Lawful Intercept and Enablement in High-Performance Networks

Lawful Intercept (LI) is the terminology used to describe the monitoring (i.e., intercepting) of traffic to and from a person or persons of interest, as requested by a legal warrant from a Law Enforcement Agency (LEA). This surveillance must be performed in a manner that is not detectable. In the United States the Communications Assistance for Law Enforcement Act of 1994 (CALEA) governs LI for telecommunications service providers. LI laws worldwide have similar requirements, although some are more restrictive than others. The traffic of interest is usually voice traffic, but could be extended to include data in the future.

With recent changes in the security environment, organizations that were treated as private and not impacted by CALEA and similar Lawful Intercept requirements in the past, now find themselves categorized as public communications providers and need to comply with LI requirements. With this change in categorization, these organizations may now be bound by LI regulations. Because their communications infrastructures are similar to service providers, they share many of the same design considerations in building LI capabilities.

The intent of this paper is to frame the general requirements for LI and to identity the role of networking elements (switches & routers) in the LI model. We will also provide recommendations for provisioning and configuring Foundry products to enable LI capabilities.

Lawful Intercept Requirements

While specific LI requirements will vary from country to country, the general requirements are similar. The United States CALEA rulemaking is representative of the LI requirements. Section 103(a) of the original CALEA act specifies the following four main capability requirements:

(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;

(2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier--

(A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and
(B) in a manner that allows it to be associated with the communication to which it pertains, except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);

(3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and

(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects--

(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and
(B) information regarding the government's interception of communications and access to call-identifying information.

Impact to "Private Networks"

Many of the organizations that have found themselves possibly bound by LI are not service providers (SP) in the traditional sense, but may need to satisfy new LI requirements. One example of how these organizations may differ from an SP is shown in the case of a university. Although a university may provide Internet access, it is not a traditional SP or telecommunications carrier. In an SP network, all network traffic transits the Internet, and there are one or more locations where the traffic must enter or exit. A passive or active tap can be placed at these locations to view all traffic from a particular source.

In a university environment, not all traffic is transiting the Internet; some may be internal only traffic. If this traffic is subject to LI regulations and requirements, then even edge switches may need to capture some or all of the traffic on its ports. This requirement can be problematic for organizations that have invested in local area network switching and routing products that cannot easily be provisioned to support traffic interception.

Some universities may provide Internet peering themselves. In this case, they would be subject to LI warrants that target specific sources that are using their infrastructure for communications. University environments that use a traditional SP would probably not be the target of an LI warrant targeting an Internet user; the warrant would most likely be presented to the SP directly.

Lawful Intercept (LI) Network Model

An LI model has been defined and is well accepted in the industry, and we will use this model as a guide for our discussions and recommendations. In this model, there are three basic elements:

- Access Function (AF)
- Delivery Function (DF)
- Collection Function (CF)

The AF is the network device through which the source data of the Lawful Intercept (LI) is transiting (ie the data or VoIP communications of interest by the law enforcement agency). This could be a switch, router, PBX or other network device.

The DF in the LI model is generally performed by what is otherwise known as a Mediation Device or MD. This device receives data from the provisioned tap or network element and correlates and formats it to indicate whether it is the Call Information data, the Call Content Data, or the Raw Data with the specific warrant information. This data is then sent to the appropriate Law Enforcement Agency using an encrypted tunnel with a protocol which is unique for each country. It may be the case that there are tap requests from multiple agencies for the same person of interest.

The Mediation device is responsible for making the copies and sending them to the requesting law enforcement agency (LEA), while ensuring that each LEA is unaware of the activity requested by another LEA. The tap information coming into the MD may be raw mirrored traffic, semi-groomed traffic (using a protocol unique to the MD vendor, or that of a standards body such as described in PacketCable for VoIP over cable modems). The MD may be sufficiently intelligent to automate the provisioning of the tap on the AF, or it may require manual configuration.

The CF is the actual collection function at the appropriate LEA location. This communications is defined by TIA standard J-STD-25A, but can vary by country.

Figure 1 below shows the typical LI model with the Access Function (AF) performed on the SP router and the Delivery Function (DF) performed on a server (there are several companies that provide this product). Generally, the DF automatically provisions the AF for target data interception after being configured to do so by a security officer or manager at the SP. Once the DF starts receiving streams from the AF, it then strips off the appropriate data and sends the data to the Collection Function (CF) at the LEA. The data received by the DF is generally only from the warrant target.

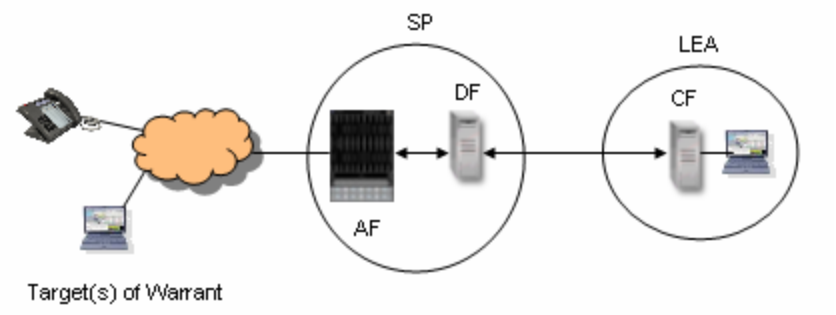

Figure 1 Service Provider Lawful Intercept Network Model

Note that the AF is in the SP infrastructure. As we will show in our new model, this may not be the case for a university or non-SP organization for which LI regulation may apply.

Enhanced Lawful Intercept Network Model

Many organizations now asking about LI do not fit into the typical SP Network model. The university example helps to illustrate the enhanced model.

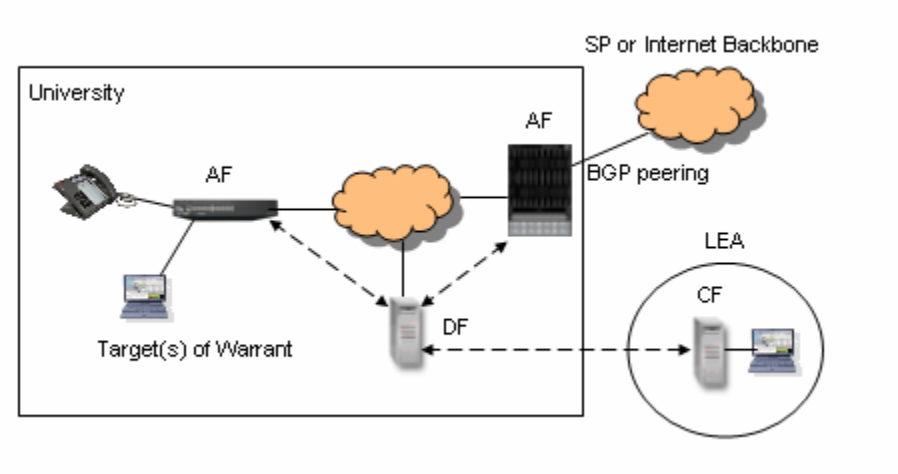

Figure 2 Enhanced Lawful Intercept Network Model

In this new model shown above, multiple network nodes in an organization may need to perform the Access Function. If a warrant is provided by the LEA, and specifies that all data from a particular user is to be intercepted, then the traffic of interest could be purely local to the organization. In this case, some facility for capturing local traffic as well as Internet-bound traffic is required.

If the university acts as its own peering point, with direct connection to multiple Internet exchanges or backbones, and the warrant calls for all data to and from a target of interest, only over the Internet, then the Access Function would need to be performed by the BGP router or routers near the perimeter of the network. If the university uses a single SP, and

the SP receives the warrant, then the model is similar to the SP Lawful Intercept model we discussed earlier (with the university not involved in the warrant).

There are two areas that most need to be addressed by organizations like universities that may be required to support LI. The first is the support of warrant target traffic interception, together with a facility for transferring this data to the DF without the target's awareness. The second is the incorporation of some kind of DF (Delivery Function) or Mediation Device in the organizations infrastructure. Current Mediation Devices (MD) are architected, packaged, and priced for large telecommunications service providers. Their pricing and packaging are not intended for university environments. The roles and responsibilities of the MD are discussed only briefly in this paper.

Role of the Switch/Router in the Lawful Intercept Model

In the Lawful Intercept model, the roles of the Access Function (AF), Delivery Function (DF), and Collection Function (CF) are generally well defined. The CF would be located at the LEA and would process the target's traffic that has been received in a format specified by the local country's LI requirements.

In a high-performance network built using Ethernet switches and routers, these products would perform the role of an Access Function (AF). The function of the AF is to capture the traffic to and from the warrant target and deliver this data to the DF, which would normally be on site with the AF. The AF does not necessarily need to encrypt the data, since the data would be transiting the internal network of the organization which received the warrant. The AF may be a switch or router that connects directly to the warrant target, or one of the interior routers.

Note also that there could be multiple AF's in an organization. This could include any router and other equipment like IP PBX's.

Enhanced Lawful Intercept Network Model Example

There are a number of a ways in which network switches and routers can be used to support the LI function. The figure below illustrates one such method using Foundry products.

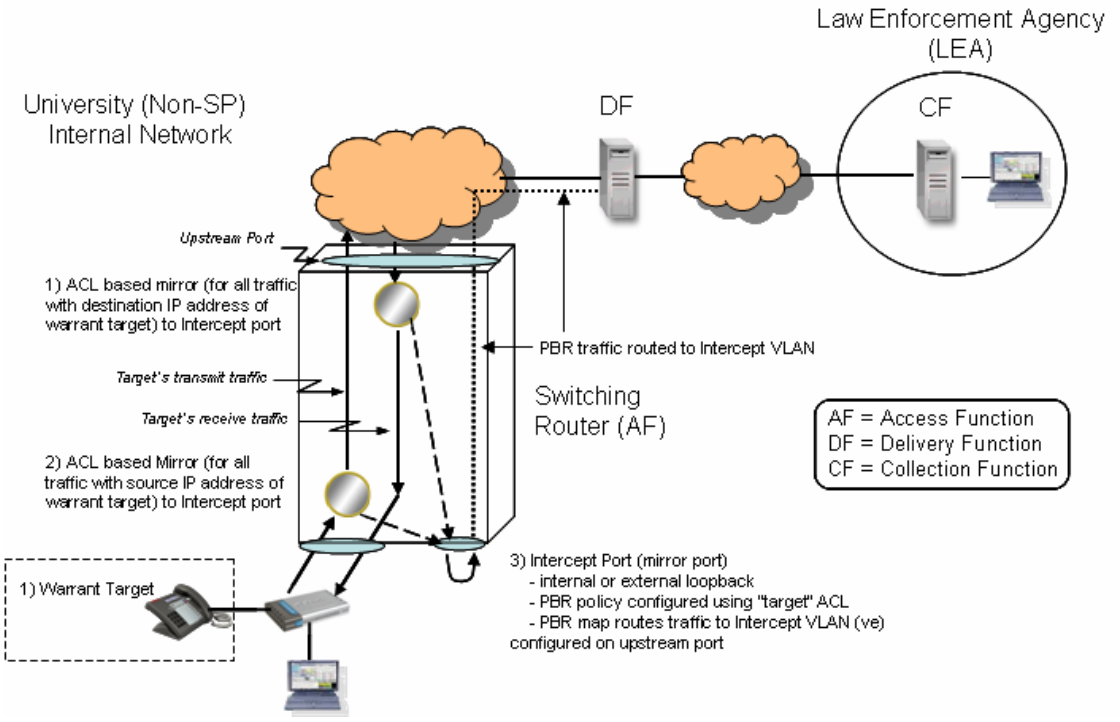

Figure 3: Enhanced Lawful Intercept Network Design

In this example, a warrant that is received from an LEA is delivered to the appropriate security personnel at the site. Through the DF, the target switch and port address are determined manually or automatically. The target port is assumed to be a shared port (i.e., traffic from multiple devices transits this port). If the target port is not shared, the configuration is simplified.

In this example, the switch port that is receiving traffic from the warrant target (may be an edge or interior switch) is provisioned as a monitor port with an ingress ACL-based port monitor filter. The filtered traffic is sent to a user-configured mirror port which is referred to as the intercept port. The ACL is configured to copy traffic being sent by the target IP address. Additionally, the upstream or northbound port is configured as a monitor port with the same ACL for mirroring traffic to the intercept port. This ACL will copy traffic that is being sent to the target IP address. The intercept port itself is configured with a loopback (either electronically or via a special loopback cable). The intercept port (i.e., the mirror port) is also configured with the target ACL and for policy based routing (PBR). A policy route map is configured to route the filtered traffic to a virtual Ethernet interface (VE) on the upstream port. The VE is configured as part of an

Intercept VLAN that includes the DF. Upstream switching routers are similarly configured with VEs configured as L2 tagged ports in the Intercept VLAN.

Because policy based routing (PBR) is the mechanism used to forward the target data into the Intercept VLAN, the participating switches must be capable of layer 3 routing.

If the warrant target is the sole device on the target switch port, no ACL would need to be applied to the target port, but the ACL based mirror would still need to be applied at the upstream port to separate warrant target traffic from other traffic.

Once the proper intercept configuration is complete, the DF receives the intercept traffic and delivers the desired formatted data to the CF at the LEA. This operation may include encrypting the data for secure delivery to the CF.

This overall design is still dependent upon the Mediation Device carrying out the task of delivering specific data (perhaps only the voice traffic) to the CF. Most MD's are designed, packaged, and priced for larger SP environments. There are few, if any, commercial MD's which are appropriate for any but the largest university environments. We expect this to change over time.

There are a number of areas not addressed by this architecture. One is mobility. If the target were to move to a different device, it may be difficult for the DF or security personnel to detect and respond to this movement, especially in a wireless environment. This architecture assumes that a warrant target is authorized to communicate only from specific locations on the network and can be located on the network.

Conclusions

Lawful Intercept requirements may now apply to organizations that were previously categorized as private and not subject to LI regulations. Consequently, some organizations, such as universities, may now be subject to LI regulations. To address these requirements, organizations must understand their obligations under the LI laws and how these can be met in a cost-effective manner. Essentially, each organization must be able to expeditiously, undetectably, and securely deliver specific target traffic data to an LEA.

The industry has defined a model for LI in which the functionality is broken into three distinct functions: the Access Function (AF), the Delivery Function (DF), and the Collection Function (CF). Typically, the AF and the DF reside at the organization that has been served the warrant. The CF exists at the Law Enforcement Agency (LEA).

In this model, Foundry products serve the role of an AF in the intercept process. In the AF role, Foundry switches are configured to copy warrant target traffic to the DF. Using access control lists, port mirroring, and layer 3 policy-based routing, Foundry products are able to filter and copy bi-directional warrant target traffic either at the edge or interior nodes of the network. Using these features, LI requirements can be satisfied without

relying on tunneling, which is difficult to manage and monitor. Once the DF receives the streams of data from the Foundry AF, the DF is responsible for securely sending the stream to the CF at the LEA.

Foundry will continue to monitor LI requirements as they evolve worldwide and provide guidance to our customers as to how to meet the growing need for networks to support LI capabilities. We welcome feedback on our LI directions and recommendations, and will work with the community to ensure that these requirements can be met using Foundry's broad range of networking products.

Foundry Product Support for Lawful Intercept

A number of Foundry's products have the ability to support ACL mirroring and policy based routing and can be configured to support LI as described above.

Consult Foundry's product datasheets for each Foundry product to determine LI support capabilities (e.g., ACL-based port mirroring, policy based routing, etc.).

References

(1) P. Branch, "Lawful Interception of IP Traffic," Centre for Advanced Internet Architectures, Swinburne University of Technology, Hawthorn, Vic 3122
(2) CALEA, "Ask CALEA – Frequently Asked Questions," <http://www.askcalea.net/calea.html>
(3) Communications Assistance for Law Enforcement Act of 1994 Pub. L. No. 103-414, 108 Stat. 4279
(4) F. Baker, B. Foster, C. Sharp, "RFC 3924 – Cisco Architecture for Lawful Intercept in IP Networks," http://www.faqs.org/rfcs/rfc3924.html
(5) IETF Network Working Group, "IETF Policy on Wiretapping," Last Update May 2003. <http://www.ietf.org/rfc2804>
(6) United States Court of Appeals for the District of Columbia Circuit. American Council on Education vs. FCC, Verizon, Verizon Wireless, Cellco Partnership. Argued May 5, 2006; Decided June 9, 2006. No. 05-1404
(7) Unkown, "VoIP Lawful Intercept – FCC Broadband Second Order CALEA, The Clock is Ticking," May 14th 2007. www.ss8.com
(8) FCC Telecommunications Act of 1996. February 8, 1996. <http://www.fcc.gov/telecom.html>