



CALEA

White Paper

ImageStream Internet Solutions, Inc.

7900 East 8th Road
Plymouth, Indiana 46563

<http://www.imagestream.com>
info@imagestream.com

Phone: 574.935.8484

Sales: 800.813.5123

Fax: 574.935.8488

INTRODUCTION

In October 1994, the U.S. Congress passed the Communications Assistance for Law Enforcement Act (CALEA), which was designed to clarify a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes. The Act obliges telephone companies to make it possible for law enforcement agencies to tap any telephone conversation carried out over their networks, as well as making call detail records available.

CALEA went into effect on January 1, 1995. On March 10th, 2004, the DOJ, FBI and DEA jointly petitioned the FCC to accelerate CALEA compliance among Internet and VoIP service providers that carry packet-based voice communications on their networks. As a result of this petition, the FCC set a new deadline of May 14th, 2007 for broadband service providers to comply with CALEA.

There are many useful on-line resources that address the entire spectrum of legal questions that you may have about CALEA compliance, such as who must comply, what forms must be filed with the FCC, and other requirements that are more administrative than technical. Fines for non-compliance can cost \$10,000 per day, so ImageStream recommends that you consult legal counsel to get competent advice on all compliance issues related to CALEA. In general, network operators located within the U.S. that offer wireless or wireline Internet connectivity with subscriber access speeds of 200 Kbps or higher are required to comply.

This White Paper discusses the technical compliance requirements for conducting lawful communications intercepts under CALEA, and the support ImageStream products provide for conducting those intercepts. It also addresses some of the technical challenges that a carrier may need to address in the process of implementing a successful CALEA compliance plan.

This White Paper does not provide a "punch list" for CALEA compliance, and it does not attempt to address all of the actions and procedures that may be required for a carrier to become CALEA compliant. Also, please note that the contents of this White Paper do not constitute legal advice.

The FCC encourages all broadband service providers to contact the FBI with questions about CALEA compliance. The FBI's "Ask CALEA" Web site (<http://www.askcalea.net>) answers frequently asked questions about CALEA. The wireless industry trade organization WISPA offers helpful CALEA compliance information at <http://www.wispa.org>. Also, the CALEA Wiki has info and links on CALEA compliance at http://en.wikipedia.org/wiki/Communications_Assistance_for_Law_Enforcement_Act.

OVERVIEW

There are many different CALEA requirements, industry standards, and accepted FBI procedures for conducting communications intercepts under a lawful court order. This White Paper will explain the pertinent requirements of the Act, related industry standards, and accepted FBI procedures that ImageStream has followed to develop its CALEA intercept solutions. In addition, this White Paper will discuss the intercept methods to be used in conjunction with Trusted Third Party (TTP) services for CALEA compliance, as well as the supported intercept methods that can be used for direct intercept delivery to law enforcement without TTP services or a separate mediation device.

A Step in the Right Direction

When the FCC ruled that CALEA applied to broadband service providers, many carriers concluded that the Act was just another way for the federal, state and local law enforcement agencies to take away additional freedom and privacy in the United States. CALEA was passed in 1994, so it was not a response to 9/11. More importantly, law enforcement agencies (LEAs) in the U.S. have been conducting lawful communications intercepts for decades before CALEA was passed, and the Act is actually designed to safeguard privacy while it improves the capacity for LEAs to conduct lawful intrercepts.

One key feature of the Act is its support for confidentiality of intercepts. Another key feature is its requirement to filter the data of non-targets before delivery to the LEA. This filtering requirement makes it impossible for the LEA to look at private data that is not covered by the warrant.

The Biggest Problem with CALEA Compliance

Congress made a good decision when it chose to allow industry organizations to develop their own standards for CALEA intercept delivery. After all, if Congress had decided to tackle the intricacies of a technical standard for CALEA intercepts, the required standard would exceed the technical understanding of most members of Congress, it would be more difficult to change as needed over time, and carriers and equipment manufacturers would probably have a much worse situation than they have now.

So now that we have credited Congress for doing the right thing by allowing industry organizations to develop their own standards for CALEA intercepts, we can move on to explain that the biggest problem with CALEA compliance today is those intercept standards.

The first set of CALEA intercept standards were developed by the Alliance for Telecommunications Industry Solutions (ATIS). ATIS focused on developing a standard that fulfilled the apparent real-time delivery requirements of CALEA. When ImageStream contacted the FBI for guidance in early 2007, the FBI recommended following the ATIS standard called T1.IAS. The FBI recommended following the T1.IAS intercept standard because it was the only standard that would be ratified before the May 14th, 2007 compliance deadline.

After reviewing T1.IAS, ImageStream engineers concluded that any CALEA intercept standard that uses the Internet for intercept delivery and allows 1% packet loss is not a reliable basis for collecting court evidence. As a result, ImageStream decided to contact the Wireless Internet Service Provider Association (WISPA) and urged them to begin development of an alternative CALEA intercept standard for wireless and wireline service providers.

On May 1st, 2007, ImageStream released its first intercept-capable router distribution, almost 2 weeks ahead of the May 14th compliance deadline. This release provides everything required to perform a CALEA-compliant intercept, including support to filter intercepts down to the target data, real-time streaming delivery, “fan-out” for delivery to multiple LEAs, and capture-to-disk.

In the process of working with WISPA’s CALEA standards committee, the FBI explained they did not approve of the T1.IAS standard, and they did not vote to adopt the final specification as a member of the ATIS standards committee. Despite the FBI’s vote to reject T1.IAS, the committee still decided to ratify the standard. The FBI says they plan to challenge T1.IAS in court. The FBI will most likely wait until an alternative like WISPA’s CALEA intercept standard is ratified before challenging T1.IAS.

Because of these standards issues, the biggest technical problem for CALEA compliance today is that the safe harbor standard that ImageStream needs is a moving target. This main difference between the ATIS standard and the WISPA standard is that the ATIS standard uses UDP to support real-time delivery with up to 1% packet loss, while the WISPA standard is a store-and-forward solution that can be implemented with existing Open Source tools like tcpdump. ImageStream plans to support the new WISPA standard and the existing ATIS standard because we believe that the LEAs may need support for both real-time and store-and-forward delivery.

ImageStream is committed to providing an intercept solution that provides a safe harbor for its customers. By law, LEAs are compelled to support intercept delivery based on a safe harbor standard like the ATIS or WISPA standards, at least until they are challenged by law enforcement in court. Even so, this does not prevent an LEA from requesting specific delivery methods such as real-time delivery or capture-to-disk. In the end, if the goal of CALEA is to support law enforcement, then it should be our goal to support the range of needs that law enforcement may need.

ImageStream expects the T1.IAS to be challenged by the FBI, and we expect ATIS to modify their standards to use TCP as a more reliable delivery mechanism than UDP. If the ATIS standard is changed as we expect, then ImageStream will make the required changes to support the updated standard.

VoIP Service Providers

A critical fork in the road to CALEA compliance depends on whether your organization provides VoIP gateway services that originate on the local network. Service providers that operate a VoIP gateway like Asterisk on the local network are subject to additional requirements including the delivery of call events.

ImageStream specializes in high-performance network transport that supports the low-latency requirements of VoIP traffic. However, the company does not support VoIP gateway services with its routers. As a result, the CALEA intercept solutions that ImageStream offers are only designed to comply with the requirements for wireless and wireline transport providers.

ImageStream can help VoIP providers achieve CALEA compliance with network transport, but the company’s wireless and wireline compliance solutions do not provide VoIP protocol analysis for constructing and delivering call events for VoIP service providers. Service providers that do not offer VoIP services in-network are only subject to the wireless and wireline requirements for CALEA intercepts, even when customers are using external VoIP services such as Vonage or Skype.

If you are operating VoIP services locally and need assistance with VoIP gateway intercepts, ImageStream recommends that you contact your VoIP gateway manufacturer or a Trusted Third Party (TTP) such as Intelleg Communications (<http://www.intelleq.net>) for assistance.

Wireless and Wireline Service Providers

If you are a service provider that does not offer VoIP services locally, then ImageStream's intercept solutions can offer an inexpensive solution for your CALEA intercept requirements. Existing ImageStream customers can simply upgrade their router software to the latest distribution that supports CALEA intercepts. New customers can expect their routers to come with the intercept software already installed. Those network operators who are unlucky enough to have routers from one of the big-name manufacturers can even save money by using ImageStream taps and routers (in place of a network "probe") to deliver CALEA intercepts cost-effectively without replacing their existing equipment or paying a lot more for software that requires mediation services.

REQUIREMENTS

General requirements for CALEA compliance are covered in the Act itself. However, Congress has tasked the FBI with developing acceptable intercept methods for all LEAs, and it is believed that following the FBI's recommendations will be acceptable to the other LEAs. CALEA does not allow law enforcement to require carriers to follow a particular intercept standard, but the LEAs have needs, and these needs must be served by those industry standards or they will be challenged in court.

It is also important to note that there is a “negotiation” that can occur between the carrier and the LEA when an intercept warrant is served. For example, the LEA may request real-time delivery and capture-to-disk, but you may be able to negotiate with them for capture-to-disk only. As another example, the LEA could request “access events” to be delivered in real-time, and you may be able to successfully negotiate delivery of these events, perhaps on a daily basis from RADIUS logs. The LEAs are expected to work with carriers in good faith to achieve an acceptable intercept delivery solution, but this assumes the carrier has already taken the necessary steps to comply with CALEA at an administrative level, and the only compliance issue that remains in question is intercept delivery.

Here is a list of compliance requirements that you may need to address as you develop your CALEA compliance plan and prepare to perform a real intercept.

1. Confidentiality
2. Authentication, Validation, and Confirmation
3. Transparency
4. Isolation
5. Completeness
6. Compression and Encryption
7. Buffering
8. Fan-out
9. Reliability
10. Intercept Content
11. Time Stamps
12. Warrant ID
13. Recordkeeping
14. Intercept Pitfalls

Confidentiality

Confidentiality is an important issue for conducting intercepts. CALEA requires that only “authorized” personnel can know that an intercept is being performed, including information in the warrant that identifies the target of the intercept. Confidentiality applies to the LEA, and information on a warrant issued by one LEA such as the FBI cannot be shared with another LEA such as the DHS or DEA.

Confidentiality is also an issue when it comes to network configuration and management. The System Security and Integrity (SSI) plan that carriers must file with the FCC names one contact that will be used for serving intercept orders to the carrier. This person is clearly authorized to have access to intercept information and associated system configurations. Unfortunately, CALEA does not explain

how additional individuals can be authorized to have access to this information. Therefore, it is not only important for the named SSI contact to keep intercept details confidential from other LEAs, staff and others, but it is also important to protect unauthorized sys admins from viewing intercept configurations.

One way carriers can use ImageStream routers to comply with this confidentiality requirement is to limit access to the router so non-authorized personnel will not have access to the intercept configurations. If the named LEA contact for serving warrants is the only person who administers the router, then there is no risk of non-authorized personnel accessing the intercept configs.

In larger service provider operations, it is impossible to have a single person administer all of the ImageStream routers on the network. For these organizations, ImageStream provides an option that encrypts the intercept configuration on the router so it cannot be viewed accidentally by unauthorized sys admins. This approach is not highly secure, because sys admins who are not authorized to view intercept configs can learn how to decrypt and view the config. But CALEA does not specify how intercept information and records must be kept confidential, and this approach is probably more secure than storing confidential paper records in a file cabinet in your office. The key to intercept confidentiality using this approach is to implement the required policies for your unauthorized sys admins that will ensure confidentiality is maintained.

ImageStream originally planned to develop a remote provisioning system for larger carriers that have multiple non-authorized sys admins who need to access the system. This plan has been delayed because of ongoing changes with the specifications for intercept delivery. ImageStream plans to continue work on the provisioning system once a stable intercept standard is ratified that can be supported by the LEAs over time. In the mean time, carriers with multiple sys admins are advised to implement encryption for intercept configurations so they cannot be viewed accidentally by non-authorized personnel.

Authentication, Validation and Confirmation

Authentication, validation, and confirmation are three critical points in one process that ensures the intercept is truly associated with the specified target. DHCP, changes to customer accounts, and other network events can disrupt a lawful intercept. The carrier is responsible for these potential issues, and must manage them accordingly.

“Authentication” ensures the intercept target is correctly associated with the IP or MAC address used to identify the target. Authentication may involve confirmation that the intercept target is correlated to an IP or MAC address by looking at an internal document where static IP or MAC addresses are recorded and assigned, or it may require the use of a RADIUS server log that keeps track of what IP address is assigned to the target. The methods for ensuring that an intercept is associated with the correct target during intercept initialization will vary from network to network, but the carrier is responsible for ensuring the intercept is correctly associated with the target. “Validation” is similar to authentication except that it ensures the intercept is correlated to the target throughout the entire intercept.

“Confirmation” is used here to mean that after the intercept has been completed, the carrier can prove that the intercept was correctly associated with the target of the intercept. This process may involve keeping records of static IP or MAC addresses assigned or otherwise identified in statically configured networks, or it may involve keeping RADIUS or other authentication logs to confirm that the intercept was correctly associated with the target.

In capture-to-disk intercepts, hash files are created to ensure the captured content is not modified by someone after the intercept is performed. The names of these hash files must be correlated to the capture files, and records must be kept so it is possible to confirm at a later date that each hash file is associated with the correct capture file or files. Intercept records including hash files must be kept confidential, and must be stored for at least 5 years, or as specified by the LEA.

Transparency

“Transparency” under CALEA generally means the target cannot detect that an intercept is being performed. For example, in networks with dynamically assigned IP addresses, it is unacceptable to reserve a block of IP addresses for intercepts, and then assign those addresses to the intercept target in response to an intercept order. It is also unacceptable to change the network configuration in any way that can be observed by the target in response to an intercept order. This means you can’t install equipment that changes the number of hops the target data must move across to reach the Internet.

There are some grey areas of transparency that may or may not be perceived as an issue for the LEA. For example, some carriers believe that it is acceptable to increase the lease on DHCP-assigned IP addresses for all customers to ensure the lease does not expire during the intercept. However, this action may be detected by the target, and the better option is to statically map the IP address to the target that the target is already using under the existing lease.

Here’s another example. Most trusted third parties (TTPs) who offer just-in-time support for intercepts are shipping hardware taps and probes that must be installed on the carriers network. While this action is being taken in response to a court ordered intercept, and the network is being interrupted and changed by installing a network tap and probe, the interruption cannot be identified by the target as being related to an intercept, and the tap and probe that is installed cannot be detected by the target.

Isolation

Isolation is about isolating target traffic from the other traffic that is not authorized for intercept by the court order. When an ImageStream router is configured to intercept traffic based on an IP or MAC address, it isolates the target traffic from non-targeted traffic based on the IP or MAC address.

It is not possible to isolate most Internet traffic on a more granular basis than by MAC or IP address. It is not the responsibility of the carrier to know who is actually using the equipment that is associated with the target’s access equipment. This means you don’t have to know who is using the target’s computer, and you are only required to isolate the authenticated of the target from other traffic on the network.

Completeness

The carrier is responsible for ensuring that the communications intercept is complete, and includes all of the traffic to and from the target during the period of time covered by the intercept order. A communications channel with the LEA will need to be established to report any anomalies or failures that may affect the completeness of the intercept.

Compression and Encryption

In general, intercepts must not be compressed or encrypted. If traffic to and from the target is compressed or encrypted as a normal part of network operations, then this traffic must be decompressed or decrypted before it is delivered to the LEA.

Buffering

If real-time intercept delivery over the Internet is used, there is a significant risk of data loss due to network issues that lie outside the LEA and the carrier. As a result, real-time intercepts must also be “buffered,” which has also been referred to in this White Paper as “capture-to-disk.” Buffering will ensure that the intercept data is captured for the LEA, even if there are problems with real-time delivery.

Fan-Out

“Fan-out” is the ability to deliver or buffer intercepts for multiple LEAs simultaneously. ImageStream routers support multiple real-time and capture-to-disk intercepts of a single target or multiple targets by simply configuring and running additional intercepts. Be sure to plan for the additional upstream bandwidth or disk space you will need to support multiple simultaneous intercepts.

Reliability

Intercept reliability is vital to the LEAs’ ability to use intercepts as evidence to support court cases against terrorists and other criminals. Intercept reliability is so important, it cannot be left to rely on the average reliability of the Internet. This is why capture-to-disk “buffering” should always be employed in addition to any real-time delivery requirement.

Network reliability issues are not limited to the Internet. Therefore, it is also important to understand potential reliability issues on your network. In general, it is always best to perform an intercept at an interface on the network that is closest to the target. Wireless ISPs should be especially careful not to depend on unreliable wireless connections to backhaul traffic to a buffering device at the CO or NOC. If the buffering device is not located at the POP closest to the target, and the intercept is incomplete due to data loss, the LEA may determine that the carrier is not CALEA compliant.

Intercept Content

Intercept content can be broken down to in-band and out-of-band (OOB) traffic. Out-of-band traffic in an IP network generally refers to the communications that take place between the customer and service provider equipment before an IP address is assigned to the customer’s access device. In-band traffic refers to the data stream that can be tied to an IP address.

Some service provider networks use statically assigned IP addresses with no OOB signaling. These networks can perform an intercept based on the target’s IP address without concern for capturing OOB traffic, which is really Layer 2 traffic. Service provider networks that use DHCP, RADIUS or some other dynamic method for assigning IP addresses to customers must use the target’s MAC address or interface name as the basis for the intercept, or the OOB traffic will not be captured. Intercepts can actually be configured to capture traffic based on MAC address and IP address for the same intercept, so this is always recommended as the most reliable way to set up an intercept when you know the target’s MAC and IP.

In-band capture content depends on the warrant. Some warrants will specify the intercept content to be packet headers only, while other warrants will require the full content of the target traffic to be delivered. These options are supported by ImageStream’s intercept tools. Configuration of these options is explained in the “Setup” section of this white paper.

Time Stamps

ImageStream's CALEA intercept tools support the requirement to provide time stamps on intercept data. This time stamping capability is built into the intercept tools, but it depends on the router's clock setting, so the time stamp is only as accurate as the system clock.

Because of this dependency, ImageStream recommends that routers subject to CALEA intercept orders should be configured to use NTP, the Network Time Protocol. NTP synchronizes the router's system clock with time servers on the Internet that are synchronized to the U.S. Naval Observatory Directorate of Time, which is the timekeeper for the U.S. and North America. When the system clock on the router is synchronized to the Directorate of Time, the time stamps that are provided in your intercepts will be relevant and useful to law enforcement.

Warrant ID

When you set up an intercept, the intercept configuration requires a warrant ID (a.k.a. "case ID") that uniquely identifies the intercept and associates it with the target. When an intercept is configured with the correct warrant ID, the intercept tools provided by ImageStream routers will label the intercept data with this ID so the intercept can always be correctly associated with the proper law enforcement case.

Recordkeeping

In general, it is recommended that you keep records of the intercepts you perform for at least 5 years, unless you negotiate a different period of record retention with the LEA. Records should include court documents, hash files from disk captures, and all written communications to and from the LEA.

There are many reasons why you might be required to communicate with the LEA regarding an intercept. For example, you may negotiate to report OOB traffic using your DHCP or RADIUS logs. If this is the case, be sure to filter out non-targeted traffic from the OOB reports, and store copies of those reports for the required period of time. VPN and other types of authentication event logs may also need to be reported, stored, and kept confidential. In addition, intercept problems, account and service changes, and even QoS modifications associated with the target may need to be reported, and these reports should also be stored and kept confidential for the prescribed period of time.

Intercept Pitfalls

There is a wide range of pitfalls that can affect the compliance of a particular intercept. This white paper cannot possibly identify all of the potential issues you may face, but it should give you enough information to identify common intercept challenges and address them, and it should help you better understand the kinds of issues that may affect your network.

Traffic Never Reaches the Router

A common intercept problem occurs when target traffic does not reach the ImageStream router where the intercept is set up. This may occur in networks where the ImageStream router is used in conjunction with another routing device or access point that does not support intercepts. In a wireline network, setting up intercepts on a core router or Internet gateway could miss local traffic that is routed at the customer edge. In wireless networks, a similar problem can occur when an access point does not support intercepts, and local traffic never makes it off the tower to the ImageStream router. Some access points actually support routing all of the local traffic off the tower to a router where the intercept

can be performed, but the AP and the router would still need to be configured with this in mind. This is why ImageStream recommends choosing an intercept location that is nearest to the customer.

Dynamic routing can also cause an intercept to fail. This should be obvious to anyone using BGP, OSPF or another dynamic routing protocol. In most cases, the interface closest to the target is not dynamically routed, so this problem can often be avoided by simply moving the intercept point to a point that is closest to the target. If it is not possible to move the intercept point, or if the target has network access over dynamically routed interfaces, then you will need to perform an intercept on each of the routers where the target traffic might end up.

Other Network Access Services

Most intercept recommendations focus on capturing the more difficult network access events such as customer authentication or DHCP transactions using the target's MAC address. But the LEAs may also require you to report additional network events if they are related to network access. For example, if a target accesses the network using an authenticated VPN service, then you may need to capture the authentication events in the logs for that service and provide them to the LEA on a negotiated basis.

On the other extreme, some service providers operate free unauthenticated Internet access services where there is no customer account, and little more than an unidentified DHCP transaction associated with the target. These are special cases where the carrier should be prepared to discuss unique intercept issues like this with the LEA, and determine the best course of action following the LEA's input. The FBI has said that CALEA does not make free unauthenticated Internet services illegal, however it is important to be prepared to cooperate with the LEA in every way possible to ensure that you can deliver intercepts based on the information they have.

Bonded Interfaces

ImageStream routers support CALEA intercepts on bonded interfaces, however the router must be installed in the production network and it must terminate the bonded interfaces. Some carriers perform intercepts using ImageStream routers and hardware taps with legacy equipment that does not support intercepts, that offers intercept software that is too expensive, or that requires TTP services for LEA delivery. An ImageStream router and tap can work in most applications as an out-of-band probe and mediation solution for intercepts, but this does not work for out-of-band intercepts with bonded circuits because the bonded interfaces must be reassembled in-band.

Network Address Translation (NAT)

Network Address Translation or "NAT" can cause serious problems with intercepts. It is virtually impossible to perform an intercept on the public side of a NATed connection. NATed traffic from different users shares the same public IP address, which makes it impossible to filter traffic down to a single target using the target's IP address.

Now we have established that intercepts must be performed on the private side of a NATed connection. But what do you do when you are using a single device for access and NAT that does not support intercepts? The quick answer is to replace the device with intercept-capable equipment, or add a device that can perform the intercept and NAT downstream from the access device. This may not be an affordable solution for some, so stay tuned to WISPA's work to see if they secure an exemption for this kind of equipment.

ARCHITECTURE

ImageStream's intercept architecture is based on one of the earliest releases of the OpenCALEA software project. Several new applications, scripts and `wan.conf` commands have been added to the 4.2.11-12 and later releases of ImageStream Linux.™ Here is a block diagram that will help you understand these system components and how they are used for different types of intercepts.

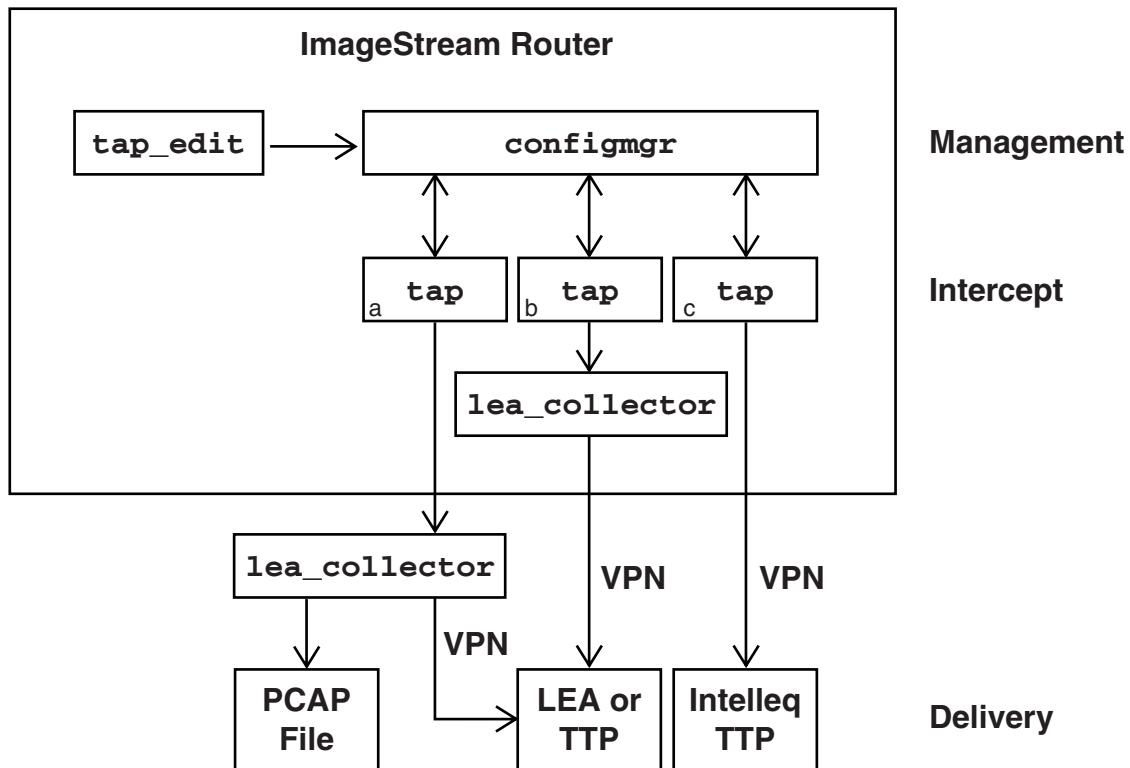


Figure 1 Intercept System Architecture

ImageStream's CALEA intercept architecture uses three key software components: `tap_edit`, `tap`, and `lea_collector`. Each intercept has a `tap` process to capture traffic and send the data to an `lea_collector` process for local storage or delivery to a TTP or LEA. Intercepts may be configured directly in the `wan.conf` configuration file, but this will leave intercept information in plain view of other sys admins. For better confidentiality protection, the `tap_edit` function is used to configure intercepts and store the configurations in an encrypted format. The intercept is run by `configmgr`, which starts and stops the `tap` processes that are configured in `wan.conf`, and configures each `tap` process based on the configuration parameters specified directly in `wan.conf` or indirectly using `tap_edit`. The `lea_collector` module is run on the router or an external file server to collect the intercept data, and deliver it, either by storing it to disk in the PCAP format or by piping it over a VPN for real-time delivery to the LEA.

`configmgr` uses a new `wan.conf` command called `run` to run the `tap_run` script which decrypts the intercept configuration file and runs the `tap` process. The `tap` process uses `libpcap` and standard PCAP/tcpdump filters to capture data. The intercept data is then delivered to an `lea_collector` process via a UDP socket in a custom packet format. The `lea_collector` cannot be run on the router if PCAP file storage is required, because the flash disk used by the router does not provide sufficient capacity to store intercepts.

Figure 1 includes examples of three different options for configuring an intercept. The “Tap A” example routes the intercept data to a collector that runs on an external server. The collector is used to support capture-to-disk as well as delivery to the LEA over a VPN.

Tap B is also shown in Figure 1, and it pumps the intercept data to the same collector software mentioned in the previous example. However, in this case the collector is running on the router, and it sends the intercept data to the LEA without performing the capture-to-disk function.

Tap C is set up to work with Intelq, ImageStream’s preferred TTP. The `tap` is configured to point to a remote `lea_collector` that is located at Intelq’s network operations center. Intelq uses the collector to pipe the data to their mediation device, which delivers the intercept data to the LEA.

INTERCEPT SETUP

Before you begin work in setting up an intercept, you need to know if you are working with a TTP or delivering intercepts directly to the LEA. You will need to know if you are conducting an in-band intercept on a production router, or if you are using the router out-of-band with a hardware tap like a combination probe and mediation device. Finally, you need to know what the warrant requires for the intercept.

Before you get too far along in the process, be sure negotiate with the LEA regarding any preferred delivery parameters or pitfalls that they need to understand in advance, and may want to address in ways that go beyond the tools provided by ImageStream. Make sure you are using a router distribution that supports CALEA intercepts (i.e. 4.2.11-12 or later). Also, be sure to consider the unique intercept requirements that may affect your network, including issues covered in the preceding sections of this white paper.

ImageStream also recommends that you contact ImageStream for technical support if you have not already performed an intercept successfully. While the information contained in this white paper may be followed to configure an intercept successfully, ImageStream engineers will have more experience setting up intercepts like this, and their help may be needed if you have problems.

Most intercept orders will specify whether you are required to capture full content or packet headers only. For direct real-time LEA delivery, the LEA will need to provide information on VPN setup to interface with their network. The LEA can install a collector device on your network if they choose to, so the exact way this will be done for your intercept must be specified by the LEA. If you are working with a TTP, the TTP will provide you with the setup information for the intercept, including the IP address of their collector, and perhaps VPN configuration information.

ImageStream recommends that you buffer all real-time intercepts, even if this is not required in the warrant. To support capture-to-disk, the collector software can simply be copied from the router to a compatible Linux server, or you can contact ImageStream support to get this software so you can install it on your own Linux server. The server must have enough network bandwidth to support the intercept, and it must have enough storage capacity to store the intercept.

You will need to know the IP address or the MAC address (or network interface) of the target to perform the intercept. In some networks, this information may already be known. In others, it may be something you have to determine from your DHCP logs, or other sources.

With all of this information in hand, you can proceed to setup an CALEA intercept. At this point, you will need to determine the best location for the intercept to be performed. While there may be several locations where data can be tapped, the best location is always the closest point on the network to the target. The best location is normally at the POP where the target accesses the network, on the interface that faces the target. If you are using hardware taps to perform an intercept, the tap would be installed on this network segment, the tap is connected to the router, and the router is connected to the network so it can talk to the LEA collector and/or the local collector.

Command Reference

The command reference that follows can be used to set up intercepts using the tools provided in 4.2.11-12 and later ImageStream Linux distributions.

Here is the syntax for the `tap` command:

```
tap -i interface -x content-id -y case-id -z iap-system-id  
[-d dest-ip] [-c] [-m cmc-port] [-n cmii-port] [-f capture-filter]
```

The interface should be the interface to listen in on. `Content-id`, `case-id`, and `iap-system-id` are assigned by the LEA. The `dest-ip` is the IP address of the collector. The `-c` option is used to specify a full stream capture as opposed to a capture of packet headers only, which is the default when the `-c` option is not used.

The `cmc-port` is the UDP port used by the `lea_collector` that will receive the full stream capture. If `-c` option is not used, the `cmc-port` option does not need to be specified. The `cmii-port` is the UDP port used by the `lea_collector` that will receive a packet-headers-only capture. This option is always required, and must be specified. The `capture-filter` is a `tcpdump`-style filter. In most cases we'll use a `host <IP>` filter, an `ether host <MAC>` filter, or both.

To support intercept confidentiality, the `tap_edit` and `tap_run` scripts can be used to store encrypted intercept configurations as separate files in the `/etc/taps` directory. The `tap_edit` script accepts a filename as its argument. Each intercept configuration should be given a unique filename. The script performs encryption and decryption automatically.

```
tap_edit filename
```

The configuration file uses the same arguments as the `tap` command line. Each argument needs to be placed on a separate line like this.

```
-i interface  
-x content-id  
-y case-id  
-z iap-system-id  
-d dest-ip  
-c  
-m cmc-port  
-n cmii-port  
-f capture-filter
```

The `tap_run` script is needed to decrypt the configuration file and invoke the `tap` program. This script should be run using the `run` command in the `wan.conf`.

```
run tap_run filename
```

Here is the syntax for the `lea_collector` command.

```
lea_collector -t cmii-capture-file [-f cmc-capture-file]
[-m cmc-port] [-n cmii-port] [-o output-interface]
```

The `cmii-capture-file` is the full path and filename of the capture file that will be written to disk for packet-header-only captures. The `cmc-capture-file` is the full path and filename of the capture file that will be written to disk for full stream captures. The `cmc-port` is the same UDP port used by the `tap` to transmit the full stream capture to the collector. The `cmii-port` is the same UDP port used by the `tap` to transmit the packet-header-only capture to the collector. The `output-interface` is the interface that can be used to retransmit the full stream capture to an LEA or TTP over a VPN or other network interface (headers are not retransmitted using this option).

Be sure that you do not specify a capture file storage location on an ImageStream router unless it has an attached hard drive. Otherwise, you will fill up the router's ramdisk, which will cause the intercept to fail. If you are running this command on an ImageStream router, specify the `-o` option to mirror the incoming CMC data to the specified output interface for delivery to the LEA or TTP.

Be sure to repeat this setup process for every delivery point and each LEA that requires an intercept, even if multiple LEAs require intercept of the same target at the same time. Be sure to use unique file names and unique UDP ports for each intercept. And finally, be sure to backup to flash, otherwise all of this work will be destroyed if the router is restarted for any reason.