Cisco Service Independent Intercept Architecture Version 2.0

Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3/15/2006</td>
<td>This document was created and includes version 108 of the PacketCable Event Message Specification, BTS versions 4.4 and 4.5, and version 2.0 of Cisco LI MIB.</td>
</tr>
</tbody>
</table>

Abstract

Cisco Service Independent Intercept (SII) architecture version 2.0 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 2.0 document describes the implementation of an LI architecture on a Cisco IP network that uses version 2.0 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 2.0 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 22
- Device Configuration Files, page 23
- Verifying the Cisco SII LI Network, page 35
- Troubleshooting a Cisco SII LI Network, page 42
- Appendix, page 43
- Glossary, page 49

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 47.)

Cisco Service Independent Intercept Architecture

The following sections describe the Cisco SII version 2.0 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 Specifications that use 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**

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

**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.
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 or 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 LI network.

Figure 2  Functional Depiction of a Cisco SII LI Network
Figure 3 shows the device interfaces in the context of the specific devices that are used in a Cisco SII network.

**Table 1**  *Cisco SII LI Network Device Interfaces*  

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Authorization: administration function and mediation device</td>
<td>The LI administration function sends intercept provisioning information (target identifier, duration of intercept, and so on) to the mediation device.</td>
</tr>
<tr>
<td>c</td>
<td>Content: mediation device and collection function</td>
<td>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 <em>PacketCable Electronic Surveillance Specification</em> document in the “Related Documents” section on page 47.</td>
</tr>
</tbody>
</table>

**Note**  
PSTN is defined as public switched telephone network.
Table 1  
Cisco SII LI Network Device Interfaces (continued)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>d1</td>
<td>IRI Delivery: IRI IAP and mediation device</td>
<td>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 47. For data, this is Remote Authentication Dial-In User Service (RADIUS) accounting messages. 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).</td>
</tr>
<tr>
<td>d2</td>
<td>CC delivery: CC IAP and mediation device</td>
<td>The CC IAP replicates call content (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 47.) The CCCID is used to associate the CC with the target. 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. The CC IAP is an edge router, trunking gateway, or access server.</td>
</tr>
<tr>
<td>e1</td>
<td>Provisioning: mediation device and IRI IAP</td>
<td>The mediation device uses Secure Shell (SSH) to provision an intercept on the IRI IAP.</td>
</tr>
<tr>
<td>e2</td>
<td>Provisioning: mediation device and CC IAP</td>
<td>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.</td>
</tr>
<tr>
<td>k</td>
<td>DNS Lookup: mediation device and DNS server</td>
<td>The mediation device queries the Domain Name Service (DNS) server to determine the fully qualified domain name (FQDN) of the CC IAP.</td>
</tr>
</tbody>
</table>

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 20
- Failure Recovery, page 21
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, the warrant 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 17
- Cisco SII Data Intercept, page 19
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 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 Media_Report 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 or network access server (NAS) 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, the edge router or NAS 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 Signaling_Stop 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 Media_Report message to the mediation device.
Step 21 When the mediation device receives the Media_Report message, it sends SNMPv3 messages to the edge router or NAS 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

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 Media_Report 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 Signaling_Stop 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 Media_Report message to the mediation device.
Step 22 When the mediation device receives the Media_Report, 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 terminating gateway sends an originating attempt message to the mediation device. |
| Step 6 | 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 7 | The mediation device sends an SNMPv3 command to the edge router to initiate the intercept. |
| Step 8 | The mediation device sends a CCOpen message with the SDP to the collection function. |
| Step 9 | The CMS delivers the call to the originating gateway. |
| Step 10 | The originating gateway rings non-target subscriber 1. |
| Step 11 | The call is connected end-to-end, the edge router intercepts and replicates all voice packets and sends the packets to the mediation device. |
| Step 12 | The mediation device delivers CC to the collection function. |
| Step 13 | The CMS sends a Call_Answer message to the mediation device. |
| Step 14 | The mediation device forwards this message as an Answer message to the collection function. |
| Step 15 | The target hook flashes to put the Hook non-target subscriber 1 on hold and initiate a second call. |
| Step 16 | The CMS sends a Signaling_Start message to the mediation device. |
| Step 17 | The terminating gateway sends an originating attempt message to the mediation device. |
| Step 18 | The terminating gateway sends SDP information to the CMS. |
| Step 19 | The CMS sends the SDP information to the mediation device in a Media_Report message. |
| Step 20 | 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 21 | The mediation device sends an SNMPv3 command to the edge router to initiate the intercept. |
| Step 22 | The mediation device sends a CCOpen message with the SDP to the collection function. |
| Step 23 | The CMS delivers the call to the originating gateway. |
| Step 24 | The originating gateway rings non-target subscriber 2. |
| Step 25 | The call is connected end-to-end, the edge router intercepts and replicates all voice packets and sends the packets to the mediation device. |
| Step 26 | The mediation device delivers CC to the collection function. |
| Step 27 | The CMS sends a Call_Answer message to the mediation device. |
| Step 28 | The mediation device forwards this message as an Answer message to the collection function. |
| Step 29 | 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 Signaling_Stop 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 Media_Report messages to the mediation device.

Step 37  When the mediation device receives the Media_Report 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.

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 Media_Report 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 Signaling_Stop 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 Media_Report message to the mediation device.

Step 18 When the mediation device receives the Media_Report 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. Although only an edge router is shown, this same topology applies if the target accesses the network via dialup and a NAS such as a Cisco AS 5350, Cisco AS 5400, or Cisco AS 5850.

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 legal intercept is expected to run on the wide-open Internet, very few assumptions should be made about how well the networks of the LEA’s and the SP’s or 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 20

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 will be the choice of the SP or ISP, and will be dependent on how the device is deployed and its relative exposure. For devices placed in open, hostile environments (such as access routers), the SP or ISP 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 22

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 22
- IP Address Provisioning Considerations, page 22

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 47 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 and Trunking Gateway Configuration, page 23
- Cisco BTS 10200 Softswitch Call Agent Configuration, page 24
- Cisco PGW 2200 Softswitch Call Agent Configuration, page 24
- SS8 Networks Xcipio Mediation Device Configuration, page 25
- DNS Server Configuration, page 34

**Note**

For additional information on the Cisco products that support LI, see Table 17 on page 44.

Aggregation Router and Trunking Gateway Configuration

The following aggregation router platforms support version 2.0 of Cisco LI MIB:

- Cisco 7200 series routers
- Cisco 7301 router

The following trunking gateway platforms support version 2.0 of Cisco LI MIB:

- Cisco AS 5350
- Cisco AS 5400
- Cisco AS 5850

The following configuration enables Cisco SII on an aggregation router or trunking router using version 2.0 of the Cisco LI MIB:

```
7200(config)# snmp-server view tapView ciscoTap2MIB included
7200(config)# snmp-server view tapView ciscoIpTapMIB included
7200(config)# snmp-server group tapGroup v3 auth read tapView write tapView notify tapView
7200(config)# snmp-server user mduserid tapGroup v3 auth md5 mdpasswd
```

Additionally, if trunking gateways support dialup data access and if intercept by session is desired, then an additional MIB must be added to view as shown below:

```
AS5400(config)# snmp-server view tapView ciscoUserConnectionTapMIB included
```

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

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

Usernames, 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 30. Passwords must be at least eight characters in length. SS8 Networks supports only MD5 authentication.

Cisco BTS 10200 Softswitch Call Agent Configuration

The Cisco Broadband Telephony Softswitch (BTS) 10200 softswitch call agent can be configured to operate in SII mode only or to operate in a mixed mode that supports both PacketCable and SII intercept access point (IAP) devices. This is configured in table Electronic Surveillance Subsystem (ESS) using the USE_PACKETCABLE_IAP parameter. If this parameter is set to N (that is, no), then BTS will support only SII IAP devices. When set to Y (that is, yes), then BTS is in mixed mode and supports both SII and PacketCable IAP devices.

To be compatible with mediation devices that support Event Message Specification I08, the PROTOCOL_VERSION in table ESS must be set to I03.

An example of table ESS configuration is shown below.

```
CDC_DF_PORT=1813
CDC_DF_ADDRESS=10.15.113.9
ENCRYPTION_KEY=0000000000000000
ACC_REQ_RETRANSMIT=3
ACC_RSP_TIMER=2
PROTOCOL_VERSION=I03
IPSEC_SA_ESP_CS=3DES-MD5,3DES-SHA1,NULL-MD5,NULL-SHA1
IPSEC_SA_LIFETIME=86400
IPSEC_SA_GRACE_PERIOD=21600
IPSEC_ULP_NAME=IP
IKE_GROUP=2
IKE_SA_LIFETIME=86400
IKE_CS=3DES-MD5,3DES-SHA1
USE_PACKETCABLE_IAP=N
```

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 Message 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.
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 Sun 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 Networks mediation device and displayed either locally or by being sent to a remote X Window server. The SS8 Networks 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 47 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 Networks Xcipio mediation device:

- Collection Function Configuration, page 26
- Collection Function TCP Interface Configuration, page 26
- IP Delivery Unit Configuration, page 27
- IP Port Pools Configuration, page 27
- Surveillance Record Configuration, page 28
- AFTDN Configuration, page 28
- IP Call Content Channel Configuration, page 29
- Access Function Configuration, page 29
- Access Function SNMPv3 Configuration, page 30
- Access Function Trunking Gateway Interface Configuration, page 31
- Access Function BTS Provisioning Interface Configuration, page 32
- Access Function Provisioning Interface Configuration, page 32
- Access Function PGW Provisioning Interface Configuration, page 33
- Access Function RADIUS Interface Configuration, page 33
- SNMP Alarms and Traps Configuration, page 34

### Collection Function Configuration

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

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

Table 2 describes the strings in the **add-cf** command.

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cfid</td>
<td>Collection function ID. Any number that has not already been used.</td>
</tr>
<tr>
<td>name</td>
<td>Any meaningful string to make the entry easily identifiable.</td>
</tr>
</tbody>
</table>

### Collection Function TCP Interface Configuration

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

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

Table 3 describes the strings in the **add-tcipcfi** command.
The \texttt{add-ipdu} command adds the IP delivery unit (IPDU). The command must be executed by user \texttt{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 Microsystems’ device as the Softswitch Delivery Function (SSDF), while additional IPDUs are located on separate Sun Microsystems devices.

\begin{verbatim}
MML_calea_adm> add-ipdu:ipduid=1,ipaddr=10.15.113.9, port=15001,hostname=brie;
\end{verbatim}

Table 4 describes the strings in the \texttt{add-ipdu} command.

### Table 3 \texttt{add-tcpipcfi} Command Strings

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cfid</td>
<td>Collection function ID. Must match a CFID that has been previously added (by the \texttt{add-cf;} command).</td>
</tr>
<tr>
<td>ipaddr</td>
<td>IP address of the LEA, which must be statically defined.</td>
</tr>
<tr>
<td>port</td>
<td>Port number used to send messages. This port number must match the port number configured on the collection function.</td>
</tr>
<tr>
<td>reqstate</td>
<td>Required state must be ACTIVE.</td>
</tr>
</tbody>
</table>

### IP Delivery Unit Configuration

The \texttt{add-ipdu} command adds the IP delivery unit (IPDU). The command must be executed by user \texttt{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 Microsystems’ device as the Softswitch Delivery Function (SSDF), while additional IPDUs are located on separate Sun Microsystems devices.

\begin{verbatim}
MML_calea_adm> add-ipdu:ipduid=1,ipaddr=10.15.113.9, port=15001,hostname=brie;
\end{verbatim}

Table 4 describes the strings in the \texttt{add-ipdu} command.

### Table 4 \texttt{add-ipdu} Command Strings

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipduid</td>
<td>IPDU ID number from 1 to 16 that uniquely identifies the IPDU.</td>
</tr>
<tr>
<td>ipaddr</td>
<td>IP address of the Sun Microsystems device.</td>
</tr>
<tr>
<td>port</td>
<td>Port ID for the first IPDU. The first port ID number must start at 15001.</td>
</tr>
<tr>
<td>hostname</td>
<td>Hostname provisioned for a Sun Microsystems device.</td>
</tr>
</tbody>
</table>

### IP Port Pools Configuration

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

\begin{verbatim}
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;
\end{verbatim}

Table 5 describes the strings in the \texttt{add-ipport} command.

### Table 5 \texttt{add-ipport} Command Strings

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipduid</td>
<td>IPDU ID number from 1 to 16 that must match an IPDU configured earlier.</td>
</tr>
<tr>
<td>portid</td>
<td>Starting port ID number.</td>
</tr>
<tr>
<td>end_portid</td>
<td>Ending port ID number.</td>
</tr>
<tr>
<td>direction</td>
<td>Allowed values are either IN or OUT.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>state</td>
<td>Two-character abbreviation for the state of surveillance.</td>
</tr>
<tr>
<td>county</td>
<td>County of surveillance.</td>
</tr>
<tr>
<td>city</td>
<td>City of surveillance.</td>
</tr>
<tr>
<td>warrantid</td>
<td>Warrant ID number.</td>
</tr>
<tr>
<td>caseid</td>
<td>String that uniquely identifies the subject.</td>
</tr>
<tr>
<td>subsid</td>
<td>Phone number of the subject, or MIN if it is a mobile phone. This string must match that provisioned on the call agent.</td>
</tr>
<tr>
<td>startdate</td>
<td>Start date that observation is to begin in mm/dd/yyyy format, or NOW if observation is to begin immediately.</td>
</tr>
<tr>
<td>expdate</td>
<td>Expiration date that observation is to end in mm/dd/yyyy format, or UNSPEC for no expiration date.</td>
</tr>
<tr>
<td>cfid</td>
<td>Collection function ID. Must match a CFID that has been previously added (by the <strong>add-cf:</strong> command).</td>
</tr>
<tr>
<td>survtype</td>
<td>Surveillance type. DATA for call data only, or CONTENT for call data and call content.</td>
</tr>
<tr>
<td>content</td>
<td>Currently, the only value supported is COMBINED, which specifies call data and call content are to be intercepted.</td>
</tr>
<tr>
<td>user</td>
<td>Person creating the surveillance instance.</td>
</tr>
<tr>
<td>access</td>
<td>PUBLIC if every mediation device web user can view the record, or PRIVATE if only the user who created the record can view it.</td>
</tr>
</tbody>
</table>

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=22221111112,afid=Cable;
```

Table 7 describes the strings in the **add-aftdn** command.
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:ipcccid=1,cccid=0001,state=AA,county=main-county,city=Home-Town,warrantid=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

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipcccid</td>
<td>IP call content channel ID</td>
</tr>
<tr>
<td>cccid</td>
<td>String appended to call content, CCOpen, and CCClose messages before they are sent to the collection function.</td>
</tr>
<tr>
<td>note</td>
<td>The cccid value should be left blank for VoIP applications since the CMS or mediation device will automatically pick up a unique cccid. The string can be used for data intercepts to force a known cccid.</td>
</tr>
<tr>
<td>state</td>
<td>Two-character abbreviation for the state of surveillance.</td>
</tr>
<tr>
<td>county</td>
<td>County of surveillance.</td>
</tr>
<tr>
<td>city</td>
<td>City of surveillance.</td>
</tr>
<tr>
<td>warrantid</td>
<td>Warrant ID number.</td>
</tr>
<tr>
<td>subsid</td>
<td>Phone number of the subject, or MIN if it is a mobile phone. This string must match that provisioned on the call agent.</td>
</tr>
<tr>
<td>cfipaddr</td>
<td>IP address of the LEA collection function.</td>
</tr>
<tr>
<td>cfport</td>
<td>Port on which the collection function receives call content.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>afid</td>
<td>Access Function ID (AFID) that is a user-specified string (up to 16 characters) that uniquely identifies the device. The AFID specified in the <code>add-af</code> command is then used to reference the device in subsequent commands.</td>
</tr>
<tr>
<td>name</td>
<td>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 Networks mediation device and is not used for any other purpose.</td>
</tr>
<tr>
<td>type</td>
<td>Type of physical device. Allowed values are BTS10200, CMS, CMTS, DCFD, GENERIC, MGC, SM, SNMPER, TGW, or SYION.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>Version of software release running on the AF (optional).</td>
</tr>
<tr>
<td>preprov</td>
<td>Time zone of the access function.</td>
</tr>
</tbody>
</table>

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,interfaceid=ANY_INTERFACE;

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

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>afid</td>
<td>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 <code>add-af</code> command.</td>
</tr>
<tr>
<td>ifid</td>
<td>Interface ID. Must be 1.</td>
</tr>
<tr>
<td>domainname</td>
<td>Domain name configured in DNS.</td>
</tr>
<tr>
<td>ipaddr</td>
<td>IP address of the access function.</td>
</tr>
</tbody>
</table>
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.

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 10: `add-afsi` Command Strings (continued)

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>Port 161 is the default for SNMP.</td>
</tr>
<tr>
<td>reqstate</td>
<td>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.</td>
</tr>
<tr>
<td>username</td>
<td>The username and passwords must match those provisioned on the access function. Passwords must be at least eight characters in length.</td>
</tr>
<tr>
<td>authpasswd</td>
<td></td>
</tr>
<tr>
<td>privpasswd</td>
<td></td>
</tr>
<tr>
<td>securitylvl</td>
<td>Must be AUTHNOPRIV. Aggregation routers will not allow NOAUTHNOPRIV.</td>
</tr>
<tr>
<td>interfaceid</td>
<td>For aggregation routers, use ANY_INTERFACE. For trunking gateways or other devices that contain Digital Signal Processors (DSPs), use VOIP_SESSION.</td>
</tr>
</tbody>
</table>

### 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.

### Table 11: `add-afti` Command Strings

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

The `add-afbi` command adds the access function BTS interface (AFBI), which provisions the interface that the SS8 Networks 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.

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

On the SS8 Networks’ 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 the SS8 Networks 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 47.

Access Function Provisioning Interface Configuration

The `add-afpi` command adds the access function provisioning interface (AFPI) which provisions the interface that the SS8 Networks’ SSDF software uses to access the TopLayer DCFD. The TopLayer DCFD is required only when data intercepts that require sniffing of RADIUS traffic are needed.

```plaintext
MML_calea_admin> add-afpi:afid=TopLayer,ifid=1,ipaddr=10.15.113.61,username=calea port=ACTIVE,reqstate=ACTIVE;
```

Table 13 describes the strings in the `add-afpi` command.

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>afid</td>
<td>Access function ID that has been previously configured in the AF table.</td>
</tr>
<tr>
<td>ifid</td>
<td>Interface ID. Each TopLayer DCFD must have a unique IFID.</td>
</tr>
</tbody>
</table>
Device Configuration Files

Cisco Service Independent Intercept Architecture Version 2.0

Access Function PGW Provisioning Interface Configuration

The `add-afgi` command adds the access function PGW interface (AFGI), which provisions the interface that SS8 Networks 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
MML_calea_adm> add-afgi:afid=PGW,ifid=1,ipaddr=10.15.113.80,username=liusr,passwd=test123,reqstate=ACTIVE
```

Table 14 describes the strings in the `add-afgi` command.

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr</td>
<td>IP address of the DCFD unit.</td>
</tr>
<tr>
<td>username</td>
<td>Username “calea” must be configured on the EMS.</td>
</tr>
<tr>
<td>port</td>
<td>Port to be used on the DCFD unit. Recommended value is 0 (zero).</td>
</tr>
<tr>
<td>reqstate</td>
<td>Required state. State is ACTIVE if this interface is trying to initialize and come into service.</td>
</tr>
</tbody>
</table>

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 Networks mediation device. The command must be executed by user `calea_adm`. 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
MML_calea_adm> add-afri:afid=Cable,ifid=1,ipaddr=10.8.100.102,port=14146,reqstate=ACTIVE,version=108,sharedsecret=0000000000000000
MML_calea_adm> add-afri:afid=Cable,ifid=2,ipaddr=10.8.100.103,port=14146,reqstate=ACTIVE,version=108,sharedsecret=0000000000000000
```

Table 15 describes the strings in the `add-afri` command.

<table>
<thead>
<tr>
<th>String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>afid</td>
<td>Access function ID that has been previously configured in the AF table.</td>
</tr>
<tr>
<td>ifid</td>
<td>Interface ID. Each PGW unit must have a unique IFID.</td>
</tr>
<tr>
<td>ipaddr</td>
<td>IP address of the PGW unit.</td>
</tr>
<tr>
<td>username</td>
<td>Must match that provisioned on the access function.</td>
</tr>
<tr>
<td>passwd</td>
<td>Password must be at least eight characters in length.</td>
</tr>
<tr>
<td>reqstate</td>
<td>Allowed values are ACTIVE or INACTIVE.</td>
</tr>
<tr>
<td>version</td>
<td>Recommended value is 0 (zero).</td>
</tr>
<tr>
<td>sharedsecret</td>
<td>Secret key shared between the call agent and the SS8 Networks mediation device.</td>
</tr>
</tbody>
</table>
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_adm.

```
MML_calea_adm> add-almdest:name=SNMP,type=SNMP;
```

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

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

For information on editing files to set up the addresses and ports of the SNMP network management server, see the *SS8 Xcipio SSDF User Manual* in the “Related Documents” section on page 47. 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 16 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, Edge Services Router (ESR)-eg2.sm02.cisco.com.

<table>
<thead>
<tr>
<th>Name(v)</th>
<th>TTL</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>—</td>
<td>PTR</td>
<td>ESR-egw.sm02.cisco.com</td>
</tr>
<tr>
<td>0</td>
<td>—</td>
<td>A</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
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 35
- Verifying the Cisco PGW 2200 Softswitch Call Agent Configuration, page 36
- Verifying the SS8 Networks Mediation Device Configuration, page 37
- Verifying the DNS Configuration from the Mediation Device, page 40
- Verifying Edge Router and Trunking Gateway Configurations, page 41

## 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.

**BTS>** `show ess`

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

```
CDC_DF_PORT=1813
CDC_DF_ADDRESS=10.15.113.9
ENCRYPTION_KEY=0000000000000000
ACC_REQ_RETRANSMIT=3
ACC_RSP_TIMER=2
PROTOCOL_VERSION=I03
IPSEC_SA_ESP_CS=3DES-MD5,3DES-SHA1,NULL-MD5,NULL-SHA1
IPSEC_SA_LIFETIME=86400
IPSEC_SA_GRACE_PERIOD=21600
IPSEC_ULP_NAME=IP
IKE_GROUP=2
IKE_CS=3DES-MD5,3DES-SHA1
USE_PACKETCABLE_IAP=Y
```

**Note**

In the above example, since USE_PACKETCABLE_IAP=Y, this example is for PacketCable mode or mixed mode. If USE_PACKETCABLE_IAP is set to N, the example is for SII mode only.

**CLI>** `show wiretap`

```
SUBSCRIBER_DN=e4d8721cb4f1d60d784195177e1c46f7
TAPTYPE=INTERCEPT
CDC_DF_ADDRESS=10.15.113.9
CDC_DF_PORT=1813
CCC_DF_ADDRESS=10.15.113.9
CCC_DF_PORT=45010
```
Verifying the Cisco SII LI Network

SUBSCRIBER_DN=e4d8721cb4f1d60dfa4bb16bbd6af81
TAPTYPE=PEN_AND_TRACE
CDC_DF_ADDRESS=10.15.113.9
CDC_DF_PORT=1813

SUBSCRIBER_DN=f9e4495092d9f3bb9928014403aacc0a
TAPTYPE=PEN_AND_TRACE
CDC_DF_ADDRESS=10.15.113.9
CDC_DF_PORT=1813

SUBSCRIBER_DN=f9e4495092d9f3bb9b85194d1ccfbc155
TAPTYPE=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: Entries 1-4 of 4 returned.

CLI>

The following command shows the wiretap information for a specific subscriber.

CLI> show wiretap subscriber_dn=6213000001

SUBSCRIBER_DN=f9e4495092d9f3bb9b85194d1ccfbc155
TAPTYPE=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>

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:IPLINK:NAME="NAME OF LINK TO MD"
MML> PROV-RTRV:SIGSVCPROP: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:

MML> wiretap-rtrv:subscriber:subscriber="target’s phone number"
MML> wiretap-rtrv:subscriber="all"
Verifying the SS8 Networks Mediation Device Configuration

The following commands can be used to verify the SS8 Networks mediation device configuration. For more information on verifying the SS8 Networks mediation device, see the *SS8 Xcipio SSDF User Manual* in the “Related Documents” section on page 47.

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

```mml
MML_calea> 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
MML_calea> 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
MML_calea> 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.
```
<table>
<thead>
<tr>
<th>CFID</th>
<th>NAME</th>
<th>TYPE</th>
<th>GRP1</th>
<th>GRP2</th>
<th>GRP3</th>
<th>CARRIER</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CF-1</td>
<td>TCPIP</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>000</td>
</tr>
<tr>
<td>2</td>
<td>CF-2</td>
<td>TCPIP</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>000</td>
</tr>
</tbody>
</table>

<SUCCESS>:: 2 records found.

<table>
<thead>
<tr>
<th>CFID</th>
<th>OWNIP</th>
<th>IPADDR</th>
<th>PORT</th>
<th>REQSTATE</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.18.137.105</td>
<td>172.18.137.94</td>
<td>43001</td>
<td>ACTIVE</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>2</td>
<td>172.18.137.105</td>
<td>172.18.137.56</td>
<td>43001</td>
<td>ACTIVE</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

<SUCCESS>:: 2 records found.

<table>
<thead>
<tr>
<th>AFID</th>
<th>NAME</th>
<th>TYPE</th>
<th>SERIAL</th>
<th>VERSION</th>
<th>PREPROV</th>
<th>INDEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>TopLayer</td>
<td>TopLayer</td>
<td>DCFD</td>
<td>N/A</td>
<td>1.0</td>
<td>000:00</td>
<td>8</td>
</tr>
<tr>
<td>PGW</td>
<td>PGW</td>
<td>PGW2000</td>
<td>N/A</td>
<td>9.6</td>
<td>000:00</td>
<td>11</td>
</tr>
<tr>
<td>7246-I1705</td>
<td>7246-I1705</td>
<td>SNMPER</td>
<td>N/A</td>
<td>12.3</td>
<td>000:00</td>
<td>3</td>
</tr>
<tr>
<td>Beyond</td>
<td>Beyond</td>
<td>BTS10200</td>
<td>N/A</td>
<td>4.4</td>
<td>000:00</td>
<td>1</td>
</tr>
<tr>
<td>Cable</td>
<td>Cable</td>
<td>BTS10200</td>
<td>N/A</td>
<td>4.4</td>
<td>000:00</td>
<td>2</td>
</tr>
<tr>
<td>7200-egw</td>
<td>7200-egw</td>
<td>SNMPER</td>
<td>N/A</td>
<td>12.4</td>
<td>000:00</td>
<td>2</td>
</tr>
<tr>
<td>7500-egw</td>
<td>7500-egw</td>
<td>SNMPER</td>
<td>N/A</td>
<td>12.4</td>
<td>000:00</td>
<td>3</td>
</tr>
<tr>
<td>ESR-egw</td>
<td>ESR-egw</td>
<td>SNMPER</td>
<td>N/A</td>
<td>12.2</td>
<td>000:00</td>
<td>1</td>
</tr>
</tbody>
</table>

<SUCCESS>:: 8 records found.

<table>
<thead>
<tr>
<th>AFID</th>
<th>IFID</th>
<th>IPADDR</th>
<th>REQSTATE</th>
<th>STATE</th>
<th>USERNAME</th>
<th>PASSWD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beyond</td>
<td>1</td>
<td>10.15.69.7</td>
<td>INACTIVE</td>
<td>INACTIVE</td>
<td>calea</td>
<td>test123</td>
</tr>
<tr>
<td>Cable</td>
<td>1</td>
<td>10.8.100.100</td>
<td>ACTIVE</td>
<td>ACTIVE</td>
<td>calea</td>
<td>test123</td>
</tr>
<tr>
<td>Cable</td>
<td>2</td>
<td>10.8.100.101</td>
<td>ACTIVE</td>
<td>ACTIVE</td>
<td>calea</td>
<td>test123</td>
</tr>
</tbody>
</table>

<SUCCESS>:: 3 records found.

<table>
<thead>
<tr>
<th>AFID</th>
<th>IFID</th>
<th>IPADDR</th>
<th>REQSTATE</th>
<th>STATE</th>
<th>USERNAME</th>
<th>PASSWD</th>
</tr>
</thead>
<tbody>
<tr>
<td>PGW</td>
<td>1</td>
<td>10.15.113.80</td>
<td>ACTIVE</td>
<td>ACTIVE</td>
<td>liuser</td>
<td></td>
</tr>
</tbody>
</table>

<SUCCESS>:: 1 record found.

<table>
<thead>
<tr>
<th>AFID</th>
<th>IFID</th>
<th>IPADDR</th>
<th>PORT</th>
<th>REQSTATE</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>TopLayer</td>
<td>1</td>
<td>10.15.113.61</td>
<td>0</td>
<td>ACTIVE</td>
<td>ACTIVE</td>
</tr>
</tbody>
</table>

<SUCCESS>:: 1 record found.
### Verifying the Cisco SII LI Network

#### MML_TH:

```mml
display-afsi:
```

<table>
<thead>
<tr>
<th>AFID</th>
<th>IFID</th>
<th>DOMAINNAME</th>
<th>IPADDR</th>
<th>PORT</th>
<th>REQSTATE</th>
<th>STATE</th>
<th>USERNAME</th>
<th>AUTHPASSWD</th>
<th>PRIVPASSWD</th>
<th>SECURITYLVL</th>
<th>INTERFACEID</th>
</tr>
</thead>
<tbody>
<tr>
<td>7200-egw</td>
<td>1</td>
<td>7200-egw.sm02.cisco.com</td>
<td>10.15.115.1</td>
<td>161</td>
<td>ACTIVE</td>
<td>ACTIVE</td>
<td>ss8user</td>
<td>ss8passwd</td>
<td>AUTHNOPRIV</td>
<td>ANY_INTERFACE</td>
<td></td>
</tr>
<tr>
<td>7500-egw</td>
<td>1</td>
<td>7500-egw.sm02.cisco.com</td>
<td>10.15.115.2</td>
<td>161</td>
<td>ACTIVE</td>
<td>ACTIVE</td>
<td>ss8user</td>
<td>ss8passwd</td>
<td>AUTHNOPRIV</td>
<td>ANY_INTERFACE</td>
<td></td>
</tr>
<tr>
<td>ESR-egw</td>
<td>1</td>
<td>ESR-egw.sm02.cisco.com</td>
<td>10.15.115.3</td>
<td>161</td>
<td>ACTIVE</td>
<td>ACTIVE</td>
<td>ss8user</td>
<td>ss8passwd</td>
<td>AUTHNOPRIV</td>
<td>ANY_INTERFACE</td>
<td></td>
</tr>
</tbody>
</table>

<SUCCESS>:: 3 records found.

#### MML_calea:

```mml
display-afti:
```

<table>
<thead>
<tr>
<th>AFID</th>
<th>IFID</th>
<th>DOMAINNAME</th>
<th>IPADDR</th>
<th>PORT</th>
<th>REQSTATE</th>
<th>STATE</th>
<th>PROTOCOL</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS5850-2</td>
<td>1</td>
<td>AS5850-2.sm02.cisco.com</td>
<td>10.15.111.6</td>
<td>2427</td>
<td>ACTIVE</td>
<td>ACTIVE</td>
<td>MGCP</td>
<td>1.0</td>
</tr>
<tr>
<td>mgxc701-11</td>
<td>1</td>
<td>mgxc701-11.sm02.cisco.com</td>
<td>10.15.112.193</td>
<td>2427</td>
<td>ACTIVE</td>
<td>ACTIVE</td>
<td>MGCP</td>
<td>1.0</td>
</tr>
</tbody>
</table>

<SUCCESS>:: 2 records found.

#### MML_TH:

```mml
display-afri:
```

<table>
<thead>
<tr>
<th>AFID</th>
<th>IFID</th>
<th>IPADDR</th>
<th>PORT</th>
<th>REQSTATE</th>
<th>VERSION</th>
<th>SHAREDSECRET</th>
</tr>
</thead>
<tbody>
<tr>
<td>PGW</td>
<td>1</td>
<td>10.15.113.80</td>
<td>14146</td>
<td>ACTIVE</td>
<td>I08</td>
<td>0000000000000000</td>
</tr>
<tr>
<td>PGW</td>
<td>2</td>
<td>10.15.113.81</td>
<td>14146</td>
<td>ACTIVE</td>
<td>I08</td>
<td>0000000000000000</td>
</tr>
<tr>
<td>Beyond</td>
<td>1</td>
<td>10.15.69.35</td>
<td>14146</td>
<td>ACTIVE</td>
<td>I08</td>
<td>0000000000000000</td>
</tr>
<tr>
<td>Beyond</td>
<td>2</td>
<td>10.15.69.36</td>
<td>14146</td>
<td>ACTIVE</td>
<td>I08</td>
<td>0000000000000000</td>
</tr>
<tr>
<td>Beyond</td>
<td>3</td>
<td>10.15.69.67</td>
<td>14146</td>
<td>ACTIVE</td>
<td>I08</td>
<td>0000000000000000</td>
</tr>
<tr>
<td>Beyond</td>
<td>4</td>
<td>10.15.69.68</td>
<td>14146</td>
<td>ACTIVE</td>
<td>I08</td>
<td>0000000000000000</td>
</tr>
<tr>
<td>Cable</td>
<td>1</td>
<td>10.8.100.102</td>
<td>14146</td>
<td>ACTIVE</td>
<td>I08</td>
<td>0000000000000000</td>
</tr>
<tr>
<td>Cable</td>
<td>2</td>
<td>10.8.100.103</td>
<td>14146</td>
<td>ACTIVE</td>
<td>I08</td>
<td>0000000000000000</td>
</tr>
</tbody>
</table>

<SUCCESS>:: 8 records found.

#### MML_calea:

```mml
display-surveillance:
```

<table>
<thead>
<tr>
<th>STATE</th>
<th>COUNTY</th>
<th>CITY</th>
<th>WARRANTID</th>
<th>JAREA</th>
<th>CASEID</th>
<th>SUBSID</th>
<th>ENTRYDATE</th>
<th>STARTDATE</th>
<th>EXPDATE</th>
<th>STATUS</th>
<th>CFID</th>
<th>SURVTYPE</th>
<th>CONTENT</th>
<th>USER</th>
<th>ACCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td>Main-County</td>
<td>Home-Town</td>
<td>0305</td>
<td>COUNTRY</td>
<td>0305</td>
<td>9844950305</td>
<td>08/30/2002</td>
<td>08/30/2002</td>
<td>12/31/2002</td>
<td>ACTIVE</td>
<td>1</td>
<td>DATA</td>
<td>None</td>
<td>calea Opr</td>
<td>PUBLIC</td>
</tr>
<tr>
<td>AA</td>
<td>Main-County</td>
<td>Home-Town</td>
<td>0306</td>
<td>COUNTRY</td>
<td>0306</td>
<td>9844950306</td>
<td>08/22/2002</td>
<td>08/22/2002</td>
<td>12/30/2002</td>
<td>ACTIVE</td>
<td>2</td>
<td>DATA</td>
<td>None</td>
<td>calea Opr</td>
<td>PUBLIC</td>
</tr>
<tr>
<td>AA</td>
<td>Main-County</td>
<td>Home-Town</td>
<td>0308</td>
<td>COUNTRY</td>
<td>0308</td>
<td>9844950308</td>
<td>08/22/2002</td>
<td>08/22/2002</td>
<td>12/30/2002</td>
<td>ACTIVE</td>
<td>2</td>
<td>CONTENT</td>
<td>COMBINED</td>
<td>calea Opr</td>
<td>PUBLIC</td>
</tr>
<tr>
<td>AA</td>
<td>Main-County</td>
<td>Home-Town</td>
<td>1001</td>
<td>COUNTRY</td>
<td>1001</td>
<td>9192621001</td>
<td>09/30/2002</td>
<td>09/30/2002</td>
<td>12/31/2003</td>
<td>ACTIVE</td>
<td>2</td>
<td>CONTENT</td>
<td>COMBINED</td>
<td>calea Opr</td>
<td>PUBLIC</td>
</tr>
<tr>
<td>AA</td>
<td>Main-County</td>
<td>Home-Town</td>
<td>0307</td>
<td>COUNTRY</td>
<td>0307</td>
<td>9844950307</td>
<td>10/01/2002</td>
<td>10/01/2002</td>
<td>11/01/2003</td>
<td>ACTIVE</td>
<td>2</td>
<td>CONTENT</td>
<td>COMBINED</td>
<td>calea Opr</td>
<td>PUBLIC</td>
</tr>
</tbody>
</table>

<SUCCESS>:: 5 records found.
Verifying the Cisco SII LI Network

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

```
MML_calea> 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_calea> display-ipccc;
------------------------------------------------------------------------------------------
---------------------------------------------
IPCCCID STATE COUNTY              CITY                WARRANTID           CCCID
SUBSID           CFIPADDR        CFPORT STATUS
------------------------------------------------------------------------------------------
---------------------------------------------
1       AA    Home-Town           Home-Town           0308                ----
9844950308       172.18.137.56   9000   ACTIVE
8       AA    Home-Town           Home-Town           9192621001          ----
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 Edge Router and Trunking Gateway Configurations

The `show snmp view` command 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.

```
7200-egw# show snmp view
*ilmi system - included permanent active
*ilmi atmForumUni - included permanent active
tapView ciscoIpTapMIB - included nonvolatile active
tapView ciscoTap2MIB - included nonvolatile active
v1default iso - included permanent active
v1default internet.6.3.15 - excluded volatile active
v1default internet.6.3.16 - excluded volatile active
v1default internet.6.3.18 - excluded volatile active
v1default ciscoIpTapMIB - excluded volatile active
v1default ciscoMgmt.395 - excluded volatile active
v1default ciscoTap2MIB - excluded volatile active
v1default ciscoMgmt.400 - excluded volatile active
```

The `show snmp view` command can be used to verify the gateway configuration for session-based intercept on a trunking gateway router.

```
AS5400-022# show snmp view
tapView ciscoIpTapMIB - included nonvolatile active
tapView ciscoTap2MIB - included nonvolatile active
tapView ciscoUserConnectionTapMIB - included nonvolatile active
v1default iso - included permanent active
v1default internet.6.3.15 - excluded volatile active
v1default internet.6.3.16 - excluded volatile active
v1default internet.6.3.18 - excluded volatile active
v1default ciscoIpTapMIB - excluded volatile active
v1default ciscoMgmt.395 - excluded volatile active
v1default ciscoTap2MIB - excluded volatile active
v1default ciscoUserConnectionTapMIB - excluded volatile active
AS5400-022#
```

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

```
7200-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.

```
7200-egw# show snmp user
User name: mduserid
Engine ID: 80000009030000B04AD1B000
storage-type: nonvolatile active
Authentication Protocol: MD5
```
Troubleshooting a Cisco SII LI Network

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

- General Troubleshooting Notes, page 42
- Troubleshooting the Mediation Device, page 42
- Troubleshooting the BTS Call Agent, page 42
- Troubleshooting Table ESS, page 43

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 Networks 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 Networks Xcipio mediation device, see the SS8 Xcipio SSDF User Manual in the “Related Documents” section on page 47.

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 Networks 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 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 47.

**Troubleshooting Table ESS**

As user calea, enter the `show ess` EXEC command to verify the data in table ESS:

```
CLI> show ess

CDC_DF_PORT=1813
CDC_DF_ADDRESS=10.15.113.9
ENCRYPTION_KEY=0000000000000000
ACC_REQ RETRANSMIT=3
ACC_RSP_TIMER=2
PROTOCOL_VERSION=I03
IPSEC_SA_ESP_CS=3DES-MD5,3DES-SHA1,NULL-MD5,NULL-SHA1
IPSEC_SA_LIFETIME=86400
IPSEC_SA_GRACE_PERIOD=21600
IPSEC_ULP_NAME=IP
IKE_GROUP=2
IKE_SA_LIFETIME=86400
IKE_CS=3DES-MD5,3DES-SHA1
USE_PACKETCABLE_IAP=N
```

Verify the following items:

- The CDC_DF_ADDRESS string equals that of the MD (and must match the string used when the MD performs an `add wiretap` command).
- The ENCRYPTION_KEY is the same string that is configured on the MD.
- The PROTOCOL_VERSION should be I03.
- The USE_PACKETCABLE_IAP value is N if you want to be in SII mode only. Use Y if you want to be in mixed mode.

**Appendix**

This section contains the following information:

- Cisco Products That Support Lawful Intercept, page 44
- Related Documents, page 47
- Standards, page 48
- MIBs, page 48
- RFCs, page 48
- Technical Assistance, page 48
Cisco Products That Support Lawful Intercept

Table 17 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
  - SIIv2—Cisco SII software that supports version 2.0 of Cisco LI MIB
  - PC—PacketCable
  - CISCO-TAP-MIB, CISCO-TAP2-MIB, CISCO-IP-TAP-MIB—version of Cisco LI MIB
- **Data Support**—describes the software versions that the platform supports:
  - SIIv1—Cisco SII software that supports version 1.0 of LI
  - SIIv2—Cisco SII software that supports version 2.0 of LI
  - PC—PacketCable
  - CISCO-TAP-MIB, CISCO-TAP2-MIB, CISCO-IP-TAP-MIB—version of Cisco LI MIB

Table 17 displays the Cisco products that support LI architecture.

<table>
<thead>
<tr>
<th>Cisco Product</th>
<th>Product Type</th>
<th>Voice Support</th>
<th>Data Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco BTS 10200</td>
<td>Call agent</td>
<td>• SIIv1 and SIIv2—supports BTS Release 4.4 and later releases</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—supports BTS Release 4.4 and later releases</td>
<td></td>
</tr>
<tr>
<td>Cisco PGW 2200</td>
<td>Call agent</td>
<td>• SIIv1 and SIIv2—supports PGW Release 9.5(1) and later releases</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—N/A</td>
<td></td>
</tr>
<tr>
<td>Cisco 7200 series</td>
<td>Aggregation router</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.3(8)T until Release 12.3(14)T</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.3(8)T until Release 12.3(14)T</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIIv2 (Cisco-TAP2-MIB, Cisco-IP-TAP-MIB)—supports Cisco IOS Release 12.3(14)T and later releases</td>
<td>• SIIv2 (Cisco-TAP2-MIB, Cisco-IP-TAP-MIB)—supports Cisco IOS Release 12.3(14)T and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—N/A</td>
<td>• PC—N/A</td>
</tr>
<tr>
<td>Cisco 7301</td>
<td>Aggregation router</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.3(8)T until Release 12.3(14)T</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.3(8)T until Release 12.3(14)T</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIIv2 (Cisco-TAP2-MIB, Cisco-IP-TAP-MIB)—Cisco IOS Release 12.3(14)T and later releases</td>
<td>• SIIv2 (Cisco-TAP2-MIB, Cisco-IP-TAP-MIB)—Cisco IOS Release 12.3(14)T and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—N/A</td>
<td>• PC—N/A</td>
</tr>
</tbody>
</table>
### Table 17  Cisco Products That Support Lawful Intercept (continued)

<table>
<thead>
<tr>
<th>Cisco Product</th>
<th>Product Type</th>
<th>Voice Support</th>
<th>Data Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 7505</td>
<td>Aggregation router</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.3(9) and later releases</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.3(9) and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—N/A</td>
<td>• PC—N/A</td>
</tr>
<tr>
<td>Cisco 7507</td>
<td>Aggregation router</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.3(9) and later releases</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.3(9) and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—N/A</td>
<td>• PC—N/A</td>
</tr>
<tr>
<td>Cisco 7513</td>
<td>Aggregation router</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.3(9) and later releases</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.3(9) and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—N/A</td>
<td>• PC—N/A</td>
</tr>
<tr>
<td>Cisco 10000</td>
<td>Aggregation router</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.0(25)S and later releases</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.0(25)S and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—N/A</td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• PC—N/A</td>
</tr>
<tr>
<td>Cisco 12000 Gigabit Switch Router (GSR)</td>
<td>Aggregation router</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.0(32)S and later releases</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.0(32)S and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—N/A</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.0(32)S and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• PC—N/A</td>
</tr>
<tr>
<td>Cisco Universal Broadband Router (uBR)7246 VXR</td>
<td>CMTS</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.3(13)a-BC and later releases</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.3(13)a-BC and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—Cisco IOS Release 12.2(15)BC1b and later releases</td>
<td>• PC—Cisco IOS Release 12.2(15)BC1b and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• PC—N/A</td>
</tr>
<tr>
<td>Cisco uBR10000</td>
<td>CMTS</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.2(15)BC1b and later releases</td>
<td>• SIIv1 (Cisco-TAP-MIB)—Cisco IOS Release 12.2(15)BC1b and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—Cisco IOS Release 12.2(15)BC1b and later releases</td>
<td>• PC—N/A</td>
</tr>
</tbody>
</table>
**Table 17  Cisco Products That Support Lawful Intercept (continued)**

<table>
<thead>
<tr>
<th>Cisco Product</th>
<th>Product Type</th>
<th>Voice Support</th>
<th>Data Support</th>
</tr>
</thead>
</table>
| Content Services Gateway (CSG)            | Blade for Cisco Catalyst 6000 and Cisco Catalyst 7600 | • SIIv1 (Cisco-TAP-MIB): Cisco Catalyst 6000:  
  - 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:  
    - SIIv1 (Cisco-TAP-MIB): Supervisor software—s72033-adventerp risek9_wan-mz.122-18.SXE  
      1.bin; s72033-advipservicesk9_wan-mz.122-18.SXE1.bin; CSG software  
      -WS-SVC-CSG-L4.0  
    - PC—N/A | • Cisco Catalyst 6000:  
  - 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:  
    - SIIv1 (Cisco-TAP-MIB): Supervisor software—s72033-adventerp risek9_wan-mz.122-18.SXE  
      1.bin; s72033-advipservicesk9_wan-mz.122-18.SXE1.bin; CSG software  
      -WS-SVC-CSG-L4.0  
    - PC—N/A |
| Cisco 3660                                | Trunking gateway            | • SIIv1 (Cisco-TAP-MIB)  
  -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            | • SIIv1 (Cisco-TAP-MIB): Cisco IOS Release 12.3(7)T until Release 12.3(14)T  
  • SIIv2 (Cisco-TAP2-MIB): Cisco IOS Release 12.3(14)T and later releases  
  • PC—N/A | — |
| Cisco MGX 8850 VG                         | Trunking gateway            | • SII—N/A  
  • PC  
    - Voice Interworking Service Module (VISM) 2.2 and later releases  
    - Voice Switch Service Module (VXSM) 2.0 and later releases | — |
### Table 17  Cisco Products That Support Lawful Intercept (continued)

<table>
<thead>
<tr>
<th>Cisco Product</th>
<th>Product Type</th>
<th>Voice Support</th>
<th>Data Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco AS 5350</td>
<td>Access server/trunking gateway</td>
<td>• SIIv1 (Cisco-TAP-MIB)—N/A</td>
<td>• SIIv1 (Cisco-TAP-MIB)—N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIIv2 (Cisco-TAP2-MIB)—Cisco IOS Release 12.3(14)T and later releases</td>
<td>• SIIv2 (Cisco-TAP2-MIB)—Cisco IOS Release 12.3(14)T and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—Cisco IOS Release 12.3(7)T and later releases</td>
<td>• PC—N/A</td>
</tr>
<tr>
<td>Cisco AS 5400</td>
<td>Access server/trunking gateway</td>
<td>• SIIv1 (Cisco-TAP-MIB)—N/A</td>
<td>• SIIv1 (Cisco-TAP-MIB)—N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIIv2 (Cisco-TAP2-MIB)—Cisco IOS Release 12.3(14)T and later releases</td>
<td>• SIIv2 (Cisco-TAP2-MIB)—Cisco IOS Release 12.3(14)T and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—Cisco IOS Release 12.3(7)T and later releases</td>
<td>• PC—N/A</td>
</tr>
<tr>
<td>Cisco AS 5850</td>
<td>Access server/trunking gateway</td>
<td>• SIIv1 (Cisco-TAP-MIB)—N/A</td>
<td>• SIIv1 (Cisco-TAP-MIB)—N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SIIv2 (Cisco-TAP2-MIB)—Cisco IOS Release 12.3(14)T and later releases</td>
<td>• SIIv2 (Cisco-TAP2-MIB)—Cisco IOS Release 12.3(14)T and later releases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PC—Cisco IOS Release 12.3(7)T and later releases</td>
<td>• PC—N/A</td>
</tr>
</tbody>
</table>

### Related Documents

Table 18 lists related documents.

### Table 18  Related Documents

<table>
<thead>
<tr>
<th>Title</th>
<th>URL or Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>PacketCable Dynamic Quality of Service Specification</td>
<td><a href="http://www.packetcable.com/specifications">http://www.packetcable.com/specifications</a></td>
</tr>
<tr>
<td>SS8 Xcipio SSDF User Manual</td>
<td>2700-2493-01</td>
</tr>
<tr>
<td>Cisco Lawful Intercept Control MIB</td>
<td><a href="http://www.ietf.org/rfc/rfc3924.txt">http://www.ietf.org/rfc/rfc3924.txt</a></td>
</tr>
</tbody>
</table>
Table 18  Related Documents (continued)

<table>
<thead>
<tr>
<th>Title</th>
<th>URL or Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawful Intercept on Cisco 12000 Series Router ISE Line Cards</td>
<td>OL-8679-01 (Rev. A0)</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>TR-45 J-STD-025A</td>
<td>Telephone Industry Association Lawfully Authorized Electronic Surveillance</td>
</tr>
<tr>
<td>PKT-SP-EM-I08</td>
<td>PacketCable Event Messages Specification</td>
</tr>
<tr>
<td>PKT-SP-ESP-I03</td>
<td>PacketCable Electronic Surveillance Specification</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-TAP-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>• CISCO-TAP2-MIB</td>
<td></td>
</tr>
<tr>
<td>• CISCO-IP-TAP-MIB</td>
<td></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1101</td>
<td>DNS Encoding of Network Names and Other Types</td>
</tr>
<tr>
<td>RFC 3924</td>
<td>Cisco Architecture for Lawful Intercept in IP Networks</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support &amp; 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.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
Glossary

AAA—authentication, authorization, and accounting
AF—access function
AFBI—access function BTS interface
AFGI—access function PGW interface
AFID—access function ID
AFPI—access function Provisioning interface
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
DNS—Domain Name Service
DSP—Digital Signal Processor
EMS—Element Management System
ESR—Edge Services Router
ESS—Electronic Surveillance Subsystem
FQDN—fully qualified domain name
GSR—Gigabit Switch Router
HMAC—Hash-based Message Authentication Code
IAD—Integrated Access Device
IAP—intercept access point
IFID—Interface ID
Glossary

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
NAS—network access server
NTP—Network Time Protocol
off-net—off 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
tcpipefi—TCP/IP collection function interface
TGW—trunking gateway
TIA—Telephone Industry Association
TKUV—Telekommunikations Überwachungsverordnung
TopLayer—A company that provides a sniffer that makes data intercepts function with SSDF.
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.