



PacketCable Lawful Intercept Architecture for BTS Version 5.0

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 I08 of the PacketCable Event Message Specification and BTS versions 4.4 and 4.5.
3	4/19/2007	This document was updated and includes version 1.5-I01 of PacketCable Event Message Specification and BTS version 5.0.

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 Version 5.0* document describes the implementation of LI architecture on a PacketCable network. This document 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 includes some information on design,



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

© 2007 Cisco Systems, Inc. All rights reserved.

implementation, operation, and troubleshooting LI on a PacketCable network. For details about the various devices such as software and memory requirements, configurations, and so forth, this document includes references to device product documentation.

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 15](#)
- [Troubleshooting a PacketCable LI Network, page 19](#)
- [Appendix, page 21](#)
- [Glossary, page 24](#)

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 because the intercept subject can detect the LI. Sophisticated users can determine that their call has been diverted because the source and destination IP addresses do not match. Therefore, the tapping must take place on equipment that is within the domain of trust of the SP or ISP on 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. This confidentiality 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 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 and broadband access providers in the United States must support LI. Three specifications define the interface to the LEAs for the purposes of meeting the CALEA requirements:

- The *Telephone Industry Association Lawfully Authorized Electronic Surveillance* standard developed by the Telephone Industry Association (TIA).
- The *PacketCable Electronic Surveillance Specification* document.
- The *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technology in Wireline Telecommunications Networks* standard developed by American National Standards for Telecommunications.

Worldwide, 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. See the “[Related Documents](#)” and “[Standards](#)” sections for additional information about these and other LI specifications and standards.

PacketCable Lawful Intercept Architecture

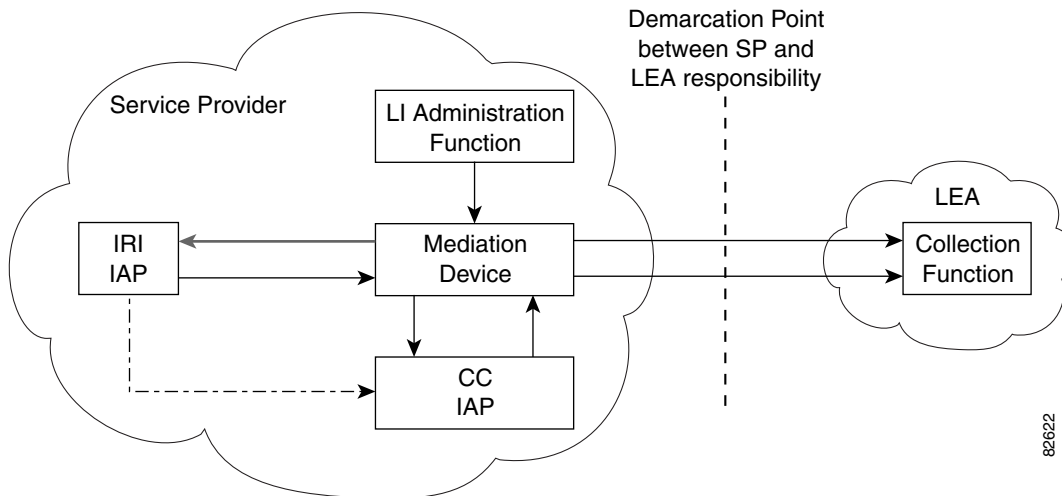
The following sections describe the Broadband Telephony Softswitch (BTS) version 5.0 PacketCable LI architecture:

- [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.

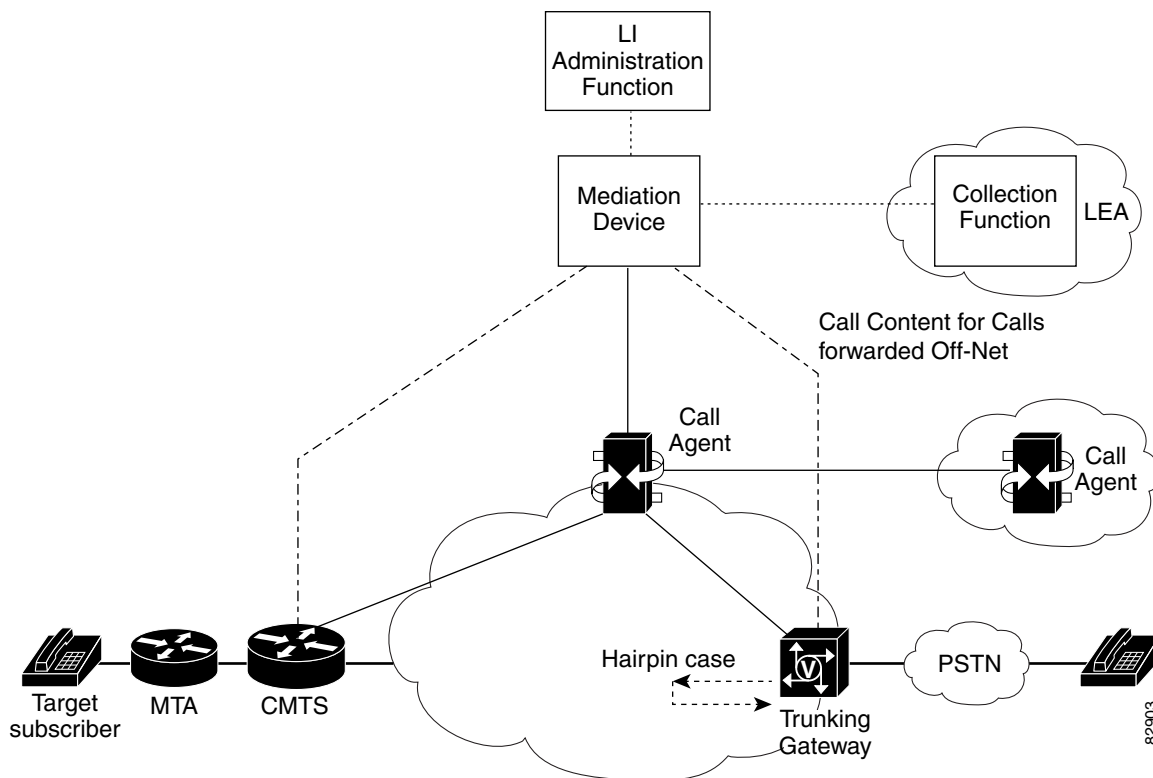
Figure 1 *Generic IP Network That Supports LI of Voice and Data Traffic*



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 5](#)
- [Mediation Device, page 5](#)
- [Intercept-Related Information Intercept Access Point, page 5](#)
- [Call Content Intercept Access Point, page 6](#)
- [Collection Function, page 6](#)

LI Administration Function

The SP uses the LI administration function to provision intercepts by interfacing with the other components in the network. The LI administration function is responsible for provisioning components in the network, administering intercept orders, and tracking and maintaining intercept information. The LI administration function 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. The mediation device 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. The mediation device is also responsible for formatting the information to be compliant with the country or technology-specific requirements for delivery to law enforcement. The mediation device is also responsible for implementing post call completion dialed digit extraction.

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 IAP for voice includes the source and destination phone numbers, IP addresses, and the time of the call. The access point 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) or Trunking Gateway Control Protocol (TGCP)-based PacketCable network, both the call agent and optionally the CMTS supply IRI IAP functionality. The call agent supplies call control-related information such as the dialed number and the call encoding, and the CMTS optionally 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.

To prevent the intercept target from being able to detect the intercept, however, the CC IAP should not be part of the MTA. 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 interfaces of interest between devices in a PacketCable voice intercept topology:

Figure 3 PacketCable Voice Intercept Device Interfaces

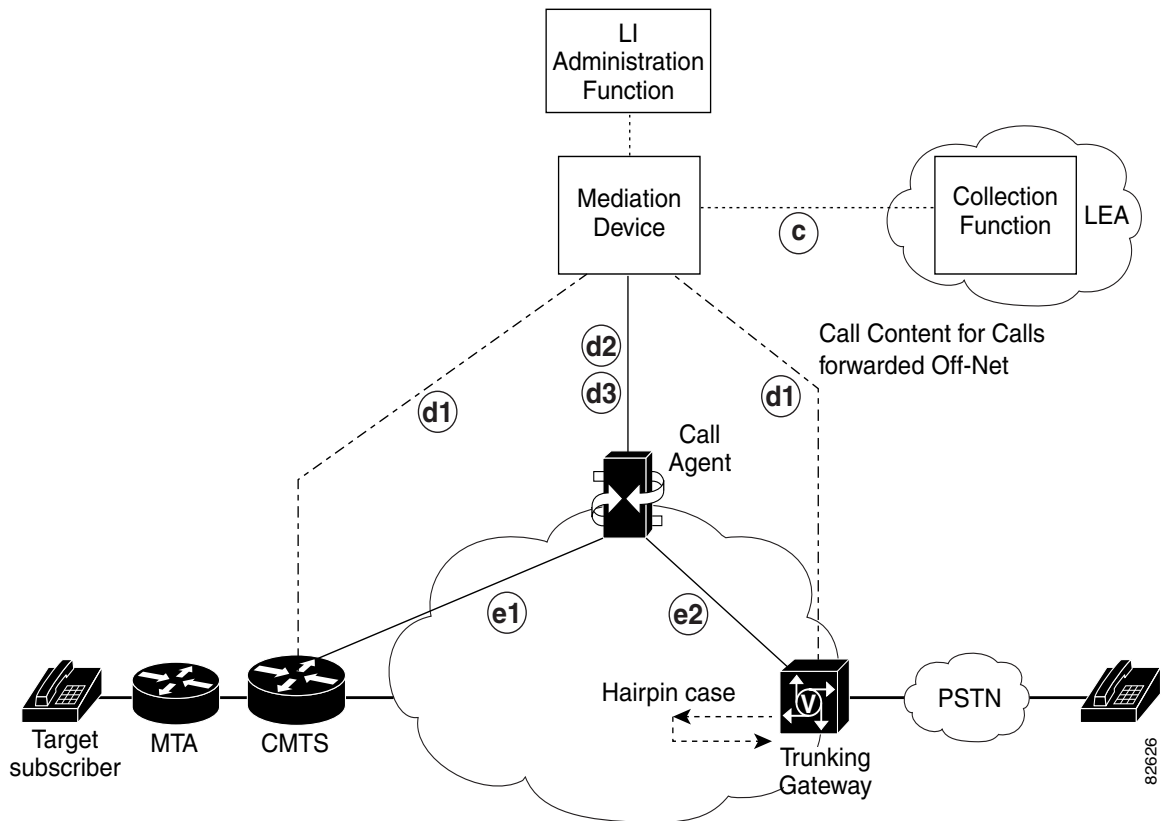


Table 1 describes the interfaces between the devices shown in Figure 3.

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 and send it to the collection function of each LEA. The mediation device will also perform post call completion dialed digit extraction. This interface meets the specifications defined in the “PacketCable Electronic Surveillance Specification” document in the “Related Documents” section on page 22.
d1	CMTS or trunking gateway and Mediation Device	<p>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 provided by call agent. The CCCID is used to associate the CC with the target.</p> <p>In a typical CC intercept scenario, the CMTS is the CC IAP. If a call comes in from the PSTN and is forwarded back to the PSTN, the trunking gateway must serve as the CC IAP.</p> <p>The CCCID is included so that the mediation device can map intercepts to the appropriate warrants. Usually, the mediation device will rewrite the CCCID before forwarding intercept information to collection functions.</p> <p>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 22.</p>
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)	<p>This is the delivery interface. The call agent uses this interface to deliver IRI to the mediation device.</p> <p>This interface is described in Appendix A of the “PacketCable Event Messages Specification” document in the “Related Documents” section on page 22.</p>
e1	Call agent and CMTS	<p>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.</p> <p>This interface is described in the “PacketCable Dynamic Quality of Service Specification” document in the “Related Documents” section on page 22.</p>
e2	Call agent and trunking gateway	The call agent uses Trunking Gateway Control Protocol (TGCP) or 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 22.

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 intercept is the most common type. This type of intercept intercepts only the IRI, which includes the source and destination phone numbers, IP addresses, and the time of the call. This intercept also includes any post-call establishment messaging such as call forwarding, three-way calling, or dialed digits. To implement the dialed digit extraction, the CMTS or gateway must always duplicate call content and forward the content to the mediation device. 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. 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 that is typically 30 days. This expiration date is configured on the mediation device. When the warrant expires, the mediation device automatically removes the configuration for the warrant. The mediation device provisioning interface can be used to remove a warrant before the expiration date.

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

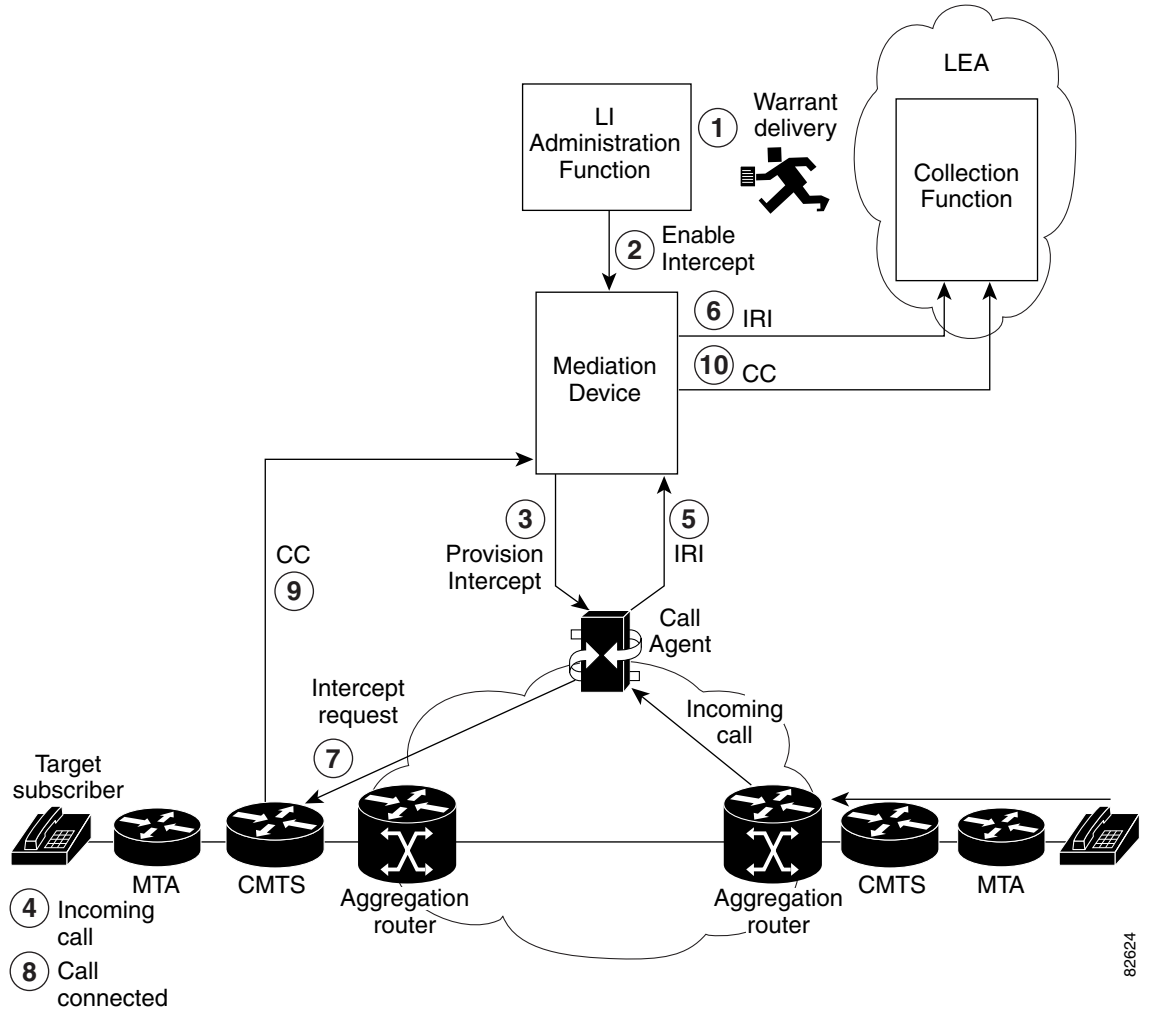


Note

The following figure 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



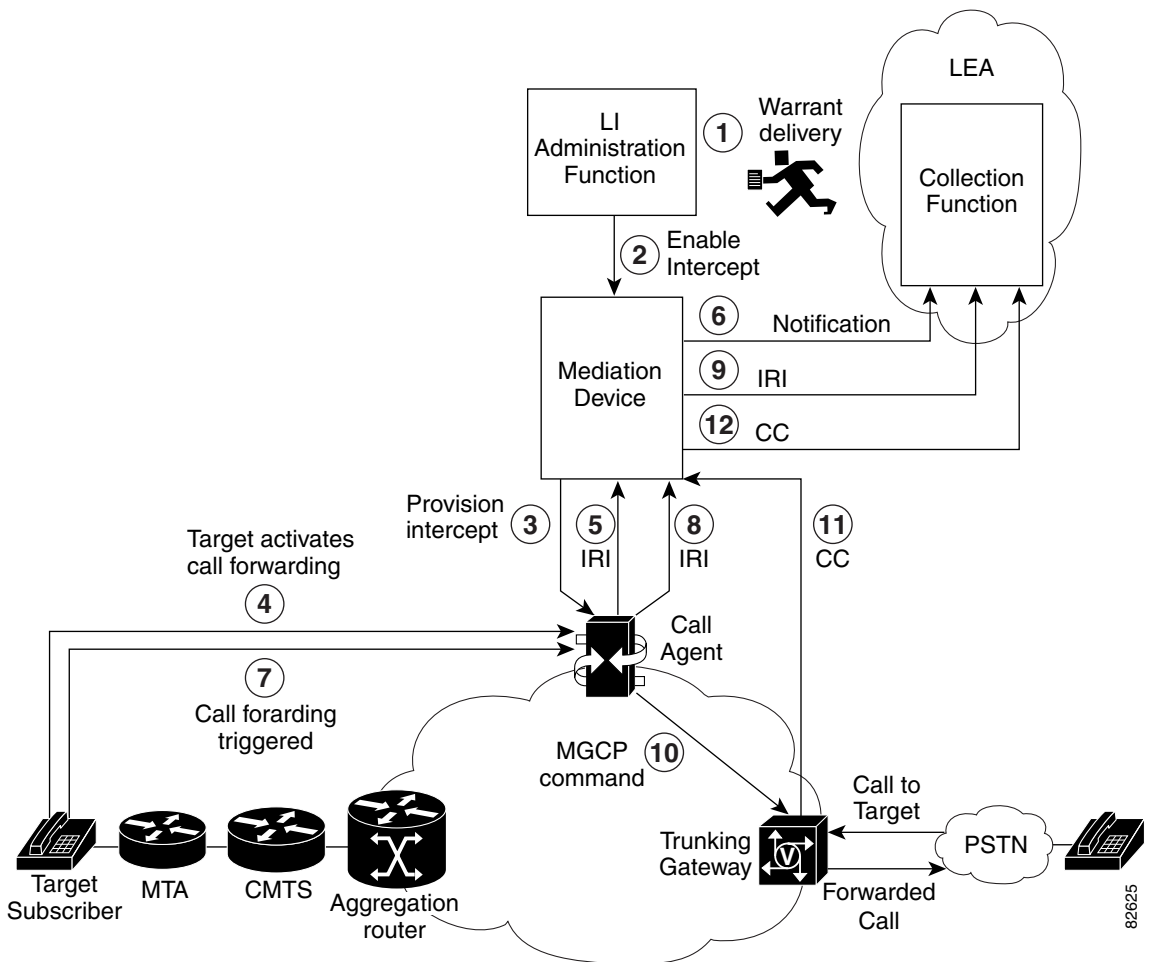
- Step 1** The LEA physically delivers a court order to the network administrator that operates the LI administration function.
- Step 2** The LI administration function sends a configuration to the mediation device that enables the intercept.
- Step 3** The mediation device sends a configuration command 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** Call agent sends an intercept request to the CMTS using dynamic quality of service (DQoS) to enable content intercept for dialed digit extraction and, if included in warrant, a copy of the voice is made and sent to LEA.
- 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 for 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 or TGCP command to the trunking gateway, to enable an intercept for dialed digit extraction and to route the call back to the PSTN. If call content is to be intercepted mediation device will forward a copy of voice packets to LEA.
- 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-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 or TGCP. 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 22. 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 22.

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 22. DQoS is used to authorize QoS for media flows within the PacketCable architecture. 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 optionally acts as an IAP for call identification information and provides QoS_Reserve, QoS_Commit, and QoS_Release event messages to the mediation device. These messages are not required to provide full functionality.

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 or TGCP and some additional parameters in the MGCP or TGCP 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 22. 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 22.

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 22.

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 22. Call agents and mediation devices run standard operating systems that 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 understand 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 such as Cisco Network Registrar to perform Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP).

The various devices involved in LI have minimum software and memory requirements that must be met. 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 22](#) 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, 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 uBR7246 VXR CMTS Configuration, page 14](#)
- [VISM Trunking Gateway Configuration, page 14](#)
- [Cisco BTS 10200 Softswitch Call Agent Configuration, page 14](#)

Cisco uBR7246 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 Call Agent Profile, page 14](#)
- [Add an Aggregation Router, page 14](#)
- [Add a Media Gateway, page 15](#)

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;USE-PACKETCABLE-IAP=Y;
Reply : Success: CLI add successful
Transaction 1035567544247 was processed.
```

Add Call Agent Profile

To create the **add call-agent-profile** script, you must log in as a user other than “calea.” For call content interception to work, the `dqos_supp` parameter in the `call-agent-profile` table must be set to Y.

```
BTS(config)# add call-agent-profile
id=CA146;cdb_billing_supp=n;em_billing_supp=N;mgc_id=7979;cms-id=6969;dqos_supp=Y;
Reply : Success: CLI add successful
Transaction 1035567644247 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
```

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 15](#)
- [Verifying the VISM Card Configuration, page 18](#)
- [Verifying the Cisco uBR 7246 VXR CMTS Configuration, page 18](#)

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:

```
CLI> show aggr

ID=10K_bundle
TSAP_ADDR=10.127.130.254
IPSEC_SA_ESP_CS=3DES-MD5,3DES-SHA1,NULL-MD5,NULL-SHA1
IPSEC_SA_LIFETIME=86400
IPSEC_SA_GRACE_PERIOD=21600
IPSEC_ULP_NAME=IP
IKE_GROUP=2
IKE_SA_LIFETIME=86400
IKE_CS=3DES-MD5,3DES-SHA1
TYPE=CMTS
STATUS=INS
AGGR_PROFILE_ID=10K_bundle

ID=N1401_bundle
TSAP_ADDR=10.127.129.254
IPSEC_SA_ESP_CS=3DES-MD5,3DES-SHA1,NULL-MD5,NULL-SHA1
IPSEC_SA_LIFETIME=86400
IPSEC_SA_GRACE_PERIOD=21600
IPSEC_ULP_NAME=IP
IKE_GROUP=2
IKE_SA_LIFETIME=86400
IKE_CS=3DES-MD5,3DES-SHA1
TYPE=CMTS
STATUS=INS
AGGR_PROFILE_ID=N1401_bundle

Reply : Success: at 2007-02-20 10:56:19 by mgavin
Entries 1-2 of 2 returned.
```

```
CLI> show aggr-profile
```

```
ID=10K_bundle
ES_SUPP=Y
ES_EVENT_SUPP=N
DQOS_SUPP=Y
KA_TIMER=2
ACK_TIMEOUT=1000
GATE_INFO_SUPP=N
GATE_AUTHORIZED_TIMER=200
GATE_RESERVED_TIMER=300
GATE_COMMITTED_TIMER=600
GATE_COMMITTED_RECOVERY_TIMER=120
GATE_CLOSE_TIMER=5
L1_RETRY_INTERVAL=1
L2_RETRY_INTERVAL=10
L1_RETRY_COUNT=1000
L2_RETRY_COUNT=100
CONFIGURATION_INFO_SUPP=N
```

```
ID=N1401_bundle
ES_SUPP=Y
ES_EVENT_SUPP=N
DQOS_SUPP=Y
KA_TIMER=2
ACK_TIMEOUT=1000
GATE_INFO_SUPP=N
GATE_AUTHORIZED_TIMER=200
GATE_RESERVED_TIMER=300
GATE_COMMITTED_TIMER=600
GATE_COMMITTED_RECOVERY_TIMER=120
GATE_CLOSE_TIMER=5
L1_RETRY_INTERVAL=1
L2_RETRY_INTERVAL=10
L1_RETRY_COUNT=1000
L2_RETRY_COUNT=100
CONFIGURATION_INFO_SUPP=N
```

```
Reply : Success: at 2007-02-20 10:57:50 by mgavin
Entries 1-2 of 2 returned.
```

```
CLI> show mgw ID=lnk990203
```

```
ID=lnk990203
TSAP_ADDR=lnk990203.sm02.cisco.com
CALL_AGENT_ID=CA146
MGW_PROFILE_ID=LinkSys
STATUS=INS
CALL_AGENT_CONTROL_PORT=0
AGGR_ID=N1401_bundle
TYPE=RGW
MGW_PORT=2427
```

```
Reply : Success: at 2007-02-20 11:04:54 by mgavin
Entry 1 of 1 returned.
```

```
CLI> status aggr id=N1401_bundle
```

```
ID -> N1401_bundle
OPER STATE -> AGGR IN Service
RESULT -> ADM configure result in success
REASON -> ADM executed successfully
```

```
Reply : Success: at 2007-02-20 11:00:04 by mgavin
```

```

CLI> status aggr id=10K_bundle

ID -> 10K_bundle
OPER STATE -> AGGR IN Service
RESULT -> ADM configure result in success
REASON -> ADM executed successfully

Reply : Success: at 2007-02-20 11:00:29 by mgavin

```

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

```

CLI> show wiretap

SUBSCRIBER_DN=64136ada69b99c20c4cdadf7a7c7ce62
TAPTYPE=INTERCEPT
CDC_DF_ADDRESS=10.15.113.9
CDC_DF_PORT=1813
CCC_DF_ADDRESS=10.15.113.9
CCC_DF_PORT=45007

SUBSCRIBER_DN=d658040dlac4868e0f43f8907150e666
TAPTYPE=INTERCEPT
CDC_DF_ADDRESS=10.15.113.9
CDC_DF_PORT=1813
CCC_DF_ADDRESS=10.15.113.9
CCC_DF_PORT=45008

SUBSCRIBER_DN=f9e4495092d9f3b9aed30da8f6922586
TAPTYPE=INTERCEPT
CDC_DF_ADDRESS=10.15.113.9
CDC_DF_PORT=1813
CCC_DF_ADDRESS=10.15.113.9
CCC_DF_PORT=45009

Reply : Success: at 2007-02-20 11:09:39 by calea
Entries 1-3 of 3 returned.

```

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

```

CLI> show wiretap subscriber-dn=6213000017

SUBSCRIBER_DN=f9e4495092d9f3b9aed30da8f6922586
TAPTYPE=INTERCEPT
CDC_DF_ADDRESS=10.15.113.9
CDC_DF_PORT=1813
CCC_DF_ADDRESS=10.15.113.9
CCC_DF_PORT=45009

Reply : Success: at 2007-02-20 11:11:09 by calea
Entry 1 of 1 returned.

```

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

```

CLI> show ess CDC_DF_ADDRESS=10.15.113.9

CDC_DF_PORT=1813
CDC_DF_ADDRESS=10.15.113.9
ENCRYPTION_KEY=0000000000000000
ACC_REQ_RETRANSMIT=3
ACC_RSP_TIMER=2
PROTOCOL_VERSION=I03

```

```

IPSEC_SA_ESP_CS=3DES-MD5,3DES-SHA1,NULL-MD5,NULL-SHA1
IPSEC_SA_LIFETIME=86400
IPSEC_SA_GRACE_PERIOD=21600
IPSEC_ULP_NAME=IP
IKE_GROUP=2
IKE_SA_LIFETIME=86400
IKE_CS=3DES-MD5,3DES-SHA1
USE_PACKETCABLE_IAP=Y
CCC_DF_ADDRESS=10.15.113.9
CCC_DF_PORT=10501
EM_PROTOCOL_VERSION_MAJOR=15
EM_PROTOCOL_VERSION_MINOR=0
GENERAL_PURPOSE_FLAG=0

```

```

Reply : Success: at 2007-02-20 11:07:26 by calea
Entry 1 of 1 returned.

```

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

```

CLI> show call-agent-profile

```

```

ID=CA146
CMS_ID=6969
MGC_ID=7979
DQOS_SUPP=Y
CDB_BILLING_SUPP=N
EM_BILLING_SUPP=N
GTD_SUPP=N
PCMM_SUPP=N
AMID=99999
PCMM_VERSION_MAJOR=1
PCMM_VERSION_MINOR=0
ENUM_SUPP=N

```

```

Reply : Success: at 2007-02-20 11:13:02 by mgavin
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 cops server 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 and the COPS and TCP handle IDs.

The following example shows successful output from the **show cops server** EXEC command:

```
ubr7246vxr-1# show cops server
COPS SERVER: Address: 10.15.123.23. Port: 55215. State: 0. Keepalive: 2 sec
  Number of clients: 1. Number of sessions: 1.
  COPS CLIENT: Client type: 32776. State: 0.
```

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:
Packetcable DQoS Enabled      : Yes
Packetcable Multimedia Enabled : No
Element ID: 52491
Max Gates : 2000
Not Allow non-PacketCable UGS
Intercept Hold Content: Enabled
Default Multimedia Timer value -
  T1          : 200000 msec
  Persistent gate : 0 hour
  Volume Limit  : STOPPED
Default DQoS Timer value -
  T0          : 30000 msec
  T1          : 300000 msec
```

Troubleshooting a PacketCable LI Network

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

- [General Troubleshooting Notes, page 19](#)
- [Troubleshooting the BTS Call Agent, page 19](#)

General Troubleshooting Notes

The most common problem encountered in configuring voice intercept on a network is general networking problems. All devices involved 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 that is not supported by PacketCable messaging.

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 20](#)
- [Troubleshooting the Call Agent to CMTS Interface, page 20](#)

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 22](#).

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=6969
MGC_ID=7979
DQOS_SUPP=Y
CDB_BILLING_SUPP=N
EM_BILLING_SUPP=N
GTD_SUPP=N
PCMM_SUPP=N
AMID=99999
PCMM_VERSION_MAJOR=1
PCMM_VERSION_MINOR=0
ENUM_SUPP=N
```

```
Reply : Success: at 2007-02-20 11:13:02 by mgavin
Entry 1 of 1 returned.
```

The CMS_SUPP, and MGC_SUPP must be set to Y. Either CDB_BILLING_SUPP or EM_BILLING_SUPP can be set to Y, but not both. The CMS_ID, MGC_ID, and financial entity ID (FEID) must all 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 MGC_SUPP is set to N, the BTS will not send event messages.

CMS_ID, MGC_ID, and FEID are PacketCable network element identifiers. Unique values for these network elements must be agreed upon by all involved parties. For the purposes of settlements, PacketCable zones are divided into one or more logical financial entities. A single call agent is assigned at most one FEID. One or more call agents may be assigned to 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 MGC_SUPP is set to N, the BTS will not send event messages.

DQOS_SUPP globally controls use of dynamic quality of service feature. This parameter must be set to Y to enable replication of call content in CMTS for CALEA.

Troubleshooting the Call Agent to CMTS Interface

Use the **show cops server EXEC** command as shown in the “[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:

-
- Step 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.
- Step 2** Enter the **status aggr** command.
- Ensure that the OPER STATE is AGGR IN_Service.
- Step 3** 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)
```
- Step 4** 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 Version 5.0, page 21](#)
- [Related Documents, page 22](#)
- [Standards, page 22](#)
- [RFCs, page 23](#)
- [Technical Assistance, page 23](#)

## Cisco Products That Support PacketCable Lawful Intercept BTS Version 5.0

[Table 2](#) provides the following additional information on the Cisco products that support PacketCable LI BTS version 5.0:

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

**Table 2** *Cisco Products That Support PacketCable LI Architecture*

| Cisco Product     | Product Type     | Voice Support                                     |
|-------------------|------------------|---------------------------------------------------|
| Cisco BTS 10200   | Call agent       | BTS Release 4.4 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     |

**Table 2 Cisco Products That Support PacketCable LI Architecture (continued)**

| Cisco Product     | Product Type                       | Voice Support                                                                                                                            |
|-------------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco MGX 8850 VG | Trunking gateway                   | Cisco Voice Interworking Service Module (VISM) 2.2 and later releases<br>Cisco Voice Switch Service Module (VXSM) 2.0 and later releases |
| Cisco AS5350      | Access server/<br>trunking gateway | Cisco IOS Release 12.3(7)T and later releases                                                                                            |
| Cisco AS5400      | Access server/<br>trunking gateway | Cisco IOS Release 12.3(7)T and later releases                                                                                            |
| Cisco AS5850      | Access server/<br>trunking gateway | Cisco IOS Release 12.3(7)T and later releases                                                                                            |

## Related Documents

| Title                                                                  | URL, RFC, or Part Number                                                                          |
|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <i>PacketCable Electronic Surveillance Specification</i>               | <a href="http://www.packetcable.com/specifications">http://www.packetcable.com/specifications</a> |
| <i>PacketCable Electronic Surveillance Call Flows Technical Report</i> | <a href="http://www.packetcable.com/specifications">http://www.packetcable.com/specifications</a> |
| <i>PacketCable Dynamic Quality of Service Specification</i>            | <a href="http://www.packetcable.com/specifications">http://www.packetcable.com/specifications</a> |
| <i>PacketCable Event Messages Specification</i>                        | <a href="http://www.packetcable.com/specifications">http://www.packetcable.com/specifications</a> |
| <i>PacketCable PSTN Gateway Call Signaling Protocol Specification</i>  | <a href="http://www.packetcable.com/specifications">http://www.packetcable.com/specifications</a> |
| <i>PacketCable CMS to CMS Signalling Specification</i>                 | <a href="http://www.packetcable.com/specifications">http://www.packetcable.com/specifications</a> |
| <i>PacketCable Security Specification</i>                              | <a href="http://www.packetcable.com/specifications">http://www.packetcable.com/specifications</a> |
| <i>BTS CALEA Interface Specification</i>                               | Cisco internal document ENG-102175                                                                |

## Standards

| Standard                             | Title                                                                                                                              |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| ATIS-1000678.2006                    | <i>Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technology in Wireline Telecommunications Networks</i> |
| PKT-SP-ESP1.5-I01                    | <i>PacketCable Electronic Surveillance Specification</i>                                                                           |
| PKT-SP-EM1.5-I01                     | <i>PacketCable Event Messages Specification</i>                                                                                    |
| TIA- J-STD-025 B (SP -3-4465-UGR2-2) | <i>Telephone Industry Association Lawfully Authorized Electronic Surveillance</i>                                                  |

## MIBs

| MIB   | MIBs Link                                                                                                                                                                                                              |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                 |
|----------|-------------------------------------------------------|
| RFC 2748 | <i>The COPS (Common Open Policy Service) Protocol</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                       | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Glossary

- AF**—access function
- AFBI**—access function BTS 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

**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

**TGCP**—Trunking Gateway Control Protocol

**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.

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

---

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.

---

© 2007 Cisco Systems, Inc. All rights reserved.