



Cisco Service Independent Intercept Architecture Version 1.0

Version History

Version Number	Date	Notes
1	7/23/2003	This document was created.
2	3/15/2006	This document was updated and includes version I03 of the PacketCable Event Message Specification, BTS versions 3.5 and 4.1, and version 1.0 of Cisco LI MIB.

Abstract

Cisco Service Independent Intercept (SII) architecture version 1.0 was developed in response to the needs of Cisco's service provider (SP) and Internet service provider (ISP) customers for compliance with Lawful Intercept (LI) legislation and regulations. It provides a common approach for intercepting IP communications using existing network elements.

LI is the process (not a specific regulatory requirement) by which law enforcement agencies (LEAs) conduct electronic surveillance as authorized by judicial or administrative order. Legislation and regulations are increasingly being adopted that require SPs and ISPs to design and implement their networks to explicitly support authorized electronic surveillance. Types of SPs and ISPs that are subject to LI mandates vary greatly from country to country. The *Cisco Service Independent Intercept Architecture Version 1.0* document describes the implementation of an LI architecture on a Cisco IP network that uses version 1.0 of Cisco LI Management Information Base (MIB) for Voice over IP (VoIP) and IP data intercepts.

This architecture is designed to support “plug-and-play” capability, which means that any architecture component can be replaced by any other Cisco SII-compliant component. Because of this flexibility in component choices, it is impractical for this document to completely describe all aspects of LI implementation for all of the possible components. Therefore, this document is intended as a high-level description of the end-to-end Cisco SII LI version 1.0 architecture including how LI works, the roles of the various components, and the available component options. The document also provides some information on design, implementation, operation, and troubleshooting of LI on a Cisco SII network. For detailed specifics on the various devices (such as image and memory requirements, configurations, and so on), this document references the product documentation of the devices.

Contents

This document contains the following sections:

- [Business Objectives of the Cisco SII LI Architecture, page 2](#)
- [Cisco Service Independent Intercept Architecture, page 3](#)
- [Implementation of Cisco SII Lawful Intercept, page 21](#)
- [Device Configuration Files, page 22](#)
- [Verifying the Cisco SII LI Network, page 33](#)
- [Troubleshooting a Cisco SII LI Network, page 40](#)
- [Appendix, page 41](#)
- [Glossary, page 47](#)

Business Objectives of the Cisco SII LI Architecture

The following sections describe the business objectives of implementing the Cisco SII LI architecture:

- [Key Requirements of LI Architecture, page 2](#)
- [Business Drivers, page 3](#)

Key Requirements of LI Architecture

The following are the key requirements any LI architecture must meet:

- LI must be undetectable by the intercept subject. Thus providing a wiretap at the customer premise equipment (CPE) or diverting the call to a conference unit (where the replication would take place) is not acceptable because the intercept subject can detect the LI. (Sophisticated users can determine that their call has been diverted because the source and destination IP addresses do not match.) Therefore, the tapping must take place on equipment that is within the domain of trust of the SP or ISP (on an edge router or access server) and must be performed along the normal path of the data.
- Multiple LEAs intercepting the same subject must not be aware of each other. This confidentiality is achieved by having a one-way flow of intercept information from the mediation device to the LEA such that no information in the flow can indicate that multiple flows to different LEAs exist. It also implies limited access of LEAs to the SP's or ISP's equipment.
- Unauthorized personnel's knowledge of and capability to perform LI must be prevented. Security mechanisms must be in place to limit unauthorized personnel from performing or knowing about wiretaps as much as possible.
- The information identifying intercepts (phone numbers, IP addresses, and so on) must be correlated with the corresponding content of the intercepts.
- The reliability of delivery of information to the LEAs must be on the same order as the original delivery of the packets to customers.

Business Drivers

SPs and ISPs are required to meet LI requirements for voice and data in a variety of countries worldwide. Communications Assistance for Law Enforcement Act (CALEA) is a public law that describes how telephony service providers in the United States must support LI. In Europe there are a number of similar laws, including the Regulation of Investigatory Powers Act (RIPA) in the United Kingdom, the Telecom Act/Telekommunikations Überwachungsverordnung (TKUV) in Germany, the Telecom Act in France, the Criminal Code in Italy, and the Telecom Act in the Netherlands. However, in Europe, legal requirements and specific interfaces vary from country to country.

Two specifications define the interface to the LEAs for the purposes of meeting the CALEA requirements:

- The J-STD-025A specification that was developed by the Telephone Industry Association (TIA).
- The *PacketCable Electronic Surveillance Specification* document. (See the “[Related Documents](#)” section on page 45.)

Cisco Service Independent Intercept Architecture

The following sections describe the Cisco SII version 1.0 of Cisco LI MIB architecture:

- [Overview, page 3](#)
- [Network Topology, page 4](#)
- [Interfaces Between Devices, page 6](#)
- [How Cisco SII LI Architecture Works, page 8](#)

Overview

The SII architecture was developed in response to the needs of Cisco’s SP and ISP customers for compliance with LI legislation and regulations. It provides a common approach for intercepting IP communications using existing network elements. The architecture addresses the key LI requirements mentioned earlier and does so in a cost-effective manner. Key features of the architecture include the following:

- Use of standard access list technology to provide the intercept.
- Encapsulation of the entire intercepted and replicated packet so that the original source and destination addresses are available (important information for intercept purposes).
- Use of a control plane for intercept that is different from call control, which prevents network operations personnel from detecting the presence of active intercepts in the network.

**Note**

A control plane defines the transport used for sending or receiving the messages that initiate the LI. Since it is important that network operations personnel not know that intercepts are active on the network, it is important to hide or keep separate the active intercept messages from those messages used for routine call setup. However, many SPs and ISPs routinely monitor all messages for diagnostic purposes.

- An integrated approach that limits the intercept activity to the router or gateway that is handling the target’s IP traffic and only activates an intercept when the target is accessing the network.

- No LI-related command-line interface (CLI) commands that could allow for the detection of intercept activity on a router or gateway.
- LI-related MIBs and traps sent only to the (third-party) equipment controlling the intercept.
- Support for multiple encapsulation and transport formats.

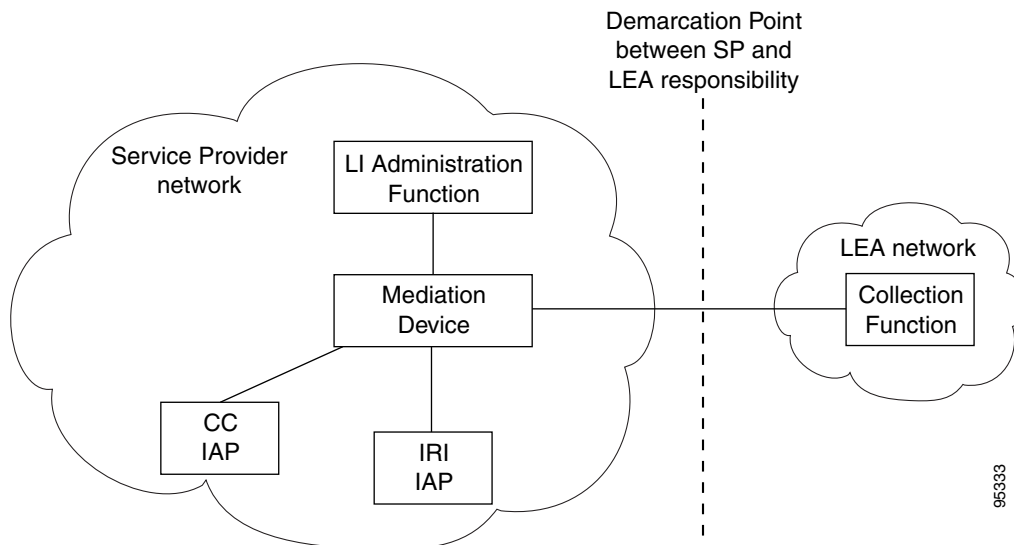
**Note**

At this time, the only format implemented is the format specified in the [PacketCable Electronic Surveillance Specification](#) document that uses User Datagram Protocol (UDP) frames to encapsulate duplicated packets.

Network Topology

Figure 1 shows a functional depiction of a generic IP network that supports LI of voice or data traffic.

Figure 1 **Functional Depiction of a Generic LI Network**

**Note**

IRI IAP is defined as the Intercept-Related Information intercept access point and CC IAP is defined as the Communication Content intercept access point.

The following sections describe the components that are integral to the Cisco SII network:

- [LI Administration Function, page 5](#)
- [Mediation Device/Delivery Function, page 5](#)
- [Intercept-Related Information Intercept Access Point, page 5](#)
- [Communication Content Intercept Access Point, page 5](#)
- [Collection Function, page 5](#)

LI Administration Function

The SP and ISP uses the LI administration function to provision intercepts by interfacing with the other components in the network. It is responsible for provisioning components in the network, administering intercept orders, and tracking and maintaining intercept information. It also supervises the security and integrity of the LI process by continuously auditing activity logs to ensure that only authorized intercepts are provisioned and that authorized intercepts are not disrupted.

**Note**

Provisioning intercepts is defined as accessing a device and changing the device's operational parameters to activate a desired function on that device.

Mediation Device/Delivery Function

The mediation device (MD) is maintained by the SP and ISP and is the center of the LI process. It sends configuration commands to the various IAPs to enable intercepts, receives intercept information (both IRI and CC), and delivers this information to the LEA. If more than one LEA is monitoring an intercept target, the mediation device duplicates the intercept information for each LEA. The mediation device is sometimes called the delivery function.

In some cases, the mediation device performs additional filtering of the information. It is also responsible for formatting the information to be compliant with the country or technology-specific requirements for delivery to law enforcement.

Mediation devices are third-party equipment. Cisco has performed end-to-end testing with a number of mediation device vendors. A list of these vendors can be found at the following URL:

http://www.cisco.com/wwl/regaffairs/lawful_intercept/index.html

Intercept-Related Information Intercept Access Point

The Intercept-Related Information intercept access point (IRI IAP) is the device that provides identification information to the mediation device. IRI for voice includes the source and destination phone numbers and IP addresses and the time of the call. It also includes any post call-establishment messaging such as call forwarding or three-way calling. IRI for data includes login and logout times and source and destination IP addresses. For voice intercepts, the IRI IAP is the call control entity. The call control entity can be a call agent, Session Initiation Protocol (SIP) proxy, or H.323 gateway. For data intercepts, the IRI IAP is the authentication, authorization, and accounting (AAA) server.

Communication Content Intercept Access Point

The Communication Content IAP (CC IAP) is the device that intercepts communication content information, replicates it, and forwards the replicated information to the mediation device. The CC IAP should be located as close to the source of the call as possible to minimize the number of simultaneous calls the device will have to monitor and to ensure that CC can be reliably intercepted. The edge device is the only device that can guarantee CC intercept. The CC IAP can be an edge router, a trunking gateway, or an access server.

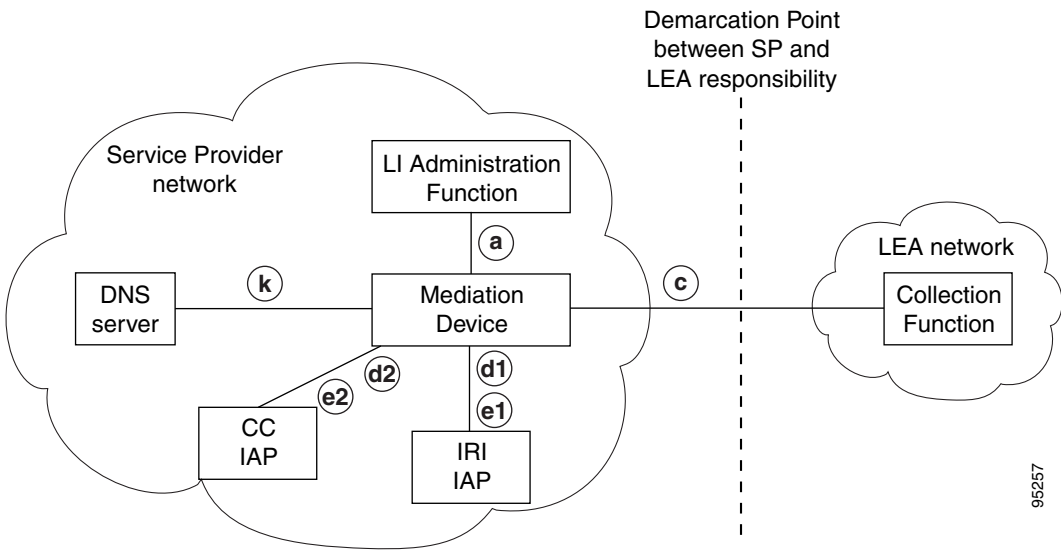
Collection Function

The collection function is a third-party device maintained by the LEA that receives, sorts, and stores intercept information from the mediation device. The collection function may also include case management capabilities.

Interfaces Between Devices

Figure 2 shows a functional depiction of the device interfaces in a Cisco SII network.

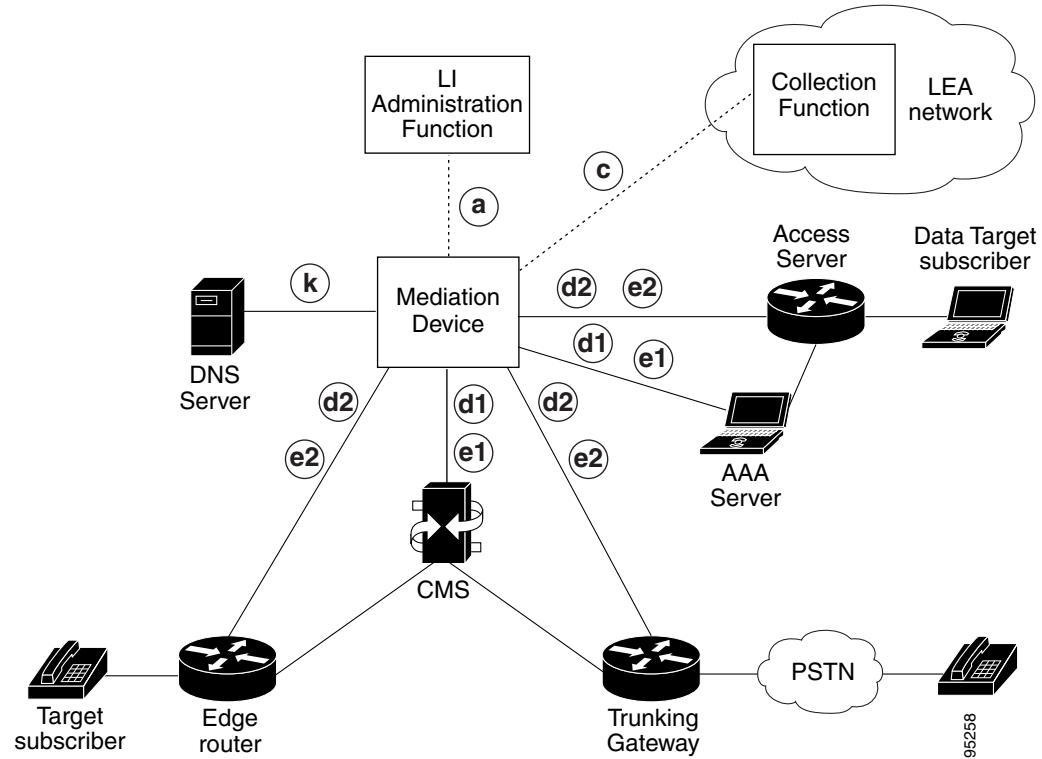
Figure 2 *Functional Depiction of a Cisco SII LI Network*



95257

Figure 3 shows the device interfaces in the context of the specific devices that are used in a Cisco SII network.

Figure 3 Cisco SII Voice Intercept Device Interfaces



Note

PSTN is defined as public switched telephone network.

Table 1 describes the interfaces between devices shown in Figure 2 and Figure 3.

Table 1 Cisco SII LI Network Device Interfaces

Interface	Description	Description
a	Authorization: administration function and mediation device	The LI administration function sends intercept provisioning information (target identifier, duration of intercept, and so on) to the mediation device.
c	Content: mediation device and collection function	The mediation device delivers intercept information to the collection function. If more than one LEA is intercepting the same target, the mediation device must duplicate the intercept information to send to the collection function of each LEA. This interface meets the specifications found in the PacketCable Electronic Surveillance Specification document in the “Related Documents” section on page 45.

Table 1 **Cisco SII LI Network Device Interfaces (continued)**

Interface	Description	Description
d1	IRI Delivery: IRI IAP and mediation device	<p>This is the delivery interface. The IRI IAP uses this interface to deliver IRI to the mediation device. For voice, this is according to the PacketCable Event Messages Specification document in the “Related Documents” section on page 45. For data, this is Remote Authentication Dial-In User Service (RADIUS) accounting messages.</p> <p>For voice intercepts, the IRI IAP is the call control entity (call agent, SIP proxy, or H.323 gateway). For data intercepts, the IRI IAP is the AAA server (or a sniffer monitoring RADIUS traffic).</p>
d2	CC delivery: CC IAP and mediation device	<p>The call content (CC) IAP replicates CC and sends it to the mediation device. The CC IAP encapsulates the packets with additional UDP and IP headers and a 32-bit call content connection identifier (CCCID) header. (See the PacketCable Electronic Surveillance Specification document in the “Related Documents” section on page 45.) The CCCID is used to associate the CC with the target.</p> <p>The CCCID is included so that the mediation device can map intercepts to the appropriate warrants. Usually, the mediation device will rewrite the CCCID before forwarding intercept information to collection functions.</p> <p>The CC IAP is an edge router, trunking gateway, or access server.</p>
e1	Provisioning: mediation device and IRI IAP	The mediation device uses Secure Shell (SSH) to provision an intercept on the IRI IAP.
e2	Provisioning: mediation device and CC IAP	The mediation device uses Simple Network Management Protocol version 3 (SNMPv3) to instruct the CC IAP to replicate CC and send it to the mediation device. The CC IAP can be either an edge router or a trunking gateway for voice. It is an edge router or access server for data.
k	DNS Lookup: mediation device and DNS server	The mediation device queries the Domain Name Service (DNS) server to determine the fully qualified domain name (FQDN) of the CC IAP.

How Cisco SII LI Architecture Works

The following sections describe how the Cisco SII LI architecture works:

- [Types of Intercepts, page 9](#)
- [Initiating an Intercept, page 9](#)
- [Terminating an Intercept, page 9](#)
- [Cisco SII Voice Intercept Process Flows, page 9](#)
- [Security Considerations, page 19](#)
- [Failure Recovery, page 20](#)

Types of Intercepts

There are two types of intercepts:

- **Intercept-Related Information only**—This is the most common type of intercept. It intercepts only the IRI. For voice intercepts, IRI includes the source and destination phone numbers and IP addresses and the time of the call, and any post call-establishment messaging, such as call forwarding or three-way calling. For data intercepts, IRI includes login and logout times and source and destination IP addresses. Intercepting IRI has minimal impact on the bandwidth and processing power of the network. This type of intercept is also referred to as Pen Register or Trap and Trace.
- **Intercept-Related Information and Communication Content**—Typically, a small percentage of intercepts require the capture of both IRI and CC. Intercepting CC has a substantial impact on network bandwidth and device processing power. This type of intercept is also referred to as a Full Content or, in the United States, as Title 3 intercept.

Initiating an Intercept

When a warrant is issued, the LEA physically delivers the warrant to the SP or ISP. When the SP or ISP receives the warrant, it uses the LI administration function to enable LI on the target specified in the warrant. If the warrant is delivered prior to the authorized start date and time, the mediation device waits until the authorized start date and time to configure the tap. Once the intercept is provisioned on the mediation device, the process of initiating individual intercepts is completely automated.

Terminating an Intercept

When a warrant is issued, it includes an expiration date that is typically 30 days. This expiration date is configured on the mediation device. When the warrant expires, the mediation device automatically removes the configuration for the warrant. The mediation device provisioning interface can be used to remove a warrant before the expiration date.

Cisco SII Voice Intercept Process Flows

The following sections describe the various Cisco SII voice intercept process flows:

- [Standard Cisco SII Voice Intercept, page 10](#)
- [Hairpin Cisco SII Voice Intercept, page 12](#)
- [Cisco SII Three-Way Voice Intercept, page 13](#)
- [Cisco SII Call Forward to Voice Mail Intercept, page 16](#)
- [Cisco SII Data Intercept, page 18](#)

Standard Cisco SII Voice Intercept

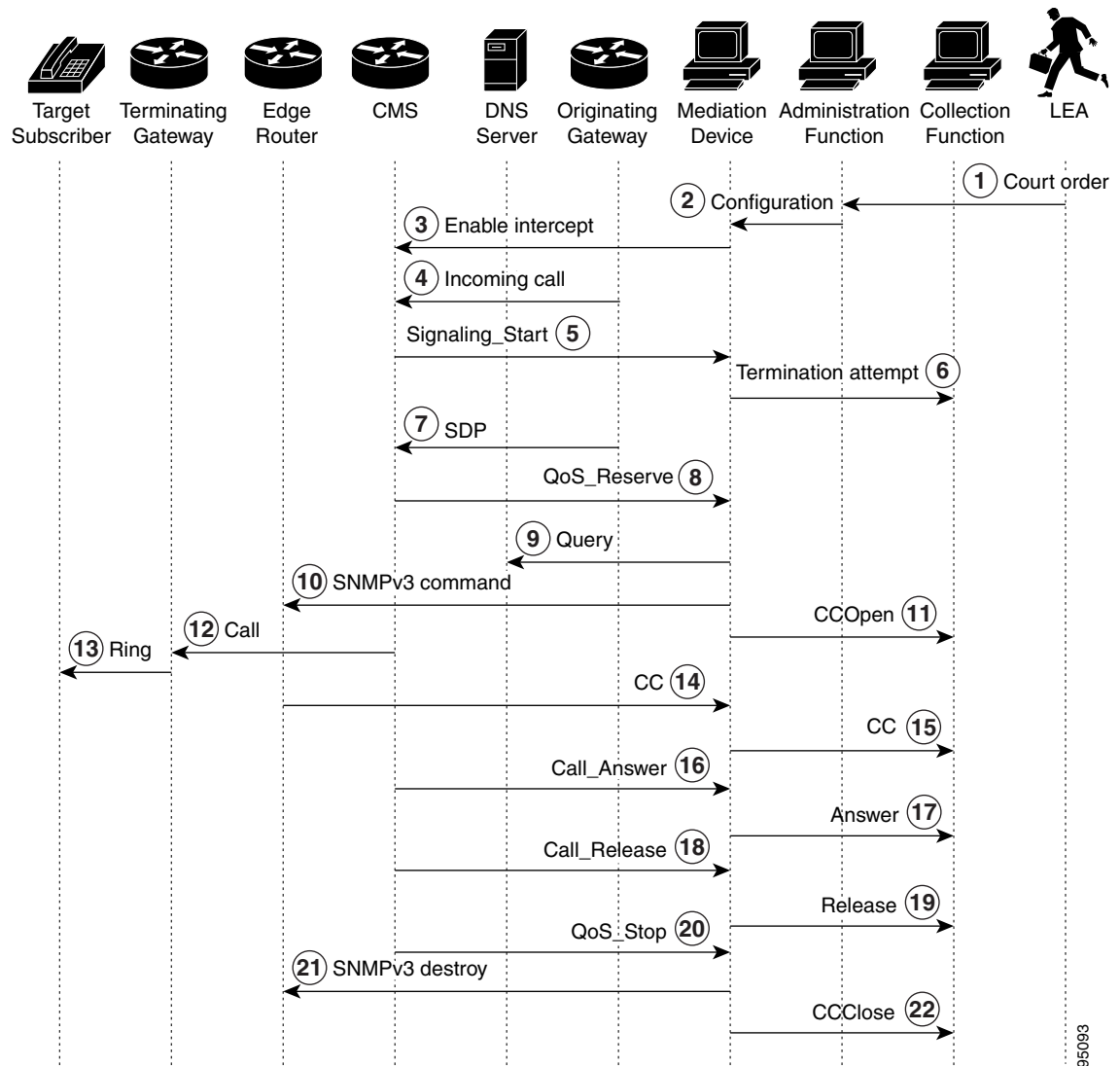
Figure 4 shows the topology for a standard Cisco SII voice intercept.



Note

This is a high-level call flow that does not include all details of the protocol messaging involved.

Figure 4 *Standard Cisco SII Voice Intercept at Trunking Gateway or Aggregation Router*



The following steps describe the sequence of events shown in Figure 4.

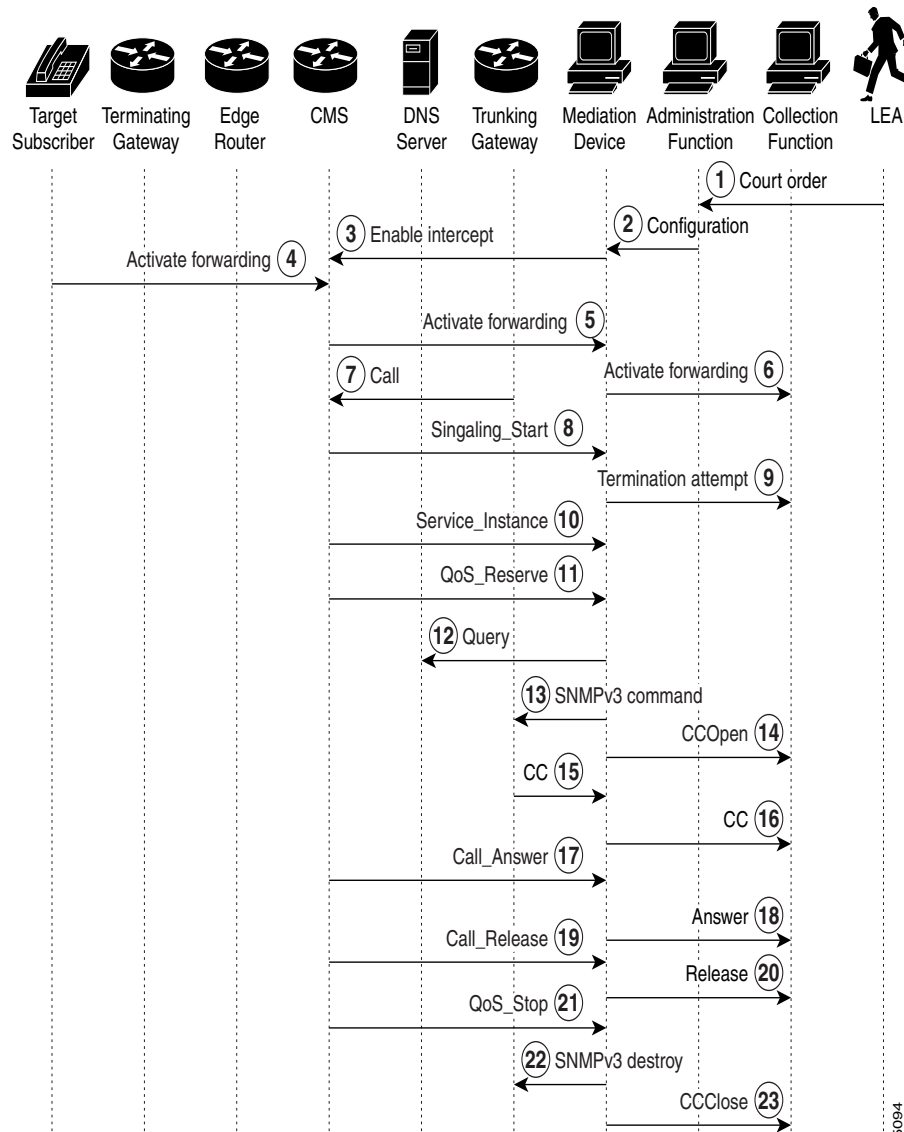
- Step 1** The LEA physically delivers a court order to the network administrator who operates the LI administration function.
- Step 2** The LI administration function sends a configuration to the mediation device that enters the intercept.
- Step 3** The mediation device sends a configuration command to the call management server (CMS) to enable the intercept.

- Step 4** The intercept target receives an incoming call.
 - Step 5** The CMS sends a Signaling_Start message to the mediation device.
 - Step 6** The mediation device sends a termination attempt message to the collection function.
 - Step 7** The originating gateway sends Session Definition Protocol (SDP) information to the CMS.
 - Step 8** The CMS sends the SDP information to the mediation device in a QoS_Reserve message.
 - Step 9** The mediation device queries the DNS server to determine the IP address of the edge router (based on the IP address of the target gateway).
 - Step 10** The mediation device sends an SNMPv3 command to the edge router to initiate the intercept.
 - Step 11** The mediation device sends a CCOpen message with the SDP to the collection function.
 - Step 12** The CMS delivers the call to the terminating gateway.
 - Step 13** The terminating gateway rings the target phone.
 - Step 14** The call is connected end-to-end, and the edge router intercepts and replicates all voice packets and sends the packets to the mediation device.
 - Step 15** The mediation device delivers CC to the collection function.
 - Step 16** The CMS sends a Call_Answer message to the mediation device.
 - Step 17** The mediation device forwards this message as an Answer message to the collection function.
 - Step 18** When the parties hang up, the CMS sends a Call_Release message to the mediation device.
 - Step 19** The mediation device forwards this message as a Release message to the collection function.
 - Step 20** The CMS sends a QoS_Stop message to the mediation device.
 - Step 21** When the mediation device receives the QoS-Stop message, it sends SNMPv3 messages to the edge router instructing it to destroy the CC monitoring sessions and the mediation device MIB. Three destroy messages are sent: one for each of the two CC streams and one for the mediation device MIB.
 - Step 22** The mediation device sends a CCClose message to the collection function.
-

Hairpin Cisco SII Voice Intercept

Figure 5 shows the topology for a Cisco SII voice intercept in a hairpin scenario (when a call coming in from the PSTN to the intercept target is forwarded off the network and back to the PSTN).

Figure 5 Hairpin Cisco SII Voice Intercept at Trunking Gateway



5094

The following steps describe the sequence of events shown in Figure 5.

- Step 1** The LEA physically delivers a court order to the network administrator who operates the LI administration function.
- Step 2** The LI administration function sends a configuration to the mediation device that enters the intercept.
- Step 3** The mediation device sends a configuration command to the CMS to enable the intercept.
- Step 4** The intercept target activates call forwarding to an off network (off-net) number.

- Step 5** The CMS informs the mediation device that the target has activated call forwarding.
- Step 6** The mediation device forwards the feature activation code for call forwarding to the collection function.
- Step 7** The target receives a call from the PSTN that triggers call forwarding.
- Step 8** The CMS sends a Signaling_Start message to the mediation device.
- Step 9** The mediation device sends a termination attempt message to the collection function.
- Step 10** The CMS sends a Service_Instance message to the mediation device indicating that the call is being forwarded.
- Step 11** The CMS sends a QoS_Reserve message to the mediation device.
- Step 12** The mediation device queries the DNS server to determine the IP address of the trunking gateway.
- Step 13** The mediation device sends an SNMPv3 command to the trunking gateway to enable an intercept (if call content is to be intercepted) and to route the call back to the PSTN.



Note If the terminating gateway does not support SNMPv3, Media Gateway Control Protocol (MGCP) is used instead.

- Step 14** The mediation device sends a CCOpen message to the collection function.
- Step 15** The trunking gateway duplicates all packets and sends them to the mediation device.
- Step 16** The mediation device delivers CC to the collection function.
- Step 17** The CMS sends a Call_Answer message to the mediation device.
- Step 18** The mediation device forwards this message as an Answer message to the collection function.
- Step 19** When the parties hang up, the CMS sends a Call_Release message to the mediation device.
- Step 20** The mediation device forwards this message as a Release message to the collection function.
- Step 21** The CMS sends a QoS-Stop message to the mediation device.
- Step 22** When the mediation device receives the QoS-Stop message, it sends SNMPv3 messages to the trunking gateway instructing it to destroy the CC monitoring sessions and the mediation device MIB. Three destroy messages are sent: one for each of the CC streams and one for the mediation device MIB.



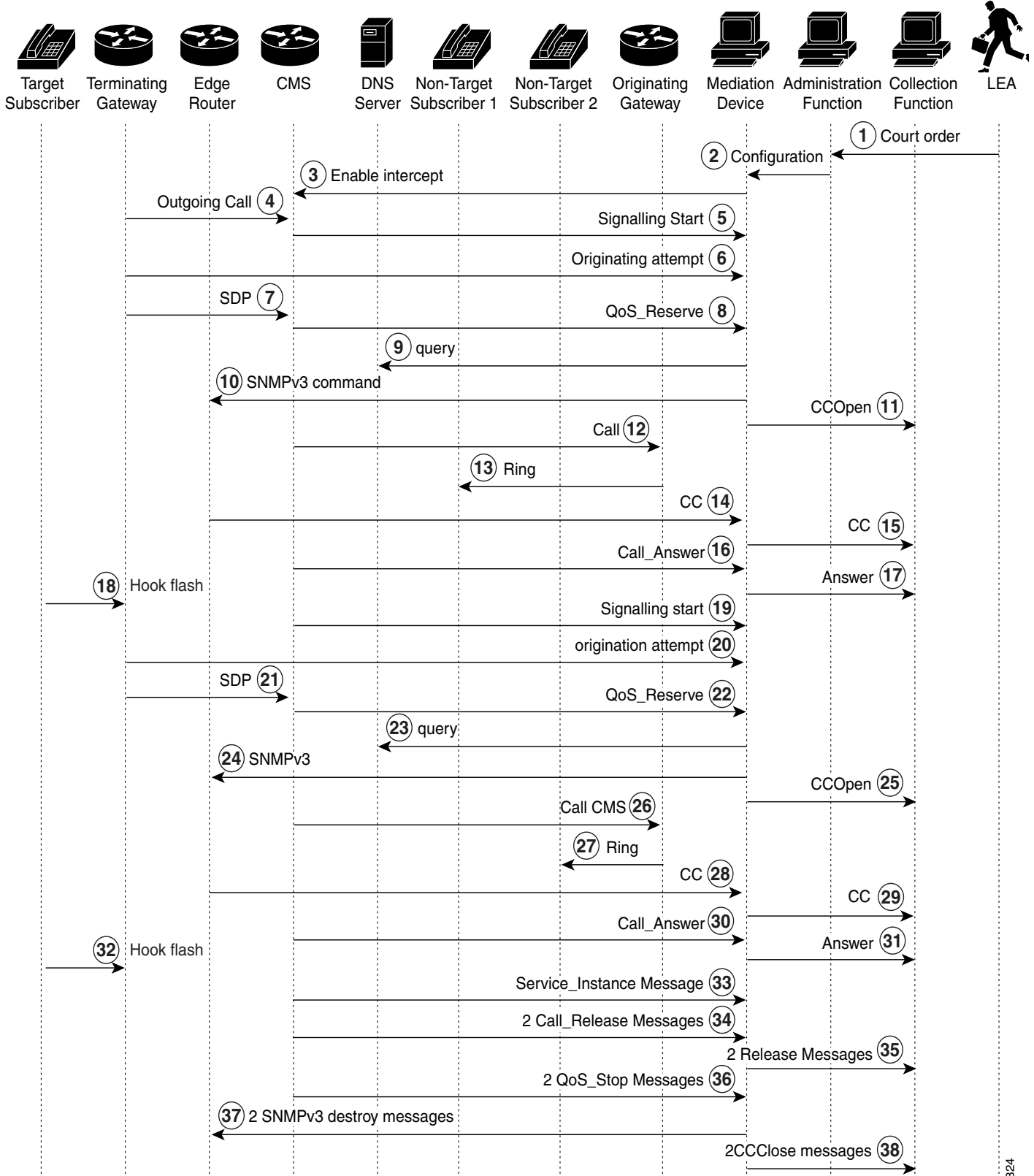
Note If MGCP was used by the mediation device to access CC, then the instruction from the CMS to delete the connection also stops CC duplication. In this case, the mediation device does not need to send any additional messages to terminate the intercept.

- Step 23** The mediation device sends a CCClose message to the collection function.
-

Cisco SII Three-Way Voice Intercept

Figure 6 shows the topology for a Cisco SII of a three-way voice conference call.

Figure 6 Cisco SII Three-Way Voice Intercept



The following steps describe the sequence of events shown in [Figure 6](#).

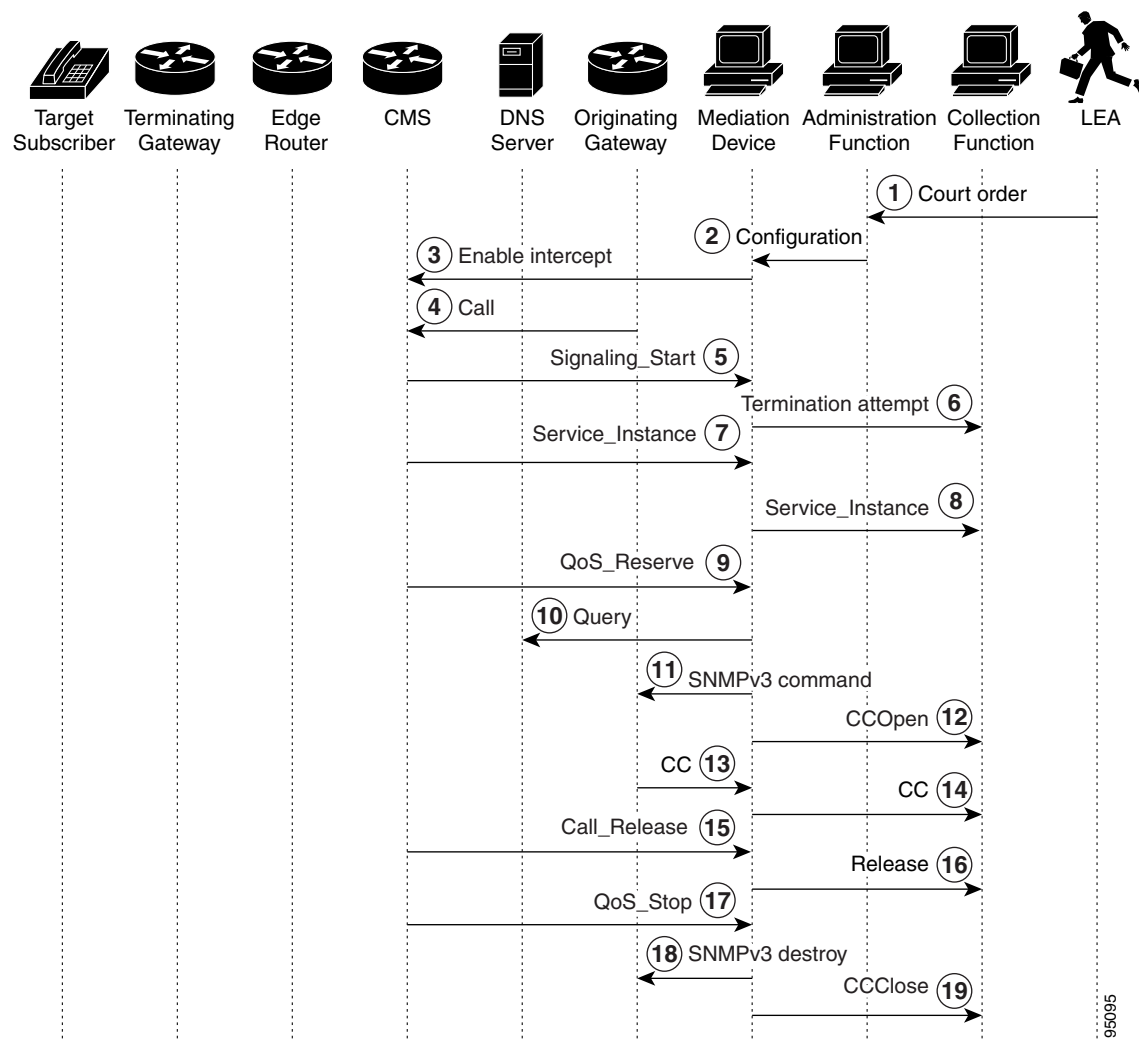
-
- | | |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | The LEA physically delivers a court order to the network administrator who operates the LI administration function. |
| Step 2 | The LI administration function sends a configuration to the mediation device that enters the intercept. |
| Step 3 | The mediation device sends a configuration command to the CMS to enable the intercept. |
| Step 4 | In this scenario, the intercept target initiates an outgoing call. |
| Step 5 | The CMS sends a Signaling_Start message to the mediation device. |
| Step 6 | The terminating gateway sends an originating attempt message to the mediation device. |
| Step 7 | The terminating gateway sends SDP information to the CMS. |
| Step 8 | The CMS sends the SDP information to the mediation device in a QoS_Reserve message. |
| Step 9 | The mediation device queries the DNS server to determine the IP address of the edge router (based on the IP address of the target gateway). |
| Step 10 | The mediation device sends an SNMPv3 command to the edge router to initiate the intercept. |
| Step 11 | The mediation device sends a CCOpen message with the SDP to the collection function. |
| Step 12 | The CMS delivers the call to the originating gateway. |
| Step 13 | The originating gateway rings non-target subscriber 1. |
| Step 14 | The call is connected end-to-end, and the edge router intercepts and replicates all voice packets and sends the packets to the mediation device. |
| Step 15 | The mediation device delivers CC to the collection function. |
| Step 16 | The CMS sends a Call_Answer message to the mediation device. |
| Step 17 | The mediation device forwards this message as an Answer message to the collection function. |
| Step 18 | The target hook flashes to put the Hook non-target subscriber 1 on hold and initiate a second call. |
| Step 19 | The CMS sends a Signaling_Start message to the mediation device. |
| Step 20 | The terminating gateway sends an originating attempt message to the mediation device. |
| Step 21 | The terminating gateway sends SDP information to the CMS. |
| Step 22 | The CMS sends the SDP information to the mediation device in a QoS_Reserve message. |
| Step 23 | The mediation device queries the DNS server to determine the IP address of the edge router (based on the IP address of the target gateway). |
| Step 24 | The mediation device sends an SNMPv3 command to the edge router to initiate the intercept. |
| Step 25 | The mediation device sends a CCOpen message with the SDP to the collection function. |
| Step 26 | The CMS delivers the call to the originating gateway. |
| Step 27 | The originating gateway rings non-target subscriber 2. |
| Step 28 | The call is connected end-to-end, and the edge router intercepts and replicates all voice packets and sends the packets to the mediation device. |
| Step 29 | The mediation device delivers CC to the collection function. |
| Step 30 | The CMS sends a Call_Answer message to the mediation device. |
| Step 31 | The mediation device forwards this message as an Answer message to the collection function. |
| Step 32 | The target hook flashes to create a three-way call. |

- Step 33** The CMS sends a Service_Instance message indicating Three_Way_Call to the mediation device.
- Step 34** When the parties hang up, the CMS sends two Call_Release messages to the mediation device, one for each part of the three-way call.
- Step 35** The mediation device forwards these messages as Release messages to the collection function.
- Step 36** The CMS sends two QoS_Stop messages to the mediation device.
- Step 37** When the mediation device receives the QoS_Stop message, it sends SNMPv3 messages to the terminating gateway instructing it to destroy the CC monitoring sessions and the mediation device MIB. Six destroy messages are sent: three for each part of the three-way call.
- Step 38** The mediation device sends two CCClose messages to the collection function.

Cisco SII Call Forward to Voice Mail Intercept

Figure 7 shows the topology for a Cisco SII of a voice call that is forwarded to voice mail.

Figure 7 Cisco SII Call Forward to Voice Mail Intercept



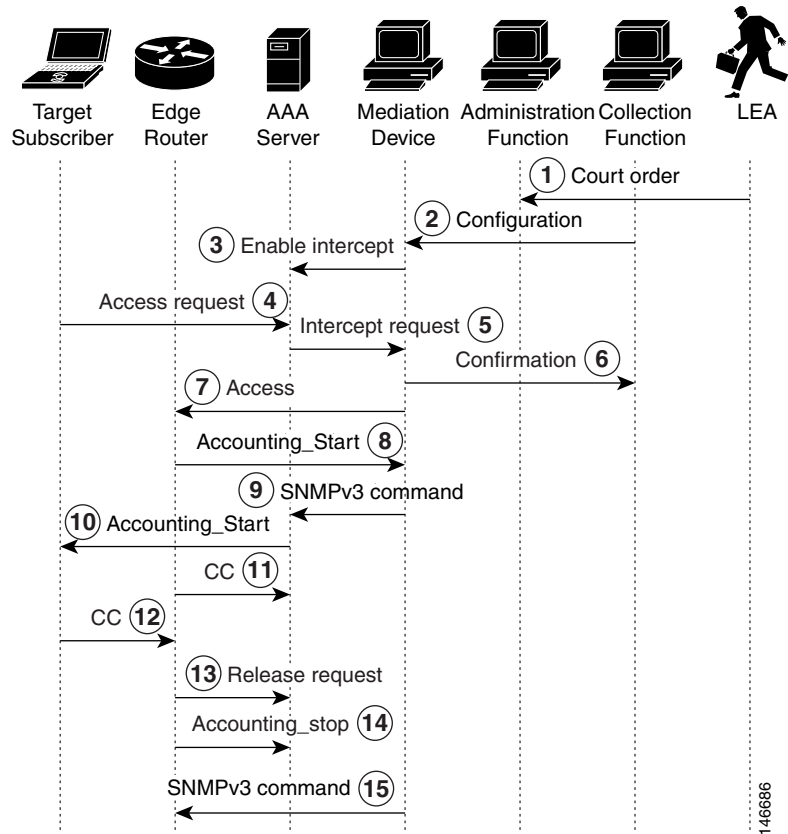
The following steps describe the sequence of events shown in [Figure 7](#).

-
- | | |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | The LEA physically delivers a court order to the network administrator who operates the LI administration function. |
| Step 2 | The LI administration function sends a configuration to the mediation device that enters the intercept. |
| Step 3 | The mediation device sends a configuration command to the CMS to enable the intercept. |
| Step 4 | The target receives a call from the PSTN that is not answered, which triggers call forwarding to voice mail. |
| Step 5 | The CMS sends a Signaling_Start message to the mediation device. |
| Step 6 | The mediation device sends a termination attempt message to the collection function. |
| Step 7 | The CMS sends a Service_Instance message to the mediation device indicating that the call is being forwarded. |
| Step 8 | The mediation device forwards the Service_Instance message to the collection function. |
| Step 9 | The CMS sends a QoS_Reserve message to the mediation device. |
| Step 10 | The mediation device queries the DNS server to determine the IP address the call is being forwarded to. When the mediation device determines the call is being forwarded to the voice mail system, it knows that the call must be intercepted on the originating side. |
| Step 11 | The mediation device sends an SNMPv3 command to the originating gateway to enable an intercept (if call content is to be intercepted). |
| Step 12 | The mediation device sends a CCOpen message to the collection function. |
| Step 13 | The originating gateway duplicates all packets and sends them to the mediation device. |
| Step 14 | The mediation device delivers CC to the collection function. |
| Step 15 | When the caller hang up, the CMS sends a Call_Release message to the mediation device. |
| Step 16 | The mediation device forwards this message as a Release message to the collection function. |
| Step 17 | The CMS sends a QoS_Stop message to the mediation device. |
| Step 18 | When the mediation device receives the QoS_Stop message, it sends SNMPv3 messages to the terminating gateway instructing it to destroy the CC monitoring sessions and the mediation device MIB. Six destroy messages are sent: three for each part of the three-way call. |
| Step 19 | The mediation device sends a CCClose messages to the collection function. |
-

Cisco SII Data Intercept

Figure 8 shows the topology for a Cisco SII data intercept.

Figure 8 Cisco SII Data Intercept



The following steps describe the sequence of events shown in Figure 8.

- Step 1** The LEA physically delivers a court order to the network administrator who operates the LI administration function.
- Step 2** The LI administration function sends a configuration to the mediation device that enters the intercept.
- Step 3** The mediation device enables the intercept on a sniffer or a probe that is configured to sniff all AAA traffic and inform the mediation device when the target subscriber authenticates in the network.
- Step 4** When the target subscriber accesses the network, the target subscriber's computer sends an access request to the AAA server.
- Step 5** The mediation device is notified that the intercepted target subscriber is active in the network by the sniffer or probe monitoring the AAA server.
- Step 6** The AAA server grants access to the target subscriber.
- Step 7** The edge router forwards the Accounting_Start message to the AAA server.

- Step 8** The mediation device is notified that the intercepted target subscriber's session has been successfully authenticated and is now active in the network.
- Step 9** The mediation device sends an SNMPv3 command to the edge router to enable the intercept (if communication content is to be intercepted).
- Step 10** When the data stream begins, the edge router intercepts the CC, replicates it, and forwards it to the mediation device.
- Step 11** The mediation device forwards the CC to the collection function.
- Step 12** The target subscriber's computer sends a release request to the edge router to disconnect the session from the network.
- Step 13** The edge router sends an Accounting_Stop message to the AAA server.
- Step 14** The mediation device is notified that the target subscriber's session has stopped.
- Step 15** The mediation device sends an SNMPv3 command to the edge router to remove the intercept and to stop duplication of the communication content.
-

Security Considerations

Given the sensitive nature of lawful intercept—both from the standpoint of the need to protect sensitive data, and to conceal the identities of law enforcement agencies and the intercept targets—the LI architecture must contain stringent security measures to combat the following types of threats:

- Impersonation of LEAs and mediation devices
- Privacy and confidentiality breaches
- Message forgery
- Replay attacks

Because LI is expected to run on the wide-open Internet, very few assumptions should be made about how well the networks of the LEA's, SP's, and ISP's can be secured. Although this document does not examine the issues of physical security, operating system, or application hardening within the principles of the LI architecture, they are clearly important considerations. In particular, both the MD and LEA servers must be considered prime targets for attacks by hackers. Hardening measures commensurate with other highly vulnerable servers, such as key distribution and AAA servers, must be considered in any design.

The following section describes security requirements:

- [Overall Security Requirements, page 19](#)

Overall Security Requirements

All interfaces must be able to provide strong cryptographic authentication to establish the identity of the principles, and must correlate the identity of the principle with the action they are attempting to perform. That is, it is *not sufficient* to expect that authentication alone implies any specific authorization. Providing the ability to use strong crypto is *not* identical to requiring its use. Since many Cisco devices do not have crypto accelerators, actual use of crypto accelerators is the choice of the SP and ISP, and is dependent on how the device is deployed and its relative exposure. For devices placed in open, hostile environments (such as access routers), SPs and ISPs must consider customer requirements for LI when making decisions about crypto acceleration hardware.

Because LI is an interesting target for attackers, all interfaces must perform some sort of cryptographic message integrity checking (such as Hash-based Message Authentication Code [HMAC]-Message Digest 5 [MD5]). Message integrity checking must also counter replay attacks. Because of privacy and confidentiality considerations, the architecture should allow for the use of encryption. Although encryption is not necessarily a requirement, it is highly recommended and may be a requirement in some LI deployments.

Interface Between MD and IRI IAP: Control

SSH is used for the control interface between the MD and the IRI IAP.

Interface Between MD and CC IAP: SNMPv3 Control

SNMPv3 View-based Access Control Model (VACM) and User-Based Security Model (USM) are used for the control interface between the MD and the CC IAP. The native SNMPv3 security module mechanism must be used, and the minimum requirement is that preshared keys must be supported. The additional requirement is that the IAP must support the ability to protect the LI MIBs from disclosure or control by unauthorized USM users. In general VACM should provide the necessary tools to limit the views to particular USM users, but there are also special considerations given that USM and VACM provide the ability to create arbitrary view/user mappings to authorized entities. The security requirements of the Cisco Lawful Intercept Control MIB (CISCO-TAP-MIB) with respect to SNMP require the following actions:

- The MIB *must* be accessed (or accessible) only via SNMPv3.
- By default, no access *must* be granted to the MIB.
- Access to the MIB *must* be granted only by an administrative authority with the highest privileges:
 - The CISCO-TAP-MIB can be added to a view only at privilege level 15 (the highest level).
 - Including CISCO-TAP-MIB into a view on a router via the SNMP-VACM-MIB will be disallowed.

SNMPv3 *must* be configured correctly to maintain security. The MD acts as a network manager and the CC IAP acts as an agent.

Interface Between MD and IRI IAP: Data

The IRI is delivered from the IRI IAP to the MD. This information is delivered in RADIUS format. Currently, this information is not encrypted.

Interface Between MD and CC IAP: Data

The CC information is delivered from the CC IAP to the MD. IP security (IPsec) (via standard router cryptographic features) is used for this interface.

Failure Recovery

The mediation device monitors the network elements involved in LI. If any network element involved in LI fails or anything else happens to interrupt an intercept, the MD implements an audit to ensure that all network elements are configured properly. If any problems are detected, the MD attempts to correct them. The errors are also reported to the LI administration function.



Note

The CC IAPs do not maintain information about active intercepts in static memory. If the CC IAP reboots or fails over to the redundant side, the MD will detect the reboot and reprovision the intercept.

Implementation of Cisco SII Lawful Intercept

The following section describes the implementation of the Cisco SII LI architecture:

- [Prerequisites and Design Considerations, page 21](#)

Prerequisites and Design Considerations

Before configuring your network for LI, you must establish or verify reliable end-to-end IP connectivity on your existing network. The main concern when designing an LI network is ensuring that the network has sufficient bandwidth and CPU capacity to handle the anticipated load of intercepts. The following sections describe design considerations for implementing LI:

- [Bandwidth and Processing Power Considerations, page 21](#)
- [IP Address Provisioning Considerations, page 21](#)

Bandwidth and Processing Power Considerations

The CPUs of the following devices will be impacted by LI:

- Edge router—must be able to intercept and replicate all intercepted IP communication on its section of the network.
- Trunking gateway—must be able to intercept and replicate all intercepted calls that are forwarded off-net.
- Mediation device—must be able to support the required maximum number of simultaneous intercepts.

The following interfaces must be engineered with sufficient bandwidth to support LI traffic:

- IRI IAP—mediation device
- CC IAP—mediation device
- Mediation device—collection functions

You should also take into consideration that three-way calls require twice the bandwidth of regular calls because they require two pairs of transmit and receive channels.

You must also provision a network management system to perform DNS and Dynamic Host Configuration Protocol (DHCP) such as Cisco Network Registrar.

The use of SNMPv3 in SII requires that Network Time Protocol (NTP) is enabled and that all network elements involved in LI are synchronized to a stable time source.

The various devices involved in LI have minimum software and memory requirements that must be met. However, because of the number of possible devices and the fact that these requirements are subject to change, see the various product documents listed in the [“Related Documents” section on page 45](#) for the specific requirements.

IP Address Provisioning Considerations

In general, Cisco recommends that service providers not use static IP addresses, particularly for CPEs. Static provisioning of IP addresses is time consuming, expensive, and error prone. On the IAPs, it can be helpful to use loopback interfaces for the interface with the mediation device because the loopback interface remains constant if physical interfaces go out of service or if the routing path changes.

Device Configuration Files

The following sections provide detailed configuration information on the devices involved in LI:

- [Aggregation Router Configurations, page 22](#)
- [Cisco BTS 10200 Softswitch Call Agent Configuration, page 23](#)
- [Cisco PGW 2200 Softswitch Call Agent Configuration, page 23](#)
- [SS8 Networks Xcipio Mediation Device Configuration, page 23](#)
- [DNS Server Configuration, page 33](#)

**Note**

For additional information on the Cisco products that support LI, see [Table 16 on page 42](#).

Aggregation Router Configurations

The following aggregation router platforms support version 1.0 of Cisco LI MIB:

- Cisco 7200 series routers
- Cisco 7301 router
- Cisco 7500 series routers
- Cisco 10000 Edge Services Router (ESR)
- Cisco 12000 Gigabit Switch Router (GSR)
- Cisco Universal Broadband Router (uBR) 7246
- Cisco uBR 10000

The following configuration enables Cisco SII on an aggregation router using version 1.0 of the Cisco LI MIB:

```
7200-egw(config)# snmp-server view tapView CTapMIB included
7200-egw(config)# snmp-server group tapGroup v3 auth read tapView write tapView notify tapView
7200-egw(config)# snmp-server user mduserid tapGroup v3 auth md5 mdpasswd
```

The following configuration synchronizes the router's clock with the mediation device and enables SNMP traps to be sent to the mediation device:

```
7200-egw(config)# snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
7200-egw(config)# snmp-server host 10.15.113.9 version 3 auth mduserid
7200-egw(config)# ntp server 10.15.113.9
```

The username "mduserid" and password "mdpasswd" must match the username and password that is provisioned on the mediation device for this particular router. In this case, the router's clock is synchronized to the mediation device's clock. A better option is to synchronize all devices in the network to an NTP time server.

**Note**

Username, passwords, and security levels must match those provisioned on the mediation device. For the SS8 Networks Xcipio mediation device, see the ["Access Function SNMPv3 Configuration" section on page 29](#). Passwords must be at least eight characters in length. SS8 Networks supports only MD5 authentication.

Cisco BTS 10200 Softswitch Call Agent Configuration

The following call agent profile must be provisioned on the Cisco Broadband Telephony Softswitch (BTS) 10200 softswitch call agent:

```
ADD CALL-AGENT-PROFILE
ID=CA146
CMS_SUPP=N
MGC_SUPP=N
DQOS_SUPP=N
CDB_BILLING_SUPP=N
EM_BILLING_SUPP=N
GTD_SUPP=N
ES_INTERCEPT_TYPE=SERVICE_INDEPENDENT_INTERCEPT
CMS_ID=12345
MGC_ID=56789
FEID=54321
```

Because the BTS 10200 call agent has no information about network topology and is not aware of aggregation routers, no configuration is necessary for aggregation routers.

On the call agent's profile for trunking gateways, local hairpinning must be disabled. The following line in the trunking gateway profile disables local hairpinning:

```
MGCP_HAIRPIN_SUPP=N
```

Cisco PGW 2200 Softswitch Call Agent Configuration

The Cisco PSTN Gateway 2200 (PGW 2200) softswitch call agent only operates in SII mode using PacketCable Event Messages Specification version I03. Provisioning on the Cisco PGW 2200 requires enabling the LI feature and identifying the mediation devices.

Before adding an MD to the Cisco PGW 2200, you should verify that LI is enabled by verifying that the "SysConnectDataAccess=true" and "LISupport=enable" parameters are set as shown in the /opt/CiscoMGC/etc/XECfgParm.dat file.

Following is an example of provisioning a mediation device using default RADIUS timeouts and retries. The recommended RADIUS key of 16 zeros is automatically provisioned.

```
mm1> prov-add:extnode:name="mdname",type="LIMD",desc="Mediation_Device"
mm1> prov-add:lipath:name="md-path",desc="MD_Path",extnode="agsacom"
mm1> prov-add:iplnk:name="md-link",desc="MD_link",svc="md-path",
ipaddr="IP_Addr2",port=14146,peeraddr="192.168.9.2",peerport=1813,pri=1
```

In the above example, the value of "ipaddr" is selected from the /opt/CiscoMGC/etc/XECfgParm.dat file and must match the physical interface that has connectivity to the mediation device.

SS8 Networks Xcipio Mediation Device Configuration

The SS8 Networks Xcipio version 3.6.x mediation device runs on a series of Sun Microsystems workstations. The first workstation can handle all call data intercepts and up to five simultaneous communication content intercepts. Each additional workstation can handle up to 20 simultaneous communication content intercepts.

**Note**

The number of intercepts described are for a typical system and may depend upon the model of Sun Microsystems workstation that is used. Both Sun Microsystems and SS8 Networks should be consulted for the latest engineering guidelines.

The SS8 Networks Xcipio mediation device includes audio and visual alarms, and it can support secure sockets and other UNIX security measures.

Most (if not all) of the initial configuration of SS8 Networks Xcipio mediation devices is performed by SS8 Networks as part of the commissioning process. The following section describes the basics of configuring the Xcipio mediation device and is not meant as an authoritative guide.

The three methods of accessing the SS8 Networks Xcipio mediation device are through a CLI, a direct GUI, and a JAVA web interface. Except for surveillance information, all configurations must be done using Man-Machine Language (MML) commands. Surveillance information can be configured using the GUI or by the user calea_gui. Some configuration information (such as call agents) can be viewed using the GUI or user calea_gui but cannot be modified through the GUI or user calea_gui.

Calea_gui is an X Window application that must be run on the SS8 mediation device and displayed either locally or by being sent to a remote X Window server. The SS8 mediation device also supports a web interface that can be used to provision targets through any web browser or UNIX or LINUX workstation.

The built-in help feature for MML commands can display all available commands. To access the help level, enter the following command:

```
MML_calea_opr> help;
```

For detailed information on a command, enter the command in help mode followed by ::. For example, to display help information for the **add-cf** command, enter:

```
HELP_MML_CMD> add-cf::
```

**Note**

Because the functions and features of the SS8 Networks Xcipio mediation device may depend upon the hardware platforms used, see the *SS8 Xcipio SSDF User Manual* described in the “[Related Documents](#)” [section on page 45](#) for details on configuring the Xcipio mediation device and for commands.

The general format for MML commands is:

```
operation - object-of-operation
```

when typical operations are ADD, DISPLAY, MODIFY, or DELETE, and typical objects of operation are collection function (cf) and TCP/IP collection function interface (tcpipcfi).

**Note**

Strings are case-sensitive in all MML commands.

The following configurations must be performed on the SS8 Xcipio mediation device:

- [Collection Function Configuration, page 25](#)
- [Collection Function TCP Interface Configuration, page 25](#)
- [IP Delivery Unit Configuration, page 25](#)
- [IP Port Pools Configuration, page 26](#)
- [Surveillance Record Configuration, page 26](#)
- [AFTDN Configuration, page 27](#)

- [IP Call Content Channel Configuration, page 27](#)
- [Access Function Configuration, page 28](#)
- [Access Function SNMPv3 Configuration, page 29](#)
- [Access Function Trunking Gateway Interface Configuration, page 30](#)
- [Access Function BTS Provisioning Interface Configuration, page 30](#)
- [Access Function PGW Provisioning Interface Configuration, page 31](#)
- [Access Function RADIUS Interface Configuration, page 32](#)
- [SNMP Alarms and Traps Configuration, page 32](#)

Collection Function Configuration

The **add-cf** command adds the collection function and must be executed by user `calea_adm`.

```
MMML_calea_adm> add-cf:cfid=1,name=PenLink;
```

[Table 2](#) describes the strings in the **add-cf** command.

Table 2 *add-cf Command Strings*

String	Description
cfid	Collection function ID. Any number that has not already been used.
name	Any meaningful string to make the entry easily identifiable.

Collection Function TCP Interface Configuration

The **add-tcpipcfi** command adds the collection function to a TCP/IP interface. The command must be executed by user `calea_adm`.

```
MMML_calea_adm> add-tcpipcfi:cfid=1,ipaddr=172.18.137.94,port=43000,reqstate=ACTIVE;
```

[Table 3](#) describes the strings in the **add-tcpipcfi** command.

Table 3 *add-tcpipcfi Command Strings*

String	Description
cfid	Must match a CFID that has been previously added (by the add-cf:: command).
ipaddr	IP address of the LEA, which must be statically defined.
port	Port number used to send messages. This port number must match the port number configured on the collection function.
reqstate	Required state must be ACTIVE.

IP Delivery Unit Configuration

The **add-ipdu** command adds the IP delivery unit (IPDU). The command must be executed by user `calea_adm`. The IPDU is used for the call content portion of intercepts, and up to 16 can be configured on the mediation device. The first IPDU is typically on the same Sun device as the Softswitch Delivery Function (SSDF), while additional IPDUs are located on separate Sun workstations.

```
MMML_calea_adm> add-ipdu:ipduid=1,ipaddr=10.15.113.9,port=15001,hostname=brie;
```

Table 4 describes the strings in the **add-ipdu** command.

Table 4 *add-ipdu Command Strings*

String	Description
ipduid	IPDU ID number from 1 to 16 that uniquely identifies the IPDU.
ipaddr	IP address of the Sun Microsystems device.
port	Port ID for the first IPDU. The first port ID number must start at 15001.
hostname	Hostname provisioned for a Sun Microsystems device.

IP Port Pools Configuration

The **add-ipport** command creates pools of ports for call content delivery. The command must be executed by user calea_adm. Both incoming and outgoing ports must be created.

```
MML_calea_adm> add-ipport:ipduid=1,portid=1,end_portid=10,direction=IN;
MML_calea_adm> add-ipport:ipduid=1,portid=11,end_portid=20,direction=OUT;
```

Table 5 describes the strings in the **add-ipport** command.

Table 5 *add-ipport Command Strings*

String	Description
ipduid	IPDU ID number from 1 to 16 that must match an IPDU configured earlier.
portid	Starting port ID number.
end_portid	Ending port ID number.
direction	Allowed values are either IN or OUT.

Surveillance Record Configuration

The **add-surveillance** command is used to add a record for each subject that is to be monitored for call data or call data and call content. It must be executed by user calea_opr. Most of the strings in this command must match corresponding strings provisioned on the LEA collection function. In particular, the caseid string is used as a key to uniquely identify surveillance data. For ease of reading, the command is divided into three lines. The command must be configured as one string with no spaces.

```
MML_calea_opr> add-surveillance:state=AA,county=main-county,city=Home-Town,warrantid=6789,
caseid=1234,subsid=1111000001,startdate=05/01/2002,expdate=06/01/2002,
cfid=1,survtype=CONTENT,content=COMBINED,user=calea_opr,access=PUBLIC;
```

Table 6 describes the strings in the **add-surveillance** command.

Table 6 *add-surveillance Command Strings*

String	Description
state	Two-character abbreviation for the state of surveillance.
county	County of surveillance.
city	City of surveillance.
warrantid	Warrant ID number.

Table 6 *add-surveillance Command Strings (continued)*

String	Description
caseid	String that uniquely identifies the subject.
subsid	Phone number of the subject, or MIN if it is a mobile phone. This string must match that provisioned on the call agent.
startdate	Start date that observation is to begin in mm/dd/yyyy format, or NOW if observation is to begin immediately.
expdate	Expiration date that observation is to end in mm/dd/yyyy format, or UNSPEC for no expiration date.
cfid	Collection function ID. Any number that has not already been used.
survtype	Surveillance type. DATA for call data only, or CONTENT for call data and call content.
content	Currently, the only value supported is COMBINED, which specifies call data and call content are to be intercepted.
user	Person creating the surveillance instance.
access	PUBLIC if every mediation device web user can view the record, or PRIVATE if only the user who created the record can view it.

AFTDN Configuration

The **add-aftdn** command adds the access function target directory number (AFTDN). It must be executed by user `calea_opr`. The AFTDN associates a subject with the call agent serving that subject. The AFTDN must be added after the surveillance record is configured (using the **add-surveillance** command).

```
MML_calea_opr> add-aftdn:subsid=222211112,afid=Cable;
```

[Table 7](#) describes the strings in the **add-aftdn** command.

Table 7 *add-aftdn Command Strings*

String	Description
subsid	Phone number of the subject, or MIN if it is a mobile phone. This string must match that provisioned on the call agent.
afid	Must match the call agent that serves the targeted phone number.

IP Call Content Channel Configuration

The **add-ipccc** command adds the IP call content channel (IPCCC) and must be executed by user `calea_opr`. The IPCCC associates a target subscriber with a particular collection function. The IPCCC must be added after the surveillance record and AFTDN have been configured.

```
MML_calea_opr> add-ipccc:ipccid=1,ccid=0001,state=AA,county=main-county,city=Home-Town,warantid=6789,subsid=3333000111,cfipaddr=172.18.137.56,cfport=9000;
```

Table 8 describes the strings in the **add-ipccc** command.

Table 8 *add-ipccc Command Strings*

String	Description
ipcccid	IP call content channel ID.
cccid	String appended to call content, CCOpen, and CCClose messages before they are sent to the collection function.
state	Two-character abbreviation for the state of surveillance.
county	County of surveillance.
city	City of surveillance.
warrantid	Warrant ID number.
subsid	Phone number of the subject, or MIN if it is a mobile phone. This string must match that provisioned on the call agent.
cfipaddr	IP address of the LEA collection function.
cfport	Port on which the collection function receives call content.

Access Function Configuration

The **add-af** command adds access functions (AF), which are devices that intercept call data or call content, including call agents, gateways, and aggregation routers. The command must be executed by user `calea_adm`.

If the network includes aggregation routers supporting SNMPv3 interfaces, they must also be added with the type of SNMPER. (SNMPER identifies devices that support an SII interface). Trunking gateways that support only MGCP LI options must be provisioned using type TGW. Trunking gateways that support SNMPv3 should be provisioned as such.


```
MML_calea_adm> add-af:afid=Cable,name=Cable,type=BTS10200,version=3.2,preprov=000:00;
MML_calea_adm> add-af:afid=7246-1705,name=7246-1705,type=CMTS,version=12.2,preprov=000:00;
MML_calea_adm> add-af:afid=AS5850-2,name=AS5850-2,type=TGW,version=12.1,preprov=000:00;
MML_calea_adm> add-af:afid=ESR-egw,name=ESR-egw,type=SNMPER,version=12.2,preprov=000:00;
```

Table 9 describes the strings in the **add-af** command.

Table 9 *add-af Command Strings*

String	Description
afid	Access function ID (AFID) that is a user-specified string (up to 16 characters) that uniquely identifies the device. The afid specified in the add-af command is then used to reference the device in subsequent commands.
name	A user-specified string (up to 16 characters) that is used for further identification of the device. The name string does not have any meaning to the SS8 mediation device and is not used for any other purpose.

Table 9 *add-af Command Strings (continued)*

String	Description
type	Type of physical device. Allowed values are BTS10200, CMS, CMTS, DCFD, GENERIC, MGC, SM, SNMPER, TGW, or SYION. <div>  Note CMS is defined as call management server. CMTS is defined as cable modem termination system. DCFD is defined as Data Collection and Filtering Device. MGC is defined as Media Gateway Controller. SM is defined as the Telecordia Service Manager. SNMPER identifies devices that support an SII interface. TGW is defined as trunking gateway. SYION is a call management server product of the Syndeo Corporation. </div>
version	Version of software release running on the AF (optional).
preprov	Time zone of the access function.

Access Function SNMPv3 Configuration

The **add-afsi** command adds the access function SNMPv3 interface (AFSI), which contains information needed to interface with the provisioning interface for Cisco SNMPv3 interfaces. It must be executed by user calea_adm. The AFSI must be added after the corresponding access function has been added with the **add-af** command.

```

MML_calea_adm> add-afsi:afid=ESR-egw,ifid=1,domainname=ESR-egw.sm02.cisco.com,
ipaddr=10.15.115.3,port=161,reqstate=ACTIVE,username=ss8user,authpasswd=ss8passwd,
privpasswd=ss8passwd,securitylvl=AUTHNOPRIV;

```

Table 10 describes the strings in the **add-afsi** command.

Table 10 *add-afsi Command Strings*

String	Description
afid	Access function ID. A user-specified string (up to 16 characters) that uniquely identifies the device. The AFID must match an AFID previously specified in the add-af command.
ifid	Interface ID. Must be 1.
domainname	Domain name configured in DNS.
ipaddr	IP address of the access function.
port	Port 161 is the default for SNMP.
reqstate	Required state. ACTIVE if this interface is to try to initialize and come into service. INACTIVE if the intercept is being pre-provisioned and is not meant to begin service.
username authpasswd privpasswd	The username and passwords must match those provisioned on the access function. Passwords must be at least eight characters in length.
securitylvl	Must be AUTHNOPRIV. Aggregation routers will not allow NOAUTHNOPRIV.

Access Function Trunking Gateway Interface Configuration

The **add-afti** command adds the access function trunking gateway interface (AFTI). The command must be executed by user `calea_adm`. The AFTI contains information required to allow access to call content for calls passing through trunking gateways that support only the MGCP LI method. Gateways that support SNMPv3 interfaces are provisioned in the AFSI table. All gateways must also be provisioned in DNS in the same way as aggregation routers so that the mediation device can map an IP address to serving gateways with the pointer record (PTR) returned.

```

MML_calea_adm> add-afti;afid=AS5850-2,ifid=1,domainname=AS5850-2.sm02.cisco.com
ipaddr=10.15.111.6,protocol=MGCP,version=1.0;

```

Table 11 describes the strings in the **add-afti** command.



Note

The AFTI table is no longer required for use with BTS; however, it may still be required if using the Cisco MGX 8850 switch as a trunking gateway with the Cisco PGW 2200. The Cisco AS5350, Cisco AS5400, and Cisco AS5850 trunking gateways should be provisioned in AFSI as they will support SII.

Table 11 *add-afti Command Strings*

String	Description
afid	Access function ID that has been previously configured in the AF table.
ifid	Interface ID. Must be 1.
domainname	Domain name configured in DNS.
ipaddr	IP address of the access function.
protocol	MGCP is the only value that should be used. If the gateway supports SNMPv3, it should be provisioned using the add-afsi command.
version	Version of MGCP software being used that must match the version provisioned on the gateway. Typically this is 1.0.

Access Function BTS Provisioning Interface Configuration

The **add-afbi** command adds the access function BTS interface (AFBI), which provisions the interface that the SS8 SSDF uses to provision wiretaps on the BTS Element Management System (EMS). The command must be executed by user `calea_adm`. Because the EMS typically consists of active and standby units that each have different IP addresses, the **add-afbi** command must be configured for both units.

```

MML_calea_adm> add-afbi;afid=Cable,ifid=1,ipaddr=10.8.100.100,username=calea
passwd=test123,reqstate=ACTIVE;
MML_calea_adm> add-afbi;afid=Cable,ifid=2,ipaddr=10.8.100.101,username=calea
passwd=test123,reqstate=ACTIVE;

```

Table 12 describes the strings in the **add-afbi** command.

Table 12 *add-afbi Command Strings*

String	Description
afid	Access function ID that has been previously configured in the AF table.
ifid	Interface ID. Each EMS unit must have a unique IFID.
ipaddr	IP address of the EMS unit.
username	Username “calea” must be configured on the EMS.
passwd	Password must match that provisioned on the EMS. Passwords must be at least eight characters in length.
reqstate	ACTIVE if this interface is to try to initialize and come into service.

**Note**

On the SS8 mediation device, in the file \$ASVCRUN/config/MML/btsrhost.cnf, uncomment the appropriate lines for provisioning BTS using either SSH (the normal default) or Telnet. You must be logged in to SS8 MD as user calea_adm to edit this file. If calea is running on the MD when this edit is made, calea must be stopped and restarted before the change will take effect. For details on this process, see the *SS8 Xcipio SSDF User Manual* in the “Related Documents” section on page 45.

Access Function PGW Provisioning Interface Configuration

The **add-afgi** command adds the access function PGW interface (AFGI), which provisions the interface that the SS8 SSDF uses to provision wiretaps on the PGW. The command must be executed by user calea_adm. Because the PGW typically consists of an active and standby unit that each have different IP addresses, the **add-afgi** command must be configured for both units.

```
MML_calea_adm> add-afgi:afid=PGW,ifid=1,ipaddr=10.15.113.80,username=liusr,
passwd=test123,reqstate=ACTIVE
```

Table 13 describes the strings in the **add-afgi** command.

Table 13 *add-afgi Command Strings*

String	Description
afid	Access function ID that has been previously configured in the AF table.
ifid	Interface ID. Each PGW unit must have a unique IFID.
ipaddr	IP address of the PGW unit.
username	Must match that provisioned on the access function.
passwd	Password must be at least eight characters in length.
reqstate	Allowed values are ACTIVE or INACTIVE.

Access Function RADIUS Interface Configuration

The **add-afri** command adds the access function RADIUS interface (AFRI), which provisions the PacketCable Event Message interface between the call agent and the SS8 mediation device. The command must be executed by user `calea_admin`. As with the **add-afbi** command, the **add-afri** command must be performed for both active and standby call agent units. The AFID is the same for both, and the IFID is unique for each.

```

MML_calea_admin> add-afri:afid=Cable,ifid=1,ipaddr=10.8.100.102,port=14146,
reqstate=ACTIVE,version=I03,sharedsecret=0000000000000000;
MML_calea_admin> add-afri:afid=Cable,ifid=2,ipaddr=10.8.100.103,port=14146,
reqstate=ACTIVE,version=I03,sharedsecret=0000000000000000;
MML_calea_admin> add-afri:afid=7246-I1705,ifid=1,ipaddr=10.8.104.5,port=1646,
reqstate=ACTIVE,version=I03,sharedsecret=0000000000000000;

```

Table 14 describes the strings in the **add-afri** command.

Table 14 *add-afri Command Strings*

String	Description
afid	An AFID that has been previously configured in the AF table.
ifid	Interface ID. Each call agent unit must have a unique IFID.
ipaddr	The IP address of the call agent unit.
port	The default RADIUS port for BTS is 14146.
reqstate	Allowed values are ACTIVE or INACTIVE.
version	Currently, the allowed value is I03, which specifies the supported version of the EMS specification.
sharedsecret	Must match the shared secret provisioned on the BTS using the add ess command by the user <code>calea</code> .

In this example, port 14146 is the default source port used by the BTS. If port validation for security is not desired, then the port number in AFRI can be set to 0 (zero).

SNMP Alarms and Traps Configuration

The **add-almdest** command configures SNMP alarms. It must be executed by user `calea_admin`.

```

MML_calea_admin> add-almdest:name=SNMP,type=SNMP;
MML_calea_admin> add-almstream:name=SNMP,group=ALL,module=ALL,number=ALL,severity=ALL,
type=ALL;

```

The **add-almstream** command configures SS8 to send SNMP traps to the network management system. It must be executed by user `calea_admin`.

```

MML_calea-admin> add-almstream:name=SNMP,group=ALL,module=ALL,number=ALL,severity=ALL,
type=PASS;

```

For information on editing files to set up the addresses and ports of the SNMP network management server, see the *SS8 Xcipro SSDF User Manual* in the “Related Documents” section on page 45. The files that need to be edited will depend upon whether the network management server supports SNMPv1 or SNMPv2. The SS8 MIB definition files will also need to be installed into the network management software.

DNS Server Configuration

The DNS server must be provisioned to allow the mediation device to map the gateway to the aggregation router. [Table 15](#) shows a DNS resource record entry that maps a range (an entire C class) of Integrated Access Device (IAD) endpoint IP addresses to the serving aggregation router, ESR-eg2.sm02.cisco.com.

Table 15 *DNS Server Configuration*

Name(v)	TTL	Type	Data
0	—	PTR	ESR-egw.sm02.cisco.com
0	—	A	255.255.255.0

For SSDF to map an analog access device IP to the serving aggregation router, DNS must be configured according to RFC 1101, *DNS Encoding of Network Names and Other Types*.



Note

By adding an “A” record to the DNS server, performance can be improved since the MD may look for the “A” record before trying to look for the PTR record. A record must contain a valid mask for the range of addresses served by the device in the PTR record.

Verifying the Cisco SII LI Network

The following sections describe how to verify that the Cisco SII LI network has been configured correctly:

- [Verifying the Cisco BTS 10200 Softswitch Call Agent Configuration, page 33](#)
- [Verifying the Cisco PGW 2200 Softswitch Call Agent Configuration, page 34](#)
- [Verifying the SS8 Mediation Device Configuration, page 35](#)
- [Verifying the DNS Configuration From the Mediation Device, page 38](#)
- [Verifying an Aggregation Router Configuration, page 39](#)

Verifying the Cisco BTS 10200 Softswitch Call Agent Configuration

The following commands can be used to verify the LI configuration on the Cisco BTS 10200 softswitch call agent. Each of these EXEC commands can be issued only by the user calea.

```
CLI> show ess
```

```
Reply: Success: Entry 1 of 1 returned.
```

```
CDC_DF_PORT=1813
CDC_DF_ADDRESS=10.8.100.17
ENCRYPTION_KEY=0000000000000000
ACC_REQ_RETRANSMIT=3
ACC_RSP_TIMER=2
CLI>
```

```
BTS> show wiretap
```

```
Reply: Success: Entry 1 of 1 returned.
```

```

SUBSCRIBER_DN=3065050208
SUB_ID=arr050208/1
TAPTTYPE=INTERCEPT
CDC_DF_ADDRESS=10.8.100.17
CDC_DF_PORT=1813
CCC_DF_ADDRESS=10.8.100.17
CCC_DF_PORT=45007

CLI>

CLI> show wiretap subscriber_dn=6213000001

SUBSCRIBER_DN=6213000001
TAPTTYPE=INTERCEPT
CDC_DF_ADDRESS=10.15.113.9
CDC_DF_PORT=1813
CCC_DF_ADDRESS=10.15.113.9
CCC_DF_PORT=45010

Reply: Success: Entry 1 of 1 returned
CLI>

```

Use the **show call-agent-profile EXEC** command to verify the call agent profile. This command must be issued by a user with generic provisioning access and not by user “calea.”

```

BTS>show call-agent-profile
Reply : Success: Entry 1 of 1 returned.

ID=CA146
CMS_ID=12345
MGC_ID=56789
FEID=54321
CMS_SUPP=Y
MGC_SUPP=Y
DQOS_SUPP=Y
CDB_BILLING_SUPP=N
EM_BILLING_SUPP=Y
GTD_SUPP=N
ES_INTERCEPT_TYPE=SERVICE_INDEPENDENT_INTERCEPT

```

Verifying the Cisco PGW 2200 Softswitch Call Agent Configuration

Use the following commands to verify the configuration on the Cisco PGW 2200 softswitch call agent configuration.

To verify the mediation device configuration, enter the following commands from a PGW user that is authorized to access MML:

```

mml> prov-rtrv:extnode:name="name of mediation device"
mml> prov-rtrv:lipath:name="name of path to MD"
mml> prov-rtrv:iplnk:name="name of link to MD"
mml> prov-rtrv:sigsvccprop:name="name of path to MD"

```



Note

At any time, you can enter a tab character in MML to provide a list of valid arguments.

To verify the wiretap configuration, enter the following commands from a PGW user that is authorized to access the wiretap command set:

```
mm1> wiretap-rtrv:subscriber:number="target's phone number"
mm1> wiretap-rtrv:subscriber:"all"
```

Verifying the SS8 Mediation Device Configuration

The following commands can be used to verify the SS8 mediation device configuration. For more information on verifying the SS8 mediation device, see the [SS8 Xcipio SSDF User Manual](#) in the “Related Documents” section on page 45.

```
MML_TH> display-almdest;;
```

```
-----
NAME      TYPE      DEST      ARG      STATUS
-----
CONSOLE   CONSOLE   stdout
LOG        LOGFILE   /opt/SS8/access/AlarmLogs AccessAlarms.0 OK
PANEL     PANEL     0x16000001 819296    OK
SNMP      SNMP
<SUCCESS>:: 4 records found.
```

```
MML_TH> display-almstream;;
```

```
-----
NAME      GROUP     MODULE NUMBER SEVERITY TYPE
-----
CONSOLE   ALL       ALL       ALL       ALL       PASS
LOG        ALL       ALL       ALL       ALL       PASS
PANEL     ALL       ALL       ALL       ALL       PASS
SNMP      ALL       ALL       ALL       ALL       PASS
<SUCCESS>:: 4 records found.
```

```
MML_TH> display-ipdu;;
```

```
-----
IPDUID  HOSTNAME      IPADDR      PORT  STATE  INSTR  INEND  OUTSTR  OUTEND
-----
1       swiss         10.15.93.29 15001 ACTIVE 45001 45128 45129 45512
<SUCCESS>:: 1 records found.
```

MML_TH> **display-ipport;;**

```
-----
IPDUID PORTID PORT  DIRECTION PROTOCOL STATE
-----
1      1      45010 IN        UDP      BUSY
1      2      45009 IN        UDP      BUSY
1      3      45008 IN        UDP      IDLE
1      4      45007 IN        UDP      IDLE
1      5      45006 IN        UDP      IDLE
1      6      45005 IN        UDP      IDLE
1      7      45004 IN        UDP      IDLE
1      8      45003 IN        UDP      IDLE
1      9      45002 IN        UDP      IDLE
1     10      45001 IN        UDP      IDLE
1     11      45138 OUT        UDP      BUSY
1     12      45137 OUT        UDP      BUSY
1     13      45136 OUT        UDP      IDLE
1     14      45135 OUT        UDP      IDLE
1     15      45134 OUT        UDP      IDLE
1     16      45133 OUT        UDP      IDLE
1     17      45132 OUT        UDP      IDLE
1     18      45131 OUT        UDP      IDLE
1     19      45130 OUT        UDP      IDLE
1     20      45129 OUT        UDP      IDLE
```

<SUCCESS>:: 20 records found.

MML_TH> **display-cf;;**

```
-----
CFID NAME                TYPE  GRP1 GRP2 GRP3 GRP4 CARRIER
-----
1   CF-1                  TCPIP N/A  N/A  N/A  N/A  000
2   CF-2                  TCPIP N/A  N/A  N/A  N/A  000
```

<SUCCESS>:: 2 records found.

MML_TH> **display-tcpipcfi;;**

```
-----
CFID OWNIP                IPADDR                PORT  REQSTATE STATE
-----
1   172.18.137.105 172.18.137.94    43001 ACTIVE  ACTIVE
2   172.18.137.105 172.18.137.56    43001 ACTIVE  ACTIVE
```

<SUCCESS>:: 2 records found.

MML_TH> **display-af;;**

```
-----
AFID                NAME                TYPE    SERIAL                VERSION                PREPROV INDEX
-----
7246-I1705          7246-I1705          SNMPER  N/A                   12.3                   000:00 3
Beyond              Beyond              BTS10200 N/A                   4.4                   000:00 1
Cable                Cable                BTS10200 N/A                   4.4                   000:00 2
7200-egw             7200-egw            SNMPER  N/A                   12.4                   000:00 2
7500-egw             7500-egw            SNMPER  N/A                   12.4                   000:00 3
ESR-egw             ESR-egw             SNMPER  N/A                   12.2                   000:00 1
```

<SUCCESS>:: 6 records found.

MML_TH> **display-afbi;;**

AFID	IFID	IPADDR	REQSTATE	STATE	USERNAME	PASSWD
Beyond	1	10.15.69.7	INACTIVE	INACTIVE	calea	test123
Cable	1	10.8.100.100	ACTIVE	ACTIVE	calea	test123
Cable	2	10.8.100.101	ACTIVE	INACTIVE	calea	test123

<SUCCESS>:: 3 records found.

MML_calea> **display-afgi;;**

AFID	IFID	IPADDR	REQSTATE	STATE	USERNAME
PGW	1	10.15.113.80	ACTIVE	ACTIVE	liusr

<SUCCESS>:: 1 record found.

MML_TH> **display-afsi;;**

AFID	IFID	DOMAINNAME	IPADDR	PORT	REQSTATE	STATE	USERNAME
AUTHPASSWD		PRIVPASSWD		SECURITYLVL			
7200-egw	1	7200-egw.sm02.cisco.com	10.15.115.1	161	ACTIVE	ACTIVE	ss8user
ss8passwd		ss8passwd		AUTHNOPRIV			
7500-egw	1	7500-egw.sm02.cisco.com	10.15.115.2	161	ACTIVE	ACTIVE	ss8user
ss8passwd		ss8passwd		AUTHNOPRIV			
ESR-egw	1	ESR-egw.sm02.cisco.com	10.15.115.3	161	ACTIVE	ACTIVE	ss8user
ss8passwd		ss8passwd		AUTHNOPRIV			

<SUCCESS>:: 3 records found.

MML_TH>

MML_TH> **display-afti;;**

AFID	IFID	DOMAINNAME	IPADDR	PORT	REQSTATE	STATE	PROTOCOL	VERSION
AS5850-2	1	AS5850-2.sm02.cisco.com	10.15.111.6	2427	ACTIVE	ACTIVE	MGCP	1.0
mgxc701-11	1	mgxc701-11.sm02.cisco.com	10.15.112.193	2427	ACTIVE	ACTIVE	MGCP	1.0

<SUCCESS>:: 2 records found.

MML_TH>

MML_TH> **display-afri;;**

AFID	IFID	IPADDR	PORT	REQSTATE	VERSION	SHAREDSECRET
PGW	1	10.15.113.80	14146	ACTIVE	I03	0000000000000000
PGW	2	10.15.113.81	14146	ACTIVE	I03	0000000000000000
7246-I1705	1	10.8.104.5	1646	ACTIVE	I03	0000000000000000
Beyond	1	10.15.69.35	1813	ACTIVE	I03	0000000000000000
Beyond	2	10.15.69.36	1813	ACTIVE	I03	0000000000000000
Beyond	3	10.15.69.67	1813	ACTIVE	I03	0000000000000000
Beyond	4	10.15.69.68	1813	ACTIVE	I03	0000000000000000
Cable	1	10.8.100.102	14146	ACTIVE	I03	0000000000000000
Cable	2	10.8.100.103	14146	ACTIVE	I03	0000000000000000

<SUCCESS>:: 7 records found.

MML_TH>

```
MML_TH> display-surveillance;;
```

```
-----
STATE COUNTY          CITY          WARRANTID          JAREA    CASEID
SUBSID          ENTRYDATE  STARTDATE  EXPDATE    STATUS  CFID SURVTYPE CONTENT  USER
ACCESS
-----
AA    Main-County    Home-Town          0305          COUNTRY  0305
9844950305      08/30/2002 08/30/2002 12/31/2002 ACTIVE  1    DATA    NONE    calea_opr
PUBLIC
AA    Main-County    Home-Town          0306          COUNTRY  0306
9844950306      08/22/2002 08/22/2002 12/30/2002 ACTIVE  2    DATA    NONE    calea_opr
PUBLIC
AA    Main-County    Home-Town          0308          COUNTRY  0308
9844950308      08/22/2002 08/22/2002 12/31/2002 ACTIVE  2    CONTENT  COMBINED calea_opr
PUBLIC
AA    Main-County    Home-Town          9192621001     COUNTRY  1001
9192621001      09/30/2002 09/30/2002 12/31/2003 ACTIVE  2    CONTENT  COMBINED calea_opr
PUBLIC
AA    Main-County    Home-Town          9844950307     COUNTRY  0307
9844950307      10/01/2002 10/01/2002 11/01/2003 ACTIVE  2    CONTENT  COMBINED calea_opr
PUBLIC
<SUCCESS>:: 5 records found.
```

In the following output from the **display-aftdn;** command, the first and last rows of output are for call data only. The three middle rows are for call data and call content. The SSDF software automatically selects the IP address and port number.

```
MML_TH> display-aftdn;
```

```
-----
SUBSID          AFID          IPADDR          PORT  REQSTATE  STATE
-----
9192621001      Cable         10.8.100.17     45009 ACTIVE  PROVED
9844950305      Cable         N/A             0     ACTIVE  PROVED
9844950306      Cable         N/A             0     ACTIVE  PROVED
9844950307      Cable         N/A             0     ACTIVE  TOBEPROV
9844950308      Cable         10.8.100.17     45010 ACTIVE  PROVED
<SUCCESS>:: 5 records found.
MML_TH>
```

```
MML_TH> display-ipccc;
```

```
-----
IPCCCID STATE COUNTY          CITY          WARRANTID          CCCID
SUBSID          CFIPADDR          CFPORT STATUS
-----
1    AA    Home-Town    Home-Town    0308          0308
9844950308      172.18.137.56  9000 ACTIVE
8    AA    Home-Town    Home-Town    9192621001     1001
9192621001      172.18.137.56  9000 ACTIVE
<SUCCESS>:: 2 records found.
```

Verifying the DNS Configuration From the Mediation Device

The following commands can be used to verify that DNS is properly configured from the SS8 mediation device. The first example of the **nslookup** command verifies that the PTR record is properly configured. The IP address of the target's IAD loopback interface is 10.142.133.2. Therefore, to mask the last octet of the IP address, the lookup is performed for 0.133.142.10.

```
brie% nslookup -type=PTR 0.133.142.10.in-addr.arpa
Server: aulander.cisco.com
Address: 172.18.135.89

0.133.142.10.in-addr.arpa      name = ESR-egw.sm02.cisco.com
133.142.10.in-addr.arpa nameserver = sm02cnra.sm02.cisco.com
```

The second example of the **nslookup** command verifies that the A record is properly configured. The IAD address is used.

```
brie% nslookup -type=A 0.133.142.10.in-addr.arpa
Server: aulander.cisco.com
Address: 172.18.135.89

Name: 0.133.142.10.in-addr.arpa
Address: 255.255.255.0
```

To subsequently determine the IP address of the edge router, the net mask is “AND”ed with the original target IP address, and another **nslookup** command is performed.

Verifying an Aggregation Router Configuration

The following commands can be used to verify the SNMPv3 configuration on an aggregation router. The **show snmp view** command displays SNMPv3 LI information, where the tapView line is the line of interest.

```
ESR-egw# show snmp view
*ilmi system - included permanent active
*ilmi atmForumUni - included permanent active
tapView cTapMIB - included nonvolatile active
vldefault internet - included volatile active
vldefault internet.6.3.15 - excluded volatile active
vldefault internet.6.3.16 - excluded volatile active
vldefault internet.6.3.18 - excluded volatile active
```

The **show snmp group** command displays information on SNMP groups, where the tapGroup line is the line of interest.

```
ESR-egw# show snmp group
groupname: ILMI                security model:v1
readview :*ilmi                writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                security model:v2c
readview :*ilmi                writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: tapGroup            security model:v3 auth
readview :tapView              writeview: tapView
notifyview: tapView
row status: active
```

The **show snmp user** command displays information about configured users of SNMP.

```
ESR-egw# show snmp user
User name: mediation-device
Engine ID: 00000009020002000000000A0
storage-type: nonvolatile      active

User name: md-admin
```

Engine ID: 0000000902000200000000A0
storage-type: nonvolatile active

Troubleshooting a Cisco SII LI Network

The following sections provide guidance in troubleshooting a Cisco SII LI network:

- [General Troubleshooting Notes, page 40](#)
- [Troubleshooting the Mediation Device, page 40](#)
- [Troubleshooting the BTS Call Agent, page 40](#)
- [Troubleshooting the Call Agent Profile, page 41](#)

General Troubleshooting Notes

The most common problem encountered in configuring LI on a network is general networking problems. All of the involved devices must have static IP addresses, and most require the use of specific ports. All of the firewalls involved (end customer, SP, ISP, LEA, and so on) must allow the static IP addresses and port numbers to go through. When firewalls prohibit ping traffic, pings cannot be used for troubleshooting. Instead, you may have to use a sniffer to verify connectivity.

Another common problem is mismatched usernames and passwords. The following sections include details about the device interfaces that must have matching usernames and passwords.

Troubleshooting the Mediation Device

If you have trouble with a mediation device, first check the mediation device logs and alarms. In case of serious trouble, the mediation devices have various tracing mechanisms. On the SS8 Xcipio mediation device, if the file `/etc/resolv.conf` is edited to add or modify IP addresses of DNS servers while the CALEA application is running, CALEA must be stopped and restarted (using the `calea_stop` and `calea_start` commands) before the application will recognize the configuration changes. For more information on troubleshooting the SS8 Xcipio mediation device, see the [SS8 Xcipio SSDF User Manual](#) in the “[Related Documents](#)” section on page 45.

When SNMPv3 is used, the usernames, passwords, and security levels provisioned on the mediation device must match those provisioned on the aggregation devices.

If the IP address or port number provisioned on the mediation device for the collection function is incorrect, the collection function will appear in the “FAIL” state on the mediation device, and logs on the mediation device will detail connection attempt failures. On the SS8 mediation device, the logs are located at `$ASVCRUN/mlog/Mlog[date]`. If the port number for call content delivery to the collection function is incorrect, the collection function will never receive call content.

The mediation device log files will also contain error records if incorrect IP addresses or port numbers are provisioned for the call agent, aggregation routers, or edge routers.

Troubleshooting the BTS Call Agent

To perform Electronic Surveillance Subsystem (ESS) and wiretap commands on the BTS, you must log in as user `calea`. All other commands can be entered by any user with the proper permissions.

When accessing the BTS, you must log in as user **calea**. The username and password must match those provisioned on the mediation device.

The BTS will not function properly if the \$ASVCRUN/config/MML/btsrhost.cnf file is not properly edited to change it from Telnet to SSH. Six lines in the file need to be edited, which are described in the software installation instructions.

The following section describes troubleshooting procedures on the BTS call agent.

For more information on debugging and tracing tools for the BTS, see the [Cisco BTS 10200 Documentation Access Information](#) document in the “Related Documents” section on page 45.

Troubleshooting the Call Agent Profile

Enter the **show call-agent-profile EXEC** command to verify the call agent profile:

```
BTS> show call-agent-profile
Reply : Success: Entry 1 of 1 returned.

ID=CA146
CMS_ID=12345
MGC_ID=56789
FEID=54321
CMS_SUPP=Y
MGC_SUPP=Y
DQOS_SUPP=Y
CDB_BILLING_SUPP=N
EM_BILLING_SUPP=Y
GTD_SUPP=N
ES_INTERCEPT_TYPE=SERVICE_INDEPENDENT_INTERCEPT
```

The EM_BILLING_SUPP, CMS_SUPP, and MGC_SUPP all must be set to Y. The CMS_ID, MGC_ID, and financial entity ID (FEID) all must be set to nonzero numbers.

CMS_SUPP controls the sending of event messages when an on-network (on-net) endpoint is involved in the call. If MGC_SUPP is set to Y, the BTS will send event messages; if it is set to N, the BTS will not send event messages.

CMS_ID, MGC_ID, and FEID are PacketCable network element identifiers. Unique values for these network elements must be agreed upon by all involved parties. For the purposes of settlements, PacketCable zones are divided into one or more logical financial entities. A single call agent is assigned at most one FEID. One or more call agents may be assigned the same FEID.

MGC_SUPP controls the sending of event messages when an off-net endpoint is involved in the call. If MGC_SUPP is set to Y, the BTS will send event messages; if it is set to N, the BTS will not send event messages.

Appendix

This section contains the following information:

- [Cisco Products That Support Lawful Intercept, page 42](#)
- [Related Documents, page 45](#)
- [Standards, page 46](#)
- [RFCs, page 46](#)

- [Technical Assistance, page 46](#)

Cisco Products That Support Lawful Intercept

Table 16 provides the following additional information on the Cisco products that support LI:

- Cisco Product—name of product that supports LI
- Product Type—the role that the product performs
- Voice Support—describes the software versions that the platform supports:
 - SIIv1—Cisco SII software that supports version 1.0 of Cisco LI MIB
 - PC—PacketCable
 - CISCO-TAP-MIB—version of Cisco MIB
- Data Support—describes the versions that the platform supports:
 - SIIv1—Cisco SII software that supports version 1.0 of Cisco LI MIB
 - PC—PacketCable
 - CISCO-TAP-MIB—version of Cisco LI MIB

Table 16 Cisco Products That Support Lawful Intercept

Cisco Product	Product Type	Voice Support	Data Support
Cisco BTS 10200	Call agent	<ul style="list-style-type: none"> • SIIv1—supports BTS Release 4.1 and earlier releases • PC—supports BTS Release 4.1 and earlier releases 	—
Cisco PGW 2200	Call agent	<ul style="list-style-type: none"> • SIIv1—supports PGW Release 9.5(1) and later releases • PC—N/A 	—
Cisco 7200 series	Aggregation router	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(8)T until Release 12.3(14)T • PC—N/A 	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(8)T until Release 12.3(14)T • PC—N/A
Cisco 7301	Aggregation router	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(8)T until Release 12.3(14)T • PC—N/A 	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(8)T until Release 12.3(14)T • PC—N/A
Cisco 7505	Aggregation router	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(9) and later releases • PC—N/A 	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(9) and later releases • PC—N/A
Cisco 7507	Aggregation router	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(9) and later releases • PC—N/A 	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(9) and later releases • PC—N/A

Table 16 Cisco Products That Support Lawful Intercept (continued)

Cisco Product	Product Type	Voice Support	Data Support
Cisco 7513	Aggregation router	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(9) and later releases • PC—N/A 	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(9) and later releases • PC—N/A
Cisco 10000	Aggregation router	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.0(25)S and later releases • PC—N/A 	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(7)XI and later releases; Layer 2 Tunneling Protocol (L2TP) support using RADIUS provisioning available in Cisco IOS Release 12.2SB1 • PC—N/A
Cisco 12000 GSR series	Aggregation router	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.0(32)S and later releases require engine 3 or engine 5 cards at the edge router (customer facing); core facing cards can be any generation • PC—N/A 	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.0(32)S and later releases require engine 3 or engine 5 cards at the edge router (customer facing); core facing cards can be any generation • PC—N/A
Cisco uBR7246 VXR	CMTS	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(13)a-BC and later releases • PC—Cisco IOS Release 12.2(15)BC1b and later releases 	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(13)a-BC and later releases • PC—N/A
Cisco uBR10000	CMTS	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.2(15)BC1b and later releases • PC—Cisco IOS Release 12.2(15)BC1b and later releases 	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—Cisco IOS Release 12.3(13)a-BC and later releases • PC—N/A

Table 16 Cisco Products That Support Lawful Intercept (continued)

Cisco Product	Product Type	Voice Support	Data Support
Content Services Gateway (CSG)	Blade for Cisco Catalyst 6000 and Cisco Catalyst 7600	<ul style="list-style-type: none"> • Cisco Catalyst 6000: <ul style="list-style-type: none"> – SIIv1 (CISCO-TAP-MIB): native IOS Release c6k222-jsu2v-mz.ZA4-LI; hybrid image c6msfc2-jsu2v-mz.ZA4-LI of Cisco IOS Release 12.2(18d)SXC – PC—N/A • Cisco Catalyst 7600: <ul style="list-style-type: none"> – SIIv1 (CISCO-TAP-MIB): Supervisor software—s72033-adventerprise9_wan-mz.122-18.SXE1.bin; s72033-advipservicesk9_wan-mz.122-18.SXE1.bin; CSG software -WS-SVC-CSG-L4.0 – PC—N/A 	<ul style="list-style-type: none"> • Cisco Catalyst 6000: <ul style="list-style-type: none"> – SIIv1 (CISCO-TAP-MIB): native IOS Release c6k222-jsu2v-mz.ZA4-LI; hybrid image c6msfc2-jsu2v-mz.ZA4-LI of Cisco IOS Release 12.2(18d)SXC – PC—N/A • Cisco Catalyst 7600: <ul style="list-style-type: none"> – SIIv1 (CISCO-TAP-MIB): Supervisor software—s72033-adventerprise9_wan-mz.122-18.SXE1.bin; s72033-advipservicesk9_wan-mz.122-18.SXE1.bin; CSG software -WS-SVC-CSG-L4.0 – PC—N/A
Cisco 3660	Trunking gateway	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB) <ul style="list-style-type: none"> – Cisco IOS Release 12.3(5) and later releases – Enterprise Plus LI software feature set • PC—Cisco IOS Release 12.3(7)T and later releases 	—
Cisco 7200 series	Trunking gateway	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB): Cisco IOS Release 12.3(7)T until Release 12.3(14)T • PC—N/A 	—
Cisco MGX 8850 VG	Trunking gateway	<ul style="list-style-type: none"> • SII—N/A • PC <ul style="list-style-type: none"> – Voice Interworking Service Module (VISM) 2.2 and later releases – Voice Switch Service Module (VXSM) 2.0 and later releases 	—
Cisco AS5350	Access server/trunking gateway	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—N/A • PC—Cisco IOS Release 12.3(7)T and later releases 	<ul style="list-style-type: none"> • SIIv1 (CISCO-TAP-MIB)—N/A • PC—N/A

Table 16 Cisco Products That Support Lawful Intercept (continued)

Cisco Product	Product Type	Voice Support	Data Support
Cisco AS5400	Access server/ trunking gateway	<ul style="list-style-type: none"> SIIv1 (CISCO-TAP-MIB)—N/A PC—Cisco IOS Release 12.3(7)T and later releases 	<ul style="list-style-type: none"> SIIv1 (CISCO-TAP-MIB)—N/A PC—N/A
Cisco AS5850	Access server/ trunking gateway	<ul style="list-style-type: none"> SIIv1 (CISCO-TAP-MIB)—N/A PC—Cisco IOS Release 12.3(7)T and later releases 	<ul style="list-style-type: none"> SIIv1 (CISCO-TAP-MIB)—N/A PC—N/A

Related Documents

Table 17 lists related documents.

Table 17 Related Documents

Title	URL or Part Number
<i>PacketCable Electronic Surveillance Specification</i>	http://www.packetcable.com/specifications
<i>PacketCable Electronic Surveillance Call Flows Technical Report</i>	http://www.packetcable.com/specifications
<i>PacketCable Event Messages Specification</i>	http://www.packetcable.com/specifications
<i>PacketCable Dynamic Quality of Service Specification</i>	http://www.packetcable.com/specifications
<i>PacketCable Security Specification</i>	http://www.packetcable.com/specifications
<i>SS8 Xcipio SSDF User Manual</i>	2700-2493-01
<i>Cisco BTS 10200 Documentation Access Information</i>	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm
<i>Cisco Lawful Intercept Control MIB</i>	http://www.ietf.org/rfc/rfc3924.txt
<i>NewNet Enhanced IP Node User Manual</i>	D-0534-US-350-000
<i>Lawful Intercept on Cisco 12000 Series Router ISE Line Cards</i>	OL-8679-01 (Rev. A0)

Standards

Standard	Title
TR-45 J-STD-025A	<i>Telephone Industry Association Lawfully Authorized Electronic Surveillance</i>
PKT-SP-EM-I03	<i>PacketCable Event Messages Specification</i>
PKT-SP-ESP-I01	<i>PacketCable Electronic Surveillance Specification</i>

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> CISCO-TAP-MIB 	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFC	Title
RFC 1101	<i>DNS Encoding of Network Names and Other Types</i>
RFC 3924	<i>Cisco Architecture for Lawful Intercept in IP Networks</i>

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Glossary

AAA	—authentication, authorization, and accounting
AF	—access function
AFBI	—access function BTS interface
AFGI	—access function PGW interface
AFID	—access function ID
AFRI	—access function Radius interface
AFSI	—access function SNMPv3 interface
AFTDN	—access function target directory number
AFTI	—access function trunking gateway interface
BTS	—Broadband Telephony Softswitch. A call agent.
CALEA	—Communications Assistance for Law Enforcement Act
CC	—call content
CCC	—call content connection
CCCID	—call content connection identifier
CC IAP	—Communication Content intercept access point
CFID	—collection function ID
CISCO-TAP-MIB	—Cisco Lawful Intercept Control MIB
CLI	—command-line interface
CMS	—call management server
CMTS	—cable modem termination system
CPE	—customer premise equipment
CSG	—Content Services Gateway
DCFD	—Data Collection and Filtering Device. A sniffer that collects and analyzes RADIUS traffic.
DHCP	—Dynamic Host Configuration Protocol
EMS	—Element Management System
ESR	—Edge Services Router
ESS	—Electronic Surveillance Subsystem
FEID	—financial entity ID
FQDN	—fully qualified domain name
GSR	—Gigabit Switch Router
HMAC	—Hash-based Message Authentication Code
IAD	—Integrated Access Device
IFID	—Interface ID
IPCCC	—IP call content channel
IPDU	—IP delivery unit
IPDUID	—IP delivery unit ID

IPsec—IP security

IRI IAP—Intercept-Related Information intercept access point

ISP—Internet service provider

L2TP—Layer 2 Tunneling Protocol

LEA—law enforcement agency

LI—lawful intercept

MD—mediation device. A hardware device that receives signal and voice information from an SP or ISP network and translate the information into the correct protocol.

MD5—Message Digest 5

MGC—Media Gateway Controller

MGCP—Media Gateway Control Protocol

MIB—Management Information Base

MML—Man Machine Language

NTP—Network Time Protocol

off-net—off-network

on-net—on-network

PGW—PSTN Gateway

PSTN—public switched telephone network

PTR—pointer record

RADIUS—Remote Authentication Dial-In User Services

reqstate—required state

RIPA—Regulation of Investigatory Powers Act

SDP—Session Definition Protocol

SII—Service Independent Intercept

SIP—Session Initiation Protocol

SM—Telecordia Service Manager. A call agent.

SMDS—Switched Multimegabit Data Service

sniffer—A network analyzer used to capture packets transmitted in a network for inspection and problem detection.

SNMPv3—Simple Network Management Protocol version 3

SP—service provider

SSDF—Softswitch Delivery Function. A software program provided by SS8 Networks called Xcipio SSDF.

SSH—Secure Shell

tcpipcfi—TCP/IP collection function interface

TGW—trunking gateway

TIA—Telephone Industry Association

TKUV—Telekommunikations Überwachungsverordnung

uBR—Universal Broadband Router

UDP—User Datagram Protocol

USM—User-based Security Model

VACM—View-based Access Control Model

VISM—Voice Interworking Service Module

VoIP—Voice over IP

VXSM—Voice Switch Service Module

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.