CHAPTER 58

CALEA IRI Interface Support

The Communications Assistance for Law Enforcement Act (CALEA) intercept-related information (IRI) Interface Support feature enables service providers to define a legal warrant on VoIP endpoints to gather both signaling and media content information. The CALEA IRI Interface Support feature is based on PacketCable 1.5 standard specifications.

The CALEA IRI Interface Support feature is applicable to both Session Initiation Protocol (SIP) and H.323 calls in a unified Session Border Controller (SBC) configuration. It is not, however, applicable to distributed SBC.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the SBC.

For a complete description of the commands used in this chapter, refer to the *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html.

For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or a Cisco IOS master commands list.

Feature History for CALEA IRI Interface Support

Release	Modification
Cisco IOS XE Release 3.1S	The CALEA IRI Interface Support feature was introduced on Cisco ASR 1000 Series Routers.

Contents

This module contains the following sections:

Information About CALEA IRI Interface Support

The SBC can be used for the dual functions of Intercepting Control Element (ICE) and Intercepting Network Element (INE). You can place a request for a warrant using the Simple Network Management Protocol (SNMP) interface. The Cisco ASR 1000 series router responds with PacketCable1.5 messages and with replicated IP/UDP/RTP media packets, as required by the warrant.

You can also define the endpoint match using username, phone number, or SIP-Uniform Resource Identifier (URI). In addition, you can set up pen, trace, pen-and-trace, or intercept type of warrant.

You can define the VoIP endpoint information along with mediation device information using Simple Network Management Protocol Version 3 (SNMPv3) MIBs. The VoIP signaling information is sent from a router to a mediation device. In addition, the media content is tapped, replicated, encapsulated, and sent to the mediation device in real time.

Define the warrant by providing only the VoIP endpoint information. A Cisco ASR 1000 Series Router determines the local pinhole being used for a particular call, and replicates the call content to the mediation device. In addition, you can define the warrant by requesting only the call signaling-related information using PacketCable1.5 Event messages (IRI).

In the context of calls coming in on an adjacency, with the inherit profile set to preset-access, the source information from the SIP header will be used to match the configured warrants. In the context of the calls coming in on an adjacency, with the inherit profile set to preset-core, the destination information from the SIP header will be used to match the configured warrants. However, the provider can override these rules by configuring the **warrant match-order** command on the adjacencies.

For a registered SIP endpoint, we recommend setting cvoiptapStreamMatchType to URI.

When the VoIP call gets tapped, the Cisco ASR 1000 series router sends the locally generated unique Call Content Connection ID (CCCID) information using the RADIUS message. The same CCCID information is then used to encapsulate the media IP packet. An mediation device can use the CCCID information to correlate the signaling and media information. The VoIP LI warrant information can be retrieved using a secure SNMPv3 interface.

For each INTERCEPT, a unique IRI stream with CCCID information is present.

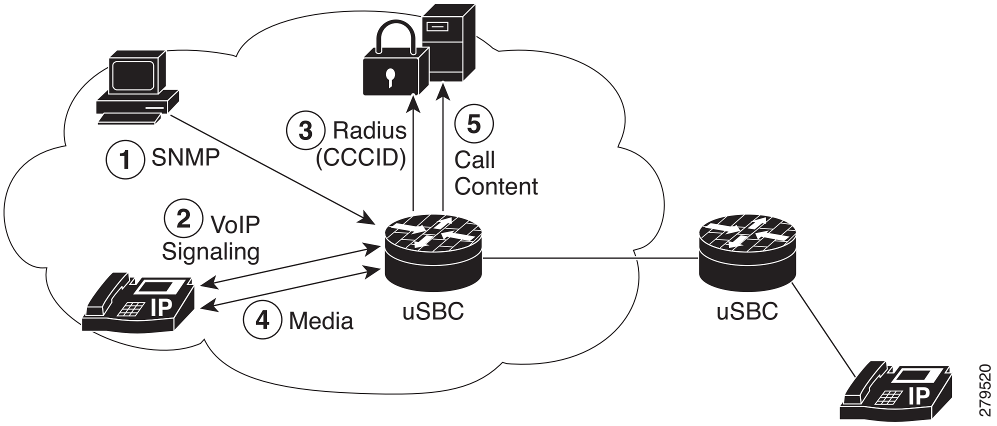
In a network setup of multiple Cisco ASR 1000 series routers, the CALEA IRI Interface Support feature is designed to tap the information on the router that is closest to the endpoint under surveillance.

This section contains the following information pertaining to the CALEA IRI Interface Support feature:

CALEA IRI Interface Support Flow

Figure 58-1 shows the flow of the CALEA IRI Interface Support feature.

Figure 58-1 Flow of the CALEA IRI Interface Support Feature



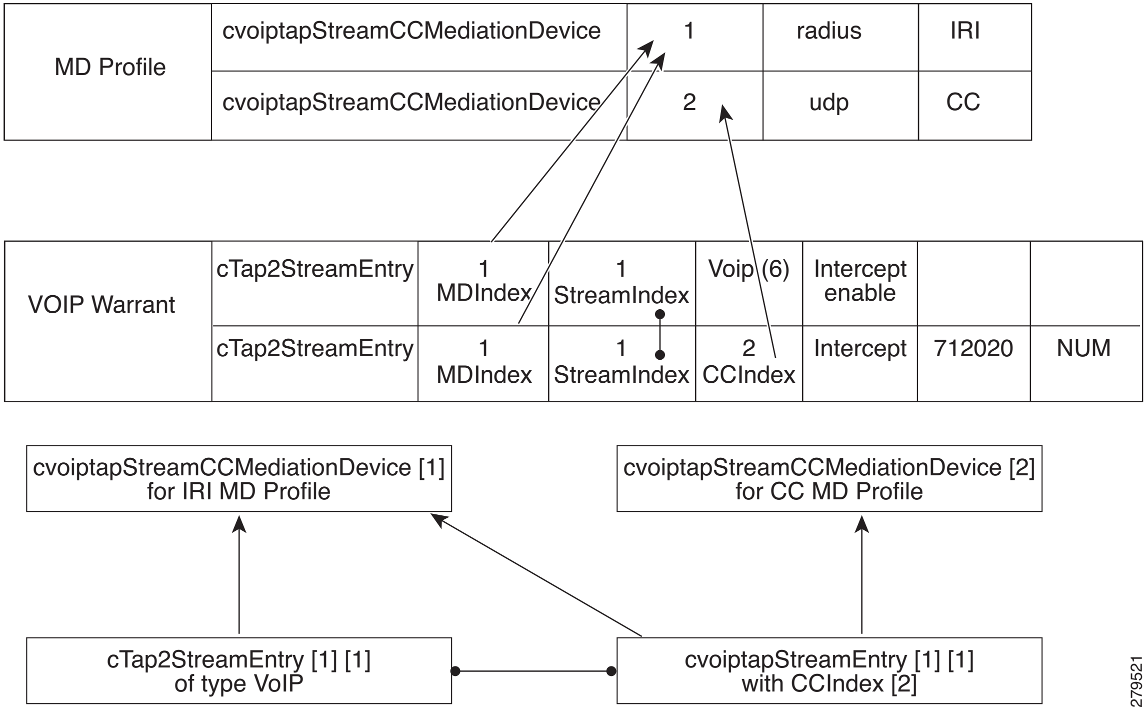
The steps pertaining to the flow of the CALEA IRI Interface Support feature are as follows:

1. Provisioning of mediation device information and VoIP warrant is done as a combination of SNMPv3 and IOS CLI commands on the Cisco ASR 1000 series router.
2. The calling party originates the call.
3. If a warrant matches the signaling parameters, RADIUS messages are sent to the mediation device. The message contains the unique CCCID generated by the Cisco ASR 1000 series router.
4. The party that was called answers, and the media information starts flowing through the Cisco ASR 1000 series router.
5. The Cisco ASR 1000 series router replicates the media information, and sends it to the mediation device.

SNMP Row Indices

Figure 58-2 represents the SNMP table and rows. There are two independent mediation device rows. The GenericStream and VoIP TAP MIB rows are the children of the IRI MD row. There is a CCIndex field in the VoIP TAP MIB row that captures the relationship with CC MD MIB row. A one-to-one relationship also exists between GenericStream and VoIP TAP MIB rows.

Figure 58-2 SNMP Row Indices


MD Profile
cvoiptapStreamCCMediationDevice
1
radius
IRI
cvoiptapStreamCCMediationDevice
2
udp
CC
VOIP Warrant
cTap2StreamEntry
1 MDIndex
1 StreamIndex
Voip (6)
Intercept enable
cTap2StreamEntry
1 MDIndex
1 StreamIndex
2 CCIndex
Intercept
712020
NUM
cvoiptapStreamCCMediationDevice [1] for IRI MD Profile
cvoiptapStreamCCMediationDevice [2] for CC MD Profile
cTap2StreamEntry [1] [1] of type VoIP
cvoiptapStreamEntry [1] [1] with CCIndex [2]
279521

Tap Interfaces

This section describes the following Tap interfaces:

- IRI Interface, page 58-5
- CC Interface, page 58-11

IRI Interface

The PacketCable 1.5 standard specifications for Electronic Surveillance contains the packet definition for all IRI-related messages. Table 58-1 details the supported call event messages that are sent for each Tapped Call.

Table 58-1 Supported Call Event Messages

Event Message	Notes
Signaling_Start	Sent when signalling has commenced (inbound), and when it is about to commence (outbound), for example, received INVITE on inbound, and about to send INVITE on outbound for a SIP endpoint.
QoS_Reserve	Sent for the inbound leg when the inbound QoS is reserved, and for the outbound leg when the outbound QoS is reserved.
Call_Answer	Indicates that the terminating party has answered, and that media has started. This message is sent for both the legs simultaneously.
QoS_Commit	Sent when QoS is committed by the SBC. This message is sent for both the legs at the same time.
Call_Disconnect	Sent when a call has been terminated, and media has ceased flowing. The message is sent for both the legs at the same time.
QoS_Release	Sent when the QoS is released by the SBC. Sent for both the legs at the same time.
Signaling_Stop	Sent when signaling is complete for each party in the call. The event is generated once for each party after the last signaling message is sent.
Media_Report	Sent by the SBC whenever a flow is created, modified, and released.
Surveillance_Stop	Sent by the SBC to indicate the end of the IRI or CC tapping or both. Generally, this means the end of a call.
Redirection	Sent by the SBC when a call has been transferred, either due to a 3XX redirect response, or a SIP REFER request.

Call Event Messages

Table 58-2 details the Signaling_Start message attributes that are supported and sent when the SBC has information that the destination is routable and the originating endpoint is allowed to make the call.

Table 58-2 Signaling_Start Message Attributes

Attribute Name	Comment
EM_Header	Common header attribute.
Direction_Indicator	Specifies if the device represents an originating or terminating part of a call. 1—originating 2—terminating

Table 58-2 Signaling_Start Message Attributes (continued)

MTA_Endpoint_Name	The SBC has no direct contact with the MTA. By default, the value is set to MTA Endpoint. Alternatively, the attribute could be configured to report adjacency or signalling address information.
Calling_Party_Number	The number of the calling party (if available). In the SBC, this is the canonical format of the number after inbound number translations, if any, and before the routing.
Called_Party_Number	The number of the called party (always present). In the SBC, this is the canonical format of the number after any inbound number translation and before routing.
Routing_Number	Indicates a routable number (always present).
User_Input	The number of the called party prior to any translation performed during inbound number analysis.
Translation_Input	The number of the called party after inbound number analysis and before routing, if different from the value supplied in User_Input.
Redirected_From_Info	If originating an INVITE in response to a 3XX or a REFER, the attribute is set to the previous destination of the call (the sender of the 3XX or REFER), the initial destination of the call (if there are multiple redirections), and the number of redirections so far on the call.
Carrier_Identification_Code	The Carrier Identification Code associated with this call.
Trunk_Group_ID	Trunk_Type set to 9. Signaling type is not specified. Trunk_Group_ID set to the Trunk Group ID associated with the side of the call that is being tapped.

The following Signaling_Start message attributes are not included in the message:

- Attribute Name
- Location_Routing_Number
- Intl_Code
- Dial_Around_Code
- Jurisdiction_Information_Parameter
- Ported_In_Calling_Number
- Ported_In_Called_Number
- Called_Party_NP_source

- Calling_Party_NP_source
- Billing_Type
- Electronic_Surveillance_Indication

Table 58-3 details the QoS_Reserve message attributes. This message is generated when the SBC has reserved bandwidth (QoS) on the network. If the reserved bandwidth changes, QoS_Reserve and QoS_Commit messages are generated anew.

Table 58-3 QoS_Reserve Message Attributes

Attribute Name	Comments
EM_Header	Common header attribute.
QoS_Descriptor	Similar to the description of the QoS_Reserve message.
MTA_UDP_Portnum	The UDP port number on the network element endpoint. Because the SBC has no direct contact with the MTA, the attribute is set to 0.
Flow_Direction	1—upstream 2—downstream
SF_ID	A Data-over-Cable Service Interface Specifications-specific attribute that is required, and generated by the CMTS in a PacketCable architecture. Because the SBC does not support DOCSIS, this attribute is always 0.
CCC_ID	The local CCC ID for this call. It is included if CC tapping is being done on the call.

Table 58-4 details the Call_Answer message attributes. This message indicates the earliest point at which two-way media is established. The SBC sends the message to the billing servers when the SBC is notified that the called party has answered the call.

Table 58-4 Call_Answer Message Attributes

Attribute Name	Comment
EM_Header	Common header attribute.
Charge_Number	The charge number during collect call, calling-card call, call billed to a third party, and so on. For the SBC, this is the calling number, unless the call has been diverted. The diverted call has a Diverted-By number.
Related_Call_Billing_Correlation_ID	The billing correlation ID (BCID) assigned to the leg from the terminating network element. The SBC does not share the BCID and financial entity ID (FEID) information with other network elements.

Note The FEID attribute is not sent in a Call_Answer message.

Table 58-5 details the QoS_Commit message attributes. This message is sent by the SBC when the gate bandwidth is committed. This message is sent after a QoS_Reserve message that has been sent previously.

Table 58-5 QoS_Commit Message Attributes

Attribute Name	Comments
EM_Header	Common header attribute containing timestamp and BCID.
MTA_UDP_Portnum	The UDP port number on the network element endpoint. Because the SBC has no direct contact with the MTA, so the attribute is set to 0.
Flow_Direction	1—upstream 2—downstream
SF_ID	This is always 0 because the SBC does not support DOCSIS.
Total_Bandwidth (attribute ID 253)	The total bandwidth being used by the streams described in a QoS_Commit message.
CCC_ID	The local CCC ID for a call. The attribute is included if CC tapping is being done on the call.

The following attributes are not included in the QoS_Commit message:

- QoS_Descriptor
- Media_Session_Desc (attribute ID 254)

Table 58-6 details the Call_Disconnect message attributes. This message is generated by the SBC when a two-way media flow is terminated. This message immediately precedes the QoS_Release and Signaling_Stop messages, and is sent only after the Call_Answer message that has been sent previously.

Table 58-6 Call_Disconnect Message Attributes

Attribute Name	Comments
EM_Header	Common header attribute.
Call_Termination_Cause	Reason for termination of call.

Table 58-7 details the QoS_Release message attributes. This message is generated by the SBC when the reserved bandwidth is released.

Table 58-7 QoS_Release Message Attributes

Attribute Name	Comments
EM_Header	Common header attribute containing timestamp and BCID.
Flow_Direction	1—upstream 2—downstream
SF_ID	A DOCSIS-specific attribute, Service Flow ID, generated by the CMTS in a PacketCable architecture. Because the SBC does not support DOCSIS, this attribute is always set to 0.
CCC_ID	The local CCC ID for a call. The attribute is included if CC tapping is being done on the call.

Note The Media_Session_Desc (attribute ID 254) attribute is not sent with the QoS_Release message.

Table 58-8 details the Signaling_Stop message attributes. This message is sent during the following events:

- A terminating signalling request, for example, a SIP BYE, from the party terminating the call is acknowledged by the SBC.
- When the terminating signalling request for the party not terminating the call is sent by the SBC, and acknowledged by that party.

Note The Signaling_Stop message is not sent if the Signaling_Start message for this call is not sent.

Table 58-8 Signaling_Stop Message Attributes

Attribute Name	Comments
EM_Header	The header attribute that must be first in the message.
Related_Call_Billing_Correlation_ID	The BCID of the other leg. For example, if BCID is the caller, the attribute is for the callee.
Call_Termination_Cause	The reason the call was terminated.

Note The FEID attribute of the Signaling_Stop message is not included.

Table 58-9 details the Surveillance_Stop message attributes. This message is sent by SIG to indicate the end of IRI or CC tapping or both. This message means the call has ended.

Table 58-9 Surveillance_Stop Message Attributes

Attribute Name	Comment
EM_Header	Common header attribute containing the timestamp and BCID.
Surveillance_Stop_Type	Always included. 1—End of all surveillance. 2—End of only CC tapping.
Surveillance_Stop_Destination	Always included. 1—Surveillance_Stop applies to local surveillance only. The value 1 is not used by the SBC. 2—Surveillance_Stop is applicable to both local and remote surveillance. 3—Surveillance_Stop is applicable only to remote surveillance.

Note The Electronic_Surveillance_Indication attribute is not included in the Surveillance_Stop message.

Table 58-10 details the Media_Report message attributes. The message is specific to a flow. Therefore, if more than one flow is created at the same time, multiple event messages are sent, one per flow.

A Media_Report message is sent during the following events, when a flow is created, modified, and released:

- A flow is considered Created when the gate bandwidth for the flow is committed. A QoS_Commit message is also sent at the same time.
- A flow is considered Modified when the flow is renegotiated.
- A flow is considered Released when the gate bandwidth for the flow is released. A Qos_Release message is also sent at the same time.

Table 58-10 Media_Report Message Attributes

Attribute Name	Comment
EM_Header	Common header attribute containing the timestamp and BCID.
CCC_ID	The local CCCID for a call. Included if CC tapping is being done on the call.
SDP_Upstream	The upstream SDP for the flow, SDP corresponding to flow in direction of caller, on side indicated by Flow_Direction, is always included.
SDP_Downstream	The downstream SDP for the flow. SDP corresponding to flow in direction of callee, on side indicated by Flow_Direction, is always included.

Table 58-10 Media_Report Message Attributes (continued)

Channel_State	Always included. 1—Open (Flow created) 2—Change (Flow modified) 3—Close (Flow released)
Flow_Direction	Always included. Specifies if the device is acting on behalf of an originating part or terminating part of a call at the time the message is generated. 1—upstream (Caller side) 2—downstream (Callee side)

Table 58-11 details the Redirection message attributes. This message is sent by the SBC when a call has been transferred either due to a 3XX redirect response or a SIP REFER request.

Table 58-11 Redirection Message Attributes

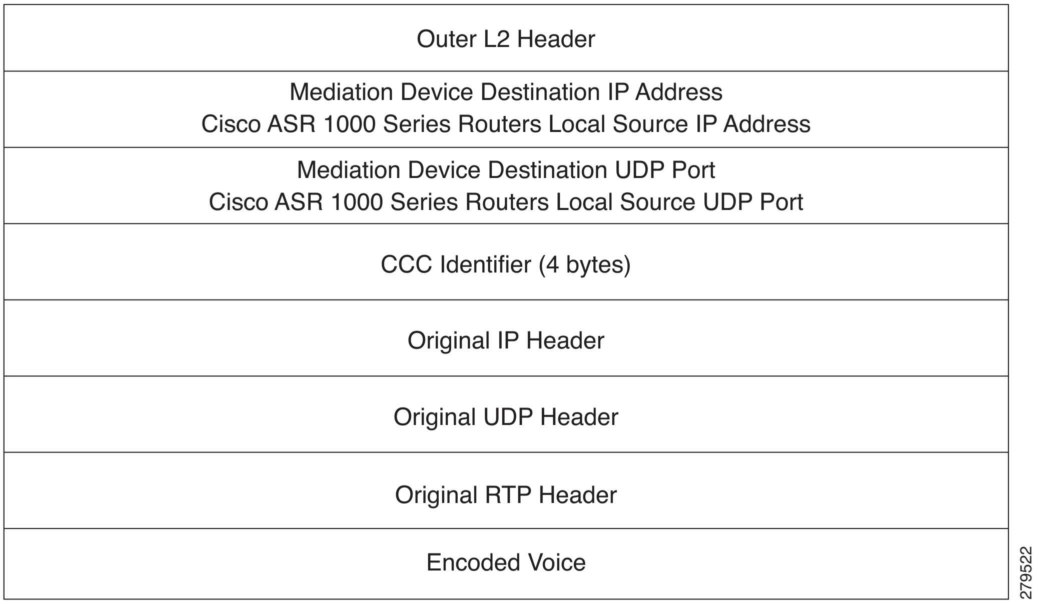
Attribute Name	Comment
EM_Header	Common header attribute containing the timestamp and BCID.
Related_Call_Billing_Correlator	Always included. The BCID used previously for the old branch of a call.
Redirected_From_Party_Number	Always included. The number of the party a call is being transferred from or forwarded from.
Redirected_To_Party_Number	Always included. The number of the party a call is being transferred to or forwarded to.
Carrier_Identification_Code	The Carrier Identification Code associated with a call.

CC Interface

The PacketCable 1.5 standard specifications contain the packet header format for replicated voice content packets.

Figure 58-3 shows a replicated packet. The first three rows of the packet are the outer Layer2, Layer3, and Layer4 information. This information consists of destination IP and UDP port of the Mediation Device, and the source IP and UDP port of the Cisco ASR 1000 series router. The fourth row of the packet is the CCC ID that is used to correlate the signaling and media information. The last four rows of the packet are the original media packet that is being TAPed. It starts from Layer 3 IP, and is followed by UDP, RTP, and media payload.

Figure 58-3 Packet Format



Outer L2 Header

Mediation Device Destination IP Address
Cisco ASR 1000 Series Routers Local Source IP Address

Mediation Device Destination UDP Port
Cisco ASR 1000 Series Routers Local Source UDP Port

CCC Identifier (4 bytes)

Original IP Header

Original UDP Header

Original RTP Header

Encoded Voice

Restrictions for Implementing CALEA IRI Interface Support

The following restrictions and limitations are applicable to CALEA IRI Interface Support feature implementing:

- Only one mediation device IP address is supported.
- The IPv6 address pertaining to the mediation device is not supported. Only IPv4 address in the global routing space is supported for mediation device. The IPv4 address should not be associated to any virtual routing and forwarding (VRF).
- The mediation device’s IP address must be accessible from the Cisco ASR 1000 series router global routing space. CISCO-TAP2-MIB does not allow mediation device IP address to be in a VRF.
- The Cisco ASR 1000 series router does not support the CLIs of the Cisco BTS 10200 Softswitch and the Cisco PGW 2200 Softswitch for warrant configuration.
- The PacketCable 2.0 standard specification for Electronic Surveillance is not supported.
- LI using the SIP P-DCS-LAES header is not supported.
- Tap is not applied to the existing calls.
- The IPv6 Media Addresses cannot be intercepted in a VRF, but can be intercepted in a global routing space. However, IPv4 Media Addresses can be intercepted both in the global routing space and the VRF.

Implementing CALEA IRI Interface Support

The following sections explain how to configure the CALEA IRI Interface Support feature:

- Configuring the SBC for CALEA IRI Interface Support, page 58-16
- Configuring VoIP LI SNMP, page 58-13
- Configuring the SBC for CALEA IRI Interface Support, page 58-16

Configuring LI

To see the SNMPv3 and SNMP View configuration information pertaining to the LI TAP definitions, see the How to Configure Lawful Intercept section in the *Cisco IOS and NX-OS Software Lawful Intercept Architecture* feature guide at:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_lawful_intercept.html#wp1077988

Use the following commands provided in the *Cisco IOS and NX-OS Software Lawful Intercept Architecture* feature guide to configure LI:

- **snmp-server view view-name MIB-name included**—Defines an SNMPv2 MIB view, and includes a MIB family in the view.
- **snmp-server group group-name v3 auth read view-name write view-name**—Defines a read and write view for a group using the User Security Model (SNMPv3) and the authNoPriv Security Level.
- **snmp-server user user-name group-name v3 auth md5 auth-password**—Defines an authentication password for a user by using the HMAC MD5 algorithm for authentication and V3 security model.

The following example shows how to enable the mediation device to access the lawful intercept MIBs. It creates an SNMP view (tapV) that includes three LI MIBs (CISCO-VoIp-Tap-MIB, CISCO-TAP2-MIB, and CISCO-IP-TAP-MIB). It also creates a user group that has read, write, and notify access to MIBs in the tapV view.

```
snmp-server view tapV ciscoVoIpTapMIB included
snmp-server view tapV ciscoIpTapMIB included
snmp-server view tapV ciscoTap2MIB included
snmp-server group tapGrp v3 auth read tapV write tapV notify tapV
snmp-server user li tapGrp v3 auth md5 cisco
snmp-server community public
```

Configuring VoIP LI SNMP

SNMP provisioning is done using the SNMP research tools available for Sun workstations. However, you can use any tool that uses the SNMPv3 protocol.

The **setany** commands listed here are executed using the SNMP application. Note that these commands are not Cisco IOS CLI commands. It is assumed that SNMP has been configured on your routing device. A secure K9 image is required for the MIBs to work.

There are four parts to the following example:

- Adding the Mediation Device Information
- Adding the VoIP User Warrant
- Retrieving the Mediation Device and VoIP User Warrant Information
- Removing the VoIP User Warrant and Mediation Device Information

Adding the Mediation Device Information

Perform the following steps to add the mediation device information:

Step 1 Configure the mediation device IP, RADIUS receiving port, transport type, and shared RADIUS Key to receive Voice signaling information from the SBC through the PacketCable1.5 Event Messages.

The following example shows how to create the TAP2 MD Row for IRI, with an IP address of 101.10.7.61, UDP port of 1813, and RADIUS key of "cisco":

```
setany -v3 172.18.37.151 li cTap2MediationStatus.1 -i 5
setany -v3 172.18.37.151 li cTap2MediationTimeout.1 -o "07 da 05 08 0e 3b 37 06"
setany -v3 172.18.37.151 li cTap2MediationDestAddressType.1 -i 1
setany -v3 172.18.37.151 li cTap2MediationTransport.1 -i 6
setany -v3 172.18.37.151 li cTap2MediationRadiusKey.1 -o "63 69 73 63 6f"
setany -v3 172.18.37.151 li cTap2MediationSrcInterface.1 -i 0
setany -v3 172.18.37.151 li cTap2MediationDscp.1 -i 0
setany -v3 172.18.37.151 li cTap2MediationDestAddress.1 -o "65 0a 07 3d"
setany -v3 172.18.37.151 li cTap2MediationDestPort.1 -g 1813
setany -v3 172.18.37.151 li cTap2MediationStatus.1 -i 1
```

Step 2 Configure the mediation device IP, Call Content (CC) receiving port, and transport type to receive Voice CC from the SBC.

The following example shows how to create the TAP2 Mediation Device Row for a CC, with an IP address of 101.10.7.61, and UDP port of 45000:

```
setany -v3 172.18.37.151 li cTap2MediationStatus.2 -i 5
setany -v3 172.18.37.151 li cTap2MediationDestAddressType.2 -i 1
setany -v3 172.18.37.151 li cTap2MediationTimeout.2 -o "07 da 05 08 0e 3b 37 06"
setany -v3 172.18.37.151 li cTap2MediationTransport.2 -i 1
setany -v3 172.18.37.151 li cTap2MediationSrcInterface.2 -i 0
setany -v3 172.18.37.151 li cTap2MediationDscp.2 -i 0
setany -v3 172.18.37.151 li cTap2MediationDestAddress.2 -o "65 0a 07 3d"
setany -v3 172.18.37.151 li cTap2MediationDestPort.2 -g 45000
setany -v3 172.18.37.151 li cTap2MediationStatus.2 -i 1
```

Adding the VoIP User Warrant

Perform the following steps to add the VoIP user warrant:

Step 1 Configure the VoIP user warrant.

The following example shows how to create the VoIP TAP SNMP Row with a matching username for "712020" and type "Intercept":

```
setany -v3 172.18.37.151 li cvoiptapStreamRowStatus.1.1 -i 5
setany -v3 172.18.37.151 li cvoiptapStreamId.1.1 -o "72 72 2d 31"
setany -v3 172.18.37.151 li cvoiptapStreamType.1.1 -i 4
setany -v3 172.18.37.151 li cvoiptapStreamMatch.1.1 -o "37 31 32 30 32 30"
setany -v3 172.18.37.151 li cvoiptapStreamMatchType.1.1 -i 1
setany -v3 172.18.37.151 li cvoiptapStreamCCMediationDevice.1.1 -i 2
setany -v3 172.18.37.151 li cvoiptapStreamRowStatus.1.1 -i 1
```

Step 2 The following example shows how to configure an associated generic stream for VoIP, and enable generic stream:

```
setany -v3 172.18.37.151 li cTap2StreamStatus.1.1 -i 5
setany -v3 172.18.37.151 li cTap2StreamType.1.1 -i 6
setany -v3 172.18.37.151 li cTap2StreamInterceptEnable.1.1 -i 1
setany -v3 172.18.37.151 li cTap2StreamStatus.1.1 -i 1
```

Retrieving the Mediation Device and VoIP User Warrant Information

Perform the following steps to retrieve the mediation device and VoIP user warrant information:

Step 1 The following example shows how to retrieve the MD TAP2 SNMP row:

```
getmany -v3 172.18.37.151 li ciscoTap2MIB

SNMP GETMANY for the configured values

cTap2MediationCapabilities.0 = ipV4SrcInterface(0), udp(2), radius(7)
cTap2MediationDestAddressType.1 = ipv4(1)
cTap2MediationDestAddressType.2 = ipv4(1)
cTap2MediationDestAddress.1 = 65 0a  07 3d
cTap2MediationDestAddress.2 = 65 0a  07 3d
cTap2MediationDestPort.1 = 1813
cTap2MediationDestPort.2 = 45000
cTap2MediationSrcInterface.1 = 0
cTap2MediationSrcInterface.2 = 0
cTap2MediationRtcpPort.1 = 0
cTap2MediationRtcpPort.2 = 0
cTap2MediationDscp.1 = 0
cTap2MediationDscp.2 = 0
cTap2MediationDataType.1 = 0
cTap2MediationDataType.2 = 0
cTap2MediationRetransmitType.1 = 0
cTap2MediationRetransmitType.2 = 0
cTap2MediationTimeout.1 = 07 da  05 08   0e 3b  37 06
cTap2MediationTimeout.2 = 07 da  05 08   0e 3b  37 06
cTap2MediationTransport.1 = radius(6)
cTap2MediationTransport.2 = udp(1)
cTap2MediationNotificationEnable.1 = true(1)
cTap2MediationNotificationEnable.2 = true(1)
cTap2MediationStatus.1 = active(1)
cTap2MediationStatus.2 = active(1)
cTap2MediationRadiusKey.1 = cisco
cTap2MediationRadiusKey.2 =

cTap2StreamType.1.1 = voip(6)
cTap2StreamInterceptEnable.1.1 = true(1)
cTap2StreamInterceptedPackets.1.1 = 0
cTap2StreamInterceptDrops.1.1 = 0
cTap2StreamStatus.1.1 = active(1)
cTap2StreamInterceptedHCPackets.1.1 = 0x000000000
cTap2StreamInterceptHCDrops.1.1 = 0x000000000
```

Step 2 The following example shows how to retrieve the VoIP TAP SNMP row:

```
getmany -v3 172.18.37.151 li ciscoVoIpTapMIB
```

```
cvoiptapStreamCapabilities.0 = tapEnable(0), usernameOrNumber(1), uri(2)
cvoiptapStreamId.1.1 = rr-1
cvoiptapStreamType.1.1 = intercept(4)
cvoiptapStreamMatch.1.1 = 712020
cvoiptapStreamMatchType.1.1 = usernameOrNumber(1)
cvoiptapStreamCCMediationDevice.1.1 = 2
cvoiptapStreamRowStatus.1.1 = active(1)
```

Removing the VoIP User Warrant and Mediation Device Information

Perform the following steps to remove the VoIP user warrant and mediation device information:

Step 1 Disable and delete the generic stream, and delete the VoIP User TAP row:

```
setany -v3 172.18.37.151 li cTap2StreamInterceptEnable.1.1 -i 2
setany -v3 172.18.37.151 li cvoiptapStreamRowStatus.1.1 -i 6
setany -v3 172.18.37.151 li cvoiptapStreamRowStatus.1.1 -i 6
```

Step 2 Remove the mediation device RADIUS receiving port:

```
setany -v3 172.18.37.151 li cTap2MediationStatus.1 -i 6
```

Step 3 Remove the MD CC receiving Port:

```
setany -v3 172.18.37.151 li cTap2MediationStatus.2 -i 6
```

Configuring the SBC for CALEA IRI Interface Support

This section details the steps involved in overriding the default match-order.

SUMMARY STEPS

1. **configure terminal**
2. **sbc** *sbc-name*
3. **sbe**
4. **adjacency sip | h323** *adjacency-name*
5. **warrant match-order** [**source** | **destination** | **diverted-by**]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`configure terminal`
	Example:
	`Router# configure terminal`
		Enables global configuration mode.

Step 2	`sbc` *sbc-name* **Example:** `Router(config)# sbc mysbc`	Enters the mode of an SBC service. • Use the *sbc-name* argument to define the name of the service.

	Command or Action	Purpose
Step 3	**sbe** **Example:** `Router(config-sbc)# sbe`	Enters the mode of a signaling border element (SBE) entity within an SBC service.
Step 4	**adjacency sip**|**h323** *adjacency-name* **Example:** `Router(config-sbc-sbe)# adjacency sip sipadj`	Enters the mode of an SBE SIP or H.323 adjacency. • Use the *adjacency-name* argument to define the name of the SIP or H.323 adjacency.
Step 5	**warrant match-order [source | destination | diverted-by]** **Example:** `Router(config-sbc-sbe-adj-sip)# warrant match-order source destination diverted-by`	Configures the lawful inforcement warrant information in an SIP or H.323 adjacency, and specifies the order of fields used to match the warrant. By default, the incoming Access adjacency matches the source information, and the Core adjacency matches the destination information. **Note** The H.323 adjacency does not support the **diverted-by** keyword.
Step 6	**exit** **Example:** `Router(config-sbc-sbe-adj-sip)# exit`	Exits the adjacency mode to the SBE mode.

The following example shows how to configure the SBC to override the default match-order:

```
configure terminal
 sbc mySBC
  sbe
   adjacency sip adj1
    warrant match-order source destination diverted-by
```