



CHAPTER 13

PacketCable and PacketCable Multimedia on the Cisco CMTS

Revised: February 5, 2007, OL-1467-08

This document describes how to configure the Cisco CMTS for PacketCable and PacketCable Multimedia operations over an existing Data-over-Cable Service Interface Specifications (DOCSIS) 1.1 cable network.

Feature Specifications for PacketCable Operations

Feature History

Release	Modification
12.2(8)BC2	This feature was introduced with the Cisco MC28U cable interface line card.
12.2(11)BC1	Support was added for version 3 of the PacketCable DQoS specification (PKT-SP-DQOS-I03-020116) and for configuring the Event Message Element ID for the Cisco uBR7246VXR router.
12.2(11)BC2	Support was added for the packetcable authorize vanilla-docsis-mta command, which allows both PacketCable and non-PacketCable DOCSIS UGS service flows when PacketCable is enabled. The show packetcable global command was also enhanced to show whether non-PacketCable UGS service flows are enabled, and the T2 and T5 timers were removed from the display to conform to the requirements of the PacketCable Engineering Change Notice (ECN) 02148.
12.2(15)BC1	PacketCable 1.x supported on the Cisco uBR7246VXR router and the Cisco uBR10012 router. In addition, several debug packetcable commands have been added or enhanced.
12.2(15)BC2	Support was added for the show packetcable event command.
12.3(9a)BC	Supported was added for Packet Cable 1.0 with CALEA on the Cisco uBR10012 router and the Cisco uBR10-MC5X20S/U broadband processing engine (BPE).
12.3(13a)BC	PacketCable Multimedia (PCMM) introduced for the Cisco uBR7246VXR router and Cisco uBR10012 router. The following PacketCable 1.x features introduced for the Cisco uBR7246VXR router and Cisco uBR10012 router: <ul style="list-style-type: none">• PacketCable Emergency 911 Cable Interface Line Card Prioritization• PacketCable Emergency 911 Services Listing and History
12.3(21)BC	Introduces the following features on the CiscoCMTS: <ul style="list-style-type: none">• High Availability Stateful Switchover (SSO) for PacketCable and PacketCable MultiMedia• PacketCable Client Accept Timeout

Supported Platforms

Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

PacketCable Contents

- [Prerequisites for PacketCable Operations, page 13-2](#)
- [Restrictions for PacketCable Operations, page 13-3](#)
- [Information About PacketCable Operations, page 13-3](#)
- [How to Configure PacketCable Operations, page 13-13](#)
- [Monitoring and Maintaining PacketCable Operations, page 13-26](#)
- [Configuration Examples for PacketCable, page 13-27](#)

PacketCable Multimedia Contents

- [Prerequisites for PacketCable Multimedia Operations, page 13-30](#)
- [Restrictions for PacketCable Multimedia Operations, page 13-30](#)
- [Information About PacketCable Multimedia Operations, page 13-31](#)
- [How to Configure PCMM Operations, page 13-35](#)
- [Monitoring and Maintaining PCMM Operations, page 13-37](#)
- [Configuration Examples for PacketCable Multimedia, page 13-37](#)

Additional Information

- [Additional References, page 13-38](#)

Prerequisites for PacketCable Operations

PacketCable Prerequisites

Cisco uBR7246VXR Router

- To support PacketCable operations on the Cisco uBR7246VXR universal broadband router, the router must be running Cisco IOS Release 12.2(8)BC2 or a later 12.2 BC release.
- To support PacketCable 1.0 and the Communications Assistance for Law Enforcement Act (CALEA) intercept capabilities, a Cisco uBR7246VXR broadband router must be running Cisco IOS Release 12.2(11)BC2 or a later 12.2 BC release.

Cisco uBR10012 Router

- To support PacketCable Multimedia operations on the Cisco uBR10012 universal broadband router, the router must be running Cisco IOS Release 12.3(13a)BC or a later 12.3BC release.
- To support PacketCable operations on the Cisco uBR10012 router, the router must be running Cisco IOS Release 12.2(15)BC1 or a later 12.2 BC release.
- To support PacketCable 1.0 and the Communications Assistance for Law Enforcement Act (CALEA) intercept capabilities, a Cisco uBR10012 router must be running Cisco IOS Release 12.2(15)BC1 or a later 12.2 BC release.

Restrictions for PacketCable Operations

PacketCable Restrictions

- Cisco IOS Release 12.2(11)BC1 supports version 3 of the PacketCable DQoS specification (PKT-SP-DQOS-I03-020116).
- To avoid packet drops of voice calls, the Cisco CMTS should be using the default token bucket configuration (**cable downstream rate-limit token-bucket shaping**). Packet drops are guaranteed to occur when the **shaping** option is not used (**cable downstream rate-limit token-bucket**).
- Supports only embedded multimedia terminal adapter (E-MTA) clients. Standalone MTA (S-MTA) clients are not supported.
- PacketCable operations can be configured together with HCCP N+1 redundancy, but the PacketCable states are not synchronized between the Working and Protect interfaces. If a switchover occurs, existing voice calls continue, but when the user hangs up, PacketCable event messages are not generated because the Protect interface is not aware of the previous call states. However, new voice calls can be made and proceed in the normal fashion.
- The 200,000 Hz channel width cannot be used on upstreams that support PacketCable voice calls, or on any upstreams that use Unsolicited Grant Service (UGS) or UGS with Activity Detection (UGS-AD) service flows. Using this small a channel width with voice and other UGS/UGS-AD service flows results in calls being rejected because of “DSA MULTIPLE ERRORS”.

Information About PacketCable Operations

This section provides an overview and other information about PacketCable operations, the components of a PacketCable network, and how they interact with the other components of a DOCSIS cable networks.

- [Feature Overview, page 301](#)
- [New Emergency 911 Features in Cisco IOS Release 12.3\(13a\)BC, page 13-4](#)
- [PacketCable Network Components, page 301](#)
- [Dynamic Quality of Service, page 302](#)
- [Benefits, page 304](#)

Feature Overview

PacketCable is a program initiative from Cablelabs and its associated vendors to establish a standard way of providing packet-based, real-time video and other multimedia traffic over hybrid fiber-coaxial (HFC) cable networks. The PacketCable specification is built upon the Data-over-Cable System Interface Specifications (DOCSIS) 1.1, but it extends the DOCSIS protocol with several other protocols for use over noncable networks, such as the Internet and the public switched telephone network (PSTN).

This allows PacketCable to be an end-to-end solution for traffic that originates or terminates on a cable network, simplifying the task of providing multimedia services over an infrastructure composed of disparate networks and media types. It also provides an integrated approach to end-to-end call signaling, provisioning, quality of service (QoS), security, billing, and network management.

Cisco IOS Release 12.2(11)BC1 supports the PacketCable 1.0 specifications and the Communications Assistance for Law Enforcement Act (CALEA) intercept capabilities of the PacketCable 1.1 specifications.

New Emergency 911 Features in Cisco IOS Release 12.3(13a)BC

Cisco IOS Release 12.3(13a)BC introduces two new Emergency 911 features, supported on PacketCable 1.x and PacketCable Multimedia networks:

- [PacketCable Emergency 911 Cable Interface Line Card Prioritization, page 13-4](#)
- [PacketCable Emergency 911 Services Listing and History, page 13-5](#)

PacketCable Emergency 911 Cable Interface Line Card Prioritization

Cisco IOS Release 12.3(13a)BC introduces PacketCable Emergency 911 cable interface line card prioritization on the Cisco CMTS. This feature enables cable interface line cards that are supporting an Emergency 911 call to be given automatic priority over cable interface line cards supporting non-emergency voice calls, even in the case of HCCP switchover events. In such cases, Protect HCCP line card interfaces automatically prioritize service to Emergency 911 voice calls, should Working HCCP cable interface line cards be disrupted. This feature is enabled by default in Cisco IOS release 12.3(13a)BC, and may not be disabled with manual configuration.



Note

Emergency 911 cable interface line card prioritization applies only to PacketCable voice calls.

During HCCP switchover events, cable modems recover in the following sequence in Cisco IOS release 12.3(13a)BC:

1. Cable modems supporting Emergency 911 voice traffic
2. Cable modems supporting non-emergency voice traffic
3. Cable modems that are nearing a T4 timeout event, in which service would be disrupted
4. Remaining cable modems

To view information about Emergency 911 voice events and cable interface line card prioritization on the Cisco CMTS, use the **show hccp <int x> <int y> modem** and **show hccp event-history** commands in privileged EXEC mode.

PacketCable Emergency 911 Services Listing and History

Cisco IOS release 12.3(1a3)BC introduces enhanced informational support for PacketCable Emergency 911 calls on the Cisco CMTS, to include the following information and related history:

- active Emergency 911 calls
- recent Emergency 911 calls
- regular voice calls
- voice calls made after recent Emergency 911 calls

This feature is enabled and supported with the following new Cisco IOS command-line interface (CLI) configuration and **show** commands:

- **cable high-priority-call-window** <minutes>
- **show cable calls** [interface cx/y | slot z]
- **show cable calls** [interface | slot] for the Cisco uBR 7200 Series
- **show cable calls** [interface | slot/subslot] for the Cisco uBR10012 router
- **show cable modem** [ip_addr | mac_addr | interface] **calls**

To set the call window (in minutes) during which the Cisco CMTS maintains records of Emergency 911 calls, use the **cable high-priority-call-window** command in global configuration mode. To remove the call window configuration from the Cisco CMTS, use the no form of this command:

```
cable high-priority-call-window minutes
```

```
no cable high-priority-call-window
```

For additional information about these and additional commands, refer to the following document on Cisco.com:

- *Cisco Broadband Cable Command Reference Guide*
http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
 - cable high-priority-call-window
 - show cable calls
 - show cable modem calls

The following command example configures the call window on the Cisco uBR10012 router to be 1 minute in length:

```
Router(config)# cable high-priority-call-window 1
```

To observe Emergency 911 calls made within the configured window, use the **show cable calls** command in privileged EXEC mode:

```
show cable calls
```

The following command example illustrates that one Emergency 911 call was made on the Cable8/1/1 interface on the Cisco uBR10012 router during the window set for high priority calls:

```
Router# show cable calls
```

Interface	ActiveHiPriCalls	ActiveAllCalls	PostHiPriCallCMs	RecentHiPriCMs
Cable5/0/0	0	0	0	0
Cable5/0/1	0	0	0	0
Cable5/1/0	0	0	0	0
Cable5/1/1	0	0	0	0
Cable5/1/2	0	0	0	0
Cable5/1/3	0	0	0	0
Cable5/1/4	0	0	0	0

Cable6/0/0	0	0	0	0
Cable6/0/1	0	0	0	0
Cable7/0/0	0	0	0	0
Cable7/0/1	0	0	0	0
Cable8/1/0	0	0	0	0
Cable8/1/1	1	1	0	0
Cable8/1/2	0	0	0	0
Cable8/1/3	0	0	0	0
Cable8/1/4	0	0	0	0
Total	1	1	0	0

The following command example illustrates the change on the Cisco uBR10012 router when this Emergency 911 calls ends:

Router# **show cable calls**

Interface	ActiveHiPriCalls	ActiveAllCalls	PostHiPriCallCMs	RecentHiPriCMs
Cable5/0/0	0	0	0	0
Cable5/0/1	0	0	0	0
Cable5/1/0	0	0	0	0
Cable5/1/1	0	0	0	0
Cable5/1/2	0	0	0	0
Cable5/1/3	0	0	0	0
Cable5/1/4	0	0	0	0
Cable6/0/0	0	0	0	0
Cable6/0/1	0	0	0	0
Cable7/0/0	0	0	0	0
Cable7/0/1	0	0	0	0
Cable8/1/0	0	0	0	0
Cable8/1/1	0	0	0	1
Cable8/1/2	0	0	0	0
Cable8/1/3	0	0	0	0
Cable8/1/4	0	0	0	0
Total	0	0	0	1

The following command example illustrates available information when making a voice call from the same MTA to another MTA on the same interface:

Router# **show cable calls**

Interface	ActiveHiPriCalls	ActiveAllCalls	PostHiPriCallCMs	RecentHiPriCMs
Cable5/0/0	0	0	0	0
Cable5/0/1	0	0	0	0
Cable5/1/0	0	0	0	0
Cable5/1/1	0	0	0	0
Cable5/1/2	0	0	0	0
Cable5/1/3	0	0	0	0
Cable5/1/4	0	0	0	0
Cable6/0/0	0	0	0	0
Cable6/0/1	0	0	0	0
Cable7/0/0	0	0	0	0
Cable7/0/1	0	0	0	0
Cable8/1/0	0	0	0	0
Cable8/1/1	0	2	1	1
Cable8/1/2	0	0	0	0
Cable8/1/3	0	0	0	0
Cable8/1/4	0	0	0	0
Total	0	2	1	1

The following command example illustrates available information when a voice call from the same MTA to another MTA on the same interface ends:

Router# **show cable calls**

Interface	ActiveHiPriCalls	ActiveAllCalls	PostHiPriCallCMs	RecentHiPriCMs
Cable5/0/0	0	0	0	0
Cable5/0/1	0	0	0	0
Cable5/1/0	0	0	0	0
Cable5/1/1	0	0	0	0
Cable5/1/2	0	0	0	0
Cable5/1/3	0	0	0	0
Cable5/1/4	0	0	0	0
Cable6/0/0	0	0	0	0
Cable6/0/1	0	0	0	0
Cable7/0/0	0	0	0	0
Cable7/0/1	0	0	0	0
Cable8/1/0	0	0	0	0
Cable8/1/1	0	0	0	1
Cable8/1/2	0	0	0	0
Cable8/1/3	0	0	0	0
Cable8/1/4	0	0	0	0
Total	0	0	0	1

The following example illustrates the **show cable modem calls** command on the Cisco uBR10012 router over a period of time, with changing call status information:

```
Router# scm call
```

```
Cable Modem Call Status Flags:
```

```
H: Active high priority calls
```

```
R: Recent high priority calls
```

```
V: Active voice calls (including high priority)
```

MAC Address	IP Address	I/F	Prim Sid	CMCallStatus	LatestHiPriCall (min:sec)
0000.cab7.7b04	10.10.155.38	C8/1/1/U0	18	R	0:39

```
Router# scm call
```

```
Cable Modem Call Status Flags:
```

```
H: Active high priority calls
```

```
R: Recent high priority calls
```

```
V: Active voice calls (including high priority)
```

MAC Address	IP Address	I/F	Prim Sid	CMCallStatus	LatestHiPriCall (min:sec)

The above example illustrates that call information disappears when a call ends. The following example illustrates a new Emergency 911 call on the Cisco CMTS:

```
Router# show cable modem calls
```

```
Cable Modem Call Status Flags:
```

```
H: Active high priority calls
```

```
R: Recent high priority calls
```

```
V: Active voice calls (including high priority)
```

MAC Address	IP Address	I/F	Prim Sid	CMCallStatus	LatestHiPriCall (min:sec)
0000.cab7.7b04	10.10.155.38	C8/1/1/U0	18	HV	1:30

The following example illustrates the end of the Emergency 911 call on the Cisco CMTS:

```
Router# show cable modem calls
```

```
Cable Modem Call Status Flags:
```

```
H: Active high priority calls
```

R: Recent high priority calls
 V: Active voice calls (including high priority)

MAC Address	IP Address	I/F	Prim Sid	CMCallStatus	LatestHiPriCall (min:sec)
0000.cab7.7b04	10.10.155.38	C8/1/1/U0	18	R	0:3

The following example illustrates a non-emergency voice call on the Cisco CMTS from the same MTA:

Router# **show cable modem calls**

Cable Modem Call Status Flags:
 H: Active high priority calls
 R: Recent high priority calls
 V: Active voice calls (including high priority)

MAC Address	IP Address	I/F	Prim Sid	CMCallStatus	LatestHiPriCall (min:sec)
0000.ca36.f97d	10.10.155.25	C8/1/1/U0	5	V	-
0000.cab7.7b04	10.10.155.38	C8/1/1/U0	18	RV	0:30

The following example illustrates a the end of the non-emergency voice call on the Cisco CMTS:

Router# **show cable modem calls**

Cable Modem Call Status Flags:
 H: Active high priority calls
 R: Recent high priority calls
 V: Active voice calls (including high priority)

MAC Address	IP Address	I/F	Prim Sid	CMCallStatus	LatestHiPriCall (min:sec)
0000.cab7.7b04	10.10.155.38	C8/1/1/U0	18	R	0:36

PacketCable Network Components

A PacketCable network contains a number of components. Some components are the same as those that exist in a DOCSIS 1.1 network, while other components are new entities that create the end-to-end infrastructure that the PacketCable network needs to establish calls. Wherever possible, the PacketCable components and protocols build on existing protocols and infrastructures to simplify implementation and interoperability.

- Cable modem (CM)—A customer premises equipment (CPE) device that connects to a DOCSIS 1.0 or DOCSIS 1.1 cable network. All DOCSIS cable modems provide high-speed data connectivity to the Internet, while other cable modems can provide additional features, such as telephone connectivity.
- Cable Modem Termination System (CMTS)—A headend-based router that connects a DOCSIS cable network to the IP backbone network. The CMTS controls the DOCSIS 1.1 MAC layer and enforces the quality of service (QoS) limits that the cable operator guarantees to its subscribers. A typical CMTS services between several hundred and several thousand cable modems. The Cisco uBR7246VXR and Cisco uBR10012 routers operate as the CMTS in the PacketCable network.



Note See the DOCSIS 1.1 specifications for information about CM and CMTS operations.

- Multimedia terminal adapter (MTA)—A CPE device that connects telephones and other end-user devices to the PacketCable network. The PacketCable specification defines two MTA types, an embedded MTA (E-MTA) and a standalone MTA (S-MTA). The E-MTA is an MTA integrated into a DOCSIS 1.1 cable modem, while the S-MTA is a separate MTA that requires a DOCSIS 1.1 cable modem to connect to the cable network.



Note Cisco IOS Release 12.2 BC supports only embedded MTA devices.

- Call management server (CMS)—A centrally located server that provides the signaling functions that allow MTAs to establish calls over the network. The CMS uses the Network-based call signaling (NCS) protocol to provide authentication and authorization, call routing, and support for special features such as three-way calling. A PacketCable network could have multiple CMS servers, depending on its size and complexity.



Note The CMS implements several protocols on top of the Common Open Policy Service (COPS) protocol to communicate with the rest of the PacketCable network.

- Gate controller (GC)—A server that controls the establishment of gates in the PacketCable network. A gate is a logical entity in the CMTS that ensures that a service flow is authorized for the QoS features it is requesting. A separate gate controls the upstream and downstream directions of a service flow. When a call is established, the GC instructs the CMTS to create each gate and supplies the set of authorized parameters for each gate, which the CMTS uses to authorize the QoS requests that the MTA is making for the call. The GC is also responsible for coordinating the creation of the two sets of gates at each end of the call so that the call can be authorized and established.



Note A PacketCable network can contain multiple GCs, although only one server at a time is in control of any particular call. Typically, the same workstation provides both the CMS and GC servers.

- Record keeping server (RKS)—Billing server that collects the information about each call as it is made. The RKS uses the Remote Authentication Dial-In User Service (RADIUS) protocol to collect the billing data from the CMTS and other PacketCable servers. The RKS generates a call data record (CDR) for every call and forwards that information to the appropriate application server at the service provider's data processing center for further processing.

Dynamic Quality of Service

A key feature of a PacketCable network is a dynamic quality of service (DQoS) capability that is similar to the dynamic services provided by DOCSIS 1.1. However, DOCSIS 1.1 DQoS authorizes and provisions services only in the cable network and does not reserve the resources needed to propagate a call from one endpoint to another across the network.

The PacketCable DQoS extends the DOCSIS 1.1 services across the entire network, so that resources can be dynamically authorized and provisioned from one endpoint to another. This prevents possible theft-of-service attacks and guarantees customers the services they are authorized to use.

**Note**

PacketCable 1.0 requires that DOCSIS 1.1 be used for resource reservation within the cable network for E-MTA clients. The PacketCable specifications allow the optional use of the Resource Reservation Protocol (RSVP) for S-MTA clients, but Cisco IOS Release 12.2(11)BC1 does not support RSVP for access reservations.

Two-Stage Resource Reservation Process

The PacketCable DQoS model uses a two-stage resource reservation process, in which resources are first reserved and then committed. This allows a bidirectional reservation process that ensures that resources are available at both endpoints of the connection before actually placing the call.

When an MTA makes a call request, the local CMTS communicates with the gate controller to authorize the call's resources. After the resources are authorized, the CMTS reserves the local resources while it negotiates with the remote end for the resources that are required at that end.

**Note**

The CMTS uses DOCSIS 1.1 Dynamic Service Addition (DSA) messages to reserve the resources, and then uses Dynamic Service Change (DSC) messages to commit the resources.

When all required resources are available, the local CMTS and remote CMTS both commit the resources, allowing traffic to flow. Usage accounting and billing do not begin until the remote MTA picks up and the call is actually in progress.

The DQoS model ensures that both endpoints of a call, as well as the backbone network, have reserved the same bandwidth, and that the bandwidth is reserved only while the call is in progress. When a call terminates, all portions of the network can release the call's resources and make them available for other users.

Making a Call Using DQoS

DOCSIS 1.1 networks use service flows to implement different QoS policies, but service flows exist only within the cable network. To control the service flows and to extend them across the entire network, a PacketCable network creates and maintains "gates."

A gate is a logical entity created on the CMTS at each side of a connection that authorizes and establishes a particular DQoS traffic flow. The CMTS communicates with the gate controller to coordinate the creation of matching gates at each side of the connection.

Gates are unidirectional, so separate gates are required for the downstream and upstream traffic flows. The same gate ID, however, is usually used for the downstream and upstream gates for a call. Each CMTS maintains its own set of gates, so a bidirectional traffic flow requires four gates to be created, two gates on the local CMTS and two gates on the remote CMTS.

For a typical call, gates progress through the following stages to create a DQoS traffic flow:

1. The local MTA makes a call request, and the gate controller sends a Gate-Allocation command to the CMTS, which creates a gate in response and puts it into the Allocated state.
2. The call management server, which might be the same server as the gate controller, parses the call request to translate the destination phone number into the appropriate destination gateway.
3. The gate controller verifies that the MTA making the call request is authorized for the required resources and sends a Gate-Set command to the CMTS, which puts the gate into the Authorized state.

4. The CMTS on each side of the connection reserves the local resources needed for the call, putting the gate into the Reserved state.
5. As the remote CMTS and local CMTS perform gate coordination, their respective gates get put into the Local_Committed and Remote_Committed states.
6. When both sides have reserved all required resources, each CMTS puts its gates into the Committed state, allowing traffic to flow.

Benefits

The PacketCable feature offers the following benefits to service providers and their customers:

Integrated Services on a Cable Network

PacketCable allows cable operators the ability to offer multimedia, real-time services, in addition to data connectivity, across their entire network. These services could include basic telephony with lifeline support, as well as telephony that offers competitive extended calling services. Operators can deploy new services while heavily leveraging their existing network infrastructures.

The widespread use of IP as the standard transport mechanism for data networks today is enabling many advanced Internet applications such as multimedia e-mail, real-time chat, streaming media (including music and video), and videoconferencing. The PacketCable initiative provides the network architecture for a cable operator to deliver these services quickly and economically.

Standardized Provisioning

PacketCable provides a standardized, efficient method to provision IP services for individual subscribers, because PacketCable specifications define a uniform, open, and interoperable network. Cable operators are assured of standardized provisioning and the associated lower costs of deployment.

Interoperability

Customer premises equipment (CPE) devices account for a major portion of the capital expense in deploying a VoIP solution at a cable plant. The PacketCable specifications ensure that vendors will build MTA clients that support the voice and other services that cable operators plan to deploy. Because these CPE devices are based on existing DOCSIS-compliant cable modems, time and cost of development is minimized.

Interoperability with the other components of the PacketCable network is also guaranteed because of the standards-based approach to the specifications. Any PacketCable-certified component will be able to interoperate within a network that conforms to the PacketCable standards.

Secure Architecture

Because PacketCable is built upon the security features available in DOCSIS 1.1, cable operators will be assured of networks that are secure from end to end, with a high standard of security that prevents the most common theft-of-service attacks. The comprehensive, standards-based PacketCable specifications are designed to create a network that is as secure as the public switched telephone network (PSTN).

CALEA Support

The PacketCable architecture was designed to accommodate the 1994 Communications Assistance for Law Enforcement Act (CALEA), which requires telecommunications carriers to assist law-enforcement agencies in conducting court-ordered electronic surveillance. PacketCable networks will be able to provide the two types of information that a carrier must provide, depending on the type of court order:

- Call-identifying information—The carrier must provide the call-identifying information for calls to or from an intercept target. For telephone calls, this information includes the phone numbers called by the target or calling the target.
- Call content—The carrier must provide the content of calls to or from an intercept target. For telephone calls, this real-time content is the voice conversation.

How to Configure PacketCable Operations

See the following sections for configuration tasks for the PacketCable feature. Each task is required unless otherwise identified as optional.

- [Enabling PacketCable Operation, page 13-13](#)
- [Disabling PacketCable Operation, page 13-14](#)
- [Configuring PacketCable Operation \(Optional\), page 13-15](#)
- [Enabling Both PacketCable and Non-PacketCable UGS Service Flows, page 13-16](#)
- [Verifying PacketCable Configuration, page 13-18](#)
- [Configuring RADIUS Accounting for RKS Servers, page 13-18](#)

Enabling PacketCable Operation

To enable PacketCable operation, use the following commands beginning in user EXEC mode. This is a required procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **packetcable**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.

	Command or Action	Purpose
Step 3	packetcable Example: Router(config)# packetcable Router(config)#	Enables PacketCable operation on all cable interfaces.
Step 4	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Disabling PacketCable Operation

To disable PacketCable operation, use the following commands beginning in user EXEC mode. This procedure is required only when you no longer want the Cisco CMTS to support PacketCable signaling.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no packetcable**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.

	Command or Action	Purpose
Step 3	no packetcable Example: Router(config)# no packetcable Router(config)#	Disables PacketCable operation on all cable interfaces.
Step 4	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Configuring PacketCable Operation (Optional)

To configure the different parameters that affect PacketCable operations, use the following commands beginning in user EXEC mode. All of these procedures are optional, because each parameter is set to a default that is appropriate for typical PacketCable operations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **packetcable element-id *n***
4. **packetcable gate maxcount *n***
5. **packetcable timer T0 *timer-value***
6. **packetcable timer T1 *timer-value***
7. **packetcable timer T2 *timer-value***
8. **packetcable timer T5 *timer-value***
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.

	Command or Action	Purpose
Step 3	packetcable element-id <i>n</i> Example: Router(config)# packetcable element-id 23 Router(config)#	Configures the Event Message Element ID for the Cisco CMTS. The valid range for <i>n</i> is 0 to 99999. If you do not manually configure the Element ID, the CMTS defaults to a random value between 0 and 99,999 when PacketCable operations are enabled.
Step 4	packetcable gate maxcount <i>n</i> Example: Router(config)# packetcable gate maxcount 524288 Router(config)#	Sets the maximum number of gate IDs to be allocated in the gate database on the Cisco CMTS. The valid range for <i>n</i> is 1 to 1048576, with a default value of 1048576 (which is 1024 * 1024).
Step 5	packetcable timer T0 <i>timer-value</i> Example: Router(config)# packetcable timer T0 40000 Router(config)#	Sets the T0 timer in milliseconds. The valid range is 1 to 1,000,000,000 milliseconds, with a default value of 30000 milliseconds (30 seconds).
Step 6	packetcable timer T1 <i>timer-value</i> Example: Router(config)# packetcable timer T1 300000 Router(config)#	Sets the T1 timer in milliseconds. The valid range is 1 to 1,000,000,000 milliseconds, with a default value of 200000 milliseconds (200 seconds).
Step 7	packetcable timer T2 <i>timer-value</i> Example: Router(config)# packetcable timer T2 3000 Router(config)#	Sets the T2 timer in milliseconds. The valid range is 1 to 1,000,000,000 milliseconds, with a default value of 2000 milliseconds (2 seconds).
Step 8	packetcable timer T5 <i>timer-value</i> Example: Router(config)# packetcable timer T5 1000 Router(config)#	Sets the T5 timer in milliseconds. The valid range is 1 to 1,000,000,000 milliseconds, with a default value of 500 milliseconds. Note The T5 timer should always be several times smaller than the T2 timer.
Step 9	exit Example: Router(config)# exit Router#	Exits global configuration mode.

Enabling Both PacketCable and Non-PacketCable UGS Service Flows

By default, when PacketCable operations are enabled using the **packetcable** command, cable modems must follow the PacketCable protocol when requesting Unsolicited Grant Service (UGS) service flows. This prevents DOCSIS cable modems that do not support PacketCable operations from using DOCSIS-style UGS service flows.

If you have a mixed network that contains both PacketCable and non-PacketCable DOCSIS CMs, you can use the **packetcable authorize vanilla-docsis-mta** command to enable both types of UGS service flows. This is an optional procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **packetcable**
4. **packetcable authorize vanilla-docsis-mta**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable Router#	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	packetcable Example: Router(config)# packetcable Router(config)#	Enables PacketCable operations.
Step 4	packetcable authorize vanilla-docsis-mta Example: Router(config)# packetcable authorize vanilla-docsis-mta Router(config)#	Enables the use of DOCSIS-style UGS service flow requests.
Step 5	exit Example: Router(config)# exit Router#	Exits global configuration mode.

**Tip**

Use the **show packetcable global** command to display whether non-PacketCable UGS service flows have been enabled.

Verifying PacketCable Configuration

To verify the PacketCable configuration, use the **show packetcable global** command in privileged EXEC mode, which displays whether PacketCable operations are enabled, as well as the values for the Element ID, the maximum number of gates, and the different CMTS-based DQoS timers.

```
Router# show packetcable global

Packet Cable Global configuration:
Enabled      : Yes
Element-ID: 12456
Max Gates   : 1048576
Allow non-PacketCable UGS
Default Timer value -
  T0        : 30000 msec
  T1        : 300000 msec

Router#
```

Configuring RADIUS Accounting for RKS Servers

To configure the Cisco CMTS so that it can communicate with the Record Keeping Servers (RKS servers) using the RADIUS protocol, use the following commands beginning in user EXEC mode. This is a required procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius *group-name***
5. **server {*hostname* | *ip-address*} [auth-port *udp-port*] [acct-port *udp-port*]**
6. **exit**
7. **aaa accounting network default start-stop group radius group *group-name***
8. **radius-server host {*hostname* | *ip-address*} [auth-port *port-number*] [acct-port *port-number*] [timeout *seconds*] [retransmit *retries*] key 0000000000000000**
9. **radius-server vsa send accounting**
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable Router#</p>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal Router(config)#</p>	Enters global configuration mode.
Step 3	<p>aaa new-model</p> <p>Example: Router(config)# aaa new-model Router(config)#</p>	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 4	<p>aaa group server radius <i>group-name</i></p> <p>Example: Router(config)# aaa group server radius packetcable Router(config-sg-radius)#</p>	Creates a group of RADIUS servers for authentication and enters RADIUS group configuration mode. The value of <i>group-name</i> is a unique, arbitrary string that identifies this group.
Step 5	<p>server {hostname ip-address} [auth-port udp-port] [acct-port udp-port]</p> <p>Example: Router(config-sg-radius)# server radius-server1 Router(config-sg-radius)#</p>	<p>Specifies the host name or IP address for the RADIUS server that is providing the RKS services. You can optionally specify the following:</p> <ul style="list-style-type: none"> • acct-port <i>udp-port</i> = UDP port for the accounting server. The valid range is 0 to 65536, with a default of 1812. • auth-port <i>udp-port</i> = UDP port for the authentication server. The valid range is 0 to 65536, with a default of 1813. <p>Note Repeat this command as needed to enter multiple RADIUS servers. The Cisco CMTS uses the servers in the order given with this command.</p>
Step 6	<p>exit</p> <p>Example: Router(config-sg-radius)# exit Router(config)#</p>	Exits RADIUS group configuration mode.

	Command or Action	Purpose
Step 7	<pre>aaa accounting network default start-stop group radius group group-name</pre> <p>Example:</p> <pre>Router(config)# aaa accounting network default start-stop group radius group packetcable Router(config)#</pre>	Enables AAA services using the group of RADIUS servers that are defined in the previously created group. The <i>group-name</i> parameter should be the same name specified in Step 4 .
Step 8	<pre>radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] key 0000000000000000</pre> <p>Example:</p> <pre>Router(config)# radius-server host radius-server1 key 0000000000000000 Router(config)#</pre>	<p>Specifies a RADIUS host. Use the same values for <i>hostname</i> or <i>ip-address</i> as for one of the servers specified in Step 5. If you also specified the auth-port or acct-port values in Step 5, you must also specify those here, as well. The key value is required and must be 16 ASCII zeros, as shown. You can optionally specify the following:</p> <ul style="list-style-type: none"> timeout seconds = Time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. The valid range is 1 to 1000, with a default of 5. retransmit retries = Number of times a RADIUS request is re-sent to a server, if that server is not responding or responding slowly. The valid range is 1 to 100, with a default of 3. <p>Note Repeat this command for each RADIUS server entered in Step 5.</p>
Step 9	<pre>radius-server vsa send accounting</pre> <p>Example:</p> <pre>Router(config)# radius-server vsa send accounting Router(config)#</pre>	Configures the Cisco CMTS to recognize and use accounting-related vendor-specific attributes (VSA).
Step 10	<pre>exit</pre> <p>Example:</p> <pre>Router(config)# exit Router#</pre>	Exits global configuration mode.

High Availability Stateful Switchover (SSO) for PacketCable and PacketCable MultiMedia

Cisco IOS Release 12.3(21)BC enhances high availability support that enables the synchronization of PacketCable and PacketCable MultiMedia (PCMM) gates during switchover events on the Cisco CMTS. This enhancement is enabled by default with Cisco IOS Release 12.3(21)BC and later supporting releases on the Cisco uBR10012 router and Cisco uBR7246VXR router.

This enhancement requires no additional configuration commands for line card redundancy in the Cisco N+1 Redundancy feature, nor the RPR+ Redundancy feature on the Cisco uBR10012 router. However, this functionality uses the existing per-interface HCCP commands that are used to associate the Working and Protect interfaces in the case of N+1 Redundancy.

This feature introduces a new debug command, however, to troubleshoot HCCP information specific to PacketCable and PCMM gates. The new command is **debug packetcable hccp**.

Debugging High Availability Stateful Switchover for PacketCable and PCMM

The new **debug packetcable hccp** command and procedure, introduced in Cisco IOS Release 12.3(21)BC, enables debugging and troubleshooting functions in cases where PacketCable and PCMM are supported in either or both N+1 Redundancy or RPR+ Redundancy on the Cisco CMTS. This command supports additional information displayed in the enhanced **show packetcable gate** summary command.

Currently after switchover, if we do a "show packetcable gate summary" we see no Gates, however, after the implementation of this feature we will see that the Gates exists. Also, after the implementation of this feature we will be able to connect to the standby LC and check if the gate information has been synchronized using the existing "show packetcable gate summary" command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **debug packetcable hccp**
4. **Ctrl-Z**
5. **show packetcable gate summary**
6. **show hccp brief**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 3	<code>debug packetcable hccp</code> Example: Router(config)# <code>debug packetcable hccp</code>	Enables debugging for gate synchronization within HCCP N+1 Redundancy and RPR+ Redundancy when they are operational on the network. To disable debugging, use the no form of this command:
Step 4	<code>Ctrl-Z</code> Example: Router(config)# <code>Ctrl^Z</code> Router#	Returns to Privileged EXEC mode.
Step 5	<code>show packetcable gate summary</code> Example: Router# show packetcable gate summary	Displays PacketCable HCCP information, supporting gate synchronization status and switchover information.
Step 6	<code>show hccp brief</code> Example: Router# show hccp brief	Displays general information pertaining to N+1 Redundancy on the Cisco CMTS.

Examples

The following abbreviated example illustrates PacketCable gate synchronization information when debugging is enabled with the `debug packetcable hccp` command:

```
GateID   i/f      SubscriberID  GC-Addr      State      Type  SFID(us) SFID(ds)

Total number of gates = 0
Total Gates committed(since bootup or clear counter) = 625
```

The following example illustrates additional information that tracks the activity as a call is made:

```
10:58:09: PktCbl(hccp): Grp 1 sync type=add from Cable5/0/0
10:58:09: PktCbl(hccp): Sync gate-add 38010 len=308
10:58:10: PktCbl(hccp): Grp 1 sync type=add from Cable5/0/0
10:58:10: PktCbl(hccp): Sync gate-add 5242 len=308
10:58:10: Pktcbl(hccp): Gate=5242 written to service flow dir US SFID=1233
10:58:10: Pktcbl(hccp): Gate=5242 written to service flow dir DS SFID=1234
10:58:10: PktCbl(hccp): Grp 1 sync type=update from Cable5/0/0
10:58:10: PktCbl(hccp): Sync gate-update 5242 len=24
10:58:10: PktCbl(hccp): Grp 1 sync type=update from Cable5/0/0
10:58:10: PktCbl(hccp): Sync gate-update 5242 len=24
```

```

10:58:10: PktCbl(hccp): Gate=38010 written to service flow dir US SFID=1235
10:58:32: PktCbl(hccp): Parse add gate 38010 sync_len=300 from 5/0 status 2
10:58:32: PktCbl(hccp): Parse add gate 5242 sync_len=300 from 5/0 status 2
10:58:32: PktCbl(hccp): Parse update gate 5242 sync_len=16
10:58:32: PktCbl(hccp): Parse update gate 5242 sync_len=16
10:58:32: PktCbl(hccp): Parse update gate 38010 sync_len=16
10:58:32: PktCbl(hccp): Parse update gate 38010 sync_len=16
10:58:10: PktCbl(hccp): Gate=38010 written to service flow dir DS SFID=1236
10:58:10: PktCbl(hccp): Grp 1 sync type=update from Cable5/0/0
10:58:10: PktCbl(hccp): Sync gate-update 38010 len=24
10:58:10: PktCbl(hccp): Grp 1 sync type=update from Cable5/0/0
10:58:10: PktCbl(hccp): Sync gate-update 38010 len=24
10:58:11: PktCbl(hccp): Gate=38010 written to service flow dir US SFID=1235
10:58:11: PktCbl(hccp): Gate=38010 written to service flow dir DS SFID=1236
10:58:11: PktCbl(hccp): Grp 1 sync type=update from Cable5/0/0
10:58:11: PktCbl(hccp): Sync gate-update 38010 len=24
10:58:11: PktCbl(hccp): Gate=5242 written to service flow dir US SFID=1233
10:58:11: PktCbl(hccp): Gate=5242 written to service flow dir DS SFID=1234
10:58:11: PktCbl(hccp): Grp 1 sync type=update from Cable5/0/0
10:58:11: PktCbl(hccp): Sync gate-update 5242 len=24
10:58:34: PktCbl(hccp): Parse update gate 38010 sync_len=16
10:58:34: PktCbl(hccp): Parse update gate 5242 sync_len=16

***** CALL IS ACTIVE **** SHOW GATE ON PRE *****
sch_3#gate
GateID      i/f      SubscriberID  GC-Addr      State      Type  SFID(us)  SFID(ds)
5242        Ca5/0/0  7.7.1.254    1.10.90.1    COMMIT    DQoS  1233      1234
38010       Ca5/0/0  7.7.1.252    1.10.90.1    COMMIT    DQoS  1235      1236

Total number of gates = 2
Total Gates committed(since bootup or clear counter) = 627

```

The following example illustrates output of the show hccp command:

```

Router# show hccp brief

Interface Config  Grp Mbr Status          WaitToResync  WaitToRestore
Ca5/0/0    Working  1  1  active          never
Ca8/0/0    Protect  1  1  standby
Ca8/0/0    Protect  1  2  non-functional
Ca8/1/0    Protect  3  1  non-functional
Ca8/1/1    Protect  4  1  non-functional
sch_3#

```

Troubleshooting Tips

If the Connection between a PacketCable CMS and the Cisco CMTS is not completely established, and the PacketCable CMS does not correctly terminate the session by sending a TCP FIN message, the connection otherwise shows a COPS server in the output of the **show cops server** command.

What to Do Next

For additional information, refer to the following documents on Cisco.com:

- *N+1 Redundancy for the Cisco CMTS*
http://www.cisco.com/en/US/tech/tk86/tk804/technologies_tech_note09186a0080204374.shtml
- *Route Processor Redundancy Plus for the Cisco uBR10012 Router*

http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/u10k_rtpro_red_plus_ps2209_TS_D_Products_Configuration_Guide_Chapter.html

- *Cisco Broadband Cable Command Reference Guide*

http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

PacketCable Client Accept Timeout

Cisco IOS Release 12.3(17a)BC introduces support for setting timeout values for COPS Telnet connections on the Cisco CMTS, and for clearing COPS telnet sessions.

Network or Cisco CMTS telnet errors can cause incomplete COPS sessions to be created. This new timeout timer enables the clearing and cleaning of allocated resources for the stale COPS Telnet sessions on the Cisco CMTS. This feature supports COPS for PacketCable on the Cisco CMTS.

The timeout timer applies to each COPS Telnet connection on the Cisco CMTS, and expiration of this timeout setting triggers the termination of the Telnet session and clears supporting resources on the Cisco CMTS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **packetcable timer client-accept *seconds***
4. **clear cops connection**
5. **Ctrl-Z**
6. **show cops server**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<pre>packetcable timer client-accept seconds</pre> <p>Example: Router(config)# packetcable timer client-accept 1800</p>	<p>Sets the timeout timer for Telnet COPS sessions on the Cisco CMTS. To remove this timeout timer, use the no form of this command.</p> <p>no packetcable timer client-accept</p> <ul style="list-style-type: none"> <i>seconds</i>—The timeout value in seconds, beyond which the Telnet COPS session is terminated, and associated resources on the Cisco CMTS are cleared. Range from 300 seconds (five minutes) to 1800 seconds (30 minutes).
Step 4	<pre>clear cops connection</pre> <p>Example: Router(config)# clear cops connection</p>	<p>Clears all COPS Telnet sessions and associated resources on the Cisco CMTS.</p>
Step 5	<pre>Ctrl-Z</pre> <p>Example: Router(config)# Ctrl^Z Router#</p>	<p>Returns to Privileged EXEC mode.</p>
Step 6	<pre>show cops server</pre> <p>Example: Router# show cops server</p>	<p>Displays COPS server and connectoin status.</p>

Examples

The following example sets the client accept timer to 30 minutes:

```
Router(config)# packetcable timer client-accept 1800
```

Troubleshooting Tips

If the Connection between a PacketCable CMS and the Cisco CMTS is not completely established, and the PacketCable CMS does not correctly terminate the session by sending a TCP FIN message, the connection otherwise shows a COPS server in the output of the **show cops server** command.

What to Do Next

For additional information, refer to the following documents on Cisco.com:

- COPS Engine Operation on the Cisco CMTS*

http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmmts_cops_eng_op_ps2209_TSD_Products_Configuration_Guide_Chapter.html
- Cisco Broadband Cable Command Reference Guide*

http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Monitoring and Maintaining PacketCable Operations

To display and maintain information about current PacketCable operations, use one or more of the following commands:

Command	Purpose
Router# <code>show packetcable gate counter commit</code>	Displays the total number of gates that the Cisco CMTS has put into the Committed state since the Cisco CMTS was last reset or since the counter was last cleared.
Router# <code>clear packetcable gate counter commit</code>	Clears the total number of gates that the Cisco CMTS has put into the Committed state, setting the counter to zero.
Router# <code>show packetcable gate [downstream upstream] {summary gate-id}</code>	<p>Displays information about one or more gates that are currently active on the Cisco CMTS. You can display a summary for all currently active gates, for all downstream or all upstream gates, or you can display detailed information about a specific gate.</p> <ul style="list-style-type: none"> • downstream = Displays only gates for the downstream direction. • upstream = Displays only gates for the upstream direction. • summary = Displays summary information for the gates, including the gate ID, subscriber IP address, gate controller IP address, and current state. • <i>gate-id</i> = Displays detailed information for a specific gate ID. Both downstream and upstream gates are displayed unless you also specify either the downstream or upstream options.
Router# <code>show packetcable event {df-group radius-server rks-group}</code>	<p>Displays information the PacketCable event message (EM) servers:</p> <ul style="list-style-type: none"> • df-group—Displays information about the Communications Assistance for Law Enforcement Act (CALEA) Delivery Function (DF) server groups that are configured on the router. • radius-server—Displays information about the EM Remote Authentication Dial In User Service (RADIUS) servers that are configured on the router. • rks-group—Displays information about the Record Keeping Server (RKS) groups that are configured on the router.

Configuration Examples for PacketCable

This section provides the following configuration examples:

- [Typical PacketCable Configuration](#)

Typical PacketCable Configuration

This section provides a typical configuration for a Cisco uBR7246VXR universal broadband router that has been configured for PacketCable operations, using default parameters. To use this configuration, you must change the IP addresses for the RADIUS and RKS servers to match the addresses for the servers in your network.

```

!
version 12.2
no parser cache
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service internal
service udp-small-servers max-servers no-limit
service tcp-small-servers max-servers no-limit
!
hostname Router
!
no logging rate-limit
aaa new-model
!
!
aaa group server radius a
  server 10.9.62.12 auth-port 1813 acct-port 1812
  server 10.9.62.13 auth-port 1813 acct-port 1812
!
aaa accounting network default start-stop group radius group a
aaa session-id common
enable password <delete>
!
cable modulation-profile 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 short 6 75 6 8 16qam scrambler 152 no-diff 144 shortened uw8
cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw8
cable modulation-profile 5 request 0 16 2 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 5 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 5 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 5 short 6 78 7 8 16qam scrambler 152 no-diff 144 shortened uw16
cable modulation-profile 5 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw16
cable qos profile 5 max-burst 1200
cable qos profile 5 max-downstream 2000
cable qos profile 5 max-upstream 128
cable qos profile 5 priority 5
cable qos profile 5 privacy
cable qos profile 7 guaranteed-upstream 87
cable qos profile 7 max-upstream 87
cable qos profile 7 privacy
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable qos permission enforce 5

```

```

cable time-server
no cable privacy accept-self-signed-certificate
ip subnet-zero
!
!
no ip domain-lookup
ip domain-name cisco.com
ip host tftp 10.8.8.8
ip host cnr 10.9.62.17
!
packetcable
packetcable element-id 12456
!
!
!
interface Tunnel0
 ip address 10.55.66.3 255.255.255.0
 load-interval 30
 tunnel source FastEthernet1/0
 tunnel destination 172.27.184.69
!
interface Tunnel10
 ip address 10.0.1.1 255.255.0.0
!
interface FastEthernet0/0
 ip address 10.9.60.10 255.255.0.0
 no ip redirects
 no ip mroute-cache
 full-duplex
!
interface FastEthernet1/0
 ip address 172.22.79.44 255.255.254.0
 no ip redirects
 no ip mroute-cache
 full-duplex
!
interface Cable3/0
 ip address 10.3.1.33 255.255.255.0 secondary
 ip address 10.4.1.1 255.255.255.0 secondary
 ip address 10.4.1.33 255.255.255.0 secondary
 ip address 10.3.1.1 255.255.255.0
 ip helper-address 10.9.62.17
 load-interval 30
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 55500000
 cable upstream 0 modulation-profile 2
 no cable upstream 0 shutdown
 cable upstream 1 frequency 12000000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 data-backoff automatic
 cable upstream 1 modulation-profile 2
 cable upstream 1 shutdown
 cable upstream 2 frequency 16000000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000
 cable upstream 2 data-backoff automatic
 cable upstream 2 modulation-profile 2
 no cable upstream 2 shutdown
 cable upstream 3 frequency 20000000
 cable upstream 3 power-level 0

```

```
cable upstream 3 channel-width 3200000
cable upstream 3 data-backoff automatic
cable upstream 3 modulation-profile 2
no cable upstream 3 shutdown
cable upstream 4 frequency 24000000
cable upstream 4 power-level 0
cable upstream 4 channel-width 3200000
cable upstream 4 data-backoff automatic
no cable upstream 4 shutdown
cable upstream 5 frequency 28000000
cable upstream 5 power-level 0
cable upstream 5 channel-width 3200000
cable upstream 5 data-backoff automatic
cable upstream 5 modulation-profile 2
no cable upstream 5 shutdown
cable dhcp-giaddr policy
!
router eigrp 48849
 network 1.0.0.0
 network 10.0.0.0
 auto-summary
 no eigrp log-neighbor-changes
!
ip default-gateway 10.9.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 172.22.78.1
ip route 10.8.0.0 255.255.0.0 10.9.0.1
ip route 192.168.80.0 255.255.255.0 Tunnel0
ip route 192.168.80.0 255.255.255.0 172.27.184.69
ip route 10.255.254.254 255.255.255.255 10.9.0.1
no ip http server
ip pim bidir-enable
!
!
cdp run
!
!
radius-server host 10.9.62.12 auth-port 1813 acct-port 1812 key 0000000000000000
radius-server retransmit 3
radius-server vsa send accounting
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
 session-timeout 33
 exec-timeout 0 0
 password <deleted>
!
ntp clock-period 17179976
ntp server 1.9.35.8
end
```

Prerequisites for PacketCable Multimedia Operations

Cisco uBR7246VXR Router

- To support PacketCable operations on the Cisco uBR7246VXR universal broadband router, the router must be running Cisco IOS Release 12.3(13a)BC or a later 12.3 BC release.
- To support PacketCable Multimedia and the Communications Assistance for Law Enforcement Act (CALEA) intercept capabilities, a Cisco uBR7246VXR broadband router must be running Cisco IOS Release 12.(13) or a later 12.3 BC release.

Cisco uBR10012 Router

- To support PacketCable Multimedia operations on the Cisco uBR10012 universal broadband router, the router must be running Cisco IOS Release 12.3(13a)BC or a later 12.3BC release.
- To support PacketCable Multimedia and the Communications Assistance for Law Enforcement Act (CALEA) intercept capabilities, a Cisco uBR10012 router must be running Cisco IOS Release 12.3(13a)BC or a later 12.3 BC release.

Restrictions for PacketCable Multimedia Operations

Beta and FCS restrictions pending confirmation and description, and the lack of Caveats cited here does not imply that such restrictions do not exist.

Information About PacketCable Multimedia Operations

PacketCable Multimedia for the Cisco CMTS is a powerful implementation of CableLabs® standards for PacketCable Multimedia and DOCSIS 1.1. PacketCable Multimedia provides enhanced Quality of Service (QoS) for multimedia applications, voice, and bandwidth-intensive services over a DOCSIS 1.1 network.

The Cisco CMTS supports DOCSIS QoS for SIP-based telephones and SIP Video Phones, Bandwidth-on-Demand applications, and network-based gaming applications, all of which place extensive bandwidth demands on the network.

At the time of publication, Cisco IOS Release 12.3(13a)BC supports the following CableLabs standards for PacketCable Multimedia:

- *PacketCable™ Multimedia Specification*, PKT-SP-MM-I02-040930, **Issued** status
- *PacketCable™ Multimedia Architecture Framework Technical Report*, PKT-TR-MM-ARCH-V01-030627, **Released** status

Both of these industry standard publications are available at the following CableLabs website, with much additional information about PacketCable Multimedia:

<http://www.cablelabs.com/packetcable/specifications/multimedia.html>

This section provides information about the following aspects of PacketCable Multimedia for the Cisco CMTS and Cisco IOS Release 12.3(13a)BC, emphasizing PCMM components that are configured with the Cisco IOS command-line interface later in this document:

- [PCMM Overview](#), page 13-32
 - [PCMM Enhancements over PacketCable 1.x](#), page 13-32
 - [PCMM and Additional Software Features on the Cisco CMTS](#), page 13-32
- [PCMM Gates](#), page 13-33
 - [PCMM Gate Overview and PCMM Dynamic Quality of Service](#), page 13-33
 - [PCMM Persistent Gate](#), page 13-33
 - [PCMM Interoperability with PacketCable 1.x Voice Services Module](#), page 13-33
- [PCMM Interfaces](#), page 13-34
 - [PCMM to COPS Interface](#), page 13-34
 - [PCMM and Distributed Cable Interface Line Cards](#), page 13-34

PCMM Overview

PCMM Enhancements over PacketCable 1.x

PacketCable Multimedia (PCMM) is a service delivery framework that leverages and uses as much of existing PacketCable 1.x deployments and functionality as possible. Furthermore, PCMM offers powerful enhancements to the VoIP service delivery framework with straightforward CLI implementation. The key enhancements offered by PCMM include the following:

- PCMM time- and volume-based network resource authorizations are based on DOCSIS 1.1 Quality of Service (QoS) mechanisms.
- PCMM uses event-based network resource auditing and management functions.
- PCMM provides a secure infrastructure that protects all interfaces at appropriate levels.
- PCMM enhances the pre-authorization model from PacketCable 1.x, in that PCMM Gate installation and management is supplemented with service flow creation, modification and deletion functions. Together, these provide delivery of secure, network-based Quality of Service (QoS).

PCMM for the Cisco CMTS introduces new or enhanced commands for PCMM configuration, testing, and monitoring. For additional information about configuring or monitoring PCMM on the Cisco CMTS, refer to the following sections:

- “How to Configure PCMM Operations” section on page 13-35
- “Monitoring and Maintaining PCMM Operations” section on page 13-37

PCMM and Additional Software Features on the Cisco CMTS

PacketCable and PCMM with Admission Control

A PacketCable or PacketCable Multimedia (PCMM) network contains a number of components that benefit from Admission Control Quality of Service. Admission Control manages and optimizes QoS for PacketCable and PCMM in these ways:

- DOCSIS 1.1 QoS for voice and data
- Cable modem registration
- Call management servers (CMS)
- Gateway controllers (GC)
- Record keeping servers (RKS)
- Video Telephony

When configuring Admission Control with either PacketCable or PCMM, PacketCable or PCMM must be fully operational on the Cisco CMTS headend prior to gaining the benefits from Admission Control.

For Admission Control configuration information, refer to the following documents on Cisco.com:

- *Admission Control for the Cisco Cable Modem Termination System:*
http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_adm.html
- *Service Flow Admission Control for the Cisco Cable Modem Termination System*
http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_svflw_ad_ctl_ps2209_TSD_Products_Configuration_Guide_Chapter.html

PCMM and High Availability Features on the Cisco CMTS

In Cisco IOS Release 12.3(13a)BC, High Availability on the Cisco CMTS only accommodates synchronization of service flows created for the PCMM applications. There is currently no PCMM Gate synchronization that fully supports PCMM High Availability features such as HCCP N+1 Redundancy and Route Processor Redundancy Plus (RPR+) on the Cisco CMTS. Such HA functionality will be enabled for PCMM in upcoming Cisco IOS releases.

PCMM Gates

PCMM Gate Overview and PCMM Dynamic Quality of Service

A PacketCable 1.x gate defines Quality of Service (QoS) parameters and policy-based authorization for subscribers, and a specific envelope of network resources. A PacketCable 1.x gate also maintains classifiers for originating and terminating IP addresses and ports. Combined, these define and limit the associated QoS-enhanced flow.

PacketCable 1.x defines a pre-authorization model. PC gates are created and installed at the Cisco CMTS prior to network resource reservation or activation requests. This process, termed Gate Control, is managed through a COPS-based policy interface on the Cisco CMTS.

In PCMM, this COPS-based interface is enhanced for QoS life-cycle management. PCMM gates maintain service flow creation, modification and deletion functions to provide for network-based QoS. Multiple PCMM gates and service flow policies can be maintained on the Cisco CMTS at a given time, and these PCMM gates are fully interoperable with PacketCable 1.x gates.

When a cable modem subscriber requests bandwidth for a network-intensive application, the network Policy Server sends a gate-set message to the Cisco CMTS. This message contains QoS, service flow, and billing information for this subscriber. This gate profile information is maintained on the Cisco CMTS, to include PCMM gate states and PCMM state transitions.

The Cisco CMTS initiates service flows with cable modems, and optimizes DOCSIS resource availability on the Cisco CMTS for bandwidth-intensive service flows characteristic to PCMM.

PCMM Persistent Gate

Cisco IOS Release 12.3(13a)BC supports the Persistent Gate feature for PacketCable Multimedia. Persistent Gate is a feature by which PCMM gate information is maintained for cable modems that go offline. Gate information is quickly enabled once a cable modem returns online. When a cable modem returns online, the Cisco CMTS scans PCMM gates previously stored, and initiates service to the cable modem according to the respective PCMM gate. The newly re-enabled service maintains traffic support profiles for that gate, and allocates DOCSIS resources according to the newly online subscriber.

PCMM Interoperability with PacketCable 1.x Voice Services Module

The Cisco CMTS maintains the PC and PCMM Gate databases separately and independently. Information for either is available with multiple **show** commands.

PCMM Interfaces

PCMM optimizes the IPC handshake between the cable interface line card and the Network Processing Engine (NPE) for the Cisco uBR7246VXR router, or the Route Processor (RP) for the Cisco uBR10012 router. Additional PCMM interface changes from PacketCable 1.x include the handling for COPS interface and distributed cable interface line cards.

PCMM to COPS Interface

PCMM differs from PacketCable 1.x in that COPS sessions on PCMM use TCP port number 3918 by default. PC uses the DQoS specification for TCP port requirements and COPS sessions.

When the PCMM module initializes for the first time, a PCMM registry is added to the cable interface line card and the route processor. The PCMM module also registers the PCMM COPS client with the COPS layer on the Cisco CMTS.

PCMM and Distributed Cable Interface Line Cards

As with PacketCable 1.x, PCMM uses IPC messages for voice support. When PCMM gates are created on the Network Processing Engine (NPE) or Route Processor (RP), the PCMM gate parameters are sent to cable interface line cards. IPC maintains all communication between the NPE or RP, and the cable interface line cards.

Event messaging is used with PCMM to support billing information based on gate-set messages. Event messaging for distributed cable interface line cards originates from the line cards, based on the success of DSX operation.

The PCMM module also registers the PCMM COPS client with the COPS layer.

How to Configure PCMM Operations

This section describes the following configuration procedures for PCMM on the Cisco CMTS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **packetcable multimedia**
4. **packetcable authorize vanilla-docsis-mta**
5. **packetcable gate maxcount**
6. **packetcable timer multimedia T1**
7. **clear packetcable gate counter commit** (optional)
8. **Ctrl-Z**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	packetcable multimedia Example: Router(config)#	Enables and displays PacketCable Multimedia processing on the Cisco CMTS. This command also starts or stops listening to PCMM COPS messages received from the PCMM Policy Server.
Step 4	packetcable authorize vanilla-docsis-mta Example: Router(config)#	Allows non-DQoS MTAs to send DOCSIS DSX messages.
Step 5	packetcable gate maxcount <n> Example: Router(config)#	Sets the maximum number of PCMM gates in the gate database. <ul style="list-style-type: none"> • <i>n</i>—Value specifies the maximum number of gates that can be allocated on the Cisco CMTS.
Step 6	packetcable timer multimedia T1 Example: Router(config)#	Sets the default timeout value for T1 timer used in PCMM gate processing. <ul style="list-style-type: none"> • <i>msec</i>—Values are in milliseconds, between 1 and 1000000000.

	Command or Action	Purpose
Step 7	<pre>clear packetcable gate counter commit [dqos multimedia]</pre> <p>Example: Router(config)#</p>	(Optional) Clears the specified PCMM gate counter. <ul style="list-style-type: none"> • dqos—Clears PC DQoS gate counters. • multimedia—Clears PCMM gate counters.
Step 8	<pre>Ctrl-Z</pre> <p>Example: Router(config)# Ctrl-Z Router#</p>	Returns to privileged EXEC mode.

What to Do Next

Once PCMM is enabled on the network, much additional information and status can be gained with monitoring, debugging, or testing commands and associated procedures. Refer to the following sections in this document for additional information:

- [“Monitoring and Maintaining PCMM Operations” section on page 13-37](#)
- [“Configuration Examples for PacketCable Multimedia” section on page 13-37](#)

Monitoring and Maintaining PCMM Operations

This section describes two flexible procedures for monitoring and testing PCMM operations on the network, once configured with the “[How to Configure PCMM Operations](#)” section on page 13-35. This section contains two procedures for monitoring and maintaining PCMM operations:

- [Using Debug Commands with PCMM, page 13-37](#)
- [Using Test Commands with PCMM, page 13-37](#)

Until this section is populated, refer to **debug**, **show** and **test** commands available in the *Cisco IOS CMTS Cable Command Reference*.

Using Debug Commands with PCMM

This topic describes the use of **debug** commands for PCMM, as supported by Cisco IOS Release 12.3(13a)BC. This sequence of debugging steps is flexible, and can be adjusted according to the troubleshooting needs for PCMM network components.

Until this section is populated, refer to **debug**, **show** and **test** commands available in the *Cisco IOS CMTS Cable Command Reference*.

Using Test Commands with PCMM

This topic describes the use of **debug** commands for PCMM, as supported by Cisco IOS Release 12.3(13a)BC. This sequence of testing steps is flexible, and can be adjusted according to the PCMM or network components to be tested.

Until this section is populated, refer to **debug**, **show** and **test** commands available in the *Cisco IOS CMTS Cable Command Reference*.

Configuration Examples for PacketCable Multimedia

Refer to examples available with the command documentation in the *Cisco IOS CMTS Cable Command Reference*.

Additional References

For additional information related to PacketCable operations, refer to the following references:

Related Documents

Related Topic	Document Title
AAA and RADIUS Configuration	For complete information on configuring the AAA and RADIUS servers, which are required for communication with the RKS servers, refer to the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2 at the following URL: http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html
CMTS commands	<i>Cisco IOS CMTS Cable Command Reference</i> http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
DHCP Configuration	To configure the DHCP server onboard the Cisco CMTS, see the “Configuring DHCP” chapter in the IP Addressing Services section of the <i>Cisco IOS IP and IP Routing Configuration Guide</i> , Release 12.2 at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/fipr_c.html For information on all DHCP commands, see the “DHCP Commands” chapters in the <i>Cisco IOS IP Addressing Services Command Reference</i> , Release 12.2 at the following URL: http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html
DOCSIS 1.1	To configure the Cisco uBR7200 series router for DOCSIS 1.1 operations, see the the following URL: http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_do cs.html
NTP or SNTP Configuration	To configure the Cisco CMTS to use Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) to set its system clock, see the “Performing Basic System Management” chapter in the “System Management” section of the <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> , Release 12.2, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/ffun_c.html

Standards

Standards ¹	Title
PKT-EM-I03-011221	<i>PacketCable™ Event Message Specification</i>
PKT-SP-DQOS-I03-020116	<i>PacketCable™ Dynamic Quality-of-Service Specification</i>
PKT-SP-EC-MGCP-I04-011221	<i>PacketCable™ Network-Based Call Signaling Protocol Specification</i>
PKT-SP-ESP-I01-991229	<i>PacketCable™ Electronic Surveillance Specification</i>
PKT-SP-ISTP-I02-011221	<i>PacketCable™ Internet Signaling Transport Protocol (ISTP) Specification</i>
PKT-SP-PROV-I03-011221	<i>PacketCable™ MTA Device Provisioning Specification</i>
PKT-SP-SEC-I05-020116	<i>PacketCable™ Security Specification</i>
PKT-TR-ARCH-V01-991201	<i>PacketCable™ 1.0 Architecture Framework Technical Report</i>
Note The PacketCable 1.0 specifications are available on the Packetcable website at http://www.cablelabs.com/packetcable/specifications/ .	
SP-BPI+-I08-020301	<i>Baseline Privacy Interface Plus Specification</i>
SP-RFIV1.1-I09-020830	<i>Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1</i>

1. Not all supported standards are listed.

MIBs

MIBs ¹	MIBs Link
No new or changed MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

1. Not all supported MIBs are listed.

RFCs

RFCs ¹	Title
RFC 1321	<i>The MD5 Message-Digest Algorithm</i>
RFC 1510	<i>The Kerberos Network Authentication Service (V5)</i>
RFC 2138	<i>Remote Authentication Dial In User Service (RADIUS)</i>
RFC 2205	<i>Resource ReSerVation Protocol (RSVP)</i>
RFC 2327	<i>SDP: Session Description Protocol</i>
RFC 2748	<i>The COPS (Common Open Policy Service) Protocol</i>

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 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/cisco/web/support/index.html