Configuring PacketCable on the Cisco uBR7200 Series Universal Broadband Router

Note This document has been superseded by the *Packetcable for the Cisco CMTS* chapter in the *Cisco CMTS Feature Guide*, which is at the following URL:

http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_pkcb.html

Feature History

Release	Modification
12.2(8)BC2	This feature was introduced on the Cisco uBR7200 series router.
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 uBR7200 series 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.

This document describes how to configure the Cisco uBR7200 series router for PacketCable operations for Cisco IOS Release 12.2(11)BC1. It contains the following major sections:

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.

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 uBR7200 series router operates as the CMTS in a 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 The current PacketCable specifications support 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

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.

Restrictions

- Cisco IOS Release 12.2(11)BC1 supports version 3 of the PacketCable DQoS specification (PKT-SP-DQOS-I03-020116).
- Supports only embedded MTA (E-MTA) clients.

Related Features and Technologies

The PacketCable specifications are built upon the DOCSIS 1.1 specifications for data and voice IP traffic over HFC cable networks.

Related Documents

AAA and RADIUS Configuration

For complete information on configuring the AAA and RADIUS servers, which are required for communication with the RKS servers, see the "Authentication, Authorization, and Accounting (AAA)" chapter in the *Cisco IOS Security Configuration Guide*, Release 12.2 at the following URL:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

Cable Command Reference Guide

For syntax and usage information on the cable-specific commands used in this chapter, see the "Cisco Cable Modem Termination System Commands" chapter of the *Cisco Broadband Cable Command Reference Guide* at the following URL:

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 and Services" section of the *Cisco IOS IP and IP Routing Configuration Guide*, 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" chapter in the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2 at the following URL:

http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfipadr.html

DOCSIS 1.1

To configure the Cisco uBR7200 series router for DOCSIS 1.1 operations, see the **DOCSIS 1.1 for Cisco uBR7200 Series Universal Broadband Routers** document at the following URL:

http://www.cisco.com/en/US/docs/cable/cmts/feature/DOCSIS11.html

NTP or SNTP Configuration

For information on configuring 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 *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*, at the following URL:

http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/ffun_c.html

Supported Platforms

- Cisco uBR7200 series universal broadband routers

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

https://tools.cisco.com/RPF/register/register.do

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

- *PacketCable™ 1.0 Architecture Framework Technical Report*, pkt-tr-arch-v01-991201
- *PacketCable™ Dynamic Quality-of-Service Specification*, PKT-SP-DQOS-I03-020116
- *PacketCable™ Network-Based Call Signaling Protocol Specification*, PKT-SP-EC-MGCP-I04-011221
- *PacketCable™ Event Message Specification*, PKT-EM-I03-011221
- *PacketCable™ Internet Signaling Transport Protocol (ISTP) Specification*, PKT-SP-ISTP-I02-011221
- *PacketCable™ MTA Device Provisioning Specification*, PKT-SP-PROV-I03-011221
- *PacketCable™ Security Specification*, PKT-SP-SEC-I05-020116

- *PacketCable™ Electronic Surveillance Specification*, PKT-SP-ESP-I01-991229
- *DOCSIS 1.1 specification* SP-RFIv1.1-I08-020301
- *Baseline Privacy Interface Plus Specification* SP-BPI+-I08-020301
- *International Telecommunications Union (ITU) X.509 Version 3.0* standard

Note The PacketCable 1.0 specifications are available on the Packetcable website at http://www.cablelabs.com/specifications/.

MIBs

- 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://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

https://tools.cisco.com/RPF/register/register.do

RFCs

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

Prerequisites

To support PacketCable operations, the Cisco uBR7200 series universal broadband router must be running Cisco IOS Release 12.2(8)BC2 or a later 12.2 BC release.

Configuration Tasks

See the following sections for configuration t asks for the PacketCable feature. Each task in the list is required unless otherwise identified as optional.

Enabling PacketCable Operation

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

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# packetcable`	Enables PacketCable operation on all cable interfaces.
Step 3	`Router(config)# exit`	Exits global configuration mode.

Disabling PacketCable Operation

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

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# no packetcable`	Disables PacketCable operation on all cable interfaces.
Step 3	`Router(config)# exit`	Exits global configuration mode.

Configuring PacketCable Operation

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

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# packetcable element-id n`	Configures the Event Message Element ID for the Cisco CMTS. The valid range for n 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 3	`Router(config)# packetcable gate maxcount n`	Sets the maximum number of gate IDs to be allocated in the gate database on the Cisco CMTS. The valid range for *n* is 1 to 1048576, with a default value of 1048576 (which is 1024 * 1024).
Step 4	`Router(config)# packetcable timer T0 timer-value`	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 5	`Router(config)# packetcable timer T1 timer-value`	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 6	`Router(config)# packetcable timer T2 timer-value`	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 7	`Router(config)# packetcable timer T5 timer-value`	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 8	`Router(config)# exit`	Exits global configuration mode.

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
  T2      : 2000 msec
  T5      : 500 msec
Router#
```

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.

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# packetcable`	Enables PacketCable operations.
Step 3	`Router(config)# packetcable authorize vanilla-docsis-mta`	Enables the use of DOCSIS-style UGS service flow requests.
Step 4	`Router(config)# exit`	Exits global configuration mode.

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

Configuring RADIUS Accounting for RKS Servers

To configure the Cisco CMTS so it can communicate with the RKS servers using the RADIUS protocol, use the following commands beginning in privileged EXEC mode. This is a required procedure.

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 3	`Router(config)# aaa group server radius` *group-name*	Creates a group of RADIUS servers for authentication and enters RADIUS group configuration mode. The value of *group-name* is a unique, arbitrary string that identifies this group.
Step 4	`Router(config-sg-radius)# server {`*hostname* `|` *ip-address*`} [auth-port` *udp-port*`] [acct-port` *udp-port*`]`	Specifies the host name or IP address for the RADIUS server that is providing the RKS services. You can optionally specify the following: • **acct-port** *udp-port* = UDP port for the accounting server. The valid range is 0 to 65536, with a default of 1812. • **auth-port** *udp-port* = UDP port for the authentication server. The valid range is 0 to 65536, with a default of 1813. **Note** Repeat this command as needed to enter multiple RADIUS servers. The Cisco CMTS uses the servers in the order given with this command.
Step 5	`Router(config-sg-radius)# exit`	Exits RADIUS group configuration mode.

	Command	Purpose
Step 6	`Router(config)# aaa accounting network default start-stop group radius group group-name`	Enables AAA services using the group of RADIUS servers that are defined in the previously created group. The *group-name* parameter should be the same name specified in Step 3.
Step 7	`Router(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] key 0000000000000000`	Specifies a RADIUS host. Use the same values for *hostname* or *ip-address* as for one of the servers specified in Step 4. If you also specified the **auth-port** or **acct-port** values in Step 4, 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: • **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. **Note** Repeat this command for each RADIUS server entered in Step 4.
Step 8	`Router(config)# radius-server vsa send accounting`	Configures the Cisco CMTS to recognize and use accounting-related vendor-specific attributes (VSA).
Step 9	`Router(config)# exit`	Exits global configuration mode.

Monitoring and Maintaining PacketCable Operations

To display and maintain information about current PacketCable operations, use the following commands beginning in privileged EXEC mode.

Command	Purpose
`Router# show packetcable gate counter commit`	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.

Command	Purpose
`Router# clear packetcable gate counter commit`	Clears the total number of gates that the Cisco CMTS has put into the Committed state, setting the counter to zero.
`Router# show packetcable gate [downstream | upstream] {summary | gate-id}`	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. • **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. • *gate-id* = 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.

Configuration Examples

This section provides the following configuration examples:

- Typical PacketCable Configuration

Typical PacketCable Configuration

This section provides a typical configuration for a Cisco uBR7200 series 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 you are using.

```
!
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
```

Command Reference

The following commands were added or modified to support the PacketCable 1.0 feature.

- **clear packetcable gate counter commit**
- **packetcable**
- **packetcable element-id**
- **packetcable gate maxcount**
- **packetcable timer**
- **packetcable authorize vanilla-docsis-mta**
- **show packetcable gate**
- **show packetcable gate counter commit**
- **show packetcable global**
- **debug packetcable all**
- **debug packetcable gate**

For complete and current information on these commands, see the appropriate chapters in the Cisco Broadband Cable Command Reference Guide, at the following URL:

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

Glossary

- AAA—Authentication, authorization, and accounting.
- CM—Cable modem.
- CMS—Call management server.
- CMTS—Cable ModemYermination System.
- COPS—Common Open Policy Service Protocol.
- DCS—Distributed call signaling.
- DQoS—Dynamic quality of service
- E-MTA—Embedded multimedia terminal adapter. An MTA device that is integrated with a cable modem.
- GC—Gate controller.
- Gate—Virtual policy control entity that controls a service flow's access to QoS services.
- MTA—Multimedia terminal adapter. A CPE device that implements DCS or NCS signaling and provides an interface that allows customer equipment to access PacketCable services.
- NCS—Network-based call signaling.
- QoS—Quality of service.
- RADIUS—Remote Authentication Dial-In User Service.
- RKS—Record Keeping Server.
- RSVP—Resource reservation protocol.
- SDP—Session Description Protocol.