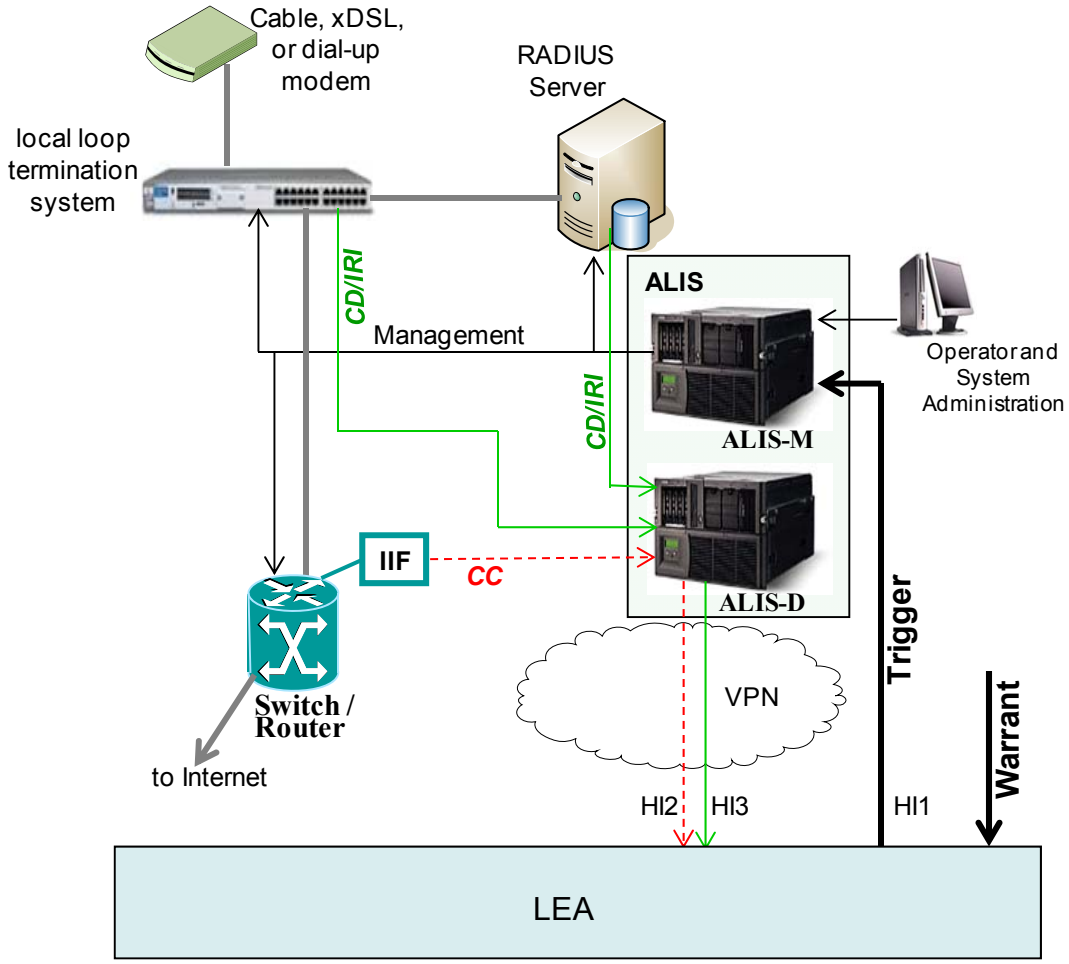


Figure 6-2. Application of the ALIS platform in the interception of a target's access to a network. For generality, the indicated access method could be cable modem, xDSL, or dial-up. The customer termination system and RADIUS server supply Call Data (IRI) to ALIS-D. The Internal Interception Function (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.

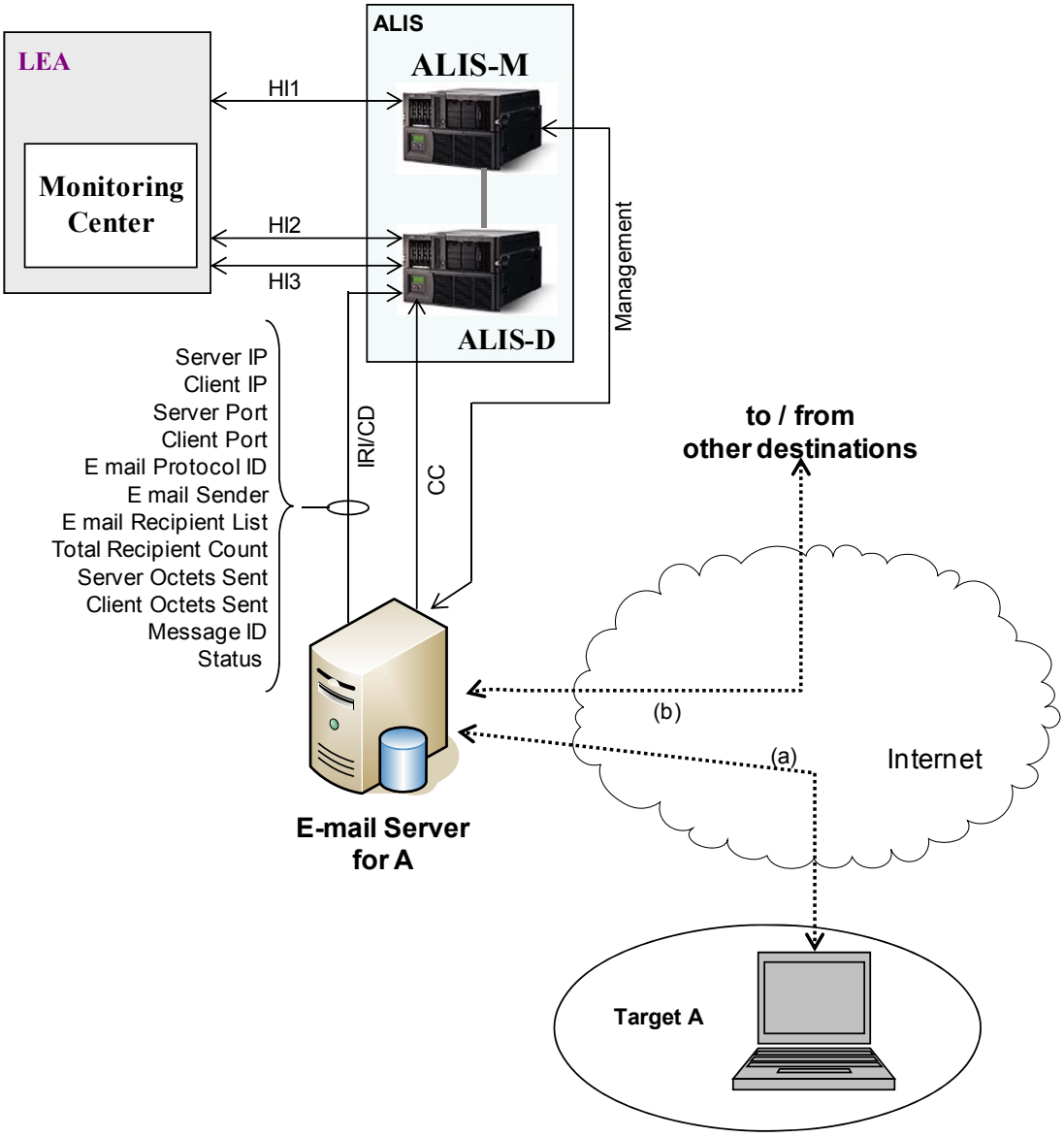


Figure 6-3. Example of E-mail interception. Here an Internal Interception Function operates within the E-mail server(s) handling outgoing and incoming messages to/from the target. Further interception can be carried out through External Interception (probes) at network points away from the E-mail server.

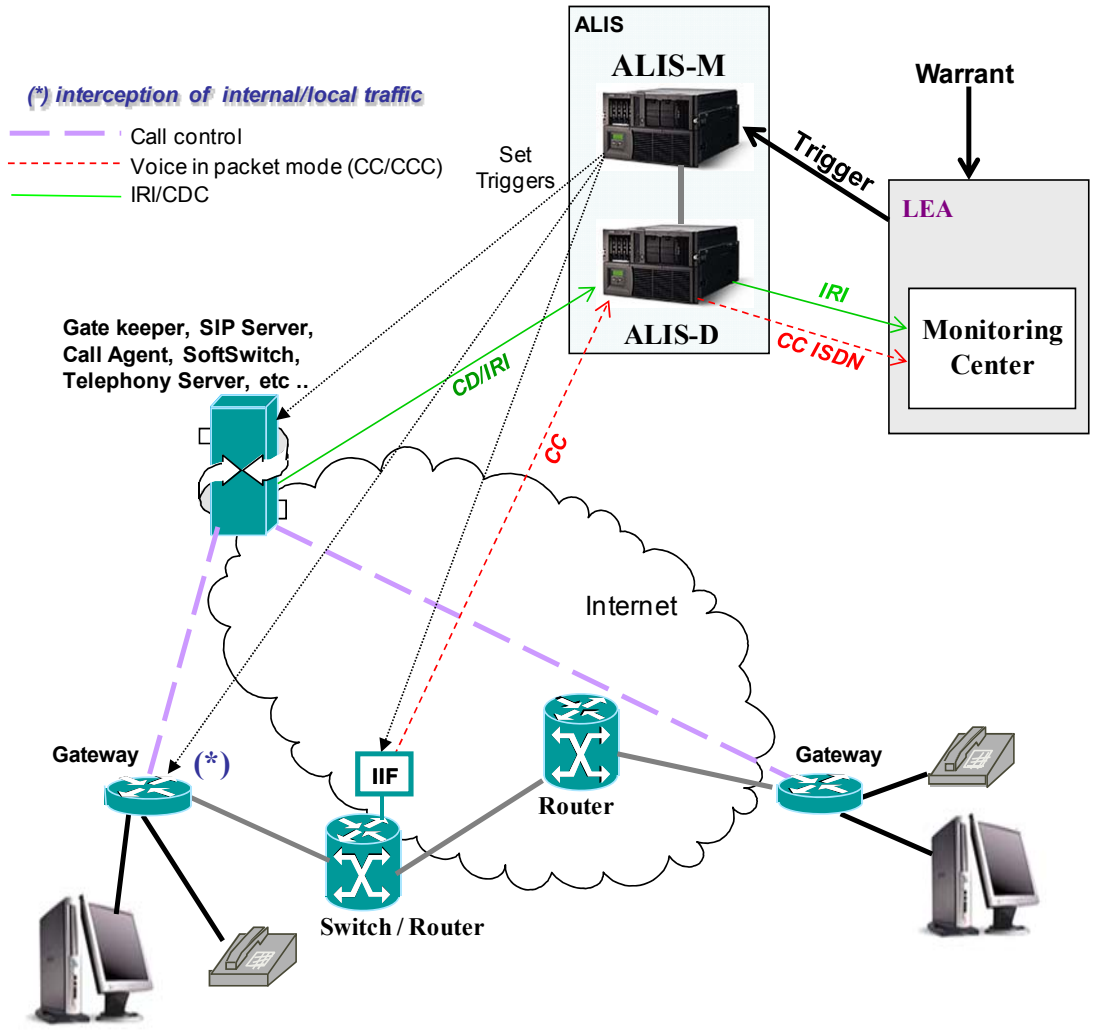


Figure 6-4. Application of the ALIS platform in the interception of VOIP. Call Data information is extracted from the Gatekeeper (or similar) device via Internal Interception and sent to ALIS-D for processing. Provisioning of pertinent network elements is carried out by ALIS-M. An Internal Interception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

References

[1] Handover Interface for the Lawful Interception of Telecommunications Traffic, ETSI ES-201-671, under Lawful Interception, Telecommunications Security, version 2.1.1, September 2001.

[2] Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover Specification for Ip Delivery, ETSI TS-102-232-1, version 2.1.1, December 2006.

[3] Lawfully Authorized Electronic Surveillance, T1P1/T1S1 joint standard, document number J-STD-025B, July 2006.

[4] Benjamin M. Lail, *Broadband Network Device Security*, Chapter 4, RSA Press / McGraw-Hill, 2002.

[5] Remote Authentication Dial-In Service (RADIUS), see IETF RFC2865 at www.ietf.org .

[6] Issues on IP Interception, ETSI TR-101-944, under Lawful Interception, Telecommunications Security, version 1.1.2, December 2001.

[7] Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP Delivery; Part 3: Service-Specific Details for Internet Access Services, ETSI TS 102 232-3, version 2.1.1, December 2006.

[8] *Wireshark* protocol analyzer (see http://www.wireshark.org)

[9] Dynamic Host Configuration Protocol (DHCP), see IETF RFC2131 at www.ietf.org .

[10] The Network Access Identifier, see IETF RFC2486 at www.ietf.org .

[11] Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP Delivery; Part 2: Service-Specific Details for E-mail Services, ETSI TS 102 232-2, version 2.1.1, December 2006..

[12] Session Initiation Protocol (SIP), see IETF RFC3261, RFC3262, RFC3263, RFC3264, RFC3265 at www.ietf.org .

[13] Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks, T1.678v2 (ATIS Document ATIS-PP-1000678.2006), May 2006.

[14] Superseded PacketCable Electronic Surveillance Specification, PKT-SP-ESP-I03-040113, Cable Television Laboratories Inc., 13 January 2004. (see also Release PacketCable 2.0 Electronic Surveillance Deliver Function to Collection Function Interface Specification, PKT-SP-ES-DCI-IO1-060914, September 2006 and PacketCable 2.0 Electronic Surveillance Intra-Network Specification, PKT-SP-ES-INF-I02-061013, October 2006).

[15] IPCableComm Part 13: Electronic Surveillance Standard, ANSI/SCTE 24-13 2006, Society of Cable Television Engineers, 2006.

[16] ITU Recommendation X.690, Information Technology: - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished Encoding Rules (DER), July 2002.