PacketCable Lawful Intercept Architecture for BTS Versions 3.5 and 4.1

Version History

Version Number	Date	Notes
1	4/10/2003	This document was created.
2	3/15/2006	This document was updated and includes version I03 of the PacketCable Event Message Specification, and BTS versions 3.5 and 4.1.

Abstract

Lawful Intercept (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 have been adopted that require service providers (SPs) and Internet service providers (ISPs) to design and implement their networks to explicitly support authorized electronic surveillance. Types of SPs and ISPs subject to LI mandates vary greatly from country to country. LI compliance in the United States is specified by the Communications Assistance for Law Enforcement Act (CALEA).

The *PacketCable Lawful Intercept Architecture for BTS Versions 3.5 and 4.1* document describes the implementation of LI architecture on a PacketCable network. It describes LI of voice traffic only—LI of data traffic is not covered. PacketCable specifications are considered a SafeHarbor for compliance with CALEA. SafeHarbor is an initiative that provides the PacketCable LI user with a stable Cisco IOS/CatOS version-of-choice. This initiative is accomplished through systems level testing of functionality that is critical to the success of the PacketCable LI architecture in Cisco products.

The LI architecture is designed to support “plug-and-play” capability, which means that any architecture component can be replaced by any other PacketCable-compliant component. Because of this flexibility in component choices, it is not practical 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 PacketCable LI architecture including how LI works, the roles of the various components, what component options are available, and some information on design, implementation, operation, and troubleshooting LI on a PacketCable network. For detailed specifics on the various devices (such as image and memory requirements, configurations, and so forth), this document references the product documentation of the devices.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

This document contains the following sections:

- Business Objectives of the PacketCable LI Architecture, page 2
- PacketCable Lawful Intercept Architecture, page 3
- Implementation of the PacketCable LI Architecture, page 12
- Device Configuration Files, page 13
- Verifying the PacketCable LI Network, page 22
- Troubleshooting a PacketCable LI Network, page 28
- Appendix, page 30
- Glossary, page 32

Business Objectives of the PacketCable LI Architecture

The following sections describe the business objectives of implementing the PacketCable 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. Providing a wiretap at the media termination adapter (MTA) or diverting the call to a conference unit (where the replication would take place) is not acceptable as 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 a cable modem termination system [CMTS] or trunking gateway) and must be performed along the normal path of the data (the CMTS).
- 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 being asked to meet LI requirements for voice and data in a variety of countries worldwide. CALEA is a public law that describes how telephony service providers in the United States must support LI. 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 31.)

In Europe, a number of specifications have been defined but legal requirements and specific interfaces vary from country to country. This document does not address LI for non-American customers.

PacketCable Lawful Intercept Architecture

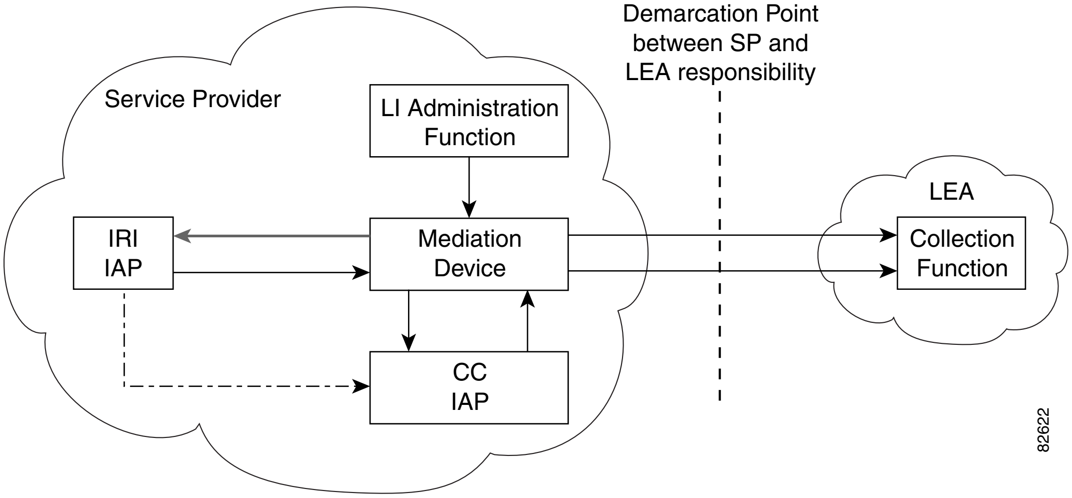
The following sections describe the Broadband Telephony Softswitch (BTS) versions 3.5 and 4.1 PacketCable LI architecture:

- Topology of Networks That Support LI, page 3
- Interfaces Between Devices, page 6
- How PacketCable LI Architecture Works, page 8

Topology of Networks That Support LI

Figure 1 shows a generic IP network that supports LI of voice and data traffic.

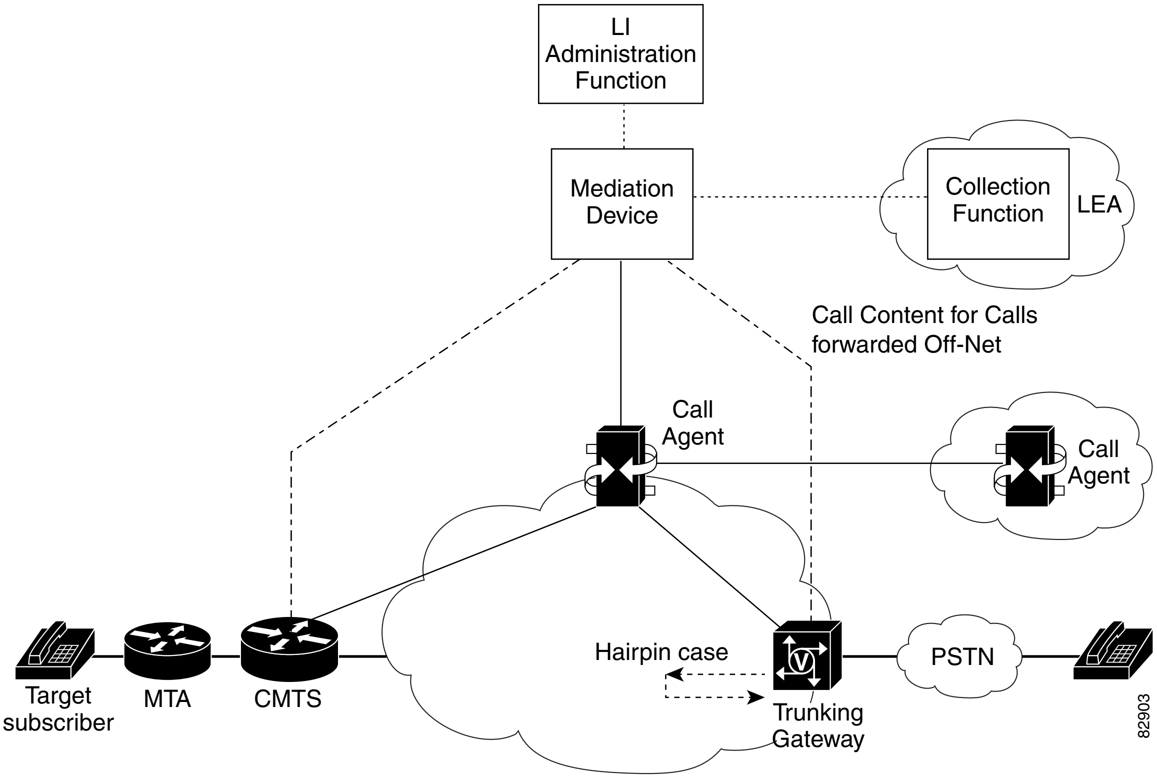
Figure 1 Generic IP Network That Supports LI of Voice and Data Traffic



Note IAP is defined as intercept access point.

Figure 2 shows a PacketCable network that supports LI of voice traffic.

Figure 2 Functional Depiction of a PacketCable LI Network



The following components are integral to the PacketCable voice intercept network:

- LI Administration Function, page 4
- Mediation Device, page 5
- Intercept-Related Information Intercept Access Point, page 5
- Call Content Intercept Access Point, page 5
- Collection Function, page 5

LI Administration Function

The SP 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

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 Intercept-Related Information [IRI] and call content [CC]), encapsulates it, and delivers it to the LEAs. 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. Depending on the architecture, the IRI IAP could be either the call agent, the CMTS, Session Initiation Protocol (SIP) proxy, or the gatekeeper. In the Media Gateway Control Protocol (MGCP)-based PacketCable network, both the call agent and the CMTS supply IRI IAP. The call agent supplies call control-related information (such as the dialed number and the call encoding) and the CMTS usually supplies QoS-related information.

Call Content Intercept Access Point

The Call Content Intercept Access Point (CC IAP) is the device that intercepts call 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.

However, the CC IAP should not be part of the MTA to prevent the intercept target from being able to detect the intercept. In the PacketCable network, the CMTS is the preferred CC IAP. If a call coming in from the public switched telephone network (PSTN) is forwarded back to the PSTN, the trunking gateway must serve as the CC IAP.

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 3 shows the interfaces of interest between the devices in a PacketCable voice intercept topology:

Figure 3 PacketCable Voice Intercept Device Interfaces

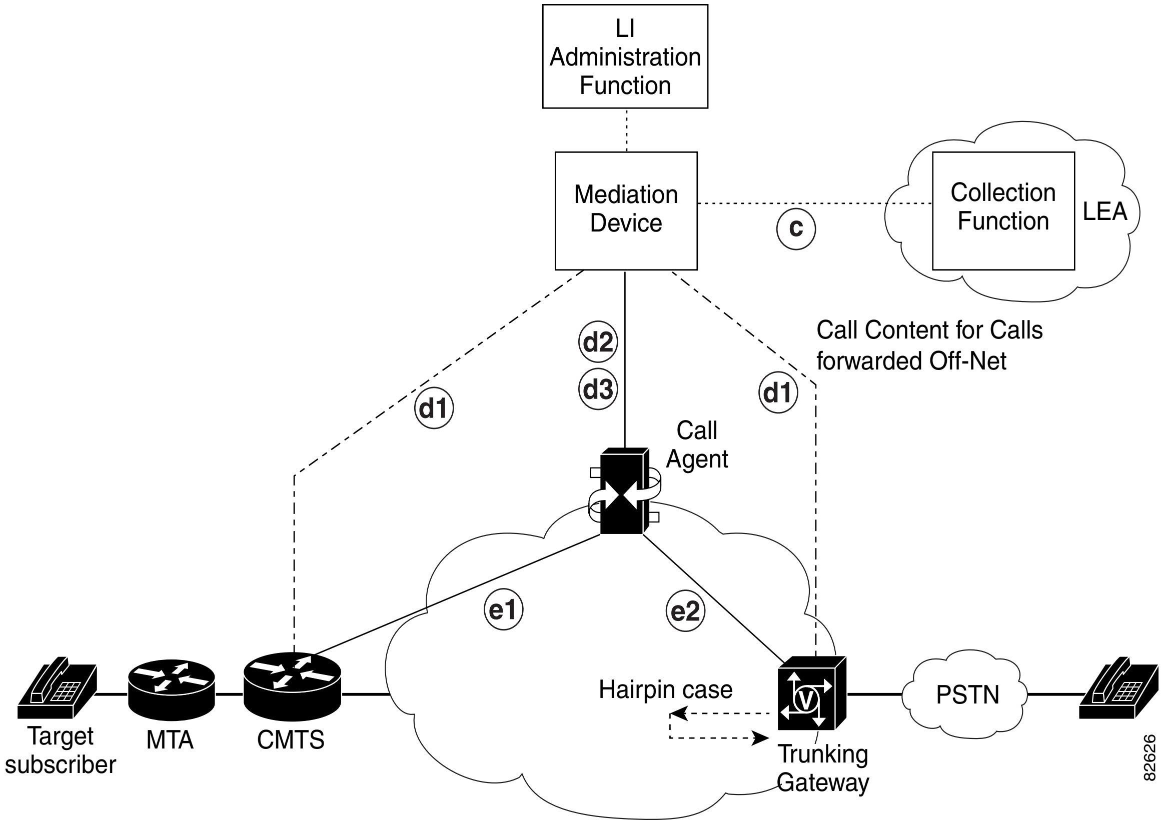


Table 1 describes the interfaces between devices shown in Figure 3.

Table 1 PacketCable LI Network Device Interfaces

Interface	Devices	Description
c	Mediation Device and Collection Function	The mediation device delivers intercept information to the collection function. If more than one LEA is intercepting the same target, the mediation device must duplicate the intercept information to send to the collection function of each LEA. This interface meets the specifications defined in the *PacketCable Electronic Surveillance Specification* document in the "Related Documents" section on page 31.
d1	CMTS or trunking gateway and Mediation Device	This is the CC interface. The CC IAP (the CMTS for a PacketCable network) duplicates CC and sends it to the mediation device. The CMTS encapsulates the packets with additional User Datagram Protocol (UDP) and IP headers and a 32-bit call content connection identifier (CCCID) header. The CCCID is used to associate the CC with the target. The CCCID is not globally unique; however, the combination of the CCCID and the IP address of the CMTS must be unique in order for the mediation device to accurately process intercepts. In a typical CC intercept scenario, the CMTS is the CC IAP. In this case, the CMTS generates the CCCID. If a call comes in from the PSTN and is forwarded back to the PSTN, the trunking gateway must serve as the CC IAP. In this case, the call agent generates the CCCID. 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 CMTS also provides QoS IRI information to the mediation device. For the format of the call content interface, see section 4 of the *PacketCable Electronic Surveillance Specification* document in the "Related Documents" section on page 31.
d2	Call agent and Mediation Device (provisioning interface)	This is the provisioning interface. The mediation device uses Secure Shell (SSH) to provision intercepts on the call agent.
d3	Call agent and Mediation Device (delivery interface)	This is the delivery interface. The call agent uses this interface to deliver IRI to the mediation device. This interface is described in Appendix A of the *PacketCable Event Messages Specification* document in the "Related Documents" section on page 31.
e1	Call agent and CMTS	The call agent instructs the CMTS to duplicate the CC and send it to the appropriate mediation device using the Common Open Policy Service (COPS) protocol. This interface is described in the *PacketCable Dynamic Quality of Service Specification* document in the "Related Documents" section on page 31.
e2	Call agent and trunking gateway	The call agent uses MGCP to instruct the trunking gateway to duplicate CC and send it to the appropriate mediation device. The parameters (local connection options) required to do this are described in the *PacketCable PSTN Gateway Call Signaling Protocol Specification* document in the "Related Documents" section on page 31.

How PacketCable LI Architecture Works

The following sections describe how the PacketCable LI architecture works:

- Types of Intercepts, page 8
- Initiating an Intercept, page 8
- Terminating an Intercept, page 8
- PacketCable Voice Intercept Call Flows, page 8
- Intercept Request Messaging Interfaces, page 11
- Packet Encapsulation and Transport, page 12
- Security Considerations, page 12
- Failure Recovery, page 12

Types of Intercepts

PacketCable architecture supports only voice intercept. There are two types of voice-related intercepts:

- Intercept-Related Information only—This is the most common type of intercept. It intercepts only the IRI, which 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. 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 Call Content—Typically, a small percentage of intercepts require the capture of both IRI and CC. Intercepting CC has a significant impact on network bandwidth and device processing power. This type of intercept is also referred to as a Full Content or Title 3 intercept.

Initiating an Intercept

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

Terminating an Intercept

When a warrant is issued, it includes an expiration date—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.

PacketCable Voice Intercept Call Flows

The following sections describe the two basic types of PacketCable voice intercept:

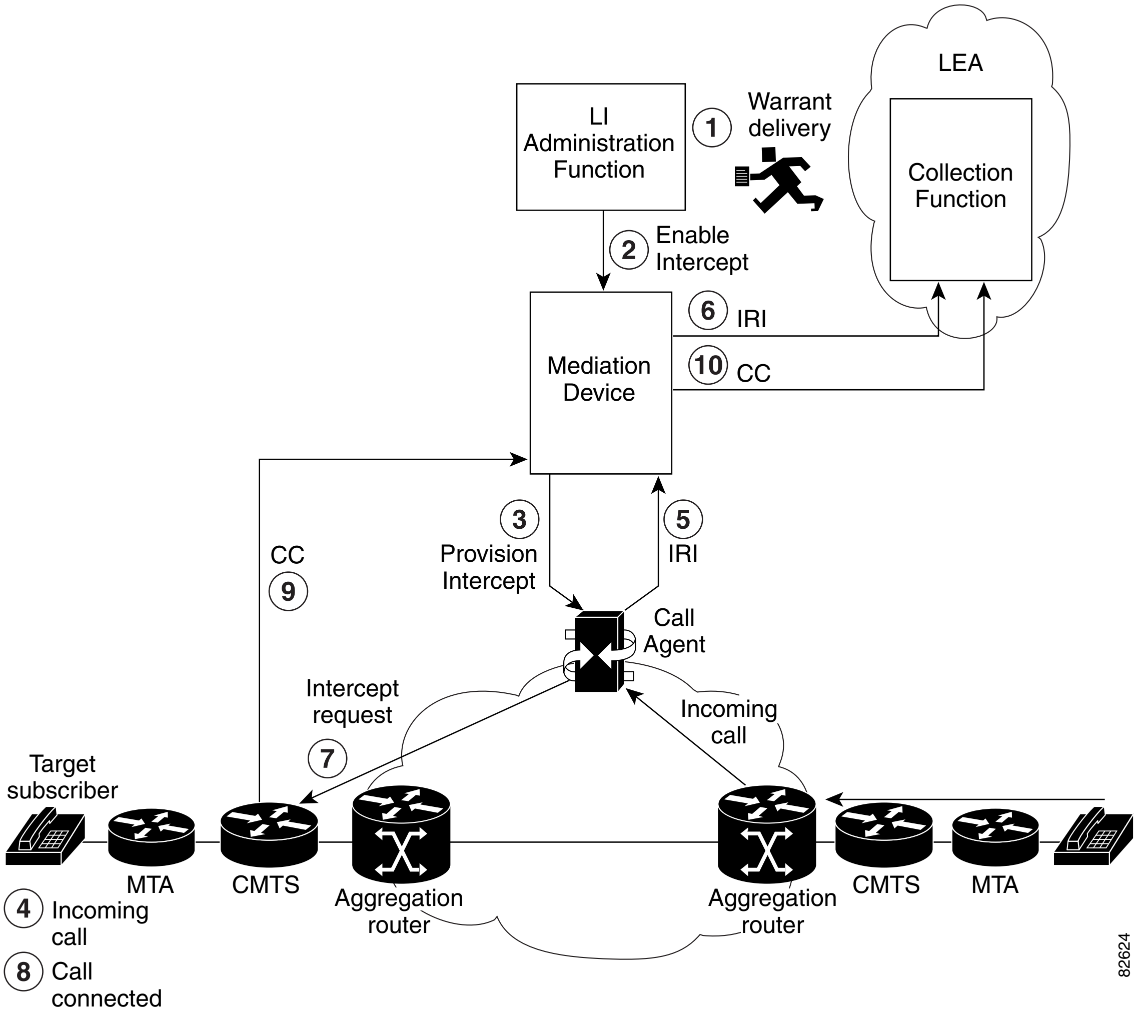
- Standard PacketCable Voice Intercept, page 9
- Hairpin PacketCable Voice Intercept, page 10

Standard PacketCable Voice Intercept

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

Figure 4 shows the topology for a standard PacketCable voice intercept:

Figure 4 Standard PacketCable Voice Intercept at CMTS or Aggregation Router



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 enables the intercept.

Step 3 The mediation device sends a configuration command to the call agent to provision the intercept.

Step 4 The target subscriber receives an incoming call.

Step 5 The call agent sends IRI to the mediation device.

Step 6 The mediation device initiates delivery of IRI to the LEA.

Step 7 If the intercept is provisioned to include call content, the call agent sends an intercept request to the CMTS using dynamic quality of service (DQoS) to enable content intercept.

Step 8 The call agent causes the target subscriber's phone to ring.

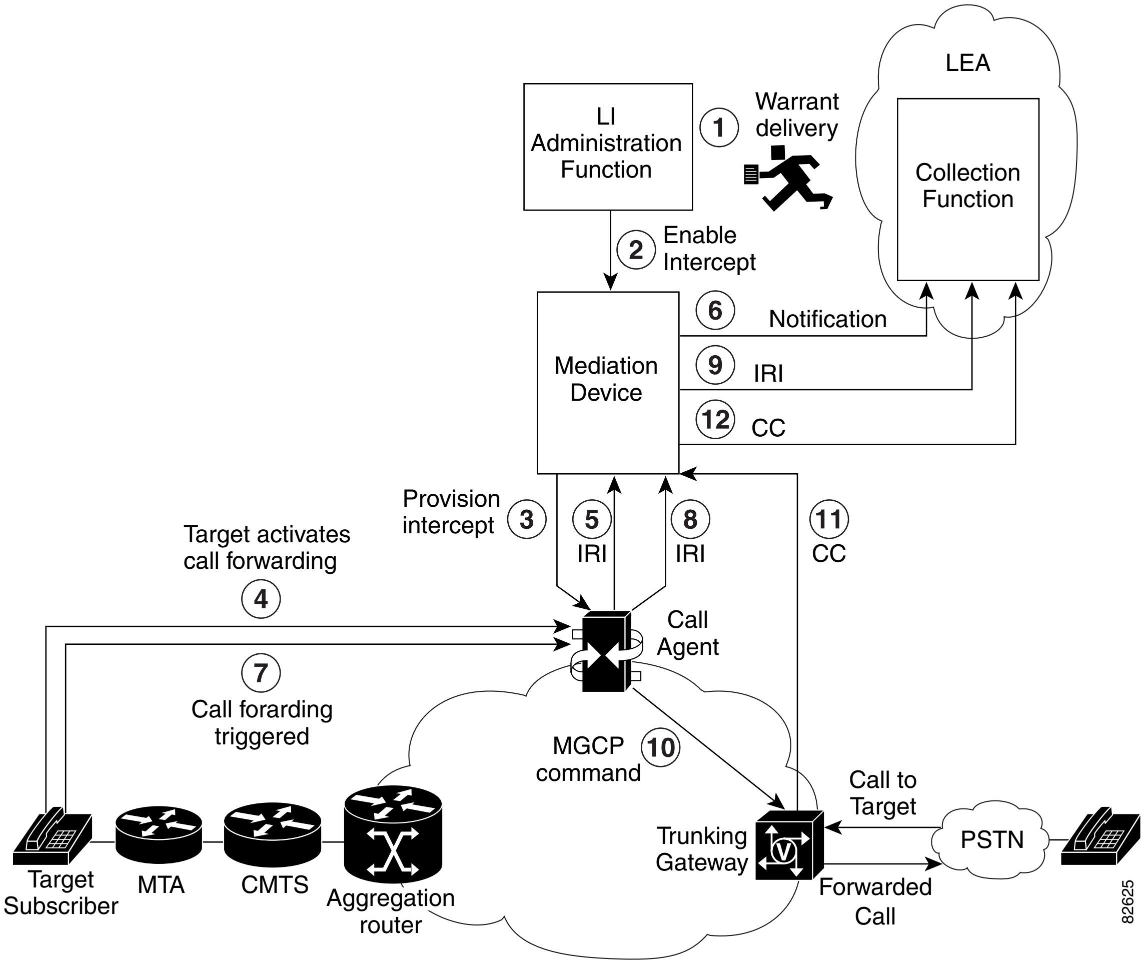
Step 9 Once the call is connected, the CMTS router intercepts and replicates all voice information from the intercept target subscriber and sends CC to the mediation device using PacketCable UDP-based encapsulation.

Step 10 The mediation device delivers CC to the collection function using PacketCable UDP-based encapsulation.

Hairpin PacketCable Voice Intercept

Figure 5 shows the topology for a PacketCable 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 PacketCable Voice Intercept at Trunking Gateway



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 enables the intercept.

Step 3 The mediation device sends a configuration command to the call agent to provision the intercept.

Step 4 The target subscriber activates call forwarding to an off-network (off-net) number.

Step 5 The call agent sends IRI to the mediation device that the target subscriber has activated call forwarding.

Step 6 The mediation device notifies the LEA that call forwarding is activated.

Step 7 The target subscriber receives a call from the PSTN that triggers call forwarding.

Step 8 The call agent sends IRI to the mediation device indicating that the call is being forwarded.

Step 9 The mediation device forwards the IRI to the LEA.

Step 10 The call agent recognizes that the incoming call is to be forwarded to the PSTN and sends the appropriate MGCP 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.

Step 11 Once the call is connected, the trunking gateway intercepts and replicates all voice information from the intercept target subscriber and sends CC to the mediation device using PacketCable UDP-based encapsulation.

Step 12 The mediation device delivers CC to the collection function using PacketCable UDP-based encapsulation.

Intercept Request Messaging Interfaces

There are three IAPs in the PacketCable network:

- Call agent—the IRI IAP.
- CMTS—the CC IAP for calls originating or terminating on-network (on-net). The call agent uses COPS to initiate an intercept on the CMTS. The CMTS delivers the CC to the mediation device in PacketCable UDP format.
- Trunking gateway—the CC IAP in the case where an off-network (off-net) call terminates to an intercept subject whose phone is configured to forward calls off-net. The call agent initiates an intercept request using MGCP. The trunking gateway delivers CC to the mediation device in PacketCable UDP format.

When DQoS is used, the CMTS also acts as an IRI IAP for providing QoS_Reserve, QoS_Commit, and QoS_Release event messages. The following sections describe the interfaces between the call agent and the CC IAPs:

- CMTS and Call Agent Interface, page 12
- Trunking Gateway and Call Agent Interface, page 12

For information on the interface between the call agent and mediation device, see the *PacketCable Event Messages Specification* document in the "Related Documents" section on page 31. For information on the interface between the mediation device and the collection function, see the *PacketCable Electronic Surveillance Specification* document in the "Related Documents" section on page 31.

CMTS and Call Agent Interface

The COPS interface for requesting CC intercept is based on the *PacketCable Dynamic Quality of Service Specification* document found in the "Related Documents" section on page 31. DQoS is used to authorize QoS for media flows within the PacketCable architecture. In order to provision a CC intercept, some additional COPS objects have been added to indicate that the media stream should be replicated and where to send the replicated stream (by specifying the IP address and port of the mediation device).

Note When DQoS is used, the CMTS also acts as an IAP for call identification information and provides QoS_Reserve, QoS_Commit, and QoS_Release event messages to the mediation device.

Trunking Gateway and Call Agent Interface

When a call coming from the PSTN is forwarded to the PSTN, the trunking gateway must be the CC IAP. The trunking gateway interfaces with the call agent using MGCP and some additional parameters in the MGCP message are used to request a CC intercept. These parameters are the "es-cci" and "es-ccd" parameters described in section 5.2.2.3 of the *PacketCable PSTN Gateway Call Signaling Protocol Specification* document in the "Related Documents" section on page 31. The parameters are used to specify the CCCID to be used and the destination of the replication stream (the IP address and port of the mediation device). The interface described here is identical to that described in the PacketCable TGCP specification and is compliant with the *PacketCable Electronic Surveillance Specification* document found in the "Related Documents" section on page 31.

Packet Encapsulation and Transport

Information on encapsulation and transport of intercepted packets is documented in section 4 of the *PacketCable Electronic Surveillance Specification* described in the "Related Documents" section on page 31.

Security Considerations

Information on security considerations for the PacketCable LI network is documented in the *PacketCable Security Specification* described in the "Related Documents" section on page 31. Call agents and mediation devices run standard operating systems, which include their own security best practices. The BTS uses an SSH interface and has dedicated usernames and passwords for accessing LI information.

Failure Recovery

The mediation device monitors the call agent. If the call agent fails or anything else happens to interrupt an intercept, the mediation device implements an audit to ensure that its database is in synchronization with the call agent database. If a CMTS reboots, all LI content on the CMTS will be lost.

Implementation of the PacketCable LI Architecture

The following section describes the implementation of the PacketCable LI architecture:

- Prerequisites and Design Considerations, page 13

Prerequisites and Design Considerations

Before configuring your network for LI, you must establish reliable end-to-end Voice over IP (VoIP) service 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 13
- IP Address Provisioning Considerations, page 13

Bandwidth and Processing Power Considerations

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

- CMTS—must be able to intercept and replicate all intercepted calls on its section of the network.
- Trunking gateway—must be able to intercept and replicate all intercepted calls that are forwarded off-network.
- 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:

- CMTS to mediation device interface
- Trunking gateway to mediation device interface
- Mediation device to collection functions interface

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 Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP) such as Cisco Network Registrar.

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 31 for the specific requirements.

IP Address Provisioning Considerations

In general, Cisco recommends that service providers not use static IP addresses, particularly for cable modems. Static provisioning of IP addresses is time consuming, expensive, and error prone. Currently, LI is not compatible with variable length subnets. 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:

- Cisco uBR 7246 VXR CMTS Configuration, page 14
- VISM Trunking Gateway Configuration, page 14
- Cisco BTS 10200 Softswitch Call Agent Configuration, page 14

- Verint STAR-GATE Mediation Device Configuration, page 15
- SS8 Networks Xcipio Mediation Device Configuration, page 15

Cisco uBR 7246 VXR CMTS Configuration

The following command must be configured on the Cisco Universal Broadband Router (uBR) 7246 VXR CMTS.

```
ubr7246vxr-1(config)# packetcable enable
```

VISM Trunking Gateway Configuration

When using the Cisco BTS 10200 call agent, call messages come from the call agent and not the mediation device; therefore, the Voice Interworking Service Module (VISM) cards do not need to be configured to interface with the mediation device. The following command enables LI on the VISM card:

```
VISM-1> cnfcalea 2
```

This command must be enabled on every VISM card on every MGX router.

Cisco BTS 10200 Softswitch Call Agent Configuration

The following three configurations must be provisioned on the Cisco BTS 10200 softswitch call agent:

- Add an Electronic Surveillance Subsystem, page 14
- Add an Aggregation Router, page 14
- Add a Media Gateway, page 14

Add an Electronic Surveillance Subsystem

To add an Electronic Surveillance Subsystem (ESS), you must log in as user “calea.”

```
BTS(config)# add ess CDC-DF-ADDRESS=10.8.100.18
  Reply : Success: CLI add successful
  Transaction 1035567544247 was processed.
```

Add an Aggregation Router

To add an aggregation router, you must log in as a user other than “calea.”

```
BTS(config)# add aggr id=I1705_bundle;TSAP-ADDR=10.8.0.1;es-supp=Y;dqos-supp=y
```

Add a Media Gateway

To add a media gateway, you must log in as a user other than “calea.”

```
BTS(config)# add mgw
id=mot050308;tsap-addr=mot050308.cactusv.cisco.com;call-agent-id=CA146;mgw-profile-id=mot;
rgw=Y;tgw=N;nas=N;iad=N;pbx=N;ans=N;ive=N;mgw-monitoring-enabled=Y;aggr-id=I1705_bundle
```

Verint STAR-GATE Mediation Device Configuration

The initial configuration on the Verint STAR-GATE must be performed using the Windows registry edit function. Verint technicians typically perform these configurations as part of the installation process. Usually, users only configure intercept information on the STAR-GATE system, which is configured by using a GUI. For information on configuring the Verint STAR-GATE, see the *Verint STAR-GATE System Description Manual* and the *Verint STAR-GATE System Administration Manual* documents in the "Related Documents" section on page 31.

SS8 Networks Xcipio Mediation Device Configuration

The SS8 Networks Xcipio 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 call content intercepts. Each additional workstation can handle up to 20 simultaneous call content intercepts.

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

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

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

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:;
```

The following is a sample configuration for the SS8 Xcipio mediation device in a network that uses BTS 10200 call agents. For more information on configuring the SS8 Xcipio mediation device, see the *SS8 Xcipio SSDF User Manual* document in the "Related Documents" section on page 31.

The following configurations are performed on the SS8 Xcipio mediation device:

- Collection Function Configuration, page 16
- Collection Function TCP Interface Configuration, page 16
- IP Delivery Unit Configuration, page 16
- IP Port Pools Configuration, page 17
- Surveillance Record Configuration, page 17
- AFTDN Configuration, page 18
- IP Call Content Channel Configuration, page 18

- Access Function Configuration, page 19
- Access Function BTS Provisioning Interface Configuration, page 20
- Access Function PGW Provisioning Interface Configuration, page 21
- Access Function RADIUS Interface Configuration, page 21
- SNMP Alarms and Traps Configuration, page 22

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 2 add-cf Command Strings

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

Collection Function TCP Interface Configuration

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

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

Table 3 describes the strings in the **add-tcpipcfi** command.

Table 3 add-tcpipcfi Command Strings

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

IP Delivery Unit Configuration

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

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

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

Table 4 add-ipdu Command Strings

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

IP Port Pools Configuration

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

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

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

Table 5 add-ipport Command Strings

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

Surveillance Record Configuration

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

```
MML_calea_opr> add-surveillance:state=NC,county=Wake,city=RTP,warrantid=6789,caseid=1234,
subsid=6213000001,startdate=05/01/2002,expdate=06/01/2002, cfid=1,survtype=CONTENT,
content=COMBINED,user=calea_opr,access=PUBLIC;
```

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

Table 6 add-surveillance Command Strings

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

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

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

AFTDN Configuration

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

```
MML_calea_opr> add-aftdn:subsid=2222111112,afid=Cable;
```

Table 7 describes the strings in the **add-aftdn** command.

Table 7 ***add-aftdn Command Strings***

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

IP Call Content Channel Configuration

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

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

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

Table 8 add-ipccc Command Strings

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

Access Function Configuration

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

If the network includes aggregation routers supporting Simple Network Management Protocol version 3 (SNMPv3) interfaces, they must also be added with the type of SNMPER. (SNMPER identifies devices that support an SNMPv3 interface). Trunking gateways that support only MGCP LI options must be provisioned using the type TGW. Trunking gateways that support SNMPv3 should be provisioned as such.

```
MML_calea_adm> add-af:afid=1,name=CactusCable,type=BTS10200,version=3.2,preprov=000:00;
MML_calea_adm> add-af:afid=I1705,name=I1705,type=CMTS,version=12.2,preprov=000:00;
MML_calea_adm> add-af:afid=ESR-egw,type=SNMPER,version=12.2,preprov=000:00;
```

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

Table 9 add-af Command Strings

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

Table 9 add-af Command Strings (continued)

String	Description
type	Type of physical device. Allowed values are BTS10200, CMS, CMTS, DCFD, GENERIC, MGC, SM, SNMPER, TGW, or SYION. **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 SNMPv3 interfaces (Cisco 10000 Edge Services Router (ESR), Cisco 7246, Cisco 7500). SYION is a call management server product of the Syndeo Corporation.
version	Version of software release running on the AF (optional).
preprov	Time zone of the access function.

Access Function BTS Provisioning Interface Configuration

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

```
MML_calea_adm> add-afbi:afid=CactusCable,ifid=1,ipaddr=10.8.100.100,username=calea
password=test123,reqstate=ACTIVE;
MML_calea_adm> add-afbi:afid=CactusCable,ifid=2,ipaddr=10.8.100.101,username=calea
password=test123,reqstate=ACTIVE;
```

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

Table 10 add-afbi Command Strings

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

Note On the SS8 mediation device, in the file $ASVCRUN/config/MML/btsrhost.cnf, uncomment the appropriate line for provisioning BTS using either SSH (the normal default) or Telnet. You must be logged in to the SS8 MD as user “calea_adm” to edit this file. If calea is running on the SS8 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 31.

Access Function PGW Provisioning Interface Configuration

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

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

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

Table 11 add-afgi Command Strings

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

Access Function RADIUS Interface Configuration

The **add-afri** command adds the access function Remote Authentication Dial-In User Services (RADIUS) interface (AFRI), which provisions the PacketCable Event Message interface between the call agent and the SS8 mediation device. The command must be executed by user calea_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_calea_adm>
add-afri:afid=CactusCable,ifid=1,ipaddr=10.8.100.102,port=14146,reqstate=ACTIVE,version=I0
3,sharedsecret=0000000000000000;
MML_calea_adm>
add-afri:afid=CactusCable,ifid=2,ipaddr=10.8.100.103,port=14146,reqstate=ACTIVE,version=I0
3,sharedsecret=0000000000000000;
MML_calea_adm>
add-afri:afid=7246-I1705,ifid=1,ipaddr=10.8.104.5,port=1646,reqstate=ACTIVE,
version=I03,sharedsecret=0000000000000000;
```

Note In this example, port 14146 is the “source” port used by BTS, which is defined in BTS file /opt/OptiCall/CA146/bin/platform.cfg in the ESA section as Args=-RadiusLocalPort 14146 -EmEncodingVersion 3. If port validation for security is not desired, then the port number in AFRI can be set to 0 (zero). If DQoS is utilized in a PacketCable environment, each CMTS must also be provisioned. This is required because each CMTS will send RADIUS messages needed for the mediation device to be able to forward call content. The default RADIUS source port is 1646. The SS8 mediation device can also be provisioned to ignore the port number by specifying port=0. If the /etc/resolv.conf file is edited to add or modify IP addresses of DNS servers while CALEA is running on the SS8, CALEA must be stopped and restarted before the application will recognize configuration changes.

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

Table 12 add-afri Command Strings

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

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

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

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

For information on editing files to set up the addresses and ports of the SNMP network management server, see the *SS8 Xcipio SSDF User Manual* in the "Related Documents" section on page 31. The files that need to be edited will depend upon whether the network management server supports SNMPv1 or SNMPv2. The SS8 Management Information Base (MIB) definition files will also need to be installed into the network management software.

Verifying the PacketCable LI Network

The following sections describe how to verify the PacketCable LI network has been successfully configured:

- Verifying the Cisco BTS 10200 Softswitch Call Agent Configuration, page 23
- Verifying the VISM Card Configuration, page 25
- Verifying the Cisco uBR 7246 VXR CMTS Configuration, page 25

- Verifying the Verint STAR-GATE Mediation Device Configuration, page 25
- Verifying the SS8 Mediation Device Configuration, page 26

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:

```
BTS> show aggr
Reply : Success:  Entries 1-3 of 3 returned.

ID=I1705_bundle
TSAP_ADDR=10.8.0.1
ES_SUPP=Y
DQOS_SUPP=Y
KA_TIMER=2
RADIUS_AUTH_KEY=0000000000000000
ACK_TIMEOUT=1000
RETRY_COUNT=0

ID=I1703_bundle
TSAP_ADDR=10.8.4.1
ES_SUPP=Y
DQOS_SUPP=Y
KA_TIMER=2
RADIUS_AUTH_KEY=0000000000000000
ACK_TIMEOUT=1000
RETRY_COUNT=0

ID=virt_aggr
TSAP_ADDR=10.8.200.31
ES_SUPP=Y
DQOS_SUPP=Y
KA_TIMER=10
RADIUS_AUTH_KEY=0000000000000000
ACK_TIMEOUT=1000
RETRY_COUNT=0

BTS> show mgw id=cva30
Reply :Success:Entry 1 of 1 returned.

ID=cva30
TSAP_ADDR=x1-6-00-04-27-a5-b4-f5.ipclab.cisco.com
CALL_AGENT_ID=CA146
MGW_PROFILE_ID=Cva
STATUS=INS
CALL_AGENT_CONTROL_PORT=2427
RGW=Y
TGW=N
NAS=N
IAD=N
PBX=N
ANS=N
IVR=N
MGW_MONITORING_ENABLED=N
OPER_STATUS=NF
AGGR_ID=CMTS1

BTS> status aggr id=i1703_bundle
Reply : Success:
```

```
AGGR ID -> i1703_bundle
OPER STATE -> AGGR Unknown State
RESULT -> ADM configure result in failure
REASON -> ADM database table(s) or entries not found

BTS> status aggr id=I1705_bundle
Reply : Success:

AGGR ID -> I1705_bundle
OPER STATE -> AGGR IN Service
RESULT -> ADM configure result in success
REASON -> ADM executed successful
```

The **show wiretap** EXEC command can be issued only by the user “calea.”

```
BTS> show wiretap
Reply : Success:  Entries 1-2 of 2 returned.

SUBSCRIBER_DN=9892121212
SUB_ID=cvafb1/1
TAPTYPE=PEN_AND_TRACE
CDC_DF_ADDRESS=10.8.100.17
CDC_DF_PORT=1813

SUBSCRIBER_DN=9891221111
SUB_ID=cvafb2/1
TAPTYPE=INTERCEPT
CDC_DF_ADDRESS=10.8.100.17
CDC_DF_PORT=1813
CCC_DF_ADDRESS=10.15.92.29
CCC_DF_PORT=45010
```

The **show wiretap subscriber** EXEC command can be issued only by the user “calea.”

```
BTS> show wiretap subscriber_dn=6213000001

SUBSCRIBER_DN=6213000001
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.
BTS>
```

The **show ess** EXEC command can be issued only by the user “calea.”

```
BTS> show ess
Reply : Success:  Entries 1-2 of 2 returned.

CDC_DF_PORT=1813
CDC_DF_ADDRESS=10.8.100.17
ENCRYPTION_KEY=0000000000000000
ACC_REQ_RETRANSMIT=3
ACC_RSP_TIMER=2

CDC_DF_PORT=1813
CDC_DF_ADDRESS=141.1.1.31
ENCRYPTION_KEY=0000000000000000
ACC_REQ_RETRANSMIT=3
ACC_RSP_TIMER=2
```

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

```
CLI> show call-agent-profile
ID=CA146
CMS_ID=12345
MGC_ID=54321
FEID=54321
CMS_SUPP=Y
MGC+SUPP=Y
DQOS_SUPP=Y
CDB_BILLING_SUPP=N
EM_BILLING_SUPP=Y
GTD_SUPP=N

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

Verifying the VISM Card Configuration

When using the BTS call agent, you only need to verify that CALEA is enabled on the VISM cards. To display the status of CALEA, use the following command:

```
VISM-1> dspcalea

CALEA : enable
```

Verifying the Cisco uBR 7246 VXR CMTS Configuration

To verify that the CMTS is connected to the call agent, use the **show packetcable gc-list** EXEC command. This command indicates if a successful COPS session has been opened between the uBR and the call agent. The output should indicate the correct IP address of the call agent along with COPS and TCP handle IDs. The following example shows successful output from the **show packetcable gc-list** EXEC command:

```
ubr7246vxr-1# show packetcable gc-list
GC-Addr        GC-Port     COPS-handle TCP-handle
10.15.113.9    0x8041        0x620F3738    0x620F3738
```

To verify that gates are enabled on the CMTS, use the **show packetcable global** EXEC command. The following example shows successful output:

```
ubr7246vxr-1# show packetcable global
Packet Cable Global configuration:
Enabled   :Yes
Max Gates :100
Default Timer value -
  T0      :30000 msec
  T1      :300000 msec
  T2      :2000 msec
  T5      :500 msec
```

Verifying the Verint STAR-GATE Mediation Device Configuration

The Verint STAR-GATE mediation device is configured and verified by using a GUI. For information on verifying the Verint STAR-GATE, see the *Verint STAR-GATE System Description Manual* and the *Verint STAR-GATE System Administration Manual* in the "Related Documents" section on page 31.

Verifying the SS8 Mediation Device Configuration

The following commands can be used to verify the SS8 mediation device configuration. For more information on verifying the SS8 mediation device, see the *SS8 Xcipio SSDF User Manual* in the "Related Documents" section on page 31.

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

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

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

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

```
MML_TH> display-cf:;
--------------------------------------------------------
CFID NAME             TYPE  GRP1 GRP2 GRP3 GRP4 CARRIER
--------------------------------------------------------
```

```
1    PenLink          TCPIP N/A  N/A  N/A  N/A  000
2    JSI              TCPIP N/A  N/A  N/A  N/A  000
<SUCCESS>:: 2 records found.

MML_TH> display-tcpipcfi:;
-------------------------------------------------------------
CFID OWNIP           IPADDR          PORT  REQSTATE STATE
-------------------------------------------------------------
1    172.18.137.105  172.18.137.94   43001 ACTIVE   ACTIVE
2    172.18.137.105  172.18.137.56   43001 ACTIVE   ACTIVE
<SUCCESS>:: 2 records found.

MML_TH> display-af:;
------------------------------------------------------------------------------------------
-
AFID             NAME             TYPE     SERIAL           VERSION  PREPROV INDEX
------------------------------------------------------------------------------------------
-
CBeyond          BTS_CBeyond      BTS10200 N/A              2.1      000:00  1
CactusCable      BTS_CactusCable  BTS10200 N/A              3.3      000:00  2
<SUCCESS>:: 2 records found.
MML_TH>

MML_TH> display-afbi:;
------------------------------------------------------------------------------------------
AFID             IFID IPADDR          REQSTATE STATE    USERNAME         PASSWD
------------------------------------------------------------------------------------------
CBeyond          1    10.15.69.7      INACTIVE INACTIVE calea            test123
CactusCable      1    10.8.100.100    ACTIVE   INACTIVE calea            test123
CactusCable      2    10.8.100.101    ACTIVE   INACTIVE calea            test123
<SUCCESS>:: 3 records found.

MML_TH> display-afsi:;
------------------------------------------------------------------------------------------
-------------------------------------------------------------------
AFID          IFID DOMAINNAME        IPADDR       PORT  REQSTATE STATE   USERNAME
AUTHPASSWD           PRIVPASSWD           SECURITYLVL
------------------------------------------------------------------------------------------
-------------------------------------------------------------------
7200-egw         1    7200-egw.sm02.cisco.com 10.15.115.1     161   ACTIVE   ACTIVE
ss8user             ss8passwd            ss8passwd            AUTHNOPRIV
7500-egw         1    7500-egw.sm02.cisco.com 10.15.115.2     161   ACTIVE   ACTIVE
ss8user             ss8passwd            ss8passwd            AUTHNOPRIV
ESR-egw          1    ESR-egw.sm02.cisco.com  10.15.115.3     161   ACTIVE   ACTIVE
ss8user             ss8passwd            ss8passwd            AUTHNOPRIV
<SUCCESS>:: 3 records found.

MML_TH> display-afri:;
---------------------------------------------------------------------------------
AFID             IFID IPADDR          PORT  REQSTATE VERSION SHAREDSECRET
---------------------------------------------------------------------------------
CBeyond          1    10.15.69.35     1813  ACTIVE   I02    0000000000000000
CBeyond          2    10.15.69.36     1813  ACTIVE   I02    0000000000000000
CBeyond          3    10.15.69.67     1813  ACTIVE   I02    0000000000000000
CBeyond          4    10.15.69.68     1813  ACTIVE   I02    0000000000000000
PGW              1    10.15.113.80    14146 ACTIVE   I03    0000000000000000
CactusCable      1    10.8.100.102    14146 ACTIVE   I03    0000000000000000
CactusCable      2    10.8.100.103    14146 ACTIVE   I03    0000000000000000
<SUCCESS>:: 7 records found.

MML_TH> display-surveillance:;
------------------------------------------------------------------------------------------
--------------------------------------------------------------------------
STATE COUNTY        CITY         WARRANTID     JAREA     CASEID      SUBSID      ENTRYDATE
```

```
STARTDATE  EXPDATE    STATUS   CFID SURVTYPE CONTENT   USER       ACCESS
------------------------------------------------------------------------------------------
-------------------------------------------------------------------------
NC    Wake          RTP          1187          COUNTRY  1187        7242711187  05/03/2002
05/03/2002 05/03/2003 ACTIVE   2    DATA     NONE      calea_opr  PUBLIC
<SUCCESS>:: 1 records found.
```

In the following output from the **display-aftdn:;** command, the first entry is for call data only. The second entry is for call data and for call content. The SS8 software automatically selects the IP address and the port number.

```
MML_TH> display-aftdn:;
------------------------------------------------------------------------------
SUBSID           AFID             IPADDR          PORT  REQSTATE   STATE
------------------------------------------------------------------------------
7242711187       1                N/A             0     ACTIVE     TOBEPROV
9192621002       2                10.15.93.29     45010 ACTIVE     TOBEPROV
<SUCCESS>:: 1 records found.

MML_TH> display-ipccc:;
------------------------------------------------------------------------------------------
-------------
IPCCID STATE COUNTY        CITY         WARRANTID   CCCID     SUBSID       CFIPADDR
CFPORT STATUS
------------------------------------------------------------------------------------------
-------------
1       NC    Wake          RTP          2621002     1002      9192621002   172.18.137.56
9000   ACTIVE
<SUCCESS>:: 1 records found.
```

Troubleshooting a PacketCable LI Network

The following sections provide guidance in troubleshooting a PacketCable LI network:

- General Troubleshooting Notes, page 28
- Troubleshooting the Mediation Device, page 29
- Troubleshooting the BTS Call Agent, page 29

General Troubleshooting Notes

The most common problem encountered in configuring voice intercept 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 through.

When firewalls prohibit ping traffic, pings cannot be used for troubleshooting. Instead, a sniffer may be used to verify connectivity.

J-STD has a test message for verifying and troubleshooting, but it is not supported by PacketCable messaging.

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. For information on troubleshooting the Verint STAR-GATE mediation device, see the *Verint STAR-GATE Maintenance and Troubleshooting Manual* in the "Related Documents" section on page 31.

On the SS8 Xcipio mediation device, if the file /etc/resolv.conf is edited to add or modify IP addresses of DNS servers while the CALEA application is running, CALEA must be stopped and re-started (using the **calea_stop** and **calea_start** commands) before the application will recognize the configuration changes. For more information on troubleshooting the SS8 Xcipio mediation device, see the *SS8 Xcipio SSDF User Manual* in the "Related Documents" section on page 31.

Troubleshooting the BTS Call Agent

To perform ESS and wiretap commands on the BTS, you must log in as user **calea**. All other commands, including the ones shown below, can be performed by any user with the proper permissions.

When accessing the BTS, you must log in as user **calea**.

The following sections describe troubleshooting procedures on the BTS call agent:

- Troubleshooting the Call Agent Profile, page 29
- Troubleshooting the Call Agent to CMTS Interface, page 30

For more information on debugging and tracing tools for the BTS, see the *BTS CALEA Interface Specification* documentation in the "Related Documents" section on page 31.

Troubleshooting the Call Agent Profile

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

```
CLI> show call-agent-profile
ID=CA146
CMS_ID=12345
MGC_ID=54321
FEID=54321
CMS_SUPP=Y
MGC_SUPP=Y
DQOS_SUPP=Y
CDB_BILLING_SUPP=N
EM_BILLING_SUPP=Y
GTD_SUPP=N

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

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

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

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

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

Troubleshooting the Call Agent to CMTS Interface

Use the **show packetcable gc-list** EXEC command as shown in the previous "Verifying the Cisco uBR 7246 VXR CMTS Configuration" section. If you do not see similar output, there is a problem with the connection between the call agent and the CMTS. Complete the following procedure to troubleshoot this connection:

1. From the BTS CLI, enter the **show aggr** command.

   Ensure that each aggregation router (AGGR) has only one entry. If any AGGR has duplicate entries with different tsap-addr, delete the incorrect one. The AGGR should use the CMTS cable interface IP address as its tsap-addr.

2. Enter the **status aggr** command.

   Ensure that the OPER STATE is AGGR IN_Service.

3. If AGGR is not in IN_Service state, then search the BTS trace for the following error string:

   ```
   "Unable to send OPN message to client layer"
   ```

   This error indicates that the CMTS client type is incorrect. For Release 3.3 on the BTS, the CMTS must support the I03 DQoS client type, which is 8008. (I02 uses client type 8005). If you encounter this error, you will need to load a different image on the CMTS that supports I03 DQoS.

4. On the CMTS, verify that the following commands are configured:

   ```
   ubr7246.241#config> packetcable enable
   ubr7246.241#config> packetcable max-gates 100  (the value 100 is used for testing)
   ```

   If you switch the CMTS image, you must re-enable these commands after the CMTS is reloaded.

5. After you have made these fixes, enter the **status aggr** command on the BTS and check if the OPER state is AGGR IN_Service.

There are various debugging commands that can be used on the CMTS, but they can impact call performance and should be used only under the direction of Cisco support.

Appendix

This section contains the following information:

- Cisco Products That Support PacketCable Lawful Intercept BTS Versions 3.5 and 4.1, page 31
- Related Documents, page 31
- Standards, page 32
- RFCs, page 32
- Technical Assistance, page 32

Cisco Products That Support PacketCable Lawful Intercept BTS Versions 3.5 and 4.1

Table 13 provides the following additional information on the Cisco products that support PacketCable LI BTS versions 3.5 and 4.1:

- Cisco Product—provides the name of the product that supports LI
- Product Type—identifies the role that the product performs
- Voice Support—describes the versions that the platform supports

Table 13 Cisco Products That Support PacketCable LI Architecture

Cisco Product	Product Type	Voice Support
Cisco BTS 10200	Call agent	Supports BTS Release 3.5 and later releases
Cisco uBR7246 VXR	CMTS	Cisco IOS Release 12.2(15)BC1b and later releases
Cisco uBR10000	CMTS	Cisco IOS Release 12.2(15)BC1b and later releases
Cisco 3660	Trunking gateway	Cisco IOS Release 12.3(7)T and later releases
Cisco MGX 8850 VG	Trunking gateway	Cisco Voice Interworking Service Module (VISM) 2.2 and later releases Cisco Voice Switch Service Module (VXSM) 2.0 and later releases
Cisco AS5350	Access server/ trunking gateway	Cisco IOS Release 12.3(7)T and later releases
Cisco AS5400	Access server/ trunking gateway	Cisco IOS Release 12.3(7)T and later releases
Cisco AS5850	Access server/ trunking gateway	Cisco IOS Release 12.3(7)T and later releases

Related Documents

Table 14 lists related documents.

Table 14 Related Documents

Title	URL, RFC, or Part Number
PacketCable Electronic Surveillance Specification	http://www.packetcable.com/specifications
PacketCable Electronic Surveillance Call Flows Technical Report	http://www.packetcable.com/specifications
PacketCable Dynamic Quality of Service Specification	http://www.packetcable.com/specifications
The COPS (Common Open Policy Service) Protocol	RFC 2748
PacketCable Event Messages Specification	http://www.packetcable.com/specifications
PacketCable PSTN Gateway Call Signaling Protocol Specification	http://www.packetcable.com/specifications
SS8 Xcipio SSDF User Manual	2700-2493-01
PacketCable CMS to CMS Signalling Specification	http://www.packetcable.com/specifications
PacketCable Security Specification	http://www.packetcable.com/specifications

Table 14 Related Documents (continued)

Title	URL, RFC, or Part Number
Verint STAR-GATE System Administration Manual	P/N 52-530-0581
Verint STAR-GATE System Description Manual	P/N 52-530-DRAFT
Verint STAR-GATE Maintenance and Troubleshooting Manual	P/N 52-530-0632
SS8 Xcipio SSDF User Manual	2700-1849-01
BTS CALEA Interface Specification	ENG-102175

Standards

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

RFCs

RFC	Title
RFC 2748	*The COPS (Common Open Policy Service) Protocol*

Technical Assistance

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

Glossary

AF—access function

AFBI—access function BTS interface

AFGI—access function PGW interface

AFID—access function ID

AFRI—access function RADIUS interface

AFTDN—access function target directory number

AGGR—aggregation router

ATA—Analog Telephone Adapter

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

CMS—call management server

CMTS—cable modem termination system

COPS—Common Open Policy Service

DCFD—Data Collection and Filtering Device. A sniffer that collects and analyzes RADIUS traffic.

DHCP—Dynamic Host Configuration Protocol

DNS—Domain Name Service

DQoS—dynamic quality of service

EMS—Element Management System

ESR—Edge Services Router

ESS—Electronic Surveillance Subsystem

FEID—financial entity ID

IAD—Integrated Access Device

IAP—intercept access point

IFID—Interface ID

IPCCC—IP call content channel

IPDU—IP delivery unit

IRI IAP—Intercept-Related Information intercept access point

ISP—Internet service provider

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 translates the information into the correct protocol.

MGC—Media Gateway Controller

MGCP—Media Gateway Control Protocol

MIB—Management Information Base

MML—Man Machine Language

MTA—media termination adapter

NAS—network access server

off-net—off-network

on-net—on-network

PGW—PSTN Gateway

PSTN—public switched telephone network

RADIUS—Remote Authentication Dial-In User Services

reqstate—required state

SIP—Session Initiation Protocol

SMDS—Switched Multimegabit Data Service

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

SNMPv3—Simple Network Management Protocol version 3

SP—service provider

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

SSH—Secure Shell

tcpipcfi—TCP/IP collection function interface

TGW—trunking gateway

TIA—Telephone Industry Association

UDP—User Datagram Protocol

uBR—Universal Broadband Router

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.

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