DOCSIS 1.1 for Cisco uBR905 and Cisco uBR925 Cable Access Routers and Cisco CVA122 Cable Voice Adapters

This document describes the support for version 1.1 of the Data-over-Cable System Interface Specification (DOCSIS 1.1) in Cisco IOS Release 12.2(15)CZ for the Cisco uBR905 and Cisco uBR925 cable access routers and Cisco CVA122 cable voice adapter. This document focuses on the new software and the changes to the existing software architecture that provide DOCSIS 1.1 support. This document also describes Cable Modem Termination System (CMTS) to cable modem interoperability and provides instructions for migrating from DOCSIS 1.0 to DOCSIS 1.1.

Feature History for DOCSIS 1.1 Support

Release	Modification
12.2(15)CZ	The DOCSIS 1.1 feature set was introduced for the Cisco uBR905 and Cisco uBR925 cable access routers and Cisco CVA122 cable voice adapter.

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

This document includes the following sections:

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

Prerequisites for DOCSIS 1.1 Support

Before you implement a DOCSIS 1.1 network, ensure that the following are true for your cable network:

- The Cisco uBR905 and Cisco uBR925 cable access routers and Cisco CVA122 cable voice adapter must contain the proper digital certificates for BPI+ operation and Secure Software Download. Initial versions of the Cisco uBR905 and Cisco uBR925 cable access routers and Cisco CVA122 cable voice adapter contained certificates for an early version of the DOCSIS 1.1 specification that are no longer valid. To upgrade these certificates, see the document *Upgrading the DOCSIS Certificates in Cisco uBR905/uBR925 Cable Access Routers and CVA122 Cable Voice Adapters* at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122cz/upgdcert.htm

  Note To update the digital certificates, you must also obtain the Cisco DOCSIS 1.1 Cable Modem Certificate Upgrade CD-ROM (part number UBR/CVA-CERT-UPG). This one CD-ROM works with the Cisco uBR905 and Cisco uBR925 cable access routers and Cisco CVA122 Cable Voice Adapters.

- Ensure that your network supports reliable broadband data transmission. Your plant must be swept, balanced, and certified to NTSC or appropriate international cable plant recommendations. Ensure that your plant meets all DOCSIS downstream and upstream RF requirements.
- Ensure that your CMTS is installed and configured to support DOCSIS 1.1 operation.
- Ensure that all other required headend or distribution hub routing and network interface equipment is installed, configured, and operational, based on the services to support. This includes all routers, servers (DHCP, TFTP, and ToD), network management systems, and other configuration or billing systems. This includes IP telephony equipment including gatekeepers and gateways; backbone and other equipment if supporting VPN; and dialup access servers, telephone circuits and connections, and other equipment if supporting telco return.
- Ensure that the system clocks on the CMTS and on the time-of-day (ToD) servers are synchronized. If this does not occur, the clocks on the CMs will not match the clocks on the CMTS, which could interfere with BPI+ operations. In particular, this could prevent the proper verification of the digital certificates on the CM.
- The DOCSIS specifications require that when the DOCSIS configuration file enables BPI+ encryption, the configuration file must also include a value for the Baseline Privacy Configuration Settings Option field (TLV 17). If this field is not included when BPI is enabled, the router rejects the BPI configuration. If MAC debugging is enabled (using the **debug cable-modem mac** command), the router also displays the displays the debugging message CMAC_LOG_BPKM_REQUIRED_TLV17_ABSENT on the console.
- Ensure that DHCP and DOCSIS 1.1 configuration files have been created and pushed to appropriate servers such that each cable modem, when initialized, can transmit a DHCP request, receive an IP address, obtain TFTP and ToD server addresses, and download DOCSIS 1.1 configuration files.

Optionally, ensure that servers are available to download Cisco IOS Release 12.2(15)CZ software images to Cisco uBR905 and Cisco uBR925 cable access routers and Cisco CVA122 cable voice adapters to enable DOCSIS 1.1 operation.

- Ensure that customer premises equipment (CPE)—cable modems or set-top boxes, PCs, telephones, or facsimile machines—meet the requirements for your network and service offerings.
- Familiarize yourself with your channel plan to ensure assigning of appropriate frequencies. Outline your strategies for setting up bundling or VPN solution sets, if applicable, to your headend or distribution hub. Know your dial plan if using H.323 for VoIP services and setting up VoIP-enabled cable modem configuration files. Obtain passwords, IP addresses, subnet masks, and device names, as appropriate.
- To use SNMPv3, the SNMP manager must support the MD5 encryption protocol and the noauthnoPriv, authNoPriv, or authPriv authentication modes. Also, the manager must be able to generate random numbers, public numbers, and secret keys as specified by RFC 2786, Diffie-Hellman USM Key.

Restrictions for DOCSIS 1.1 Support

Cisco IOS Release

The Cisco uBR905 and Cisco uBR925 cable access routers and Cisco CVA122 cable voice adapters must be running Cisco IOS Release 12.2(15)CZ (or later release) to support DOCSIS 1.1. The CMTS must also support the DOCSIS 1.1 feature set.

Baseline Privacy Interface Plus

BPI+ encryption and authentication must be supported and enabled by both the cable modem and the CMTS. In addition, the CMTS and cable modem must contain a digital certificate that conforms to the DOCSIS 1.1 and BPI+ specifications.

Also, the DOCSIS specifications require that when the DOCSIS configuration file enables BPI or BPI+ encryption, the configuration file must also include a value for the Baseline Privacy Configuration Settings Option field (TLV 17). If this field is not included when BPI is enabled, the router rejects the BPI configuration. If MAC debugging is enabled (using the **debug cable-modem mac** command), the router also displays the displays the CMAC_LOG_BPKM_REQUIRED_TLV17_ABSENT debugging message on the console.

Note All production models of the Cisco uBR905 and Cisco uBR925 cable access routers and Cisco CVA122 cable voice adapters include digital certificate support. However, some models might require an upgrade of those certificates before being able to perform BPI+ operation. See the document, *Upgrading the DOCSIS Certificates in Cisco uBR905/uBR925 Cable Access Routers and CVA122 Cable Voice Adapters*, which is at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122cz/upgdcert.htm

Tip Ensure that the system clocks on the CMTS and on the time-of-day (ToD) servers are synchronized. If this does not occur, the clocks on the CMs will not match the clocks on the CMTS, which could interfere with BPI+ operations. In particular, this could prevent the proper verification of the digital certificates on the CM.

Maximum Burst Size

Previously, the maximum concatenated burst size parameter could be set to zero to specify an unlimited value. In a DOCSIS 1.1 environment, this parameter should be set to a nonzero value, with a maximum value of 1522 bytes for DOCSIS 1.0 cable modems.

If a cable modem attempts to register with a maximum concatenation burst size of zero, the DOCSIS 1.1 CMTS refuses to allow the cable modem to come online. This avoids the possibility that a DOCSIS 1.0 cable modem could interfere with voice traffic on the upstream by sending extremely large data packets. Since DOCSIS 1.0 does not support fragmentation, transmitting such data packets could result in unwanted jitter in the voice traffic.

In addition, DOCSIS 1.1 requires that the maximum transmit burst size be set to either 1522 bytes or the maximum concatenated burst size, whichever is larger. Do not set the maximum concatenation burst size to values larger than 1522 bytes for DOCSIS 1.0 cable modems.

Note This change requires you to change any DOCSIS configuration files that specify a zero value for the maximum concatenation burst size. This limitation does not exist for DOCSIS 1.1 cable modems unless fragmentation has been disabled.

Provisioning

The format and content of the TFTP configuration file for a DOCSIS 1.1 cable modem are significantly different from the file for a DOCSIS 1.0 cable modem. A dual-mode configuration file editor is used to generate a DOCSIS 1.0 style configuration file for DOCSIS 1.0 cable modems and a DOCSIS 1.1 configuration file for DOCSIS 1.1 cable modems.

Registration

A DOCSIS 1.1 CMTS is designed to handle the existing registration TLVs from DOCSIS 1.0 cable modems as well as the new type TLVs from DOCSIS 1.1 cable modems. A DOCSIS 1.0 and DOCSIS 1.1 cable modem can successfully register with the same DOCSIS 1.1 CMTS.

A DOCSIS 1.1 cable modem can be configured to make an indirect reference to a service class that has been statically defined at the CMTS, instead of explicitly asking for particular service class parameters. When this registration request is received by a DOCSIS 1.1 CMTS, it encodes the actual parameters of the service class in the registration response and expects a DOCSIS 1.1-specific registration-acknowledge MAC message from the cable modem.

When a DOCSIS 1.1 cable modem registers with a DOCSIS 1.0 CMTS, it responds with DOCSIS 1.0 style registration messages and does not use the DOCSIS 1.1 feature set.

Performance

DOCSIS 1.0 cable modems lack the ability to explicitly request and provide scheduling parameters for advanced DOCSIS 1.1 scheduling mechanisms, such as unsolicited grants and real-time polling. DOCSIS 1.1 cable modems on the same upstream channel can benefit from the advanced scheduling mechanisms and a DOCSIS 1.1 CMTS can still adequately support voice traffic from DOCSIS 1.1 cable modems with DOCSIS 1.0 cable modems on the same upstream channel.

Information About DOCSIS 1.1 Support

DOCSIS 1.1 is the first major revision of the initial DOCSIS 1.0 standard for cable networks. Although the initial standard provided quality data traffic over the coaxial cable network, the demands of real-time traffic such as voice and video required many changes to the DOCSIS specification. DOCSIS 1.1 also includes support for the Baseline Privacy Interface Plus (BPI+) features, which improves and enhances the DOCSIS 1.0 BPI security and authorization mechanisms.

Note At the time of publication, the DOCSIS 1.1 and BPI+ specifications are still being finalized. See the CableLabs specifications web site (http://www.cablemodem.com/specifications.html) for the current status on these specifications.

The following sections describe the DOCSIS 1.1 features in more detail:

DOCSIS 1.1 Overview

The DOCSIS 1.1 specification provides the following functional enhancements over DOCSIS 1.0 coaxial cable networks:

- Enhanced quality-of-service (QoS) to give priority for real-time traffic such as voice and video:
  - The DOCSIS 1.0 QoS model (a service ID [SID] associated with a QoS profile) has been replaced with a service flow model that allows greater flexibility in assigning QoS parameters to different types of traffic and in responding to changing bandwidth conditions.
  - Support for multiple service flows per cable modem allows a single cable modem to support a combination of data, voice, and video traffic.
  - Greater granularity in QoS per cable modem in either direction, using unidirectional service flows.
  - Dynamic MAC messages create, modify, and delete traffic service flows to support on demand traffic requests. The CMTS can also dynamically change the upstream and downstream channels that the cable modem is using to proactively deal with potential congestion or noise problems.
- Supported QoS models for the upstream are:
  - Best-effort—Data traffic sent on a nonguaranteed best-effort basis.
  - Committed information rate (CIR)—Guaranteed minimum bandwidth for data traffic.
  - Real-time polling (RTPS)—Real-time service flows, such as video, that produce unicast, variable-size packets at fixed intervals.

  - Unsolicited grants (UGS)—Constant bit rate (CBR) traffic, such as voice, that is characterized by fixed-size packets at fixed intervals.
  - Unsolicited grants with activity detection (USG-AD)—Combination of UGS and RTPS, to accommodate real-time traffic that might have periods of inactivity (such as voice using silence suppression). The service flow uses UGS fixed grants while active, but switches to RTPS polling during periods of inactivity to avoid wasting unused bandwidth.
- Service flows for Voice-over-IP (VoIP) calls can be flexibly created using the following methods:
  - Dynamic quality-of-service (DQoS)—The router is initialized with a primary upstream service flow and a primary downstream service flow. When a VoIP call is made, the router sends a request for a UGS service flow with a Dynamic Service Addition Request (DSA-REQ) message. After the call, the router deletes the service flow using a Dynamic Service Deletion Request message (DSD-REQ) message.
  - Provisioned quality-of-service (PQoS)—The router is initialized with a primary upstream service flow, a primary downstream service flow, and two secondary upstream service flows that are reserved for VoIP calls. The router keeps the secondary flows in the admitted state until a VoIP call is made. The router then activates the appropriate flow with a Dynamic Service Change Request (DSC-REQ) message with a classifier for UGS service that specifies the IP parameters needed for the voice call. After the call, the router deletes the classifier and deactivates the service flow by sending another DSC-REQ message.

Note If the CMTS does not support DOCSIS 1.1 dynamic services, the router can also use the previous DOCSIS 1.0+ mechanisms to create VoIP calls.

- Enhanced time-slot scheduling mechanisms to support guaranteed delay and jitter-sensitive traffic on the shared multiple access upstream link.
- Payload header suppression (PHS) conserves link-layer bandwidth by suppressing unnecessary packet headers on both upstream and downstream traffic flows.
- Layer 2 fragmentation on the upstream prevents large data packets from affecting real-time traffic, such as voice and video. Large data packets are fragmented and then transmitted in the time slots that are available between the time slots used for the real-time traffic.
- Concatenation allows a cable modem to send multiple MAC frames in the same time slot, as opposed to making an individual grant request for each frame. This avoids wasting upstream bandwidth when sending a number of very small packets, such as TCP acknowledgement packets.
- Advanced authentication and security through X.509 digital certificates and Triple Data Encryption Standard (3DES) dual public key encryption.
- Support for IP multicast encryption and for Internet Group Management Protocol (IGMP) groups.
- Secure software download allows a service provider to remotely upgrade a cable modem's software, without risk of interception or alteration.
- SNMPv3 Support, which includes:
  - DES 56-bit encryption.
  - Authentication based on the HMAC-MD5 or HMAC-SHA algorithms that ensures that each packet is from a valid source.
  - An improved security model that provides for a larger number of security levels, with a greater granularity in determining per-user access.
  - MIBs are updated as required for DOCSIS 1.1 support.

- DOCSIS 1.1 cable modems can coexist with DOCSIS 1.0 and 1.0+ cable modems in the same network—a DOCSIS 1.1 CMTS provides the levels of service that are appropriate for each cable modem.

Baseline Privacy Interface Plus

DOCSIS 1.0 included a Baseline Privacy Interface (BPI) to protect user data privacy across the shared-medium cable network and to prevent unauthorized access to DOCSIS-based data transport services across the cable network. BPI encrypts traffic across the RF interface between the cable modem and CMTS, and also includes authentication, authorization, and accounting (AAA) features.

BPI supports access control lists (ACLs), tunnels, filtering, protection against spoofing, and commands to configure source IP filtering on RF subnets to prevent subscribers from using source IP addresses that are not valid. These lists can be implemented either through CLI commands or by setting SNMP attributes through the DOCSIS configuration file.

DOCSIS 1.1 enhances these security features with Baseline Privacy Interface Plus (BPI+), which includes the following enhancements:

- X.509 digital certificates provide secure user identification and authentication. Each DOCSIS 1.1 cable modem contains a certificate that uniquely identifies it to the CMTS. This certificate is chained to the manufacturer's digital certificate, which securely authenticates the cable modem. The manufacturer's certificate in turn is chained to and verified by the DOCSIS certificate authority (CA) root certificate.
- Key encryption uses 168-bit Triple DES (3DES) encryption that is suitable for the most sensitive applications.
- 1024-bit public key exchange Pkcs#1 Version 2.0 encryption to ensure the secure generation and transmission of the public encryption keys between the CMTS and CM.
- Encryption of multicast broadcasts allows users to receive only those broadcasts they are authorized to use.
- Secure software download, using a Pkcs#7 digital signature, allows a service provider to upgrade a cable modem's software remotely, without the threat of interception, interference, or alteration.

Note BPI+ is described in the Baseline Privacy Interface Plus Specification (SP-BPI+-I08-020301), available from CableLabs (http://www.cablelabs.com).

X.509 Digital Certificates

BPI+ uses digital certificates and a public key infrastructure (PKI) that are based on the International Telecommunications Union (ITU) X.509 Version 3.0 standard. The key components of the X.509 standard are the following:

- Digital certificate—Uniquely identifies the cable modem. The digital certificate contains the following information:
  - User name and organization—Identify the product and its manufacturer.
  - Certificate effective date and expiration Date—Give the range of dates for which the certificate is valid.
  - User public key—Allows other entities, such as the CMTS, to verify the certificate.

  - Issuer certificate authority (CA) name and signature—Provide a way of verifying that the certificate and keys have not been altered.

  A DOCSIS 1.1 cable modem contains two digital certificates programmed into it at the factory: a cable modem certificate that uniquely identifies it, and a manufacturing certificate that identifies the cable modem's manufacturer (in this case, Cisco Systems).

- Public and private keys—Keys used to sign and verify the certificate. The cable modem uses its private key to sign its digital certificate to create an unforgeable digital signature that identifies the signer. Other entities, such as the CMTS, use the public key to unsign and verify the certificate. For security, the cable modem never transmits or displays its private key, but the public key is included as part of the certificate to allow for its verification.

  Note The cable modem's private and public keys are never changed after being programmed at the factory.

- Digital signature—Created when a private key signs a digital certificate. The digital signature becomes part of the certificate, allowing the CMTS to verify that the certificate came from the cable modem claiming to have issued it.
- Certificate authority (CA)—To prevent users from creating their own certificates and private key and public key pairs, each certificate is also signed by an issuing CA. After the CMTS verifies a digital certificate with the cable modem's public key, it then verifies that the certificate has been properly signed by the issuing CA. This process continues until the CMTS can verify the certificate against a known and trusted CA (typically the root CA).
- Root CA—A known and trusted CA that serves as the ultimate verification for a digital certificate. For DOCSIS 1.1 cable modems, the root CA is the DOCSIS Root CA certificate, which is available from Verisign at http://www.verisign.com/products/cable/root.html. The root CA is self-signed, which does not present a security problem because it is originating at a known and trusted source.
- DOCSIS root code signing CA—Similar to the Root CA but used to verify the digital certificates that are used whenever a DOCSIS 1.1 cable modem downloads new software code.

During BPI+ initialization, the cable modem sends both of its signed digital certificates, the cable modem certificate (CMC) and the manufacturer's certificate (MC), to the CMTS. The CMTS verifies the cable modem certificate against the manufacturer's certificate, and then verifies the manufacturer's certificate against the DOCSIS Root CA certificate. This chain of verifications ensures that the CMTS can securely identify and authenticate each cable modem.

In addition, the CMTS can check the certificates against a Hot List of invalid certificates. The Hot List, which can be maintained by trusted authorities, such as a service provider or CA, can list certificates for individual cable modems that might have been stolen, hacked, or otherwise compromised. The list can also contain manufacturer's certificates for models of cable modems that the service provider does not support.

If all certificate verifications are successful, the CMTS begins the public key exchange process, which allows data encryption and decryption to begin.

Public Key Exchange

The secure use of X.509 digital certificates depends on both the cable modem and the CMTS possessing the proper encryption and decryption keys. For security and flexibility, DOCSIS 1.1 uses a dual-key public key exchange: the first set of keys, key encryption key (KEK), are used to encrypt and transmit the second set of keys, traffic encryption key (TEK), which are then used to encrypt and decrypt data.

Both sets of keys have a limited lifetime and must be renewed periodically. When a key reaches approximately half its lifespan, the cable modem begins the process to request a new set of keys. While the new set of keys is being exchanged, the cable modem can continue to use the old set to encrypt and decrypt data. The KEK keys have a longer lifetime than the TEK keys to ensure that the cable modem and CMTS will always be able to obtain new TEK keys, allowing data transmissions to continue without interruptions.

Secure Software Download

DOCSIS 1.1 supports secure software download to allow a service provider to remotely upgrade a cable modem's software without risk of interception or alteration. Secure software download also prevents users from upgrading the cable modem to unauthorized software images.

The manufacturer digitally signs the software image using a Pkcs#7 digital signature that is encrypted using the Rivest-Shamir-Adleman (RSA) algorithm and secure hash algorithm-1 (SHA-1). This digital signature is chained to the DOCSIS root code signing certificate so that it can be easily verified.

The cable operator can optionally also digitally sign the software image in a similar manner, using another digital signature that is chained to the DOCSIS root code signing certificate. This allows cable operators greater control over which software images are used on the cable network.

The cable operator initiates the software download by filling in the software filename and TFTP server fields (TLVs 9 and 21) in the DOCSIS configuration file that it sends to the cable modem during registration. You can also initiate a software download by using SNMP commands. In either case, the cable modem then requests the specified file and downloads it from the specified TFTP server.

The cable modem verifies the manufacturer's digital signature and, if present, the cable operator's digital signature, using the code verification certificates (CVCs) provided in the DOCSIS configuration file. If the signatures are valid, the cable modem loads and runs the software.

When a cable modem is running DOCSIS 1.1 software, it must use the secure software download feature to download a software image through the DOCSIS configuration file or through SNMP commands. Even if you disable BPI+, a DOCSIS 1.1 cable modem still accepts only digitally signed software images that can be verified through the secure software download process.

Note The secure software download feature does not prevent a user with console or Telnet access, and who knows the proper passwords, from loading an unsigned software image directly into the cable modem's Flash memory by using the **copy tftp** command.

The secure software download feature requires the following prerequisites:

- The Cisco uBR905, Cisco uBR925, or Cisco CVA122 must be running a DOCSIS 1.1 software image.

  If the cable modem is currently running a DOCSIS 1.0 software image, you cannot use the secure software download to upgrade to a DOCSIS 1.1 image. Instead, you must use the DOCSIS 1.0 software upgrade process to load an unsigned DOCSIS 1.1 software image. Then you will be able to use the secure software download process to load a digitally signed DOCSIS 1.1 software image.
- The desired software image must be digitally signed by the manufacturer. The cable operator can also optionally digitally sign the image. Unsigned images cannot be loaded using the secure software download process.

  Note You cannot use the **copy tftp** command to load digitally signed images into the Flash memory on the cable modem.

- You must load at least one CVC into the cable modem through the DOCSIS configuration file. The cable modem uses the CVC to verify that a downloaded software image is from the proper manufacturer and has not been altered during transmission. You can load two types of CVCs into the cable modem:
  - Manufacturer's CVC (M-CVC)—Verifies that the downloaded software image has been digitally signed by the manufacturer (Cisco Systems). The M-CVC is loaded into the cable modem by specifying TLV 32 (MFG CVC) in the DOCSIS configuration file.
  - Cosigner's CVC (C-CVC)—Verifies that the downloaded software image has been digitally signed by both the manufacturer (Cisco Systems) and the cable operator. The C-CVC is loaded into the cable modem by specifying TLV 33 (MSO CVC) in the DOCSIS configuration file.

  If you load the M-CVC into the cable modem, you can download only those software images that Cisco Systems has digitally signed. If you load the C-CVC into the cable modem, you can download only those software images that Cisco Systems and the cable operator have digitally signed.

Note A DOCSIS 1.1 cable modem must use the secure software download feature when upgrading its software image through the DOCSIS configuration file or through SNMP commands. However, users can still use CLI commands to copy an unsigned software image from a TFTP server, if they know the enable password and are allowed console or Telnet access.

After the cable modem loads and runs the DOCSIS 1.1 image, the cable modem must use the secure software download process for all future upgrades. In particular, this means that the cable modem cannot be downgraded to a DOCSIS 1.0 software image unless the manufacturer provides a digitally signed DOCSIS 1.0 image. After downgrading to a DOCSIS 1.0 image, you cannot use the secure software download process again until you have upgraded the cable modem to a new DOCSIS 1.1 image.

Tip Cisco IOS software images that include "cvc" as part of the software image filename (ubr925cvc-k9o3sv9y5-mz) are digitally signed. Unsigned software images do not have "cvc" as part of the filename (ubr925-k9o3sv9y5-mz). If you are using secure software download, you *must* use a digitally signed image (includes "cvc"). If you are not using secure software download, you *must* use an unsigned image (does not include "cvc").

DOCSIS 1.1 Quality-of-Service

DOCSIS 1.1 implemented a number of changes to allow great flexibility in the ability of a cable modem and service provider to transmit almost any combination of data traffic and real-time traffic, such as voice and video. These changes required a fundamental shift in how a cable modem requests service and how traffic can be transmitted across the cable network.

Overview

The DOCSIS 1.1 QoS framework is based on the following objects:

- Service class—A collection of settings maintained by the CMTS that provide a specific QoS service tier to a cable modem that has been assigned a service flow within a particular service class.
- Service flow—A MAC-layer transport service that provides unidirectional transport of packets to upstream packets transmitted by the cable modem or to downstream packets transmitted by the CMTS. A service flow is characterized by a set of QoS parameters such as latency, jitter, and throughput assurances.

- Packet classifier—A set of packet header fields used to classify packets onto a service flow to which the classifier belongs. When a packet is presented to the DOCSIS MAC layer at the CMTS or cable modem, it is compared to a set of packet classifiers until a matching classifier is found. The SFID from this classifier is used to identify the service flow on which the packet will be sent.
- PHS rule—A set of packet header fields that are suppressed by the sending entity before transmitting on the link, and are restored by the receiving entity after receiving a header-suppressed frame transmission. Payload header suppression increases the bandwidth efficiency by removing repeated packet headers before transmission.

In the upstream direction, the output queues at the cable modem get remotely served by the CMTS MAC scheduler, based on DOCSIS 1.1 slot scheduling constraints such as grant-interval and grant-jitter. In the downstream direction, the CMTS packet scheduler serves the flow queues depending on the flow attributes like traffic priority, guaranteed rate, and delay bound.

DOCSIS 1.1 adds several new MAC scheduling disciplines to provide guaranteed QoS for real-time service flows on the multiple access upstream channel. Multiple grants per interval helps in supporting multiple subflows (such as voice calls) on the same SID. Multiple subflows per SID reduces the minimum SID requirement in cable modem hardware.

The CMTS is responsible for supporting QoS for all cable modems in its control. The traffic in the downstream is assumed to be a combination of voice, committed information rate (CIR) data, and excess burst best-effort data. To provide QoS support, the following functions must be performed:

- Packet classification—Mapping packets to service flows based on header information
- Policing (rate limiting) the individual flows
- Queuing packets into appropriate output queues based on the type of service
- Serving the output queues to meet delay and rate guarantees

The admission control block helps the overall downstream QoS block to track the current bandwidth reservation state on a per-downstream basis. Decisions can be made whether to admit or reject a request for a new service flow on that DS channel, based on this reservation state and the QoS guarantees requested by the new service-flow.

IP packet classifiers help in filtering out unique service flows on an interface for differential QoS treatment. Rather than doing per-cable modem downstream rate shaping, DOCSIS 1.1 software provides rate shaping at a much more granular level of individual service flows of the cable modem.

Note Cisco uBR905 and uBR925 cable access routers and Cisco CVA122 cable voice adapters running Cisco IOS Release 12.2(15)CZ can transparently interoperate with CMTS routers running DOCSIS 1.0, DOCSIS 1.0+ extensions, or DOCSIS 1.1.

Service Flows and Packet Classifiers

Every cable modem establishes a primary service flow in both the upstream and downstream directions. The primary flows maintain connectivity between the cable modem and the CMTS at all times.

In addition, a DOCSIS 1.1 cable modem can establish multiple secondary service flows. The secondary service flows either can be permanently created (they persist until the cable modem is reset or powered off) or can be created dynamically to meet the needs of the on-demand traffic being transmitted.

A service flow gets created at the time of cable modem registration (a static service flow) or as a result of a dynamic MAC message handshake between the cable modem and the CMTS (a dynamic service flow). At any given time, a service flow might be in one of three states (provisioned, admitted, or active). Only active flows are allowed to pass traffic on the DOCSIS link.

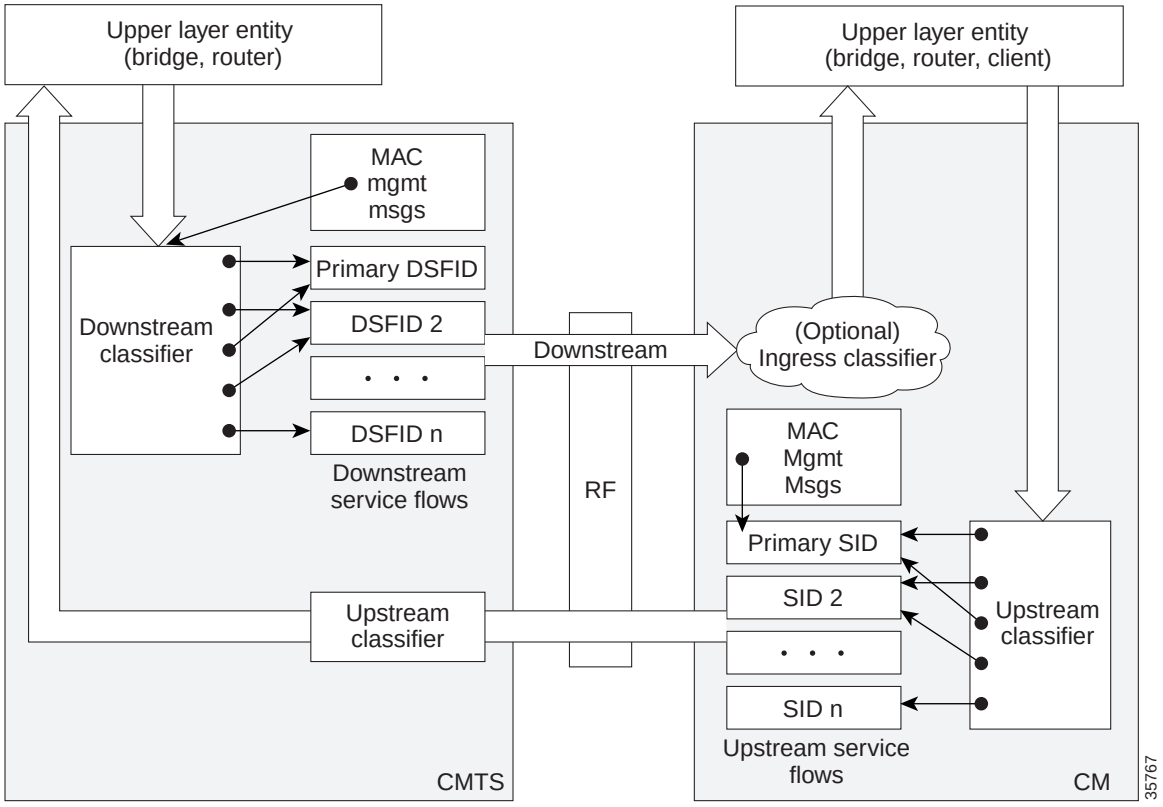
Each service flow has a set of QoS attributes associated with it. These QoS attributes define a particular class of service and determine characteristics such as the maximum bandwidth for the service flow and the priority of its traffic. The class of service attributes can be inherited from a preconfigured CMTS local service class (class-based flows), or they can be individually specified at the time of the creation of the service flow.

Every service flow also has a unique (unique per DOCSIS MAC domain) identifier called the service flow identifier (SFID). The upstream flows in the admitted and active state have an extra Layer 2 SID associated with them. The SID is the identifier used by the MAC scheduler when specifying time-slot scheduling for different service flows.

Each service flow has multiple packet classifiers associated with it, which determine the type of application traffic allowed to be sent on that service flow. Each service flow can also have a payload header suppression (PHS) rule associated with it to determine which portion of the packet header will be suppressed when packets are transmitted on the flow.

Figure 1 illustrates the mapping of packet classifiers.

Figure 1 Classification Within the MAC Layer



Dynamic Channel Change

DOCSIS 1.1 supports Dynamic Channel Change (DCC) requests, which allow the CMTS to change the upstream or downstream frequency that the cable modem is using. This allows the CMTS to move cable modems to another channel when the current one is either becoming congested or is encountering growing noise problems that could eventually force the cable modems offline.

The Cisco uBR905 and Cisco uBR925 cable access routers and the Cisco CVA122 Cable Voice Adapter automatically support DCC requests when running Cisco IOS Release 12.2(15)CZ.

Dynamic Quality-of-Service

DOCSIS 1.1 adds support Dynamic Services MAC-layer messages that provide for Dynamic QoS (DQoS) between the cable modem and the CMTS. These messages are DOCSIS link-layer equivalents of the higher-layer messages that create, tear down, and modify a service flow. These messages are collectively known as DSX messages to represent the three types of dynamic service messages:

- Dynamic Service Add (DSA)—Creates a new service flow.
- Dynamic Service Change (DSC)—Changes the attributes of an existing service flow. These changes can include the following:
  - Adding, replacing, or deleting a classifier from the service flow.
  - Changing the flow's Admitted and Active QoS parameter sets.
  - Adding, setting, or deleting payload header suppression (PHS) rules for the service flow.
- Dynamic Service Deletion (DSD)—Deletes an existing service flow.

The DSX state machine module on the cable modem manages the several concurrent dynamic service transactions between cable modems and the CMTS. The DSX state machine supports all three DOCSIS1.1 DSX MAC messages (DSA, DSC, DSD).

Provisioned QoS

Provisioned QoS (PQoS) allows the cable modem to create the service flows it needs for voice calls and other real-time traffic at the time it registers with the CMTS, without actually using the bandwidth for those flows. The service flow is kept in the admitted state and is activated only when the cable modem signals a voice call using the DOCSIS 1.1 Dynamic Service Request (DSC-REQ) message. Bandwidth is used only when the voice call is actually in progress.

To use PQoS services, you must configure the cable modem with secondary service flows for VoIP calls. (If you do not define any secondary service flows, DQoS is used instead of PQoS). You can use any voice signaling that is supported by the cable modem for VoIP traffic.

Table 1 compares how the router sets up and tears down VoIP calls when using DQoS and PQoS:

Table 1 Comparison of DQoS and PQoS Call Setup and Teardown Operation

Quality-of-Service Type	VoIP Signaling Type	Call Setup Description
Dynamic QoS	H.323	Sends DSA at off-hook and DSD at on-hook.
	SGCP/MGCP/SIP	Sends DSA at off-hook, DSC when the call setup parameters are received from the gateway, and DSD at on-hook.
Provisioned QoS	H.323	Sends DSC at off-hook to activate the provisioned service flows and DSD at on-hook.
	SGCP/MGCP/SIP	Sends DSC at off-hook to activate the provisioned service flows, a second DSC when the call setup parameters are received from the gateway, and DSD at on-hook.

Service Flow Manager

The Service Flow Manager is a new module that manages different activities related to service flows on a cable interface. Typical events include the creation of new DOCSIS service flows, modification of the attributes of existing service flows, and the deletion of service flows.

Quality-of-Service Comparison

Quality-of-service (QoS) is a measure of performance for a transmission system that reflects its transmission quality and service availability. This section describes the differences in QoS between DOCSIS 1.1 and DOCSIS 1.0 and 1.0+.

DOCSIS 1.0

DOCSIS 1.0 uses a static QoS model that is based on a class of service (CoS) that is preprovisioned in the TFTP configuration file for the cable modem. The CoS is a bidirectional QoS profile that has limited control, such as peak rate limits in either direction and relative priority on the upstream.

DOCSIS 1.0 defines the concept of a service identifier (SID), which specifies the devices allowed to transmit and which provides device identification and CoS. In DOCSIS 1.0, each cable modem is assigned only one SID, creating a one-to-one correspondence between a cable modem and the SID. All traffic originating from, or destined for, a cable modem is mapped to that cable modem's SID.

Typically, a DOCSIS 1.0 cable modem has one CoS and treats all traffic the same, which means that data traffic on a cable modem can interfere with the quality of a voice call in progress. The CMTS, however, can prioritize downstream traffic based on IP precedent type-of-service (ToS) bits. For example, voice calls using higher IP precedence bits receive a higher queueing priority (but without a guaranteed bandwidth or rate of service). A DOCSIS 1.0 cable modem could increase voice call quality by permanently reserving bandwidth for voice calls, but then that bandwidth would be wasted whenever a voice call is not in progress.

DOCSIS 1.0+ Extensions

In response to the limitations of DOCSIS 1.0 in handling real-time traffic, such as voice calls, Cisco created the DOCSIS 1.0+ extensions to provide the more important QoS enhancements that were expected in DOCSIS 1.1. In particular, the DOCSIS 1.0+ enhancements provide basic Voice-over-IP (VoIP) service over the DOCSIS link.

Cisco DOCSIS 1.0+ extensions include the following DOCSIS 1.1 features:

- Multiple SIDs per cable modem, creating separate service flows for voice and data traffic. This allows the CMTS and cable modem to give higher priority for voice traffic, preventing the data traffic from affecting the quality of the voice calls.
- Cable modem-initiated dynamic MAC messages—Dynamic Service Addition (DSA) and Dynamic Service Deletion (DSD). These messages allow dynamic SIDs to be created and deleted on demand, so that the bandwidth required for a voice call can be allocated at the time a call is placed and then freed up for other uses when the call is over.
- Unsolicited grant service (CBR-scheduling) on the upstream—This helps provide a higher-quality channel for upstream VoIP packets from an Integrated Telephony Cable Modem (ITCM) such as the Cisco uBR924 cable access router.

- Ability to provide separate downstream rates for any given cable modem, based on the IP-precedence value in the packet. This helps separate voice signaling and data traffic that goes to the same ITCM to address rate shaping purposes.
- Concatenation allows a cable modem to send several packets in one large burst, instead of having to make a separate grant request for each.

Caution All DOCSIS 1.0 extensions are available only when using a cable modem (such as the Cisco uBR924 cable access router) and CMTS (such as the Cisco uBR7200 series universal broadband router) that supports these extensions. The cable modem activates the use of the extensions by sending a dynamic MAC message. DOCSIS 1.0 cable modems continue to receive DOCSIS 1.0 treatment from the CMTS.

SNMPv3 Support

DOCSIS 1.1 also requires support of v3 of the Simple Network Management Protocol (SNMPv3). SNMPv3 offers a number of significant improvements over SNMPv1 and SNMPv2:

- DES 56-bit encryption that encrypts each packet to prevent interception or alteration intransit. SNMP attributes can be set and retrieved without exposing confidential information on a public network.
- Authentication based on the HMAC-MD5 or HMAC-SHA algorithms that ensures that each packet is from a valid source.
- An improved security model that provides for a larger number of security levels, with a greater granularity in determining per-user access. Each SNMPv3 user belongs to a group, which defines the security model and security level for its users. This includes the level of access to SNMP objects and the list of notifications that users can receive.

SNMPv3 Diffie-Hellman Kickstart

To ensure SNMPv3 security, the Multi-Service Operator (MSO) must perform an initialization procedure the first time the cable modem comes online. This procedure, which the DOCSIS 1.1 specification refers to as the *SNMPv3 Diffie-Hellman Kickstart*, sends a public key to the cable modem as part of the DOCSIS configuration file. The cable modem creates a secret number and encrypts it using the public key it received in the configuration file.

The cable modem then publishes the encrypted number to the CMTS, which uses its private key to decrypt it so as to produce the cable modem's secret number. This secret number becomes a shared secret value that the CMTS and CM can use to exchange SNMPv3 encryption keys.

For information on the SNMPv3 Diffie-Hellman Kickstart configuration, see the "Configuring the SNMPv3 Diffie-Hellman Kickstart Public Key" section on page 22.

MIB Enhancements

DOCSIS 1.1 also expands the MIB support for SNMP management, including the following changes and additions to the DOCSIS 1.0 MIB structure:

- DOCS-BPI-PLUS-MIB—Describes the Baseline Privacy Interface Plus (BPI+) attributes and replaces the DOCS-BPI-MIB, which was used in DOCSIS 1.0. This is revision 05 of the MIB.
- DOCS-QOS-MIB—Describes the quality-of-service (QoS) attributes. This is revision 04 of the MIB.

- DOCS-SUBMGT-MIB—Describes the subscriber management attributes. This is revision 02 of the MIB.
- RFC 2933—Describes the IGMP protocol attributes, as defined in RFC 2933.
- DOCS-CABLE-DEVICE-MIB—Describes the operation of the CM and the CMTS, as defined as RFC 2669.
- DOCS-CABLE-DEVICE-TRAP-MIB—Defines the traps supported by CMs and the CMTS and is the extension of RFC 2669 (DOCS-CABLE-DEVICE-MIB).
- DOCS-IF-EXT-MIB—Extends RFC 2670 (DOCS-IF-MIB) to provide information about whether the CMs and the CMTS support DOCSIS 1.0 or DOCSIS 1.1.

Additional DOCSIS 1.1 Features in Cisco IOS Release 12.2(15)CZ

The following sections describe the DOCSIS 1.1 software features that appear in Cisco IOS Release 12.2(15)CZ.

Concatenation

Concatenation allows the cable modem to make a single time-slice request for multiple packets and send all packets in a single large burst on the upstream. Concatenation was introduced in the upstream receive driver in DOCSIS1.0+ releases.

Fragmentation

Grant fragmentation allows the upstream MAC scheduler to slice large data requests to fit into the scheduling gaps between UGS (voice slots). This reduces the jitter experienced by the UGS slots when large data grants preempt the UGS slots. The grant fragmentation gets triggered in the MAC scheduler, and fragment reassembly happens in the upstream receive driver.

Note DOCSIS fragmentation should not be confused with the fragmentation of IP packets, which is done to fit the packets on network segments with smaller maximum transmission unit (MTU) size. DOCSIS Fragmentation is Layer 2 fragmentation that is primarily concerned with efficiently transmitting lower-priority packets without interfering with high-priority real-time traffic, such as voice calls. IP fragmentation is done at Layer 3 and is primarily intended to accommodate routers that use different maximum packet sizes.

IP Multicast Support

By default, a DOCSIS CMTS transmits IP multicast traffic without encryption. All DOCSIS cable modems receiving that multicast traffic must forward it to its attached CPE devices, without regard to whether any of the devices have requested the traffic. This can waste network bandwidth and require network devices to waste processor power in forwarding and processing undesired multicast traffic.

A DOCSIS 1.1 CMTS can instead use the Internet Group Management Protocol (IGMP) to maintain the multicast group memberships of its DOCSIS 1.1 cable modems. BPI+ encryption is used to encrypt the multicast packets so that only the cable modems with the appropriate public keys can decrypt the packets and forward them to their attached customer premises equipment (CPE) devices.

If a cable modem has not been granted the decryption keys for a particular multicast service flow, it does not forward the traffic to its CPE devices. This ensures that only authorized subscribers can receive the multicast traffic, and prevents cable modems from loading down their local networks by forwarding unnecessary multicast traffic.

DOCSIS 1.1 uses the concept of Security Associations (SA), which are dynamically created and maintained to provide the service flows required to transmit IP multicast traffic on the downstream. A cable modem sends an SA Map Request message to request the SA for the downstream service flow that is carrying the desired multicast traffic.

If the cable modem is not authorized to receive the multicast traffic, or if the traffic is not available on BPI+ encrypted SA, the CMTS sends an SA Map Reject message. The cable modem then does not repeat any further SA Map Requests for this particular multicast traffic. However, if the traffic is available on an unencrypted service flow, it begins forwarding that traffic to its CPE devices.

If the cable modem is authorized to receive the multicast traffic, and if the traffic is available, the CMTS replies with an SA Map Reply message to provide the information that allows the cable modem to receive the multicast traffic. The SA Map Reply message contains the SA identifier (SAID) for the traffic and the cryptographic suite that is necessary to decrypt the multicast traffic.

If the cable modem supports the cryptographic suite being used, it sends a Key Request to the CMTS, requesting the public keys it needs to decrypt the multicast service flow. If the CMTS replies with a Key Reply that contains the requested public keys, the cable modem begins decrypting the multicast traffic and forwarding it to its attached CPE devices.

The multicast traffic can be mapped to the cable modem's primary SA, a static SA, or a dynamically created SA. One service flow can support multiple multicast traffic flows, each with its own SAID. Multicast traffic mapped to a primary SA can be received only by the cable modem that is assigned the associated primary service flow. Multicast traffic mapped to static and dynamic SAs can be received by all cable modems that are assigned the associated secondary service flows.

Payload Header Suppression and Restoration

The PHS feature is used to suppress repetitive or redundant portions in packet headers before transmission on the DOCSIS link. This is a new feature in the DOCSIS1.1 MAC driver. The upstream receive driver is now capable of restoring headers suppressed by cable modems, and the downstream driver is capable of suppressing specific fields in packet headers before forwarding the frames to the cable modem.

Migrating from Earlier Versions of DOCSIS

DOCSIS 1.1 cable modems have additional features and better performance than earlier DOCSIS 1.0 and 1.0+ models, but all three models can coexist in the same network. DOCSIS 1.0 and 1.0+ cable modems will not hamper the performance of a DOCSIS 1.1 cable modem, nor will they interfere with operation of DOCSIS 1.1 features. There is full forward and backward compatibility in the standards.

For this configuration...	The result is...
DOCSIS 1.1 cable modems with DOCSIS 1.0 CMTS	Cable modems receive DOCSIS 1.0 features and capabilities. BPI is supported if it is available and enabled on the CMTS.
DOCSIS 1.1 cable modems with DOCSIS 1.0+ CMTS	Cable modems receive basic DOCSIS 1.0 support. BPI is supported if it is available and enabled on the CMTS. In addition, cable modems also receive the following DOCSIS 1.1 features: • Multiple SIDs per cable modem • Dynamic Service MAC messaging initiated by the cable modem • Unsolicited grant service (UGS, CBR-scheduling) on the upstream • Separate downstream rates for any given cable modem, based on the IP-precedence value • Concatenation
DOCSIS 1.1 cable modems with DOCSIS 1.1 CMTS	Cable modems receive all the DOCSIS 1.1 features listed in this document. BPI+ is supported if it is available and enabled on the CMTS.

Benefits

DOCSIS 1.1 includes a rich set of features that provide advanced and flexible QoS capabilities for various types of traffic (voice, data, and video) over the cable network. It also provides enhanced security and authentication features.

Baseline Privacy Interface Plus Enhancement

The Plus (+) version of the Baseline Privacy Interface (BPI+) in DOCSIS 1.1 provides a set of extended services within the MAC sublayer that increase performance and system security. Digital certificates provide secure authentication for each cable modem, to prevent identity theft on the basis of MAC and IP addresses. Advanced encryption provides a secure channel between the cable modem and the CMTS, and secure software download allows a service provider to upgrade the software on cable modems, without the threat of interception, interference, or alteration of the software code.

Dynamic Service Flows

The dynamic creation, modification, and deletion of service flows allows for on-demand reservation on Layer 2 bandwidth resources. The CMTS can now provide special dynamic QoS (DQos) to the cable modem dynamically for the duration of a voice call or video session, as opposed to the static provisioning and reservation of resources at the time of cable modem registration. This provides a more efficient use of the available bandwidth.

Concatenation

The cable modem concatenates multiple upstream packets into one larger MAC data frame, allowing the cable modem to make only one time-slot request for the entire concatenated MAC frame, as opposed to requesting a time slot for each individual packet. This reduces the delay in transferring the packet burst upstream.

Enhanced QoS

Extensive scheduling parameters allow the CMTS and the cable modem to communicate QoS requirements and achieve more sophisticated QoS on a per service-flow level.

Different new time-slot scheduling disciplines help in providing guaranteed delay and jitter bound on shared upstream. Activity detection helps to conserve link bandwidth by not issuing time slots for an inactive service flow. The conserved bandwidth can then be reused for other best-effort data slots.

Packet classification helps the CMTS and the cable modem to isolate different types of traffic into different DOCSIS service flows. Each flow could be receiving a different QoS service from the CMTS.

Provisioned QoS

Provisioned QoS (PQoS) allows the cable modem to create service flows for voice calls and other real-time traffic at the time it registers with the CMTS, without actually using the bandwidth for those flows. When such a service flow is specified in the DOCSIS configuration file, the cable modem creates a flow that uses the DOCSIS 1.1 unsolicited grant service (UGS). The service flow, however, is not activated until the cable modem signals the voice call using the DOCSIS 1.1 Dynamic Service Change Request (DSC-REQ) message. Bandwidth is used only when the voice call is actually in progress.

Fragmentation

The MAC scheduler fragments data slots to fill the gaps in between UGS slots. Fragmentation reduces the jitter experienced by voice packets when large data packets are transmitted on the shared upstream channel and preempt the UGS slots used for voice. Fragmentation splits the large data packets so that they fit into the smaller time slots available around the UGS slots.

Multiple Subflows per SID

This feature allows the cable modem to have multiple calls on a single hardware queue. This approach scales much better than requiring a separate SID hardware queue on the cable modem for each voice call.

Payload Header Suppression

Payload header suppression (PHS) allows the CMTS and the cable modem to suppress repetitive or redundant portions in packet headers before transmitting on the DOCSIS link. This helps to conserve link bandwidth, especially with types of traffic, such as voice, where the header size tends to be as large as the size of the actual packet.

Service Classes

The QoS attributes of a service flow can be specified in two ways: either explicitly by defining all attributes, or implicitly by specifying a service class name. A service class name is a string that the CMTS associates with a QoS parameter set.

The service class serves the following purposes:

- It allows operators to move the burden of configuring service flows from the provisioning server to the CMTS. Operators provision the modems with the service class name; the implementation of the name is configured at the CMTS. This allows operators to modify the implementation of a given service to local circumstances without changing modem provisioning. For example, some scheduling parameters might need to be set differently for two different CMTSs to provide the same service. As another example, service profiles could be changed by time of day.
- It allows CMTS vendors to provide class-based-queuing if they choose, where service flows compete within their class, and classes compete with each other for bandwidth.
- It allows higher-layer protocols to create a service flow by its service class name. For example, telephony signaling might direct the cable modem to instantiate any available provisioned service flow of class G.711.

Note The service class is optional. The flow scheduling specification may always be provided in full; a service flow may belong to no service class whatsoever. CMTS implementations *may* treat such unclassed flows differently from classed flows with equivalent parameters.

Any service flow can have its QoS parameter set specified in any of three ways:

- By explicitly including all traffic parameters.
- By indirectly referring to a set of traffic parameters by specifying a service class name.
- By specifying a service class name along with modifying parameters.

The service class name is expanded to its defined set of parameters at the time the CMTS successfully admits the service flow.

Secure Software Download

Secure software download ensures that the cable modem downloads only the proper software image from a properly authenticated server. The software transfer is encrypted to prevent users and hackers from intercepting the download and substituting their own software image in its place.

How to Configure DOCSIS 1.1 Support

The Cisco uBR905 and Cisco uBR925 cable access routers and Cisco CVA122 cable voice adapters automatically support all DOCSIS 1.1 features when running Cisco IOS Release 12.2(15)CZ. Many DOCSIS 1.1 features, however, must be specifically enabled through the DOCSIS configuration file that is downloaded to the router at initialization time. Special configuration is also needed to use provisioned quality-of-service (PQoS) for VoIP calls.

See the following sections for the configuration tasks for each feature. Each tasks in the list is identified as either required or optional.

- Creating a DOCSIS 1.1 Configuration File, page 20 (Required)
- Performing a Secure Software Download, page 27 (Optional)
- Configuring for Provisioned Quality-of-Service, page 30 (Optional)
- Verifying the DOCSIS 1.1 Configuration, page 33 (Optional)
- Verifying the SNMPv3 Diffie-Hellman Configuration, page 34 (Optional)

Creating a DOCSIS 1.1 Configuration File

No special configuration is needed to enable basic DOCSIS 1.1 operation, but the DOCSIS configuration file can be used to control which DOCSIS 1.1 features are enabled and used during a session.

In addition to enabling the different DOCSIS 1.1 features, special fields in the DOCSIS configuration files are needed to enable SNMPv3 operation and to configure the router for the secure software download procedure. The following sections describe these procedures:

- DOCSIS 1.1 Feature Configuration, page 21
- Configuring the SNMPv3 Diffie-Hellman Kickstart Public Key, page 22
- Configuring for Secure Software Download, page 24

These procedures assume that you are using the Cisco DOCSIS Configurator Tool, version 3.6 or later, to generate the DOCSIS 1.1 configuration files for the cable modems. This tool is available on Cisco.com at http://www.cisco.com/cgi-bin/tablebuild.pl/cpe-conf.

DOCSIS 1.1 Feature Configuration

A DOCSIS 1.1-capable cable modem informs the CMTS that it is capable of DOCSIS 1.1 operation by sending a DHCP request that includes option 60, Vendor Class Identifier, with a value of "docsis1.1:xxxxxxx", where xxxxxxx is an ASCII string with the hexadecimal encoding of the encoding of the modem's capabilities. This field informs the CMTS of the following information:

- DOCSIS version
- Concatenation support
- Fragmentation support
- Payload header suppression (PHS) support
- DOCSIS-compliant IGMP support
- BPI or BPI+ support
- Number of downstream SAIDs supported
- Number of upstream SAIDs supported
- Packet filtering support
- Dynamic Channel Change (DCC) support

The option 60 message does not enable DOCSIS 1.1 operation but only informs the CMTS of the cable modem's capabilities. To enable the different DOCSIS 1.1 features, you must specifically enable the following options in the DOCSIS configuration file:

- Baseline privacy configuration setting
- Privacy enable configuration setting
- Payload header suppression
- Downstream service flow encodings
- Upstream service flow encodings
- Maximum number of classifiers

Note For more information about these parameters, see Appendix D, "CM Configuration Interface Specification," in the DOCSIS 1.1 specification, *Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification* (SP-RFIv1.1-I08-020301).

Configuring the SNMPv3 Diffie-Hellman Kickstart Public Key

Before a DOCSIS 1.1 cable modem can initiate BPI+ encryption, it must be configured with a shared public key that allows it to securely transfer the BPI+ encryption keys with the CMTS. Use the following procedure to configure the Cisco uBR905, Cisco uBR925, or Cisco CVA122 with the required public key.

The DOCSIS 1.1 specification refers to this procedure as *SNMPv3 Diffie-Hellman Kickstart*. This procedure needs to be done only once, unless the public keys are changed on the CMTS, or the Cisco uBR905, Cisco uBR925, or Cisco CVA122 is moved to a different CMTS that uses a different public key.

Step 1 Use your SNMPv3 manager software to generate a 128-byte (1024-bit) public key for the CMTS.

Step 2 Add this public key to a DOCSIS configuration file along with the built-in DOCSIS operator "docsisOperator" in the "SnmpV3 Kickstart Value" field (TLV 34). Put the "docsisOperator" value in field 34.1 and the public key in field 34.2.

For example, if you are creating an ASCII file and using the Cisco DOCSIS Configurator tool to convert it into the binary DOCSIS configuration file, you would specify lines such as the following:

```
34 (SNMPv3 Kickstart Values)
 S01 (Kickstart Security Name) = docsisOperator
 S02 (Kickstart Mgr Public Number) = b1 01 c2 0F F4 3C ... (exactly 128 hex bytes)
```

To enter this data directly into the Configurator tool, click on the SNMP tab and enter this data into the first available row in the "SNMP V3 Kickstart Value" table. Figure 2 shows an example of this using version 3.7 of the Cisco DOCSIS Configurator tool. Figure 3 shows an example of this using version 4.0 of the Cisco Broadband Configurator tool.

Figure 2 Entering the Kickstart Values into Cisco DOCSIS Configurator Version 3.7

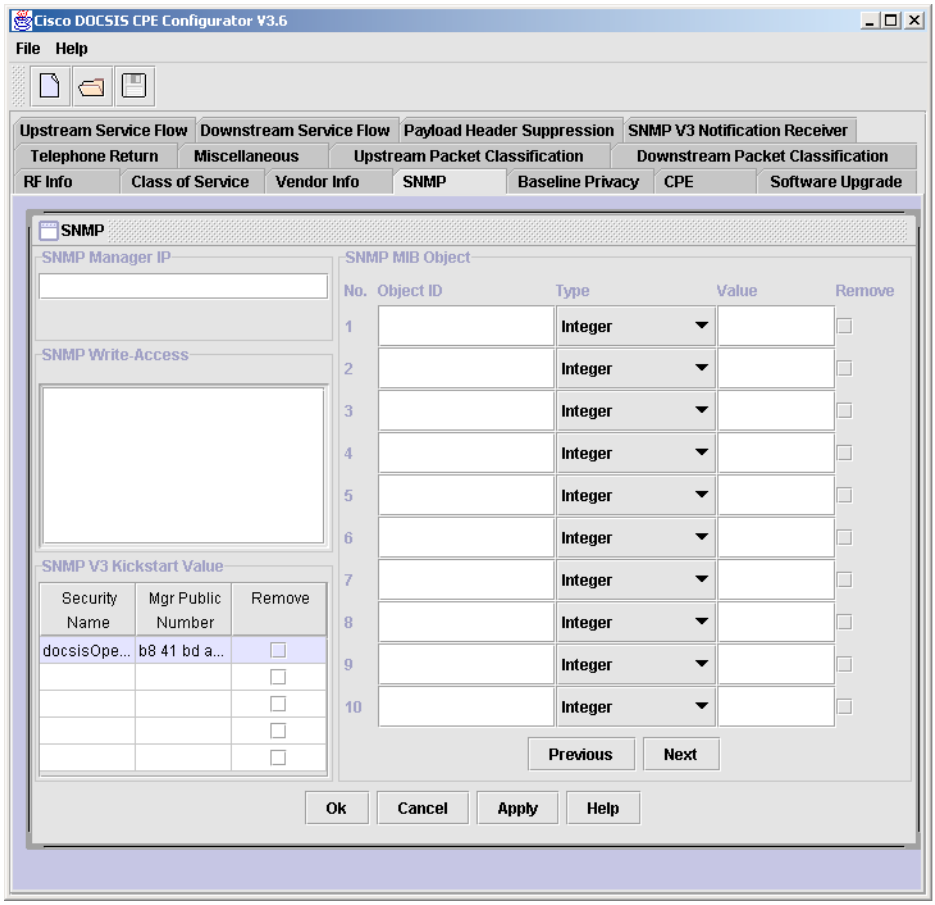
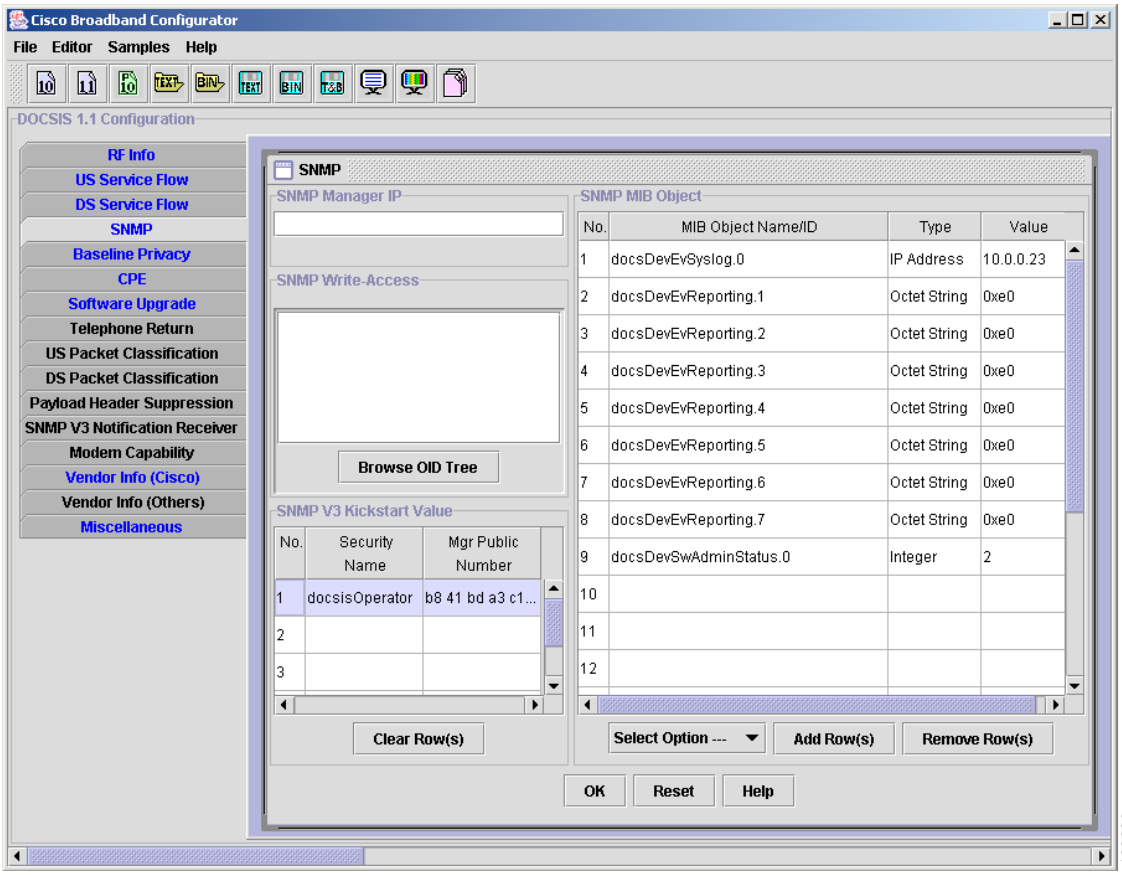


Figure 3 Entering the Kickstart Values into Cisco Broadband Configurator Version 4.0



Tip Enter the hexadecimal digits of the public key separated either by spaces or by hyphens, and without a "0x" hexadecimal prefix. The public key must contain exactly 128 hexadecimal bytes.

Step 3 After entering all other required values into the DOCSIS configuration file, reset the Cisco uBR905, Cisco uBR925, or Cisco CVA122, and download the DOCSIS configuration file to it.

Configuring for Secure Software Download

Before a DOCSIS 1.1 cable modem can perform a secure software download, it must be configured with the code verification certificates (CVCs) that allow it to securely transfer the software file from the CMTS. The manufacturer's CVC (M-CVC) verifies that the software image has been properly signed by the manufacturer (in this case, Cisco Systems). The optional cosigner's CVC (C-CVC) verifies that the software image has been signed by the Multi-Service Operator (MSO) that is providing the cable network.

Use the following procedure to configure the Cisco uBR905, Cisco uBR925, or Cisco CVA122 with the required certificates.

Step 1 Add the manufacturer's CVC to a DOCSIS configuration file in the "Manufacturer Code Verification Certificate" field (TLV 32). If using the graphical interface of the DOCSIS Configurator tool, enter the CVC data directly into the Configurator tool by clicking the Miscellaneous tab and entering the data in the "Manufacturer CVC" field. See Figure 4.

Figure 4 shows an example of this using version 3.7 of the Cisco DOCSIS Configurator tool. Figure 5 shows an example of this using version 4.0 of the Cisco Broadband Configurator tool.

Figure 4 Entering the M-CVC into Cisco DOCSIS Configurator Release 3.7

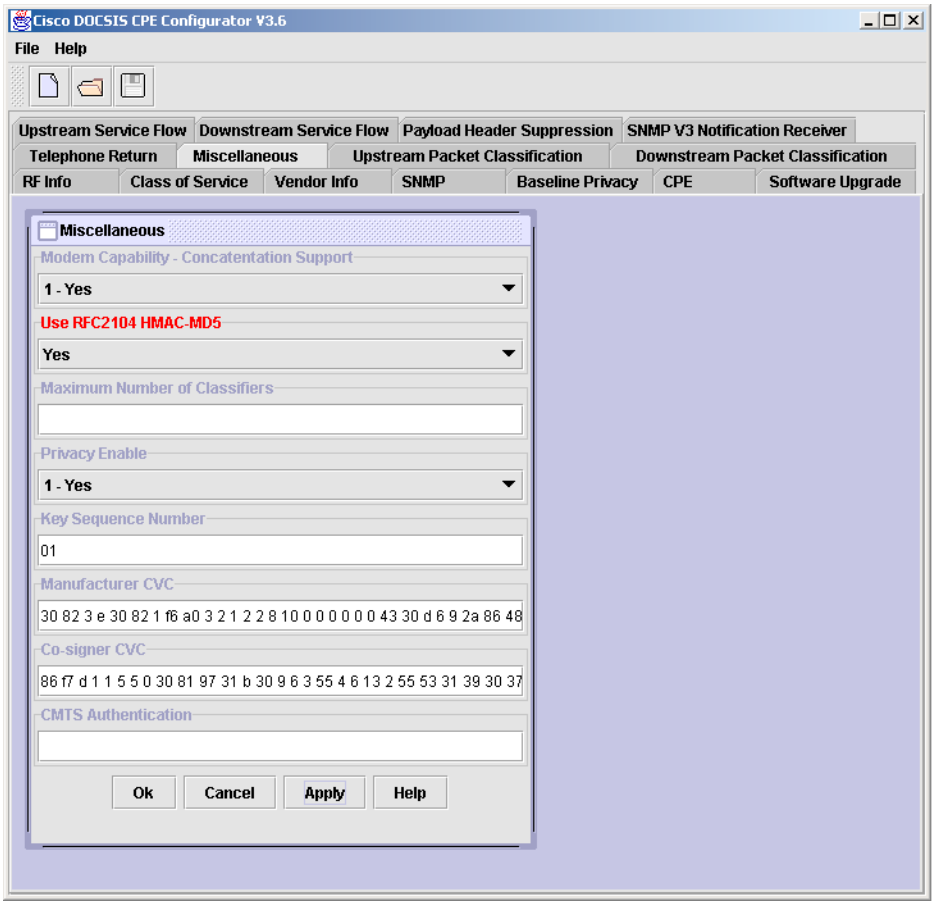
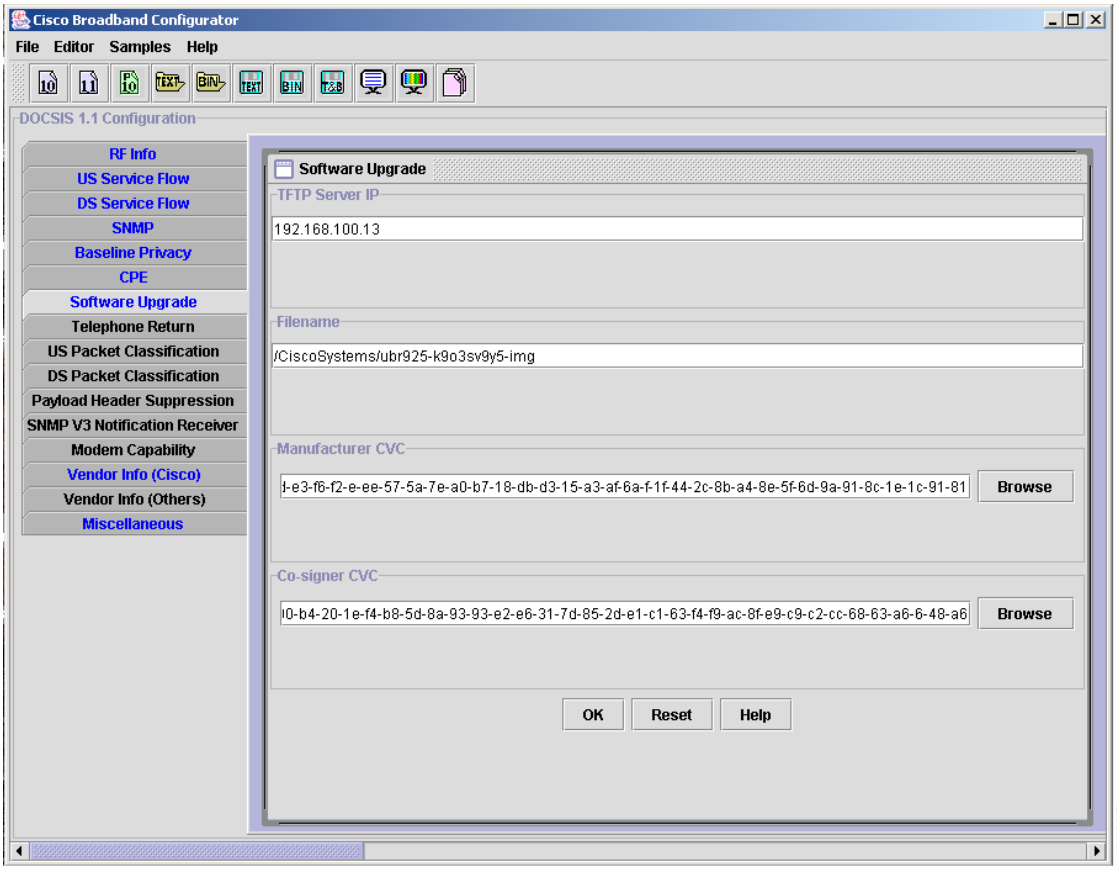


Figure 5 Entering the M-CVC into Cisco Broadband Configurator Release 4.0



Tip Enter the hexadecimal digits of the public key separated either by spaces or by hyphens, and without a "0x" hexadecimal prefix. The public key must contain exactly 128 hexadecimal bytes.

You can also create an ASCII file and use the DOCSIS Configurator tool to convert it into the binary DOCSIS configuration file. However, if the M-CVC contains more than 254 bytes, you must break it apart into successive fields, with each field except the last containing exactly 254 bytes.

The following shows a typical example of an M-CVC that is greater than 254 bytes:

```
32 (Manufacturer CVC)          = 30 A2 4E 23 ... F1 C5 (exactly 254 bytes)
32 (Manufacturer CVC)          = 21 36 A4 9F ... 3E 13 (exactly 254 bytes)
32 (Manufacturer CVC)          = 0F 12 13 (254 bytes or less)
```

If you are using Release 3.7 or later of the DOCSIS Configurator tool, you can also specify TLV 320, which allows you to specify the location of the actual M-CVC binary file on the local disk. The Configurator then reads the file and saves the CVC as part of the DOCSIS configuration file. This avoids having to convert the CVC into a hexadecimal format, as shown above.

For example, if you are running the DOCSIS Configurator on a Windows workstation, and you have saved the M-CVC in the file D:\CiscoM.cvc, use the following line into the ASCII file:

```
320 (Manufacturer CVC)          = D:\CiscoM.cvc
```

Step 2 If required, add the optional cosigner's code verification certificate (C-CVC) to a DOCSIS configuration file in the Co-Signer's code verification certificate field (TLV 33). To enter this data directly into the Configurator tool, click on the Miscellaneous tab and enter this data in the Co-signer CVC table (see Figure 4 on page 25).

If you are creating an ASCII configuration file and converting it into the binary DOCSIS configuration file, and if the C-CVC contains more than 254 bytes, you must break it apart into successive TLV 33 fields, and each field except the last must contain exactly 254 bytes. The following shows a typical example of an C-CVC that is greater than 254 bytes:

```
33 (Co-signer CVC)          = 03 2A E4 35 ... E7 D2 (exactly 254 bytes)
33 (Co-signer CVC)          = 12 A4 36 4B ... 11 1F (exactly 254 bytes)
33 (Co-signer CVC)          = AB D0 F4 (254 bytes or less)
```

If you are using Release 3.7 or later of the DOCSIS Configurator tool, you can also specify TLV 330, which allows you to specify the location of the actual C-CVC binary file on the local disk. The Configurator then reads the file and saves the CVC as part of the DOCSIS configuration file. This avoids having to convert the CVC into a hexadecimal format, as shown above.

For example, if you are running the DOCSIS Configurator on a Windows workstation, and you have saved the C-CVC in the file D:\MSO.cvc, use the following line into the ASCII file:

```
330 (Co-signer CVC)          = D:\MSO.cvc
```

Note If you use TLV 320 or TLV 330, you must specify the location of the actual CVC file, in its binary, encoded form. Do not specify a text file with a hexadecimal dump of the CVC.

Step 3 After entering all other required values into the DOCSIS configuration file, reset the Cisco uBR905, Cisco uBR925, or Cisco CVA122, and download the DOCSIS configuration file to it.

Performing a Secure Software Download

Use the following procedures to download a digitally signed software image to the router using the secure software download procedure.

- Downloading the Image During Initialization Through the DOCSIS Configuration File, page 28
- Downloading the Image After Initialization Through SNMP, page 30

These procedures assume that the required CVCs have been downloaded to the router (see the "Configuring for Secure Software Download" section on page 24) and that the router is already running a DOCSIS 1.1 software image.

Note If the cable modem did not receive a valid CVC in the DOCSIS configuration file, the secure software download fails with the debug message "Boot file is current." This indicates that the cable modem is continuing to use the current software image. Verify that the DOCSIS configuration file contains a valid CVC for the software image being downloaded.

Caution It is also possible to upgrade the Cisco IOS software by setting the configuration register to 0x00 and booting the router into the ROM monitor (ROMMON). However, this method is not recommended because it requires manually connecting a terminal to the router's console port and downloading the software image using the X-Modem protocol. Also, this *must never* be done on the Cisco CVA122 Cable Voice Adapters because these routers do not have a console port. You will not be able to recover the Cisco CVA122 if you boot it into the ROM monitor, and instead will have to return it to the factory for repair or replacement.

Tip Cisco IOS software images that include "cvc" as part of the filename (ubr925cvc-k9o3sv9y5-mz) are digitally signed. Unsigned software images do not include "cvc" as part of the filename (ubr925-k9o3sv9y5-mz). If you are using secure software download, you *must* use a digitally signed image (includes "cvc"). If you are not using secure software download, you *must* use an unsigned image (does not include "cvc"). To avoid confusion, Multi-Service Operators (MSO) should choose a different suffix to identify images that they cosign for use on their network.

Downloading the Image During Initialization Through the DOCSIS Configuration File

After you have upgraded the router to Cisco IOS Release 12.2(15)CZ, or another DOCSIS 1.1 software image, the router must use the DOCSIS 1.1 secure software download feature to upgrade its software image. During initialization, the cable modem compares its current software image with the one specified in the DOCSIS configuration file and, if they do not match, the cable modem downloads the new software image from the specified TFTP server. The router verifies the digital signature of the downloaded file to ensure that the software image has not been corrupted or altered during transmission.

Use the following procedure to copy the Cisco IOS software image and new DOCSIS 1.1 certificates to the TFTP server used by the cable modems.

Note If you have not already downloaded the required CVCs to the router, you must also do that now by setting TLVs 32 or 33 in the DOCSIS configuration file. See the "Configuring for Secure Software Download" section on page 24 for more information. If you do not load the CVCs into the cable modem before sending the SNMP commands, the download fails with an error status.

Step 1 Copy the Cisco IOS Release 12.2(15)CZ software images to the TFTP server for the cable modems. Typically, they should be put into the same directory that contains the other Cisco IOS software images.

For a DOCSIS secure software download, you must use a digitally signed software image, which includes "cvc" as part of the software image filename.

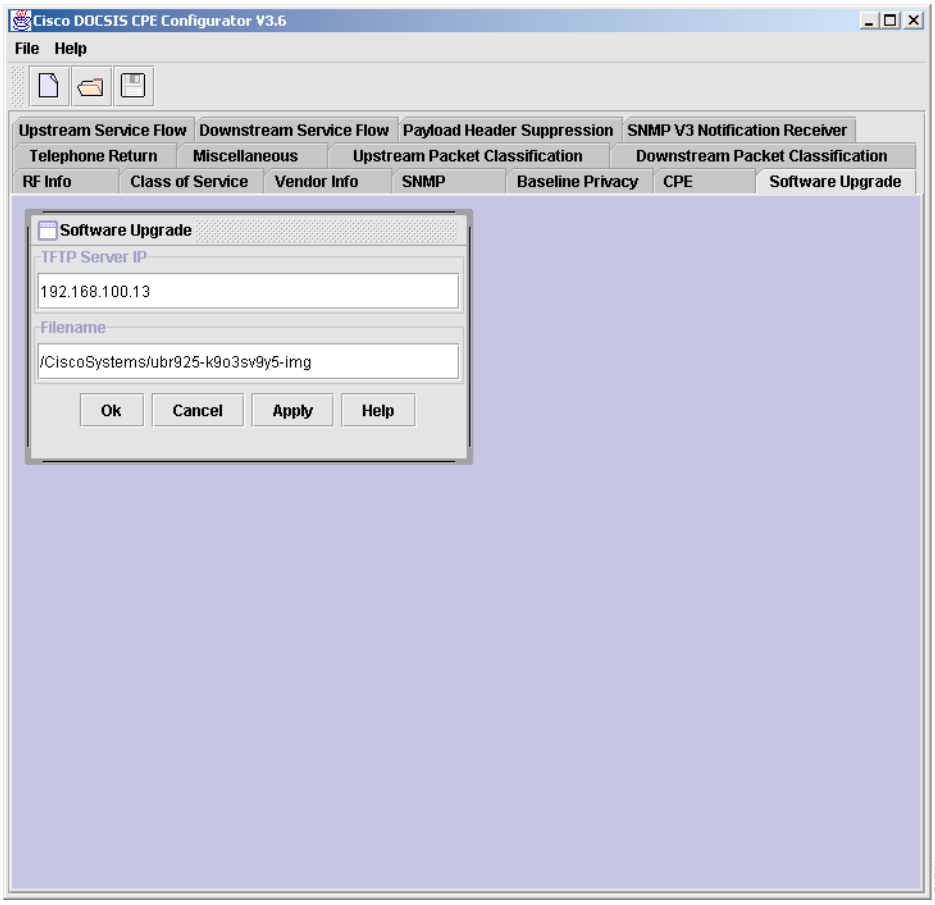
Note The Cisco uBR905 and Cisco uBR925 cable access routers and Cisco CVA122 Cable Voice Adapters will not upgrade the software image unless the Cisco IOS Release 12.2(15)CZ software image filename is different than the filename of the software image that the router is currently running. An easy way to ensure this is by adding "12215CZ" to the filename (for example, cva120-k8o3v9y5-mz.12215CZ.bin or ubr925cvc-k9o3sy5-mz.12215CZ.bin).

Step 2 Create a DOCSIS 1.1 configuration file that instructs the Cisco uBR905 or Cisco uBR925 cable access router, or the Cisco CVA122 Cable Voice Adapter to download the new Cisco IOS Release 12.2(15)CZ software image. This information is contained in the following configuration file options:

- Software Upgrade Filename (Option 9)—Specifies the full filename and path for the software image on the TFTP server. To support a secure software download, you must specify a software image that has been digitally signed (includes “cvc” as part of the filename).
- TFTP Server IP (Option 21)—IP address of the TFTP server that will provide the new software image.
- Manufacturer CVC (Option 32)—Specifies the code verification certificate (CVC) that Cisco Systems used to digitally sign the Cisco IOS software image. The router uses this CVC to verify the software image that is downloaded using DOCSIS secure software download.

You can create this file using any DOCSIS 1.1 configuration file editor, such as the Cisco DOCSIS Configurator Tool (release 3.7). For example, Figure 6 shows an example that specifies the image ubr925cvc-k9o3sv9y5-mz in the directory /CiscoSystems on the TFTP server at IP address 192.168.100.13. (See Figure 5 on page 26 for an example of Cisco Broadband Configurator version 4.0.)

Figure 6 Software Upgrade Parameters



If you are creating an ASCII configuration file and using the DOCSIS Configurator tool to convert it into the binary DOCSIS configuration file, you would enter these same values as follows:

```
09 (Software Upgrade Filename) =  /CiscoSystems/ubr925cvc-k9o3sv9y5-mz

21 (TFTP Server IP)            = 192.168.100.13
```

Step 3 Configure the DOCSIS 1.1 configuration file with the other parameters appropriate for your network and for this router. In particular, you should enable BPI+ operation.

Step 4 Copy the DOCSIS 1.1 configuration file to your TFTP server.

Step 5 Configure your DOCSIS cable provisioning software (such as a DHCP server or Cisco Network Registrar) so that it sends the DOCSIS 1.1 configuration file as the DHCP bootfile during the initial provisioning.

Step 6 Restart the router, either by turning it off and then back on, or by using the **reload** command in privileged EXEC mode.

When the router or Cisco CVA122 Cable Voice Adapter is restarted, it downloads the DOCSIS 1.1 configuration file, which forces the router to download the Cisco IOS Release 12.2(15)CZ software image using the DOCSIS secure software download. The router then reloads and boots the Cisco IOS Release 12.2(15)CZ image.

Downloading the Image After Initialization Through SNMP

You can download a new software image to a DOCSIS 1.1 cable modem by setting the following SNMP attributes in the DOCS-CABLE-DEVICE-MIB:

- docsDevSwServer—Specifies the IP address for the Software Upgrade TFTP Server.
- docsDevSwFilename—Specifies the fully qualified Software Upgrade Filename. This attribute has a maximum size of 64 characters, so if the fully qualified filename is larger than this, you must move the file to a different subdirectory so that the full filename is 64 bytes or fewer.
- docsDevSwAdminStatus—Sets to 1 (upgradeFromMgt) to initiate the secure software download procedure, using the current values in the docsDevSwServer and docsDevSwFilename attributes.

You can monitor the status of the download by polling the docsDevSwOperStatus attribute, which returns 1 (inProgress) while the download is progressing and 3 (completeFromMgt) when the download is complete. You can also enable Secure Software Download traps using the **snmp-server enable traps docsis-cm** command, so that the SNMP manager is notified when the download succeeds.

Note If you have not already downloaded the required CVCs to the router, you must also do that now by setting TLVs 32 or 33 in the DOCSIS configuration file. See "Configuring for Secure Software Download" section on page 24 for more information. If you do not load the CVCs into the cable modem before sending the SNMP commands, the download fails with an error status.

Configuring for Provisioned Quality-of-Service

To use provisioned quality-of-service (PQoS) for outgoing VoIP calls, configure the outgoing dial-peer with the **req-qos** command, and optionally with the **ip qos dscp** command. The following example shows an H.323v2 dynamic mapping configuration for an outgoing dial peer that uses the Registration, Admission, and Status (RAS) protocol to allow a remote gatekeeper to translate phone numbers (E.164 addresses) to the IP addresses of the specific dial peers.

Note The information in this section applies only to the Cisco CVA122 Cable Voice Adapter and the Cisco uBR925 cable access router. Complete VoIP configuration information is given in the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2T.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *id-number* **voip**
4. **destination-pattern** *digits*
5. **session target ras**
6. **codec** {**g711alaw** | **g711ulaw** | **g723ar53** | **g723ar63** | **g726r16** | **g726r24** | **g726r32** | **g729br8** | **g729r8**}
7. **dtmf-relay** {**cisco-rtp** | **h245-signal** | **h245-alphanumeric**}
8. **req-qos** {**best-effort** | **controlled-load** | **guaranteed-delay**}
9. **ip precedence** *number*
10. **ip qos dscp** *class-selector* **media**
11. **exit**
12. **gateway**
13. **exit**

DETAILED STEPS

	Command	Description

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	**dial-peer voice** *id-number* **voip**
	
	Example:
	`Router(config)# dial-peer voice 13 voip`
	`Router(config-dial-peer)#`
		Specifies a unique ID number for this outgoing dial peer and enter dial-peer configuration mode.

Step 4	**destination-pattern** *digits*
	
	Example:
	`Router(config-dial-peer)# destination-pattern 5551212`
	`Router(config-dial-peer)#`
		Specifies the telephone numbers associated with this dial peer.

	Command	Description

Step 5	**session target ras**
	
	Example:
	`Router(config-dial-peer)# session target ras`
	`Router(config-dial-peer)#`
		Specifies that RAS will be used to resolve the destination for the dial peer.

Step 6	**codec** {**g711alaw** | **g711ulaw** | **g723ar53** | **g723ar63** | **g726r16** | **g726r24** | **g726r32** | **g729br8** | **g729r8**}
	
	Example:
	`Router(config-dial-peer)# codec g711ulaw`
	`Router(config-dial-peer)#`
		(Optional) Specifies the codec algorithm to be used for these calls. The default is g711r8 (8Kbps compression; A-Law and Mu-Law are 64 Kbps compression).

Step 7	**dtmf-relay** {**cisco-rtp** | **h245-signal** | **h245-alphanumeric**}
	
	Example:
	`Router(config-dial-peer)# dtmf-relay cisco-rtp`
	`Router(config-dial-peer)#`
		(Optional) Configures the dial peer to support out-of-band signaling of DTMF tones.

Step 8	**req-qos** {**best-effort** | **controlled-load** | **guaranteed-delay**}
	
	Example:
	`Router(config-dial-peer)# req-qos guaranteed-delay`
	`Router(config-dial-peer)#`
		Specifies the desired method of QoS for calls to this dial peer:
		• **best-effort**—(Default) Indicates that Resource Reservation Protocol (RSVP) makes no bandwidth reservation.
		• **controlled-load**—Indicates that RSVP guarantees a single level of preferential service, presumed to correlate to a delay boundary. The controlled load service uses admission (or capacity) control to ensure that preferential service is received even when the bandwidth is overloaded.
		• **guaranteed-delay**—Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.
		Note For PQoS services, specify **guaranteed-delay**.

Step 9	**ip precedence** *number*
	
	Example:
	`Router(config-dial-peer)# ip precedence 5`
	`Router(config-dial-peer)#`
		(Optional) Specifies an IP packet precedence level (1-5) for packets carrying calls to this dial peer (1-5, where 5 is the highest precedence for normal IP flows).

	Command	Description

Step 10	**ip qos dscp** *class-selector* **media**
	
	Example:
	`Router(config-dial-peer)# ip qos dscp cs5 media`
	`Router(config-dial-peer)#`
		(Optional) Specifies that the packet's IP precedence level is specified in the Differentiated Services Code Point (DSCP) field in the IP packet. The class-selector specifies the precedence level:
		• cs1—codepoint 1 (precedence 1)
		• cs2—codepoint 2 (precedence 2)
		• cs3—codepoint 3 (precedence 3)
		• cs4—codepoint 4 (precedence 4)
		• cs5—codepoint 5 (precedence 5)
		• cs5—codepoint 6 (precedence 6)
		• cs7—codepoint 7 (precedence 7)

	Typically, the **ip qos dscp** command should be used instead of the **ip precedence** command.	

Step 11	**exit**
	
	Example:
	`Router(config-dial-peer)# exit`
	`Router(config)#`
		Exits dial-peer configuration mode.

Step 12	**gateway**
	
	Example:
	`Router(config)# gateway`
	`Router(config)#`
		Enables the VoIP gateway on the router.

Step 13	**exit**
	
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Verifying the DOCSIS 1.1 Configuration

To display the DOCSIS 1.1 QoS statistics, including the type of service flow and packet classifiers being used for each queue, use the **show controllers cable-modem qos** command:

```
Router# show controllers cable-modem 0 qos

Queue   SID     SID     SFID    TX      TX      RX      RX      Capabilities
                Type            Pkts    Bytes   Pkts    Bytes   cbr cc fr nbr

0       1       Primary 3       40      5740    2780    209346   F  T  T  F
1       56      Dynamic 91      1782    160140  0       0        T  T  T  T
2       58      Dynamic 93      690     61946   0       0        T  T  T  T
3       0       NA      0       0       0       0       0        F  F  F  F


Queue    SF Type
0        BE
1        BE
2        UGS_AD
```

```
3        NA


Packet Classifiers

Class id   SFID   Pri     valid    Match     SIDT
   1       91     0       D6       1782      80D2754C
   2       93     0       D6       691       80D275C0

Packet Classifier Details

Classifier id = 1    SFID =  91
IP source: 10.188.1.88
IP dest: 10.188.1.66
UDP/TCP source range: 18416   to  18416
UDP/TCP dest range: 16740   to  16740
IP Protocol: 17
PHS: Inactive

Classifier id = 2    SFID =  93
IP source: 10.188.1.88
IP dest: 10.188.1.66
UDP/TCP source range: 16796   to  16796
UDP/TCP dest range: 19138   to  19138
IP Protocol: 17
PHS: Inactive

Downstream Payload Header Suppression

Router#
```

Verifying the SNMPv3 Diffie-Hellman Configuration

Use the following procedure to verify that the SNMPv3 Diffie-Hellman Kickstart configuration has been accomplished and that SNMPv3 operations are enabled on the router.

Step 1 Display the current SNMP users using the **show snmp user** command. The dhKickstart user should be shown as a permanent and active user.

```
Router# show snmp user

User name: docsisUser
Engine ID: 800000090300000164FFE2E0
storage-type: nonvolatile        active

User name: dhKickstart
Engine ID: 800000090300000164FFE2E0
storage-type: permanent  active

User name: docsisManager
Engine ID: 800000090300000164FFE2E0
storage-type: nonvolatile        active

User name: docsisMonitor
Engine ID: 800000090300000164FFE2E0
storage-type: nonvolatile        active

User name: docsisOperator
Engine ID: 800000090300000164FFE2E0
storage-type: permanent  active
```

```
Router#
```

Step 2 Display the current SNMP groups using the **show snmp group** command. The dhKickstart user should be shown as a permanent and active user.

```
Router# show snmp group

groupname: docsisUser                   security model:v3 auth
readview :docsisUserView                writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active

groupname: dhKickstart                  security model:v3 noauth
readview :dhKickRestricted              writeview: <no writeview specified>
notifyview: <no notifyview specified>
row status: active

groupname: docsisManager                security model:v3 priv
readview :docsisManagerView             writeview: docsisManagerView
notifyview: docsisManagerView
row status: active

groupname: docsisMonitor                security model:v3 auth
readview :docsisMonitorView             writeview: <no writeview specified>
notifyview: docsisMonitorView
row status: active

groupname: docsisOperator               security model:v3 priv
readview :docsisManagerView             writeview: docsisOperatorWriteView
notifyview: docsisManagerView
row status: active

Router#
```

Step 3 Use an SNMP manager to display the cable modem's and manager's public keys by using an SNMPv3 GET request for the dhKickstart attribute. The following example shows a typical display using a UNIX workstation.

```
% getmany -v3 3.107.1.26 dhKickstart usmDHKickstartTable

Enter Authentication password :
usmDHKickstartMyPublic.1 =
68 9d  bf 85   14 60  e6 b1    fc 82  3d 8c   74 11  75 e0
c1 db  dc 84   82 55  a3 a0    a2 72  22 b7   66 a5  a2 cf
53 27  6d c7   4a ec  73 51    f8 25  51 4a   e8 ce  3c bf
1a e4  27 0b   a6 dd  8e 91    ef 6c  0f 9b   86 6d  28 75
dc e5  a9 36   c2 1f  fc aa    0d 50  06 67   83 1e  e8 79
63 b1  b4 1e   5a f1  36 8f    30 cd  2e 95   f9 3f  68 35
a0 a5  5a 1e   63 13  ab c5    72 95  9e 1d   21 20  63 13
b9 e1  5f 63   d8 6d  b5 85    1c 13  e2 53   49 c8  d1 5f
usmDHKickstartMgrPublic.1 =
cb 93  08 0f   fe 24  32 06    4c 28  ed 8b   de e8  37 a3
d5 be  9d 7b   87 45  6e 4e    e5 2c  10 ff   48 aa  cc b0
3c d3  ef 09   c0 e9  c6 84    29 6b  9b ed   3b f6  a6 9d
a5 7e  90 2b   31 bc  1a 42    5e 2d  e3 ae   46 c4  2d 92
35 66  bc 7c   ce 5c  bf a3    4f 9d  f4 48   b8 e8  2d 35
6c bd  1d c1   01 53  2b d3    91 eb  4f 9e   10 da  96 65
09 b6  6f ec   ec a2  21 5e    2e 30  7b 6c   36 27  76 0e
b4 7e  f4 0f   49 26  67 70    f5 9d  df d9   63 fc  5b 5a
usmDHKickstartSecurityName.1 = docsisOperator
End of MIB.
```

```
%
```

Configuration Examples for DOCSIS 1.1 Support

The following shows a typical DOCSIS 1.1 configuration example for a Cisco uBR925 cable access router or Cisco CVA122 Cable Voice Adapter. In this example, the router is in DOCSIS bridging mode and is configured for PQoS mode for VoIP calls.

```
version 12.2
no parser cache
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
!
!
docsis cvc mfg organization "Cisco Systems"
docsis cvc mfg codeAccessStart 011219000000Z
docsis cvc mfg cvcAccessStart 011219000000Z
clock timezone - -8
ip subnet-zero
no ip routing
!
ip audit notify log
ip audit po max-events 100
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0
 ip address 10.107.1.39 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 bridge-group 59
 bridge-group 59 spanning-disabled
!
interface cable-modem0
 ip address docsis
 no ip route-cache
 no ip mroute-cache
 bridge-group 59
 bridge-group 59 spanning-disabled
!
interface usb0
 ip address 10.107.1.39 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 arp timeout 0
```

```
 bridge-group 59
 bridge-group 59 spanning-disabled
!
ip default-gateway 10.107.1.1
ip classless
ip pim bidir-enable
no ip http server
no ip http cable-monitor
!
!
snmp-server user docsisUser docsisUser v3
snmp-server user docsisMonitor docsisMonitor v3
snmp-server user docsisOperator docsisOperator v3
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps docsis-cm
snmp-server packetsize 4096
snmp-server manager
bridge cmf
call rsvp-sync
!
voice-port 0
 input gain -2
 output attenuation 0
 ren 0
!
voice-port 1
 input gain -2
 output attenuation 0
 ren 0
!


mgcp profile default
 !
 dial-peer voice 100 pots
  destination-pattern 7271
  port 0
 !
 dial-peer voice 1000 voip
  huntstop
  destination-pattern 1...
  session target ras
  req-qos guaranteed-delay
  codec g711ulaw
  ip qos dscp cs3 media
  no vad
 !
 dial-peer voice 2000 voip
  huntstop
  destination-pattern 2...
  session target ras
  req-qos guaranteed-delay
  codec g711ulaw
  ip qos dscp cs3 media
  no vad
 !
 dial-peer voice 3000 voip
  huntstop
  destination-pattern 3...
  session target ras
  req-qos guaranteed-delay
  codec g711ulaw
  ip qos dscp cs3 media
  no vad
```

```
 !
 dial-peer voice 4000 voip
  huntstop
  destination-pattern 4...
  session target ras
  req-qos guaranteed-delay
  codec g711ulaw
  ip qos dscp cs3 media
  no vad
 !
 dial-peer voice 5000 voip
  huntstop
  destination-pattern 5...
  session target ras
  req-qos guaranteed-delay
  codec g711ulaw
  ip qos dscp cs3 media
  no vad
 !
 gateway

!
line con 0
line vty 0 4
 login
!
scheduler max-task-time 5000
end
```

Additional References

The following sections provide references related to DOCSIS 1.1 Support.

Related Documents

Related Topic	Document Title
Additional DOCSIS 1.1 configuration	• *Migrating Simple Data over Cable Services to DOCSIS 1.1* • *DOCSIS CPE Configurator Help* • *Classifying VoIP Signaling and Media with DSCP for QoS* • *Upgrading the DOCSIS Certificates in Cisco uBR905/uBR925 Cable Access Routers and CVA122 Cable Voice Adapters*
Hardware Installation	• *Cisco uBR905 Hardware Installation Guide* • *Cisco uBR925 Hardware Installation Guide* • *Cisco uBR905 Cable Access Router Subscriber Setup Quick Start Card* • *Cisco uBR925 Cable Access Router Subscriber Setup Quick Start Card* • *Cisco uBR925 Quick Start User Guide* • *Cisco CVA122 Cable Voice Adapter Hardware Installation Guide* • *Cisco CVA122 Cable Voice Adapter Subscriber Setup Quick Start Card*
Software Configuration	• *Cisco uBR905/uBR925 Software Configuration Guide* • *Cisco CVA122 Cable Voice Adapter User Guide* • *Cisco CVA122 Cable Voice Adapter Features*
Command Reference Guide	• *Cisco Broadband Cable Command Reference Guide*

Standards

Standards	Title
SP-RFIv1.1-I08-020301	DOCSIS 1.1 specification
SP-BPI+-I08-020301	Baseline Privacy Interface Plus Specification
PKT-SP-DQOS-I03-020116	PacketCable™ Dynamic Quality-of-Service Specification
ITU X.509	International Telecommunications Union (ITU) X.509 Version 3.0 standard

MIBs

MIBs	MIBs Link
• DOCS-BPI-PLUS-MIB (replaces DOCS-BPI-MIB, which is supported only in DOCSIS 1.0)[1] • DOCS-QOS-MIB • DOCS-SUBMGT-MIB[2] • DOCS-CABLE-DEVICE-MIB (RFC 2669) • DOCS-IF-MIB (RFC 2670) • DOCS-CABLE-DEVICE-TRAP-MIB (extends RFC 2669, DOCS-CABLE-DEVICE-MIB) • DOCS-IF-EXT-MIB (extends RFC 2670, DOCS-IF-MIB) • IGMP-STD-MIB (RFC 2933) • SNMP-COMMUNITY-MIB (RFC 2576) • SNMP-USM-MIB (RFC 2574) • SNMP-USM-DH-OBJECTS-MIB (RFC 2786)	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. As required by the DOCSIS specifications, a DOCSIS 1.1 CMTS and CM support only the attributes in DOCS-BPI-PLUS-MIB and not the attributes in DOCS-BPI-MIB.
2. In addition, the CLI supports a new command (**cable submgmt default**) to set the default value of attributes in DOCS-SUBMGT-MIB. This command can be included in the Cisco IOS configuration file so that the new values are automatically set after a reboot or reload of the Cisco uBR7200 series router.

RFCs

RFCs	Title
RFC 1112	*Host Extensions for IP Multicasting*
RFC 2104	*HMAC: Keyed-Hashing for Message Authentication*
RFC 2236	*Internet Group Management Protocol, Version 2*
RFC 2271	*An Architecture for Describing SNMP Management Frameworks*
RFC 2272	*Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*
RFC 2273	*SNMPv3 Applications*
RFC 2275	*View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*
RFC 2412	*OAKLEY Key Determination Protocol*
RFC 2459	*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*
RFC 2574	*User-Based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
RFC 2576	*Coexistence Between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework (SNMP-COMMUNITY-MIB)*

RFCs	Title
RFC 2669	*DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems* (DOCS-CABLE-DEVICE-MIB)
RFC 2670	*Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS Compliant RF interfaces* (DOCS-IF-MIB)
RFC 2786	*Diffie-Hellman USM Key—Management Information Base and Textual Convention* (SNMP-USM-DH-OBJECTS-MIB)
RFC 2933	*Internet Group Management Protocol MIB* (IGMP-STD-MIB)

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/public/support/tac/home.shtml

Command Reference

This section documents commands that are new or modified in Cisco IOS Release 12.2(15)CZ for DOCSIS 1.1 support. All other commands used with this feature are documented in the software documents and command reference guide listed in the "Additional References" section on page 39.

- debug cable-modem mac messages
- debug docsis ssd
- docsis cvc mfg
- docsis cvc mso
- docsis cvc test
- show controllers cable-modem
- show controllers cable-modem bpkm
- show controllers cable-modem classifiers
- show controllers cable-modem cmcert
- show controllers cable-modem mac
- show controllers cable-modem manuf-cert
- show controllers cable-modem phs
- show controllers cable-modem qos
- show controllers cable-modem service-flows
- snmp-server enable traps docsis-cm

In addition, the **show controllers cable-modem des** command has been renamed to the **show controllers cable-modem crypto des** command.

debug cable-modem mac messages

To display debugging messages for specific MAC-layer messages, use the **debug cable-modem mac messages** command in privileged EXEC mode. To turn off debugging for the MAC layer, use the **no** form of this command.

Cisco uBR904, Cisco uBR905, Cisco uBR924, and Cisco uBR925 Cable Access Routers, and Cisco CVA122 Cable Voice Adapter

debug cable-modem mac messages *message-type*

no debug cable-modem mac messages *message-type*

Syntax Description

message-type	Specific type of MAC-layer message type to display: • **dcc-ack**—Displays the Dynamic Channel Change Acknowledge (DCC-ACK) messages received by the CM. • **dcc-req**—Displays the Dynamic Channel Change Request (DCC-REQ) messages received by the CM. • **dcc-rsp**—Displays the Dynamic Channel Change Response (DCC-RSP) messages transmitted by the CM. • **dynsrv**—Displays the Dynamic Service messages transmitted and received by the CM (for more information, see the **debug cable-modem mac messages dynsrv** command). • **map**—Displays the MAP messages received by the CM. • **reg-ack**—Displays the Registration Acknowledge (REG-ACK) messages transmitted by the CM. • **reg-req** —Displays the Registration Request (REG-REQ) messages transmitted by the CM. • **reg-rsp**—Displays the Registration Response (REG-RSP) messages received by the CM. • **rng-req**—Displays the Ranging Request (RNG-REQ) messages transmitted by the CM. • **rng-rsp**—Displays the Ranging Response (RNG-RSP) messages received by the CM. • **sync**—Displays the Time Synchronization (SYNC) messages received by the CM. • **ucc-req**—Displays the Upstream Channel Change Request (UCC-REQ) messages received by the CM. • **ucc-rsp**—Displays the Upstream Channel Change Response (UCC-RSP) messages transmitted by the CM. • **ucd—**Displays the Upstream Channel Descriptor (UCD) messages received by the CM. • **up-dis**—Displays the Upstream Transmitter Disable (UP-DIS) messages received by the CM.

Command Modes

Privileged EXEC

Command History

Release	Modifications
11.3(4)NA	This command was introduced on the Cisco uBR904 cable access router.
12.0(4)XI1	Support was added for the Cisco uBR924 cable access router.
12.1(3)XL	Support was added for the Cisco uBR905 cable access router.
12.1(5)XU1	Support was added for the Cisco CVA122 Cable Voice Adapter.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(15)CZ	The **dcc-ack**, **dcc-req**, and **dcc-rsp** options were added to support DOCSIS 1.1 operations.
12.3(2)T	The **up-dis** option was supported.

Usage Guidelines

The output from this command is very verbose, displaying the details of the DOCSIS MAC-layer messages, and is usually not needed for normal interface debugging. The command is most useful when attempting to attach a router to a CMTS that is not DOCSIS-qualified.

Caution This command should be used only while debugging CM operation. Displaying debugging messages consumes system resources, and turning on too many messages could negatively affect system performance.

Examples

The following example shows typical output from the **debug cable-modem mac messages** command. A separate command must be given for each message type to be displayed.

Much of the information, such as REG-REQ messages, is displayed in hexadecimal dump format, using the Type/Length/Value (TLV) format required by the DOCSIS specification.

Note For complete descriptions of the MAC-layer management messages, see the *DOCSIS Radio Frequency Interface Specification* (SP-RFIv1.1-I07-010829 or later), available from CableLabs at http://www.cablemodem.com/specifications.html.

```
Router# debug cable mac messages ucd
ucd message debugging is on

Router# debug cable mac messages map
map message debugging is on

Router# debug cable mac messages rng-rsp
rng-rsp message debugging is on

Router#
*Mar  7 01:44:06:
*Mar  7 01:44:06: UCD MESSAGE
*Mar  7 01:44:06: -----------
*Mar  7 01:44:06:   FRAME HEADER
*Mar  7 01:44:06:     FC                          - 0xC2 == MAC Management
*Mar  7 01:44:06:     MAC_PARM                    - 0x00
*Mar  7 01:44:06:     LEN                         - 0xD3
```

```
*Mar  7 01:44:06:   MAC MANAGEMENT MESSAGE HEADER
*Mar  7 01:44:06:     DA                        - 01E0.2F00.0001
*Mar  7 01:44:06:     SA                        - 00E0.1EA5.BB60
*Mar  7 01:44:06:     msg LEN                   - C1
*Mar  7 01:44:06:     DSAP                      - 0
*Mar  7 01:44:06:     SSAP                      - 0
*Mar  7 01:44:06:     control                   - 03
*Mar  7 01:44:06:     version                   - 01
*Mar  7 01:44:06:     type                      - 02 == UCD
*Mar  7 01:44:06:     RSVD                      - 0
*Mar  7 01:44:06:   US Channel ID               - 1
*Mar  7 01:44:06:   Configuration Change Count  - 4
*Mar  7 01:44:06:   Mini-Slot Size              - 8
*Mar  7 01:44:06:   DS Channel ID               - 1
*Mar  7 01:44:06:   Symbol Rate                 - 8
*Mar  7 01:44:06:   Frequency                   - 20000000
*Mar  7 01:44:06:   Preamble Pattern            - CC CC CC CC CC CC CC CC CC CC CC 0D 0D
*Mar  7 01:44:06:   Burst Descriptor 0
*Mar  7 01:44:06:     Interval Usage Code       - 1
*Mar  7 01:44:06:     Modulation Type           - 1 == QPSK
*Mar  7 01:44:06:     Differential Encoding     - 2 == OFF
*Mar  7 01:44:06:     Preamble Length           - 64
*Mar  7 01:44:06:     Preamble Value Offset     - 56
*Mar  7 01:44:06:     FEC Error Correction      - 0
*Mar  7 01:44:06:     FEC Codeword Info Bytes   - 16
*Mar  7 01:44:06:     Scrambler Seed            - 0x0152
*Mar  7 01:44:06:     Maximum Burst Size        - 1
*Mar  7 01:44:06:     Guard Time Size           - 8
*Mar  7 01:44:06:     Last Codeword Length      - 1 == FIXED
*Mar  7 01:44:06:     Scrambler on/off          - 1 == ON
*Mar  7 01:44:06:   Burst Descriptor 1
*Mar  7 01:44:06:     Interval Usage Code       - 3
*Mar  7 01:44:06:     Modulation Type           - 1 == QPSK
*Mar  7 01:44:06:     Differential Encoding     - 2 == OFF
*Mar  7 01:44:06:     Preamble Length           - 128
*Mar  7 01:44:06:     Preamble Value Offset     - 0
*Mar  7 01:44:06:     FEC Error Correction      - 5
*Mar  7 01:44:06:     FEC Codeword Info Bytes   - 34
*Mar  7 01:44:06:     Scrambler Seed            - 0x0152
*Mar  7 01:44:06:     Maximum Burst Size        - 0
*Mar  7 01:44:06:     Guard Time Size           - 48
*Mar  7 01:44:06:     Last Codeword Length      - 1 == FIXED
*Mar  7 01:44:06:     Scrambler on/off          - 1 == ON
*Mar  7 01:44:06:   Burst Descriptor 2
*Mar  7 01:44:06:     Interval Usage Code       - 4
*Mar  7 01:44:06:     Modulation Type           - 1 == QPSK
*Mar  7 01:44:06:     Differential Encoding     - 2 == OFF
*Mar  7 01:44:06:     Preamble Length           - 128
*Mar  7 01:44:06:     Preamble Value Offset     - 0
*Mar  7 01:44:06:     FEC Error Correction      - 5
*Mar  7 01:44:06:     FEC Codeword Info Bytes   - 34
*Mar  7 01:44:06:     Scrambler Seed            - 0x0152
*Mar  7 01:44:06:     Maximum Burst Size        - 0
*Mar  7 01:44:06:     Guard Time Size           - 48
*Mar  7 01:44:06:     Last Codeword Length      - 1 == FIXED
*Mar  7 01:44:06:     Scrambler on/off          - 1 == ON
*Mar  7 01:44:06:   Burst Descriptor 3
*Mar  7 01:44:06:     Interval Usage Code       - 5
*Mar  7 01:44:06:     Modulation Type           - 1 == QPSK
*Mar  7 01:44:06:     Differential Encoding     - 2 == OFF
*Mar  7 01:44:06:     Preamble Length           - 72
*Mar  7 01:44:06:     Preamble Value Offset     - 48
*Mar  7 01:44:06:     FEC Error Correction      - 5
*Mar  7 01:44:06:     FEC Codeword Info Bytes   - 75
```

```
*Mar  7 01:44:06:     Scrambler Seed            - 0x0152
*Mar  7 01:44:06:     Maximum Burst Size        - 0
*Mar  7 01:44:06:     Guard Time Size           - 8
*Mar  7 01:44:06:     Last Codeword Length      - 1 == FIXED
*Mar  7 01:44:06:     Scrambler on/off          - 1 == ON
*Mar  7 01:44:06:
*Mar  7 01:44:06:
*Mar  7 01:44:06: MAP MESSAGE
*Mar  7 01:44:06: -----------
*Mar  7 01:44:06:   FRAME HEADER
*Mar  7 01:44:06:     FC                        - 0xC3 == MAC Mement with Extended Header
*Mar  7 01:44:06:     MAC_PARM                  - 0x02
*Mar  7 01:44:06:     LEN                       - 0x42
*Mar  7 01:44:06:     EHDR                      - 0x00 0x00
*Mar  7 01:44:06:   MAC MANAGEMENT MESSAGE HEADER
*Mar  7 01:44:06:     DA                        - 01E0.2F00.0001
.
*Mar  7 01:44:17: RNG-RSP MESSAGE
*Mar  7 01:44:17: ---------------
*Mar  7 01:44:17:   FRAME HEADER
*Mar  7 01:44:17:     FC                        - 0xC2 == MAC Management
*Mar  7 01:44:17:     MAC_PARM                  - 0x00
*Mar  7 01:44:17:     LEN                       - 0x2B
*Mar  7 01:44:17:   MAC MANAGEMENT MESSAGE HEADER
*Mar  7 01:44:17:     DA                        - 00F0.1EB2.BB61
.
*Mar  7 01:44:20: REG-REQ MESSAGE
*Mar  7 01:44:20: ---------------
*Mar  7 01:44:20: C20000A5 000000E0  1EA5BB60 00F01EB2
*Mar  7 01:44:20: BB610093 00000301  06000004 03010104
*Mar  7 01:44:20: 1F010101 0204003D  09000304 001E8480
*Mar  7 01:44:20: 04010705 04000186  A0060200 0C070101
*Mar  7 01:44:20: 080300F0 1E112A01  04000000 0A020400
*Mar  7 01:44:20: 00000A03 04000002  58040400 00000105
*Mar  7 01:44:20: 04000000 01060400  00025807 04000000
*Mar  7 01:44:20: 3C2B0563 6973636F  06105E4F C908C655
*Mar  7 01:44:20: 61086FD5 5C9D756F  7B730710 434D5453
*Mar  7 01:44:20: 204D4943 202D2D2D  2D2D2D2D 0C040000
*Mar  7 01:44:20: 00000503 010100
*Mar  7 01:44:20:
*Mar  7 01:44:20:
*Mar  7 01:44:20: REG-RSP MESSAGE
*Mar  7 01:44:20: ---------------
*Mar  7 01:44:20:   FRAME HEADER
*Mar  7 01:44:20:     FC                        - 0xC2 == MAC Management
*Mar  7 01:44:20:     MAC_PARM                  - 0x00
*Mar  7 01:44:20:     LEN                       - 0x29
*Mar  7 01:44:20:   MAC MANAGEMENT MESSAGE HEADER
*Mar  7 01:44:20:     DA                        - 00F0.1EB2.BB61
```

Related Commands

Command	Description
debug cable-modem mac messages dynsrv	Displays the dynamic service messages.

debug docsis ssd

To display debugging information about the parsing and verification of the DOCSIS code verification certificates (CVCs) that are part of a software image downloaded with the Secure Software Download (SSD) procedure, use the **debug docsis ssd** command in privileged EXEC mode. To disable the debugging output, use the **no** form of this command.

Cisco uBR905 and Cisco uBR925 Cable Access Routers, and Cisco CVA122 Cable Voice Adapter

debug docsis ssd

no debug docsis ssd

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)CZ	This command was introduced for the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

Usage Guidelines

This command displays whether the Secure Software Download procedure could validate the manufacturer's CVC and optional cosigner's CVC (if present) that are part of the downloaded software image.

Examples

The following example shows typical output for a successful Secure Software Download procedure for a software image that has been signed by both the manufacturer and by a cosigner:

```
Router# debug docsis ssd

secure software download debugging is on
Router#
SSD: decrypt process suspended and continued
SSD: decrypt process suspended and continued
Code Verification Successful (Manufacturer CVC/CVS)
Verifying Co-Signer CVC/CVS
SSD: decrypt process suspended and continued
SSD: decrypt process suspended and continued
Co-signer CVC has been validated
Code Verification Successful (Co-Signer CVC/CVS)

Router#
```

If the manufacturer's signature on the software image file cannot be validated using the manufacturer's CVC on the router, the following messages are displayed:

```
MFG code signature does not validate
MFG CVC validation has failed
```

If the Multi-Service Operator (MSO) cosigner's signature on the software image file cannot be validated using the cosigner's CVC on the router, the following messages are displayed:

```
Co-signer code signature does not validate
Co-signer CVC validation has failed
```

If the software image was signed either before or after the allowable time range specified as part of the manufacturer's CVC, one of the following messages is displayed:

```
signingTime is before saved codeAccessStart
signingTime is before CVC validNotBefore
signingTime is after CVC validNotAfter
CVC validity start is less than save cvcAccessStart
```

Related Commands

Command	Description
docsis cvc mfg	Configures the access start times and organization name for the manufacturer's code verification certificate (CVC).
docsis cvc mso	Configures the access start times and organization name for the optional MSO cosigned code verification certificate (CVC).
docsis cvc test	Tests the root CA public key and CM private key that are installed on the router.

docsis cvc mfg

To configure the access start times and organization name for the manufacturer's code verification certificate (CVC) to enable the DOCSIS 1.1 secure software download feature on the router, use the **docsis cvc mfg** command in global configuration mode. To delete this information, use the **no** form of this command.

Cisco uBR905 and Cisco uBR925 Cable Access Routers, and Cisco CVA122 Cable Voice Adapter

docsis cvc mfg {**codeAccessStart** *start-time* | **cvcAccessStart** *start-time* | **organization** *name*}

no docsis cvc mfg {**codeAccessStart** *start-time* | **cvcAccessStart** *start-time* | **organization** *name*}

Syntax Description

codeAccessStart *start-time*	Specifies the code Access Start Time as a UTC time value (*YYMMDDhhmmssZ*) in Greenwich Mean Time.
cvcAccessStart *start-time*	Specifies the CVC Access Start Time as a UTC time value (*YYMMDDhhmmssZ*) in Greenwich Mean Time.
organization *name*	Specifies the name of the manufacturer of the code file. Use quotes if the *name* value contains more than one word.

Defaults

The **codeAccessStart** and **cvcAccessStart** times default to 011219000000Z (midnight on December 19, 2001 Greenwich Mean Time). The organization defaults to Cisco Systems.

Note Typically, the default values should not be changed unless you are instructed to do so by Cisco TAC or field service engineers.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)CZ	This command was introduced on the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

Usage Guidelines

This command configures the access start times and organization name that are required by Appendix D in the DOCSIS BPI+ specification. The time values are specified as UTC time values in Greenwich Mean Time, with a two-digit year. If the year is between 50 and 99, it is interpreted as 1950 to 1999. If the year is between 00 and 49, it is interpreted as 2000 to 2049.

The router uses the **codeAccessStart** value to verify the Code Verification Signature (CVS) that is affixed to the code file downloaded using the secure software download feature. The router uses the **ccvAccessStart** value to verify the CVC for the code file. The router also uses the **organization** value to verify that the code file has been created by the proper manufacturer.

Tip These values are the same that are set using the docsBpi2CodeMfgCodeAccessStart, docsBpi2CodeMfgCvcAccessStart, and docsBpi2CodeMfgOrgName attributes in the BPI+ MIB (DOCS-BPI2-MIB).

Examples

The following example shows the default configuration for the **docsis cvc mfg** commands:

```
Router(config)# docsis cvc mfg organization "Cisco Systems"
Router(config)# docsis cvc mfg codeAccessStart 011219000000Z
Router(config)# docsis cvc mfg cvcAccessStart 011219000000Z
Router(config)#
```

Note You must set the organization name using the **docsis cvc mfg organization** command before you can set either access start time.

Related Commands

Command	Description
docsis cvc mso	Configures the access start times and organization name for the optional Multi-Service Operator (MSO) cosigned code verification certificate (CVC).
docsis cvc test	Tests the root CA public key and CM private key that are installed on the router.

docsis cvc mso

To configure the access start times and organization name for the optional Multi-Service Operator (MSO) cosigned code verification certificate (CVC) for the DOCSIS 1.1 secure software download feature, use the **docsis cvc mso** command in global configuration mode. To delete the information, use the **no** form of this command.

Cisco uBR905 and Cisco uBR925 Cable Access Routers, and Cisco CVA122 Cable Voice Adapter

docsis cvc mso {**codeAccessStart** *start-time* | **cvcAccessStart** *start-time* | **organization** *name*}

no docsis cvc mso {**codeAccessStart** *start-time* | **cvcAccessStart** *start-time* | **organization** *name*}

Syntax Description

codeAccessStart *start-time*	Code Access Start Time as a UTC time value (*YYMMDDhhmmssZ*) in Greenwich Mean Time.
cvcAccessStart *start-time*	CVC Access Start Time as a UTC time value (*YYMMDDhhmmssZ*) in Greenwich Mean Time.
organization *name*	Name of the manufacturer of the code file. Use quotes if *name* contains more than one word.

Defaults

No default values or behavior (no cosigner is used).

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)CZ	This command was introduced on the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

Usage Guidelines

This command configures the optional cosigner access start times and organization name that are specified by Appendix D in the DOCSIS BPI+ specification. The time values are specified as UTC time values in Greenwich Mean Time, with a two-digit year. If the year is between 50 and 99, it is interpreted as 1950 to 1999. If the year is between 00 and 49, it is interpreted as 2000 to 2049.

You do not need to use this command unless the MSO or service provider is digitally signing the Cisco IOS software images that it plans to download to the Cisco cable modems. If so, then this command must be used to set the appropriate access times and organization name, so that the cable modem can properly authenticate the software images during a secure software download.

The router uses the **codeAccessStart** value to verify the cosigner's Code Verification Signature (CVS) that is affixed to the code file downloaded using the secure software download feature. The router uses the **ccvAccessStart** value to verify the cosigner's CVC that is affixed to the code file. The router also uses the **organization** value to verify that the code file has been signed by the proper MSO or cable operator.

Tip These values are the same that are set using the docsdocsBpi2CodeCoSignerCodeAccessStart, Bpi2CodeCoSignerCvcAccessStart, and docsBpi2CodeCoSignerOrgName attributes in the BPI+ MIB (DOCS-BPI2-MIB).

Examples

The following example shows the **docsis cvc mso** commands being used to configure the router for a cosigned CVC from an organization named "MSO Organization" and with certificate access times of midnight on March 1, 2002 Greenwich Mean Time:

```
Router(config)# docsis cvc mfg organization "MSO Organization"
Router(config)# docsis cvc mfg codeAccessStart 020301000000Z
Router(config)# docsis cvc mfg cvcAccessStart 020301000000Z
Router(config)#
```

Note You must set the organization name using the **docsis cvc mso organization** command before you can set either access start time.

Related Commands

Command	Description
docsis cvc mfg	Configures the access start times and organization name for the manufacturer's code verification certificate (CVC).
docsis cvc test	Tests the root CA public key and CM private key that are installed on the router.

docsis cvc test

To test the root certificate authority (CA) public key and cable modem (CM) private key that are installed on the router, use the **docsis cvc test** command in global configuration mode.

Cisco uBR905 and Cisco uBR925 Cable Access Routers, and Cisco CVA122 Cable Voice Adapter

docsis cvc test

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)CZ	This command was introduced on the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

Usage Guidelines

This command verifies that the root CA public key and the private key that are installed in the router at the factory are valid. The command uses the root CA public key to encrypt a string, and then it uses the router's private key to decrypt the key.

Typically, the root CA public key and private key are installed at the factory and never need to be updated. However, DOCSIS allows the keys to be updated as part of the secure software download procedure. If this occurs, you can use the **docsis cvc test** command to verify that the keys are valid and are properly installed.

Examples

The following example shows a typical successful result of the **docsis cvc test** command:

```
Router# config terminal
Router(config)# docsis cvc test

Encrypted sting: This is a test
Encrypt result: xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Decrypt result: This is a test
Router(config)#
```

Note If the decrypt result is not "This is a test," then the test failed, which indicates that either the public key or the private key is not valid.

Related Commands

Command	Description
docsis cvc mfg	Configures the manufacturer's CVC access start time and organization values.
docsis cvc mso	Configures the Multi-Service Operator (MSO) cosigned CVC access start time and organization values.

show controllers cable-modem

To display high-level controller information for the router's cable interface, use the **show controllers cable-modem** command in privileged EXEC mode.

Cisco uBR904, uBR905, uBR924, uBR925 cable access routers, Cisco CVA122 Cable Voice Adapter

show controllers cable-modem *number* [**all**]

Syntax Description

number	Identifies the cable interface (always **0**).
all	(Optional) Displays detailed, multi-page output, including chip-level settings, transmit and receive ring contents, and MAC-layer and PHY-layer registers and buffers.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(4)NA	This command was introduced for the Cisco uBR904 cable access router.
12.0(4)XI1	Support was added for the Cisco uBR924 cable access router.
12.1(3)XL	Support was added for the Cisco uBR905 cable access router.
12.1(5)XU1	Support was added for the Cisco CVA122 Cable Voice Adapter.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.

Usage Guidelines

The **show controllers cable-modem** display begins with information from the first few registers of the Broadcom BCM3300 chip. Next is buffer information for the receive, receive MAC message, buffer descriptor, and packet descriptor rings. Then comes MIB statistics from the BCM3300 chip, DMA base registers to indicate where the rings start, global control and status information, and finally interrupts for the interrupt code.

When using this command, be sure to check the tx_count and the tx_head and tx_tail values for the buffer descriptor (TX BD) and packet descriptor (TX PD) rings. The tx_count should be greater than 0, and the tx_head and tx_tail values should not be equal. If these values do not change for several minutes, it could indicate that there are packets stuck on the ring. This condition is often caused by the CMTS not giving grants.

Examples

The following shows typical output for the **show controllers cable-modem** command:

```
Router# show controllers cable-modem 0
BCM Cable interface 0:
BCM3300 unit 0, idb 0x200EB4, ds 0x82D4748, regaddr = 0x800000, reset_mask 0x80
station address 0010.7b43.aa01  default station address 0010.7b43.aa01
PLD VERSION: 32

MAC State is ranging_2_state, Prev States = 7
MAC mcfilter 01E02F00  data mcfilter 01000000
```

```
DS: BCM 3116 Receiver: Chip id = 2
US: BCM 3037 Transmitter: Chip id = 30B4

Tuner: status=0x00
Rx: tuner_freq 699000000, symbol_rate 5055849, local_freq 11520000
    snr_estimate 33406, ber_estimate 0, lock_threshold 26000
    QAM in lock, FEC in lock, qam_mode QAM_64
Tx: tx_freq 20000000, power_level 0x3E, symbol_rate 1280000

DHCP: TFTP server = 4.0.0.32, TOD server = 4.0.0.188
      Security server = 0.0.0.0, Timezone Offset = 0.0.4.32
      Config filename =

buffer size 1600

RX data PDU ring with 32 entries at 0x201D40
  rx_head = 0x201D78 (7), rx_p = 0x831BE04 (7)
    00 pak=0x8326318 buf=0x225626 status=0x80 pak_size=0
    01 pak=0x83241A0 buf=0x21DE5A status=0x80 pak_size=0
    02 pak=0x83239C0 buf=0x21C22A status=0x80 pak_size=0
    03 pak=0x8328C70 buf=0x22EA22 status=0x80 pak_size=0
    04 pak=0x8325F28 buf=0x22480E status=0x80 pak_size=0
    05 pak=0x8327CB0 buf=0x22B1C2 status=0x80 pak_size=0
    06 pak=0x8323BB8 buf=0x21C936 status=0x80 pak_size=0

RX MAC message ring with 8 entries at 0x201E80
  rx_head_mac = 0x201E88 (1), rx_p_mac = 0x831BE80 (1)
    00 pak=0x8326120 buf=0x224F1A status=0x80 pak_size=0
    01 pak=0x8324590 buf=0x21EC72 status=0x80 pak_size=0
    02 pak=0x8323FA8 buf=0x21D74E status=0x80 pak_size=0
    03 pak=0x8326EE8 buf=0x22806E status=0x80 pak_size=0
    04 pak=0x8328E68 buf=0x22F12E status=0x80 pak_size=0
    05 pak=0x8327AB8 buf=0x22AAB6 status=0x80 pak_size=0
    06 pak=0x8328880 buf=0x22DC0A status=0x80 pak_size=0
    07 pak=0x8326CF0 buf=0x227962 status=0xA0 pak_size=0

TX BD ring with 8 entries at 0x201FB8, tx_count = 0
  tx_head = 0x201FD8 (4), head_txp = 0x831BF20 (4)
  tx_tail = 0x201FD8 (4), tail_txp = 0x831BF20 (4)
    00 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
    01 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
    02 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
    03 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
    04 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
    05 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
    06 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
    07 pak=0x000000 buf=0x200000 status=0x20 pak_size=0

TX PD ring with 8 entries at 0x202038, tx_count = 0
  tx_head_pd = 0x202838 (4)
  tx_tail_pd = 0x202838 (4)
    00 status=0x00 bd_index=0x0000 len=0x0000 hdr_len=0x0000
    ehdr: 01 06 02 74 34 11
    01 status=0x00 bd_index=0x0001 len=0x0000 hdr_len=0x0000
    ehdr: 01 06 02 74 34 11
    02 status=0x00 bd_index=0x0002 len=0x0000 hdr_len=0x0000
    ehdr: 01 06 02 74 34 11
    03 status=0x00 bd_index=0x0003 len=0x0000 hdr_len=0x0000
    ehdr: 01 06 02 74 34 11
    04 status=0x00 bd_index=0x0004 len=0x0000 hdr_len=0x0000
    ehdr: 01 06 02 74 34 11
    05 status=0x00 bd_index=0x0005 len=0x0000 hdr_len=0x0000
    ehdr: 01 06 02 74 34 11
    06 status=0x00 bd_index=0x0006 len=0x0000 hdr_len=0x0000
```

```
    ehdr: 01 06 02 74 34 11
    07 status=0x20 bd_index=0x0007 len=0x0000 hdr_len=0x0000
    ehdr: 01 06 02 74 34 11

MIB Statistics
  DS fifo full = 0, Rerequests = 0
  DS mac msg overruns = 0, DS data overruns = 0
  Qualified maps = 348, Qualified syncs = 73
  CRC fails = 0, HDR chk fails = 0
  Data pdus = 0, Mac msgs = 423
  Valid hdrs = 423

BCM3300 Registers:
downstream dma:
  ds_data_bd_base=0x001D40, ds_mac_bd_base=0x001E80
  ds_data_dma_ctrl=0x98, ds_mac_dma_ctrl=0xD8
  ds_dma_data_index=0x0007, ds_dma_msg_index=0x0000
upstream dma:
  us_bd_base=0x001FB8, us_pd_base=0x002038
  us_dma_ctrl=0x80, us_dma_tx_start=0x00
Global control and status:
  global_ctrl_status=0x00
interrupts:
  irq_pend=0x0008, irq_mask=0x00F7
Router#
```

The following shows an excerpt from the display for the **all** option:

```
Router# show controllers cable-modem 0 all
BCM MAC/PHY: Chip id = BCM3300 Revision A (1)

BCM3220 unit 0, idb 0x81068880, ds 0x8106B8A0, regaddr = 0x10100000, reset_mask 0x80
station address 0006.53b6.57bd  default station address 0006.53b6.57bd
MAC mcfilter 01E02F00  data mcfilter 00000000

buffer size 1856
RX data PDU ring with 32 entries at 0x10030F00
  rx_head = 0x10030F78 (15), rx_p = 0x8106B8F8 (15)
    00 pak=0x810798C0 buf=0x10044F56 status=0x80 pak_size=0
    01 pak=0x81079BB4 buf=0x1004575E status=0x80 pak_size=0

...

Tuner: status=0x00
Rx: tuner_freq 645000000, symbol_rate 5056000, local_freq 11520000
    snr_estimate 345(TenthdB), ber_estimate 0, lock_threshold 23000
    QAM in lock, FEC in lock, qam_mode QAM_64   (Annex B)
Tx: tx_freq 27984000, symbol rate 16 (2560000 sym/sec)
     power_level: 29.75 dBmV (current)
                  30  (gain in US AMP units)
                  5   (BCM3300 attenuation in .4 dB units)
IF AGC=0x2010 (8208)  RF AGC=0x3753 (14163)
Combined AGC = 22371 (band = 1)

Estimated Downstream Power: 7.9 dBmV

Platform check 8400000

Router#
```

Note The **show controllers cable-modem 0 all** command displays extensive information about the current state of the modem and its MAC-layer and PHY-layer registers and buffers. You need to open a capture buffer on your terminal or Telnet software to log this information before you give this command.

Table 2 describes the significant fields shown by the **show controllers cable-modem** command. For more information, see the Broadcom documentation for the BCM3300 chip.

Table 2 show controllers cable-modem Field Descriptions

Field	Description
BCM3300 unit	Unit number of this BCM3300 chip.
idb	Interface description block number.
ds	Downstream channel.
regaddr	Indicates the start of the BCM3300 registers.
reset_mask	Indicates the bit to hit when resetting the chip.
station address	MAC address of this router's cable interface.
default station address	Default MAC address assigned by the factory for this router.
PLD VERSION	PLD version of the BCM3300 chip.
MAC State	Current MAC state of the router.
Prev States	Number of states that have previously existed since initialization.
MAC mcfilter	MAC control filter for MAC messages.
data mcfilter	MAC control filter for data.
DS	Downstream Broadcom receiver chip number and ID.
US	Upstream Broadcom transmitter chip number and ID.
Tuner: status	Current status of the tuner.
Rx: tuner_freq	Downstream frequency (in Hz) that the router searched for and found.
symbol_rate	Downstream frequency in symbols per second.
local_freq	Frequency on which the transmitter and the tuner communicate.
snr_estimate	Estimate of signal-to-noise ratio (SNR) in dB multiplied by 1000.
ber_estimate	Estimate of bit error rate (always 0).
lock_threshold	Minimum signal-to-noise ratio (SNR) that the router will accept as a valid lock.
qam_mode	The modulation scheme used in the downstream direction.
Tx: tx_freq	Upstream frequency sent to the router by the CMTS in the UCD message.
power_level	Transmit power level as set in the hardware, expressed as a hexadecimal value. The units are unique to the hardware used. Use the **show controllers cable-modem mac state** command to see the power level in dBmV.
symbol_rate	Upstream frequency in symbols per second.
TFTP server	IP address of the TFTP server at the CMTS.
TOD server	IP address of the time-of-day server at the CMTS.
Security server	IP address of the security server at the CMTS.

Table 2 show controllers cable-modem Field Descriptions

Field	Description
Timezone Offset	Correction received from the DHCP server to synchronize the router time clock with the CMTS.
Config filename	Name of the file stored on the cable company's TFTP server that contains operational parameters for the router.
buffer size	Size in bytes of the BCM3300 message buffers.
RX data PDU ring:	Indicates the memory location of the beginning of buffer information for the receive data ring.
rx_head	Indicates current head buffer descriptor.
rx_p	Indicates current head packet descriptor.
RX MAC message ring:	Indicates the memory location of the beginning of buffer information for the receive MAC message ring.
rx_head_mac	Indicates current head buffer descriptor.
rx_p_mac	Indicates current head packet descriptor.
TX BD ring:	Indicates the memory location of the beginning of buffer information for the transmit buffer descriptor ring.
tx_count	If tx_count is 0, or if tx_head and tx_tail are equal and there is no change for a period of time, it means there are packets stuck on the ring. This condition may be caused by the CMTS not giving grants.
tx_head	Indicates current head transmit packet descriptor.
head_txp	The next packet descriptor to get used, along with its index.When head_txp and tail_txp are the same, the transmit queue is empty.
tx_tail	Indicates current tail transmit packet descriptor.
tail_txp	The next packet descriptor to get sent, along with its index. When head_txp and tail_txp are the same, the transmit queue is empty.
TX PD ring:	Indicates the memory location of the beginning of buffer information for the transmit packet descriptor ring.
tx_head_pd	Indicates current head packet descriptor.
tx_tail_pd	Indicates current tail packet descriptor.
ehdr	Extended MCNS header.
MIB Statistics	
DS fifo full	Number of times the downstream input first-in first-out (FIFO) buffer became full on the router.
rerequests	Number of times a bandwidth request generated by the router was not responded to by the CMTS.
DS mac msg overruns	Number of times the router's DMA controller had a downstream MAC message and there were no free MAC message buffer descriptors to accept the message.
DS data overruns	Number of times the router's DMA controller had downstream data and there were no free data PDU buffer descriptors to accept the data.
Qualified maps	Number of times a MAP message passed all filtering requirements and was received by the router.

Table 2 show controllers cable-modem Field Descriptions

Field	Description
Qualified syncs	Number of times a timestamp message was received by the router.
CRC fails	Number of times a MAC message failed a cyclic redundancy check (CRC).
HDR chk fails	Number of times a MAC header failed its 16-bit CRC check. The MAC header CRC is a 16-bit Header Check Sequence (HCS) field that ensures the integrity of the MAC header even in a collision environment.
Data pdus	Total number of data protocol data units (PDUs) of all types received by the router.
Mac msgs	Number of MAC messages received by the router.
Valid hdrs	Number of valid headers received by the router, including PDU headers, MAC headers, and headers only.
Global control and status:	Used to reset the BCM3300 chip.
interrupts:	Hexadecimal values of the pending IRQ interrupt and IRQ mask.

Tip In Cisco IOS Release 12.2(8)T and later releases, you can add a timestamp to **show** commands using the **exec prompt timestamp** command in line configuration mode.

Related Commands

Command	Description
show controllers cable-modem bpkm	Displays information about the baseline privacy key management exchange between the router and the CMTS.
show controllers cable-modem des	Displays information about the DES engine registers.
show controllers cable-modem filters	Displays the registers in the MAC hardware that are used for filtering received frames.
show controllers cable-modem lookup-table	Displays the mini-slot lookup table for the cable interface.
show controllers cable-modem mac	Displays detailed MAC-layer information for the cable interface.
show controllers cable-modem phy	Displays the contents of the registers used in the downstream physical hardware for the cable interface.
show controllers cable-modem tuner	Displays the settings for the upstream and downstream tuners used by the cable interface.

show controllers cable-modem bpkm

To display information about the Baseline Privacy Interface (BPI) or BPI Plus (BPI+) key management (BPKM) exchange between the router and the CMTS, use the **show controllers cable-modem bpkm** command in privileged EXEC mode.

Cisco uBR904, Cisco uBR905, Cisco uBR924, and Cisco uBR925 Cable Access Routers, and Cisco CVA122 Cable Voice Adapter

show controllers cable-modem *number* **bpkm**

Syntax Description

number	Cable interface (always 0).

Command Modes

Privileged EXEC

Command History

Release	Modifications
11.3(4)NA	This command was introduced on the Cisco uBR904 cable access router.
12.0(4)XI1	Support was added for the Cisco uBR924 cable access router.
12.1(3)XL	Support was added for the Cisco uBR905 cable access router.
12.1(5)XU1	Support was added for the Cisco CVA122 Cable Voice Adapter.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(15)CZ	Support for DOCSIS 1.1 and BPI+ operation was added for the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

Usage Guidelines

Baseline privacy key management exchanges take place only when both the router and the CMTS are running code images that support Baseline Privacy Interface (BPI) or BPI Plus (BPI+) encryption, and the privacy class of service is enabled via the configuration file that is downloaded to the router. Baseline privacy code images for the router contain k1, k8, or k9 in the code image name.

Examples

The following shows typical output for the **show controllers cable-modem bpkm** command for DOCSIS 1.0 BPI operation when the CMTS does not have baseline privacy enabled:

```
Router# show controllers cable-modem 0 bpkm

CM Baseline Privacy Key Management
  configuration (in seconds):
      authorization wait time:    10
      reauthorization wait time:  10
      authorization grace time:   600
      operational wait time:      1
      rekey wait time:            1
      tek grace time:             600
      authorization rej wait time: 60
  kek state:    STATE_B_AUTH_WAIT
  sid 4:
```

```
      tek state: No resources assigned
Router#
```

Table 3 describes the fields shown in the display for BPI operation.

Table 3 show controllers cable-modem bpkm Field Descriptions (BPI)

Field	Description
authorization wait time	The number of seconds the router waits for a reply after sending the Authorization Request message to the CMTS.
reauthorization wait time	The number of seconds the router waits for a reply after it has sent an Authorization Request message to the CMTS in response to a reauthorization request or an Authorization Invalid message from the CMTS.
authorization grace time	The number of seconds before the current authorization is set to expire that the grace timer begins, signaling the router to begin the reauthorization process.
operational wait time	The number of seconds the traffic encryption key (TEK) state machine waits for a reply from the CMTS after sending its initial Key Request for its SID's keying material.
rekey wait time	The number of seconds the TEK state machine waits for a replacement key for this Service ID (SID) after the TEK grace timer has expired and the request for a replacement key has been made.
tek grace time	The number of seconds before the current TEK is set to expire that the TEK grace timer begins, signaling the TEK state machine to request a replacement key.
authorization rej wait time	Number of seconds the router waits before sending another Authorization Request message to the CMTS after it has received an Authorization Reject message.
kek state	The current state of the key encryption key (KEK) that the CMTS uses to encrypt the traffic encryption keys it sends to the router. See Table 5 on page 64 for the possible values.
tek state	The current state of the traffic encryption key state machine for the specified SID. See Table 5 on page 64 for the possible values.

The following shows typical output for the **show controllers cable-modem bpkm** command for DOCSIS 1.1 BPI+ operation when baseline privacy is enabled:

```
Router# show controllers cable-modem 0 bpkm

CM Baseline Privacy Key Management
Privacy Version:            BPI+ (PLUS)
  public key:
      30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E560B2
      4F6777A1 731AF856 CE936615 BF513F15 44CE2D02 95167EAD 139FE25C C1E7D4E5
      99B34020 D96608B2 A87C0AA1 C171B265 3E87FF7F F70FD3B1 AE96F0EE B2E75172
      6B06F661 EA631817 0D317D6F 22FC733B F150E65F 44AE535A 5FB0532F 14519F3B
      80A9D442 05D7B7EF 58A5993C 49BB5028 9A3A980A 36AEDC53 E762FA4D 63020301 01
  keks:   even 4184D17A0C0AEDA3 odd C07A8454DBAA7F1B
  hmac upstream key even:
      4E0A5108 A8451B24 BAC3A8CA D8DF459F 6D37448D
  hmac upstream key odd:
      5D04EEDD 43129682 F7A474EA 4E9F888B 5EC18478
  hmac downstream key even:
```

```
      7B6595D6 75B435FB 2FA7204D 2F203CB1 FBA80950
  hmac downstream key odd:
      E15FC10B 7F1BAFE8 6295315F E91FE97C F0DE3A73
  configuration (in seconds):
      authorization wait time:    5
      reauthorization wait time:  30
      authorization grace time:   60
      operational wait time:      2
      rekey wait time:            2
      tek grace time:             60
      authorization rej wait time: 60
      sa map wait time:       1
      sa map retries:         4
  kek state:     STATE_C_AUTHORIZED
  kek life:      86450 sec
  sid 2:
      tek state: STATE_D_OPERATIONAL
      tek life:  21654 sec
      keys:      even 1730E9E1F0B1C4C, odd 23021AE604610E38
      ivectors:  even 16FB0175256819FD, odd B802057107302F8
      sequence:  12
 DSA map List


Router#
```

Table 4 describes the fields shown in the display for BPI+ operation.

Table 4 show controllers cable-modem bpkm Field Descriptions (BPI+)

Field	Description
Privacy Version	Whether BPI or BPI+ is being run.
public key	Diffie-Hellman public key that the router uses to establish a BPI+ session with the CMTS.
keks	Odd and even values for the key encryption key (KEK).
hmac upstream keys	Odd and even values for the hash message authentication code (HMAC) key used in upstream key requests.
hmac downstream keys	Odd and even values for the HMAC message authentication key used in downstream key replies, key rejects, and invalid TEK messages.
authorization wait time	Number of seconds the router waits for a reply after sending the Authorization Request message to the CMTS.
reauthorization wait time	Number of seconds the router waits for a reply after it has sent an Authorization Request message to the CMTS in response to a reauthorization request or an Authorization Invalid message from the CMTS.
authorization grace time	Number of seconds before the current authorization is set to expire that the grace timer begins, signaling the router to begin the reauthorization process.
operational wait time	Number of seconds the TEK state machine waits for a reply from the CMTS after sending its initial Key Request for its SID's keying material.
rekey wait time	Number of seconds the TEK state machine waits for a replacement key for this SID after the TEK grace timer has expired and the request for a replacement key has been made.

Table 4 show controllers cable-modem bpkm Field Descriptions (BPI+) (continued)

Field	Description
tek grace time	Number of seconds before the current TEK is set to expire that the TEK grace timer begins, signaling the TEK state machine to request a replacement key.
authorization rej wait time	Number of seconds the router waits before sending another Authorization Request message to the CMTS after it has received an Authorization Reject message.
sa map wait time	Number of seconds the router waits for a response after sending a Security Association (SA) map request before timing out and resending the request.
sa map retries	Number of times the router attempts an SA map request before it rejects the attempt to create a new downstream service flow.
kek state	Current state of the key encryption key that the CMTS uses to encrypt the traffic encryption keys it sends to the router. See Table 5 for the possible values.
tek state	Current state of the traffic encryption key state machine for the specified SID. See Table 5 for the possible values.

Table 5 describes the valid values for the kek state and tek state fields.

Table 5 State Values for KEK and TEK State Fields

State	Description
Key Encryption Key (KEK) States	
STATE_A_START	The router is still completing the DOCSIS provisioning process. If this state persists, it indicates that BPI/BPI+ encryption was not enabled for the router in its DOCSIS configuration file.
STATE_B_AUTH_WAIT	DOCSIS provisioning has been completed, and the router has sent an authorization request to the CMTS and is waiting for a reply. If this state persists, it indicates that the CMTS has not enabled BPI/BPI+ operations.
STATE_C_AUTHORIZED	The router has received a valid authorized reply from the CMTS, completing the KEK exchange, and allowing the TEK exchange to begin.
STATE_D_REAUTH_WAIT	The router sent a reauthorization request and is waiting for the reply from the CMTS. A reauthorization request can be sent if the initial request is rejected, or when existing keys have expired and must be reacquired.
STATE_E_AUTH_REJ_WAIT	The router has received a nonpermanent authorization reject response from the CMTS and is waiting for the timeout period before sending another request.
STATE_F_SILENT	The router has received a permanent authorization reject response from the CMTS and has been placed in silent mode, in which it does not pass traffic but does accept SNMP management requests. (Valid only for BPI+ operations.)

Table 5 State Values for KEK and TEK State Fields (continued)

State	Description
Traffic Encryption Key (TEK) States	
STATE_A_START	The router is still completing the DOCSIS provisioning process, or is still performing the KEK key exchange. If this state persists, it indicates that KEK authorization failed, or that BPI/BPI+ encryption was not enabled for the router in its DOCSIS configuration file.
STATE_B_OP_WAIT	The router has successfully completed the KEK key exchange, has sent a key request to the CMTS, and is waiting for a reply.
STATE_C_OP_REAUTH_WAIT	The router has sent a reauthorization request and is waiting for a reply, or the TEK key has been declared invalid. BPI/BPI+ encryption has not yet begun. If this state persists, it indicates that the TEK key exchange has failed.
STATE_D_OPERATIONAL	The router has completed the TEK key exchange, and BPI or BPI+ encryption is operational between the router and the CMTS.
STATE_E_REKEY_WAIT	The existing TEK keys have expired, and the router has requested a key update from the CMTS.
STATE_F_REKEY_REAUTH_WAIT	The router has requested a key update from the CMTS and is waiting for a reply. BPI/BPI+ encryption can continue using the existing keys until they expire.

Related Commands

Command	Description
show controllers cable-modem	Displays high-level controller information about the cable interface.
show controllers cable-modem classifiers	Displays the DOCSIS 1.1 classifiers currently in use on the router.
show controllers cable-modem mac	Displays detailed MAC-layer information for the cable interface.
show controllers cable-modem phy	Displays the contents of the registers used in the downstream physical hardware for the cable interface.
show controllers cable-modem phs	Displays the currently defined parameters for Payload Header Suppression (PHS) for the router.
show controllers cable-modem service-flows	Displays the parameters for each of the service flows defined on the router's upstream and downstream.

show controllers cable-modem classifiers

To display the DOCSIS 1.1 classifiers currently in use on the router, use the **show controllers cable-modem classifiers** command in privileged EXEC mode.

Cisco uBR905 and uBR925 cable access routers, Cisco CVA122 Cable Voice Adapter

show controllers cable-modem *number* **classifiers** [*classifier-id* | **summary**]

Syntax Description

number	Identifies the cable interface (always **0**).
classifier-id	(Optional) Displays information for a specific classifier. The valid range is 1 to 65535.
summary	(Optional) Displays a brief summary of all classifiers.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)CZ	This command was introduced for the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

Usage Guidelines

This command displays the classifiers that are currently defined for both the upstream and downstream. The information shown corresponds to the Quality of Service classifier parameters that are listed in Appendix C of the DOCSIS 1.1 specification.

Examples

The following example shows typical output for both upstream and downstream classifiers on the **show controllers cable-modem classifiers** command:

```
Router# show controllers cable-modem 0 classifiers

Upstream Packet Classifiers parameters
  Classifier Reference:    1
  Classifier ID:            2
  Service Flow Reference:  1
  Service Flow ID:         101
  Rule Priority:           0
  Activation State:        1
  Dynsrv Change Action:    0
  SID:                     90
IP classifiers:
  ToS:                     0x1 0x3 0xFF
  Protocol:                258
  Source Address:          0.0.0.0
  Source Mask:             255.255.255.255
  Destination Address:     0.0.0.0
  Destination Mask:        255.255.255.255
  Source Port Start:       65
  Source Port End:         65
  Destination Port Start:  0
```

```
  Destination Port End:    65535
LLC Classifiers:
  Destination MAC address: 0:0:0:0:0:0:0:0:0:0:0:0
Source MAC address:      0:0:0:0:0:0
  Ether Type:              0x0 0x0 0x0

Downstream Packet Classifiers parameters
  Classifier Reference:    1
  Classifier ID:           1
  Service Flow Reference:  6
  Service Flow id:         5
  Rule Priority:           22
  Activation State:        1
  Dynsrv Change Action:    0
  SID:                     0

IP classifiers
  Tos:                     0x1 0x3 0xFF
  Protocol:                258
  Source Address:          0.0.0.0
  Source Mask:          255.255.255.255
  Destination Address:     0.0.0.0
  Destination Mask:     255.255.255.255
  Source Port Start:       0
  Source Port End:         65535
  Destination Port Start:  0
  Destination Port End:    65535
LLC Classifiers
 Source MAC address:      0:0:0:0:0:0
  Ether Type:              0x0 0x0 0x0

Downstream Packet Classifiers parameters
  Classifier Reference:    2
  Classifier ID:           2
  Service Flow Reference:  7
  Service Flow id:         6
  Rule Priority:           23
  Activation State:        1
  Dynsrv Change Action:    0
  SID:                     0

IP classifiers
  Tos:                     0x5 0x5 0xD
  Protocol:                258
  Source Address:          0.0.0.0
  Source Mask:          255.255.255.255
  Destination Address:     0.0.0.0
  Destination Mask:     255.255.255.255
  Source Port Start:       0
  Source Port End:         65535
LLC Classifiers
  Destination MAC address: 0:0:0:0:0:0:0:0:0:0:0:0
  Source MAC address:      0:0:0:0:0:0
  Ether Type:              0x0 0x0 0x0

Downstream Packet Classifiers parameters
  Classifier Reference:    3
  Classifier ID:           3
  Service Flow Reference:  8
  Service Flow id:         7
  Rule Priority:           24
  Activation State:        1
  Dynsrv Change Action:    0
  SID:                     0
```

```
IP classifiers
  Tos:                     0x8 0xFF 0xF8
  Protocol:                258
  Source Address:          0.0.0.0
  Source Mask:          255.255.255.255
  Destination Address:     0.0.0.0
Destination Mask:     255.255.255.255
  Source Port Start:       0
  Source Port End:         65535
  Destination Port Start:  0
  Destination Port End:    65535
LLC Classifiers
  Destination MAC address: 0:0:0:0:0:0:0:0:0:0:0:0
  Source MAC address:      0:0:0:0:0:0
  Ether Type:              0x0 0x0 0x0
Router#
```

The following shows the typical display for the **summary** option:

```
Router# show controllers cable-modem 0 classifiers summary

SFID  SF    Classifier  Classifier  Rule      State
      Ref   ID          Ref         priority
675   1     4           10          0         active
676   2     8           11          0         active
1911  3     3           12          0         active
1914  4     7           13          0         active
1912  5     2           14          0         active
1915  6     6           15          0         active
1913  7     1           16          0         active
1916  8     5           17          0         active

Router#
```

The following shows the detailed information that is displayed for a specific classifier:

```
Router# show controllers cable-modem 0 classifiers 4

Upstream Packet Classifiers parameters
  Classifier Reference:    10
  Classfier ID:            4
  Service Flow Reference:  1
  Service Flow ID:         675
  Rule Priority:           0
  Activation State:        1
  Dynsrv Change Action:    0
  SID:                     565
IP classifiers:
  ToS:                     0x0 0x0 0x0
  Protocol:                258
  Source Address:          12.0.0.1
  Source Mask:             255.255.255.255
  Destination Address:     6.0.0.1
  Destination Mask:        255.255.255.255
  Source Port Start:       0
  Source Port End:         65535
  Destination Port Start:  0
  Destination Port End:    65535
LLC Classifiers:
  Destination MAC address: 0:0:0:0:0:0:0:0:0:0:0:0
  Source MAC address:      0:0:0:0:0:0
  Ether Type:              0x0 0x0 0x0
```

Table 6 describes the fields shown in these displays.

Table 6 show controllers cable-modem classifiers Field Descriptions

Field	Description
Classifier Reference, Classifier Ref	The reference ID to uniquely identify the classifier in the DOCSIS configuration file and MAC management messages.
Classfier ID	The ID used to uniquely identify the classifier in each service flow.
Service Flow Reference, SF Ref	The reference ID that uniquely identifies the service flow.
Service Flow ID, SFID	The ID that uniquely identifies the service flow.
Rule Priority	The priority assigned to the classifier, 0 to 255, with a higher value indicating a higher priority.
Activation State, State	Whether the classifier is activate (1) or inactive (0).
Dynsrv Change Action	The action taken for this classifier in dynamic service change messages: • 0 = Add the classifier. • 1 = Replace the classifier. • 2 = Delete the classifier.
SID	The service ID (SID) associated with this classifier.
IP Classifiers	
ToS	The matching Type of Service (Tos) low byte, high byte, and masking value.
Protocol	The matching IP protocol type, as given in RFC 1700. A value of 256 matches any IP protocol, and a value of 257 matches TCP and UDP traffic.
Source Address and Source Mask	The matching IP source address, where the source address is ANDed with the source mask to specify the valid range of source addresses.
Destination Address and Destination Mask	The matching IP destination address, where the destination address is ANDed with the destination mask to specify the valid range of destination addresses.
Source Port Start and Source Port End	The low end and high end matching source TCP/UDP port values.
Destination Port Start and Destination Port End	The low end and high end matching destination TCP/UDP port values.
LLC Classifiers	
Destination MAC address	The six-byte matching MAC destination address and six-byte mask. The first six bytes (address) are ANDed with the last six bytes (mask) to specify the valid range of MAC destination addresses.

Table 6 show controllers cable-modem classifiers Field Descriptions

Field	Description
Source MAC address	The six-byte matching MAC source address.
Ether Type	The one-byte Ethernet protocol type and two-byte matching layer 3 protocol ID in the Ether frame. The first byte can have the following values, which control the meaning of the following two bytes: • 0x00 = no matching Ethernet protocol is required. • 0x01 = Ethertype DIX or SNAP frames that match the two-byte packet type. • 0x02 = non-SNAP IEEE 802.2 encapsulation frames that match the eight-bit packet type. • 0x03 = MAC Management Messages with a type field between the two bytes, except that RNG_RSP, REG_REQ, REG_RSP, and REG_ACK frames are always matched. • 0x04 = matches all data PDU packets, regardless of the two-byte protocol ID.

Related Commands

Command	Description
show controllers cable-modem phs	Displays the currently defined parameters for Payload Header Suppression (PHS) for the router.
show controllers cable-modem service-flows	Displays the parameters for each of the service flows defined on the router's upstream and downstream.

show controllers cable-modem cmcert

To display the router's public key X.509 certificate, use the **show controllers cable-modem cmcert** command in privileged EXEC mode.

Cisco uBR905 and Cisco uBR925 Cable Access Routers, and Cisco CVA122 Cable Voice Adapter

show controllers cable-modem *number* **cmcert**

Syntax Description

number	Cable interface (always 0).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)CZ	This command was introduced on the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

Usage Guidelines

This command displays the router's X.509 DOCSIS cable-modem certificate, which uniquely identifies the router during the BPI+ negotiation process. This command shows the individual X.509 components of the certificate, starting with the DOCSIS restricted X.501 Distinguished Name and ending with the 1024-bit public key.

Tip This command displays the certificate that is burned into the router at the factory and is not normally changed. The **show controllers cable-modem manuf-cert** command displays the manufacturer's certificate that is incorporated into the Cisco IOS image that the router is currently running. Upgrading the Cisco IOS image could also update the manufacturer's certificate.

Examples

The following example shows the starting lines and ending lines of typical output for the **show controllers cable-modem cmcert** command:

```
Router# show controllers cable-modem 0 cmcert

Cable Modem Certificate:
SEQ(878)
    SEQ(727)
        Context-specific [A0](3)
            INT(1):2
            END
        INT(10): 62 E0 07 47 00 00 00 00 FA 62
1w3d:          SEQ(13)
            OID(9):SHA Signature 1.2.840.113549.1.1.5
1w3d:               NULL
            END
        SEQ(114)
            SET(11)
                SEQ(9)
```

```
                    OID(3):Country 2.5.4.6
1w3d:                     PRT(2):US
                    END
                END
            SET(22)
                SEQ(20)
                    OID(3):Organization 2.5.4.10
1w3d:                     PRT(13):Cisco Systems
                    END
                END
            SET(15)
                SEQ(13)
                    OID(3):Organization Unit 2.5.4.11
1w3d:                     PRT(6):DOCSIS
                    END
                END
            SET(58)
                SEQ(56)
                    OID(3):Common Name 2.5.4.3
1w3d:                     PRT(49):Cisco Cable Modem Root Certificate Authority R
                    END
                END

...

1w3d:          C7 9A A8 5C BD F3 30 5A E5 B6 66 1F 1E 3A C9 2E
1w3d:          04 5D B5 57 3E 75 ED A3 0A AB B6 5D 73 87 E9 BE
1w3d:          ED 1A 68 7B B3 08 DA 0F E9 AA 05 28 E2 61 1B 3D
1w3d:     END

Router#
```

Note You must manually enter a return to redisplay the router prompt after the certificate has been displayed.

Related Commands

Command	Description
show controllers cable-modem manuf-cert	Displays the manufacturer's X.509 certificate for the router.

show controllers cable-modem mac

To display detailed MAC-layer information for the router's cable interface, use the **show controllers cable-modem mac** command in privileged EXEC mode.

Cisco uBR904, uBR905, uBR924, uBR925 Cable Access Routers, Cisco CVA122 Cable Voice Adapter

show controllers cable-modem *number* **mac** {**errors** | **hardware** | **log** | **resets** | **state**}

Syntax Description

number	Cable interface (always **0**).
errors	Log of the error events that are reported to SNMP. This keyword enables you to look at the error events without accessing a MIB.
hardware	All MAC hardware registers.
log	History of MAC log messages, up to 1023 entries. This is the same output that is displayed when using the **debug cable-modem mac log** command.
resets	Summary of the reset causes out of the MAC log file.
state	Summary of the MAC state.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(4)NA	This command was introduced for the Cisco uBR904 cable access router.
12.0(4)XI1	Support was added for the Cisco uBR924 cable access router.
12.1(3)XL	Support was added for the Cisco uBR905 cable access router.
12.1(5)XU1	Support was added for the Cisco CVA122 Cable Voice Adapter.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(15)CZ	Support for DOCSIS 1.1 and BPI+ operation was added to the **state** option for the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

Usage Guidelines

MAC log messages are written to a circular log file even when debugging is not turned on. These messages include timestamps, events, and information pertinent to these events. Use the **show controllers cable-modem mac log** command to view MAC log messages.

If the router interface fails to come up or resets periodically, the MAC log captures what happened. For example, if an address is not obtained from the DHCP server, an error is logged, initialization starts over, and the router scans for a downstream frequency.

The most useful keywords for troubleshooting a router are **log**, **errors**, and **resets**. See the following examples for typical outputs for these options.

Examples

The following shows a typical display of the MAC log file for a cable interface that has successfully registered with the CMTS:

```
Router# show controllers cable-modem 0 mac log

00:14:24:    864.124 CMAC_LOG_DRIVER_INIT_IDB_RESET             0x080B7430
00:14:24:    864.128 CMAC_LOG_LINK_DOWN
00:14:24:    864.132 CMAC_LOG_RESET_FROM_DRIVER
00:14:24:    864.134 CMAC_LOG_STATE_CHANGE                      wait_for_link_up_state
00:14:24:    864.138 CMAC_LOG_LINK_UP
00:14:24:    864.142 CMAC_LOG_STATE_CHANGE                     ds_channel_scanning_state
00:14:24:    864.270 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
81/453000000/855000000/6000000
00:14:24:    864.276 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
82/93000000/105000000/6000000
00:14:24:    864.280 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
83/111025000/117025000/6000000
00:14:24:    864.286 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
84/231012500/327012500/6000000
00:14:24:    864.290 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
85/333025000/333025000/6000000
00:14:24:    864.294 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
86/339012500/399012500/6000000
00:14:24:    864.300 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
87/405000000/447000000/6000000
00:14:24:    864.304 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
88/123012500/129012500/6000000
00:14:24:    864.310 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
89/135012500/135012500/6000000
00:14:24:    864.314 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
90/141000000/171000000/6000000
00:14:24:    864.320 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
91/219000000/225000000/6000000
00:14:24:    864.324 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
92/177000000/213000000/6000000
00:14:24:    864.330 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
93/55752700/67753300/6000300
00:14:24:    864.334 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
94/79753900/85754200/6000300
00:14:24:    864.340 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
95/175758700/211760500/6000300
00:14:24:    864.344 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
96/121756000/169758400/6000300
00:14:24:    864.348 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
97/217760800/397769800/6000300
00:14:24:    864.354 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
98/73753600/115755700/6000300
00:14:24:    864.358 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND
99/403770100/997799800/6000300
00:14:24:    864.364 CMAC_LOG_WILL_SEARCH_SAVED_DS_FREQUENCY    213000000
00:14:25:    865.450 CMAC_LOG_UCD_MSG_RCVD                      1
00:14:25: %LINK-3-UPDOWN: Interface cable-modem0, changed state to up
00:14:26:    866.200 CMAC_LOG_DS_64QAM_LOCK_ACQUIRED            213000000
00:14:26:    866.204 CMAC_LOG_DS_CHANNEL_SCAN_COMPLETED
00:14:26:    866.206 CMAC_LOG_STATE_CHANGE                      wait_ucd_state
00:14:26: %LINEPROTO-5-UPDOWN: Line protocol on Interface cable-modem0, changed state to
down
00:14:27:    867.456 CMAC_LOG_UCD_MSG_RCVD                      1
00:14:29:    869.470 CMAC_LOG_UCD_MSG_RCVD                      1
00:14:29:    869.472 CMAC_LOG_ALL_UCDS_FOUND
00:14:29:    869.476 CMAC_LOG_STATE_CHANGE                      wait_map_state
00:14:29:    869.480 CMAC_LOG_UCD_NEW_US_FREQUENCY              20000000
00:14:29:    869.484 CMAC_LOG_SLOT_SIZE_CHANGED                 8
```

```
00:14:29:    869.564 CMAC_LOG_FOUND_US_CHANNEL                   1
00:14:31:    871.484 CMAC_LOG_UCD_MSG_RCVD                       1
00:14:31:    871.692 CMAC_LOG_MAP_MSG_RCVD
00:14:31:    871.694 CMAC_LOG_INITIAL_RANGING_MINISLOTS          40
00:14:31:    871.696 CMAC_LOG_STATE_CHANGE                       ranging_1_state
00:14:31:    871.700 CMAC_LOG_RANGING_OFFSET_SET_TO              9610
00:14:31:    871.704 CMAC_LOG_POWER_LEVEL_IS                     32.0  dBmV (commanded)
00:14:31:    871.708 CMAC_LOG_STARTING_RANGING
00:14:31:    871.710 CMAC_LOG_RANGING_BACKOFF_SET                0
00:14:31:    871.714 CMAC_LOG_RNG_REQ_QUEUED                     0
00:14:32:    872.208 CMAC_LOG_RNG_REQ_TRANSMITTED
00:14:32:    872.216 CMAC_LOG_RNG_RSP_MSG_RCVD
00:14:32:    872.218 CMAC_LOG_RNG_RSP_SID_ASSIGNED               16
00:14:32:    872.222 CMAC_LOG_ADJUST_RANGING_OFFSET              2853
00:14:32:    872.224 CMAC_LOG_RANGING_OFFSET_SET_TO              12463
00:14:32:    872.228 CMAC_LOG_ADJUST_TX_POWER                    8
00:14:32:    872.230 CMAC_LOG_POWER_LEVEL_IS                     34.0  dBmV (commanded)
00:14:32:    872.234 CMAC_LOG_STATE_CHANGE                       ranging_2_state
00:14:32:    872.238 CMAC_LOG_RNG_REQ_QUEUED                     16
00:14:32:    872.848 CMAC_LOG_RNG_REQ_TRANSMITTED
00:14:32:    872.852 CMAC_LOG_RNG_RSP_MSG_RCVD
00:14:32:    872.856 CMAC_LOG_RANGING_SUCCESS
00:14:32:    872.874 CMAC_LOG_STATE_CHANGE                       dhcp_state
00:14:33:    873.386 CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS           188.188.1.62
00:14:33:    873.388 CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS           4.0.0.32
00:14:33:    873.392 CMAC_LOG_DHCP_TOD_SERVER_ADDRESS            4.0.0.32
00:14:33:    873.396 CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
00:14:33:    873.398 CMAC_LOG_DHCP_TZ_OFFSET                     60
00:14:33:    873.402 CMAC_LOG_DHCP_CONFIG_FILE_NAME              platinum.cm
00:14:33:    873.406 CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
00:14:33:    873.410 CMAC_LOG_DHCP_COMPLETE
00:14:33:    873.536 CMAC_LOG_STATE_CHANGE                       establish_tod_state
00:14:33:    873.546 CMAC_LOG_TOD_REQUEST_SENT
00:14:33:    873.572 CMAC_LOG_TOD_REPLY_RECEIVED                 3140961992
00:14:33:    873.578 CMAC_LOG_TOD_COMPLETE
00:14:33:    873.582 CMAC_LOG_STATE_CHANGE
security_association_state
00:14:33:    873.584 CMAC_LOG_SECURITY_BYPASSED
00:14:33:    873.588 CMAC_LOG_STATE_CHANGE                       configuration_file_state
00:14:33:    873.592 CMAC_LOG_LOADING_CONFIG_FILE                platinum.cm
00:14:34: %LINEPROTO-5-UPDOWN: Line protocol on Interface cable-modem0, changed state to
up
00:14:34:    874.728 CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
00:14:34:    874.730 CMAC_LOG_STATE_CHANGE                       registration_state
00:14:34:    874.734 CMAC_LOG_REG_REQ_MSG_QUEUED
00:14:34:    874.744 CMAC_LOG_REG_REQ_TRANSMITTED
00:14:34:    874.754 CMAC_LOG_REG_RSP_MSG_RCVD
00:14:34:    874.756 CMAC_LOG_COS_ASSIGNED_SID                   1/16
00:14:34:    874.760 CMAC_LOG_RNG_REQ_QUEUED                     16
00:14:34:    874.768 CMAC_LOG_REGISTRATION_OK
00
:14:34:    874.770 CMAC_LOG_REG_RSP_ACK_MSG_QUEUED             0
00:14:34:    874.774 CMAC_LOG_STATE_CHANGE                       establish_privacy_state
00:14:34:    874.778 CMAC_LOG_PRIVACY_NOT_CONFIGURED
00:14:34:    874.780 CMAC_LOG_STATE_CHANGE                       maintenance_state
00:14:34:    874.784 CMAC_LOG_REG_RSP_ACK_MESSAGE_EVENT
00:14:34:    874.788 CMAC_LOG_REG_RSP_ACK_MSG_SENT
```

The following example gives the typical error messages that appear in the MAC log when the DHCP server cannot not be reached:

```
Router# show controllers cable-modem 0 mac log

00:14:32:    872.874 CMAC_LOG_STATE_CHANGE                       dhcp_state
```

```
00:14:33:    873.386 CMAC_LOG_RNG_REQ_TRANSMITTED
00:14:33:    873.388 CMAC_LOG_RNG_RSP_MSG_RCVD
00:14:33:    873.386 CMAC_LOG_RNG_REQ_TRANSMITTED
00:14:33:    873.392 CMAC_LOG_RNG_RSP_MSG_RCVD
00:14:33:    873.396 CMAC_LOG_WATCHDOG_TIMER
00:14:33:    873.398 CMAC_LOG_RESET_DHCP_WATCHDOG_EXPIRED
00:14:33:    873.402 CMAC_LOG_STATE_CHANGE                       reset_interface_state
00:14:33:    873.406 CMAC_LOG_DHCP_PROCESS_KILLED
Router#
```

In this situation, use the MAC error display also contains information indicating that the DHCP server could not be reached:

```
Router# show controllers cable-modem 0 mac errors

497989.804 D01.0  Discover sent no Offer received.  No available DHCP Server.
498024.046 D01.0  Discover sent no Offer received.  No available DHCP Server.
498058.284 D01.0  Discover sent no Offer received.  No available DHCP Server.
Router#
```

The following is a typical display of the MAC error log information, which is the same information that is also available using SNMP:

```
Router# show controllers cable-modem 0 mac errors

 74373.574 R02.0  No Ranging Response received.  T3 time-out.
 74374.660 R02.0  No Ranging Response received.  T3 time-out.
 74375.508 R02.0  No Ranging Response received.  T3 time-out.
 74375.748 R02.0  No Ranging Response received.  T3 time-out.
 74375.748 R03.0  Ranging Request Retries exhausted.
 74376.112 R02.0  No Ranging Response received.  T3 time-out.
 74376.354 R02.0  No Ranging Response received.  T3 time-out.
 74376.778 R02.0  No Ranging Response received.  T3 time-out.
 74377.442 R02.0  No Ranging Response received.  T3 time-out.
Router#
```

This output indicates that the router acquired a downstream lock, successfully read a Upstream Channel Descriptor (UCD), and successfully read a MAP. However, it was unable to communicate with the CMTS after ranging through all upstream transmit power levels. The router will try to communicate with the CMTS 16 times, and if it cannot receive a response from the CMTS, it resets the cable interface to try to find a better downstream frequency.

The **show controllers cable-modem 0 mac resets** command shows only the entries in the MAC log that begin with the field CMAC_LOG_RESET. These fields provide you with a summary of the most recent reasons why the cable interface was reset.

Reset messages and brief explanations are included in the following examples. However, the reset messages do not commonly occur.

The following example shows the errors that are logged when the configuration file downloaded from the TFTP server could not be read, typically because the file might not exist, or because the file might have incorrect permissions.

```
Router# show controllers cable-modem 0 mac resets

 62526.114 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
 62564.368 CMAC_LOG_RESET_T4_EXPIRED
 62677.178 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
 62717.462 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
 62757.746 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
 62796.000 CMAC_LOG_RESET_T4_EXPIRED
 62908.808 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
 62949.092 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
```

```
 62989.380 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
 63029.662 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
 63069.944 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
 63110.228 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
 63148.484 CMAC_LOG_RESET_T4_EXPIRED
 63261.296 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
Router#
```

The following example shows that the DHCP server could not be reached, or that it took too long to respond.

```
Router# show controllers cable-modem 0 mac resets

497989.804 CMAC_LOG_RESET_DHCP_WATCHDOG_EXPIRED
498024.046 CMAC_LOG_RESET_DHCP_WATCHDOG_EXPIRED
498058.284 CMAC_LOG_RESET_DHCP_WATCHDOG_EXPIRED
Router#
```

The following example indicates that an event in the cable interface driver caused the interface to reset. This often occurs because a **shutdown** command was just issued on the interface.

```
Router# show controllers cable-modem 0 mac resets

527986.444 CMAC_LOG_RESET_FROM_DRIVER
528302.042 CMAC_LOG_RESET_FROM_DRIVER
528346.600 CMAC_LOG_RESET_FROM_DRIVER
528444.494 CMAC_LOG_RESET_FROM_DRIVER
Router#
```

Table 7 describes the status messages that can appear in the **show controllers cable-modem mac resets** command.

Table 7 show controllers cable-modem mac resets Field Descriptions

Message	Description
CMAC_LOG_RESET_CONFIG_FILE_PARSE_FAILED	The format of the DOCSIS configuration file acquired from the TFTP server is not acceptable.
CMAC_LOG_RESET_LOSS_OF_SYNC	Synchronization with the CMTS has been lost (SYNC messages are not being received).
CMAC_LOG_RESET_T4_EXPIRED	The maintenance ranging opportunities for this router are not being received from the CMTS.
CMAC_LOG_RESET_DHCP_WATCHDOG_EXPIRED	The DHCP server took too long to respond.
CMAC_LOG_RESET_TOD_WATCHDOG_EXPIRED	The time-of-day (ToD) server took too long to respond.
CMAC_LOG_RESET_PRIVACY_WATCHDOG_EXPIRED	The baseline privacy exchange with the CMTS took too long.
CMAC_LOG_RESET_CHANGE_US_WATCHDOG_EXPIRED	The router was unable to transmit a response to a UCC-REQ message.
CMAC_LOG_RESET_SECURITY_WATCHDOG_EXPIRED	A “full security” exchange with the CMTS took too long.
CMAC_LOG_RESET_CONFIG_FILE_WATCHDOG_EXPIRED	The TFTP server took too long to respond.
CMAC_LOG_RESET_ALL_FREQUENCIES_SEARCHED	All downstream frequencies to be searched have been searched. **Note** This message indicates that downstream frequencies were found, but the router failed to acquire a downstream lock.
CMAC_LOG_RESET_T2_EXPIRED	Initial ranging opportunities are not being received.

Table 7 show controllers cable-modem mac resets Field Descriptions (continued)

Message	Description
CMAC_LOG_RESET_T3_RETRIES_EXHAUSTED	The CMTS failed too many times to respond to a RNG-REQ message. **Note** After 16 T3 timeouts, the router resets the cable interface.
CMAC_LOG_RESET_RANGING_ABORTED	The CMTS commanded the router to abort the ranging process.
CMAC_LOG_RESET_NO_MEMORY	The router has run out of memory.
CMAC_LOG_RESET_CANT_START_PROCESS	The router was unable to start an internal process necessary to complete ranging and registration.
CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED	The reading of the configuration file from the TFTP server failed. **Note** The file might not exist, or it might have incorrect permissions.
CMAC_LOG_RESET_AUTHENTICATION_FAILURE	The router failed authentication as indicated in a REG-RSP message from the CMTS.
CMAC_LOG_RESET_SERVICE_NOT_AVAILABLE	The CMTS has failed the router's registration because a required or requested class of service is not available.
CMAC_LOG_RESET_T6_RETRIES_EXHAUSTED	The CMTS failed too many times to respond to a REG-REQ message.
CMAC_LOG_RESET_MAINTENANCE_WATCHDOG_DRIVER	The router MAC layer failed to detect a change in the interface driver.
CMAC_LOG_RESET_NET_ACCESS_MISSING	The Network Access parameter is missing from the DOCSIS configuration file.
CMAC_LOG_RESET_FAILED_WRITE_ACCESS_CONTROL	The router was unable to set the Write Access Control for an SNMP parameter as specified by the DOCSIS configuration file.
CMAC_LOG_RESET_DHCP_FAILED	The DHCP server did not respond with all the required values. The required values are: IP address, network mask, TFTP server IP address, ToD server IP address, DOCSIS configuration filename, and time zone offset.
CMAC_LOG_RESET_CANT_START_DS_TUNER_PRCESS	The router was unable to start the internal process used to manage the downstream tuner.
CMAC_LOG_RESET_TOO_MANY_DS_LOCKS_LOST	Downstream QAM/FEC lock has been lost too many times.
CMAC_LOG_RESET_NO_SEND_TO_DS_TUNER_PROCESS	The router MAC-layer process was unable to communicate with the downstream tuner management process.
CMAC_LOG_RESET_DS_TUNER_WATCHDOG	The downstream tuner process failed to report its continuing operation for a long period of time.
CMAC_LOG_RESET_UNABLE_TO_SET_MIB_OBJECT	The router was unable to set an SNMP parameter as specified by the DOCSIS configuration file.
CMAC_LOG_RESET_MIB_OBJECT_PROCESS_WATCHDOG	The internal MIB object took too long to process the entries in the DOCSIS configuration file.

The following example is a typical display for the **show controllers cable-modem 0 mac hardware** command. The most interesting bit is the station address (hardware address). The MIB statistics reflect the MAC hardware counters for various events, but these counters are typically reset every few seconds, so their contents are not accurate in this display.

```
Router# show controllers cable-modem 0 mac hardware

PLD VERSION: 32

BCM3300 unit 0, idb 0x200EB4, ds 0x82D4748, regaddr = 0x800000, reset_mask
0x80
station address 0010.7b43.aa01  default station address 0010.7b43.aa01
MAC mcfilter 01E02F00  data mcfilter 01000000

buffer size 1600
RX data PDU ring with 32 entries at 0x201D40
  rx_head = 0x201D40 (0), rx_p = 0x82D4760 (0)
    00 pak=0x82DF844 buf=0x227F1A status=0x80 pak_size=0
    01 pak=0x82E0BF4 buf=0x22C56A status=0x80 pak_size=0
    02 pak=0x82DF454 buf=0x22710A status=0x80 pak_size=0
    03 pak=0x82DF64C buf=0x227812 status=0x80 pak_size=0
    04 pak=0x82E0024 buf=0x229B3A status=0x80 pak_size=0
    05 pak=0x82DBF2C buf=0x21B332 status=0x80 pak_size=0
    06 pak=0x82DFE2C buf=0x229432 status=0x80 pak_size=0
    07 pak=0x82E0FE4 buf=0x22D37A status=0x80 pak_size=0
    08 pak=0x82DF064 buf=0x2262FA status=0x80 pak_size=0
    09 pak=0x82DEC74 buf=0x2254EA status=0x80 pak_size=0
    10 pak=0x82DEA7C buf=0x224DE2 status=0x80 pak_size=0
    11 pak=0x82DE884 buf=0x2246DA status=0x80 pak_size=0
    12 pak=0x82DE68C buf=0x223FD2 status=0x80 pak_size=0
    13 pak=0x82DE494 buf=0x2238CA status=0x80 pak_size=0
    14 pak=0x82DE29C buf=0x2231C2 status=0x80 pak_size=0
    15 pak=0x82DE0A4 buf=0x222ABA status=0x80 pak_size=0
    16 pak=0x82DDEAC buf=0x2223B2 status=0x80 pak_size=0
    17 pak=0x82DDCB4 buf=0x221CAA status=0x80 pak_size=0
    18 pak=0x82DDABC buf=0x2215A2 status=0x80 pak_size=0
    19 pak=0x82DD8C4 buf=0x220E9A status=0x80 pak_size=0
    20 pak=0x82DD6CC buf=0x220792 status=0x80 pak_size=0
    21 pak=0x82DD4D4 buf=0x22008A status=0x80 pak_size=0
    22 pak=0x82DD2DC buf=0x21F982 status=0x80 pak_size=0
    23 pak=0x82DD0E4 buf=0x21F27A status=0x80 pak_size=0
    24 pak=0x82DCEEC buf=0x21EB72 status=0x80 pak_size=0
    25 pak=0x82DCCF4 buf=0x21E46A status=0x80 pak_size=0
    26 pak=0x82DCAFC buf=0x21DD62 status=0x80 pak_size=0
    27 pak=0x82DC904 buf=0x21D65A status=0x80 pak_size=0
    28 pak=0x82DC70C buf=0x21CF52 status=0x80 pak_size=0
    29 pak=0x82DC514 buf=0x21C84A status=0x80 pak_size=0
    30 pak=0x82DC31C buf=0x21C142 status=0x80 pak_size=0
    31 pak=0x82DC124 buf=0x21BA3A status=0xA0 pak_size=0
RX MAC message ring with 8 entries at 0x201E80
  rx_head_mac = 0x201EB0 (6), rx_p_mac = 0x82D480C (6)
    00 pak=0x82E0DEC buf=0x22CC72 status=0x80 pak_size=0
    01 pak=0x82E021C buf=0x22A242 status=0x80 pak_size=0
    02 pak=0x82E060C buf=0x22B052 status=0x80 pak_size=0
    03 pak=0x82E11DC buf=0x22DA82 status=0x80 pak_size=0
    04 pak=0x82DFC34 buf=0x228D2A status=0x80 pak_size=0
    05 pak=0x82E09FC buf=0x22BE62 status=0x80 pak_size=0
    06 pak=0x82DEE6C buf=0x225BF2 status=0x80 pak_size=0
    07 pak=0x82DFA3C buf=0x228622 status=0xA0 pak_size=0
TX BD ring with 8 entries at 0x201FB8, tx_count = 0
  tx_head = 0x201FB8 (0), head_txp = 0x82D4888 (0)
  tx_tail = 0x201FB8 (0), tail_txp = 0x82D4888 (0)
    00 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
    01 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
    02 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
    03 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
    04 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
    05 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
    06 pak=0x000000 buf=0x200000 status=0x00 pak_size=0
```

```
    07 pak=0x000000 buf=0x200000 status=0x20 pak_size=0
TX PD ring with 8 entries at 0x202038, tx_count = 0
  tx_head_pd = 0x202038 (0)
  tx_tail_pd = 0x202038 (0)
    00 status=0x00 bd_index=0x0000 len=0x0000 hdr_len=0x0000
    ehdr:  00 00 00 2E FF FF
    01 status=0x00 bd_index=0x0001 len=0x0000 hdr_len=0x0000
    ehdr:  00 00 00 2E FF FF
    02 status=0x00 bd_index=0x0002 len=0x0000 hdr_len=0x0000
    ehdr:  00 00 00 2E FF FF
    03 status=0x00 bd_index=0x0003 len=0x0000 hdr_len=0x0000
    ehdr:  00 00 00 2E FF FF
    04 status=0x00 bd_index=0x0004 len=0x0000 hdr_len=0x0000
    ehdr:  00 00 00 2E 00 00
    05 status=0x00 bd_index=0x0005 len=0x0000 hdr_len=0x0000
    ehdr:  00 00 00 2E 00 00
    06 status=0x00 bd_index=0x0006 len=0x0000 hdr_len=0x0000
    ehdr:  00 00 00 00 00 00
    07 status=0x20 bd_index=0x0007 len=0x0000 hdr_len=0x0000
    ehdr:  00 00 00 00 00 00

MIB Statistics
  DS fifo full = 0, Rerequests = 0
  DS mac msg overruns = 0, DS data overruns = 0
  Qualified maps = 0, Qualified syncs = 0
  CRC fails = 0, HDR chk fails = 0
  Data pdus = 0, Mac msgs = 0
  Valid hdrs = 0
BCM3300 Registers:
downstream dma:
  ds_data_bd_base=0x001D40, ds_mac_bd_base=0x001E80
  ds_data_dma_ctrl=0x98, ds_mac_dma_ctrl=0x98
  ds_dma_data_index=0x0000, ds_dma_msg_index=0x0000
upstream dma:
  us_bd_base=0x001FB8, us_pd_base=0x002038
  us_dma_ctrl=0x00, us_dma_tx_start=0x00
global control and status:
  global_ctrl_status=0x00
interrupts:
  irq_pend=0x0018, irq_mask=0x00E7
timing recovery circuit:
  loop_enable=0x00, minislot_divisor=0x00
  K0_ctrl=0x06, K1_ctrl=0x07, acq_threshhold=0x01
  err_threshhold=0x04, timeout_threshold=0xFF
  nco_bias=0x4F7004F7, ranging_offset=0x00000000
  ts_err=0x00, sync_valid=0x00, delta_F=0x00
  timeout_err=0x00
spi:
  dynamic_ctrl=0x09, static_ctr=0x9F, autonomous=0x01
  irq_ack=0x00, spi_cmd=0x51, spi_addr=0x11
  spi_data= FF/00/00/00/00/00/00
burst profiles:
  profile 0:
             01 19 1D 00 00 00 00 00 00 00 00 00 00 00 00 00
             00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
             00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
             00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  profile 1:
             01 19 1D 03 00 00 00 00 00 00 00 00 00 00 00 00
             00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
             00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
             00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  profile 2:
             01 19 1D 04 00 00 00 00 00 00 00 00 00 00 00 00
```

```
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  profile 3:
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Router#
```

Table 8 describes the MIB statistics shown in the display for this command.

Table 8 MIB Statistics Field Descriptions

Field	Description
DS fifo full	Number of times the downstream receive buffer on the router has become full.
Rerequests	Number of registration requests sent by the router to the CMTS.
DS mac msg overruns	Number of times the Direct Memory Access (DMA) controller has had a downstream MAC message and there were no free MAC message buffer descriptors to accept the message.
DS data overruns	Number of times the DMA controller has had downstream data and there were no free data protocol data unit (PDU) buffer descriptors to accept the data.
Qualified maps	Number of valid MAP messages received by the router.
Qualified syncs	Number of times the router has received synchronization with the downstream channel.
CRC fails	Number of cyclic redundancy checks (CRCs) generated by the far-end device that did not match the checksums calculated from the message portions of the packets received.
HDR check fails	Number of cyclic redundancy checks (CRCs) generated by the far-end device that did not match the checksums calculated from the MAC headers of the packets received. The MAC header CRC is a 16-bit header check sequence (HCS) field that ensures the integrity of the MAC header even in a collision environment.
Data pdus	Total number of data PDUs of all types received by the cable interface.
Mac msgs	Number of MAC messages received by the cable interface.
Valid hdrs	Number of valid MAC headers received by the cable interface.

Below the MIB statistics in the **show controllers cable-modem 0 mac hardware** display, the BCM3300 registers section shows the DMA locations of the indicated processing routines of the Broadcom 3220 MAC chip within the router.

The following is typical output from the **show controllers cable-modem mac state** command that summarizes the state of the cable MAC layer and provides a list of downstream search frequency bands and the order in which they are searched. The normal operational state of the interface is the maintenance_state. If the cable MAC layer is in the wait_for_link_up_state, the information shown in the display corresponds to the last time the interface was up.

```
Router# show controller cable-modem 0 mac state

MAC State:                  maintenance_state
```

```
Ranging SID:                5
Registered:                 TRUE
Privacy Established:        TRUE
Privacy Version:            BPI+ (PLUS)
DOCSIS Operating Mode:      DOCSIS 1.1

Snmp Operating Mode:        Co-existence Mode

MIB Values:
  Mac Resets:       0
  Sync lost:        0
  Invalid Maps:     0
  Invalid UCDs:     0
  Invalid Rng Rsp:  0
  Invalid Reg Rsp:  0
  T1 Timeouts:      0
  T2 Timeouts:      0
  T3 Timeouts:      4
  T4 Timeouts:      0
  Range Aborts:     0

DS ID:                      1
DS Frequency:               663000000
DS Symbol Rate:             5056941
DS QAM Mode                 64QAM
DS Search:
  88 453000000 855000000 6000000
  89  93000000 105000000 6000000
  90 111250000 117250000 6000000
  91 231012500 327012500 6000000
  92 333015000 333015000 6000000
  93 339012500 399012500 6000000
  94 405000000 447000000 6000000
  95 123015000 129015000 6000000
  96 135012500 135012500 6000000
  97 141000000 171000000 6000000
  98 219000000 225000000 6000000
  99 177000000 213000000 6000000
US ID:                      1
US Frequency:               20000000
US Power Level:             34.0 (dBmV)
US Symbol Rate:             1280000
Ranging Offset:             12460
Mini-Slot Size:             8
Change Count:               4
Preamble Pattern:           CC CC CC CC CC CC CC CC  CC CC CC CC CC CC 0D 0D
                               A9 17 D9 C3 52 2F B3 86  A4 5F 67 0D 48 BE CE 1A
                               91 7D 9C 35 22 FB 38 6A  45 F6 70 D4 8B EC E1 A9
                               17 D9 C3 52 2F B3 86 A4  5F 67 0D 48 BE CE 1A 91
                               F3 F3 F3 F3 F3 F3 F3 F3  F3 F3 F3 F3 F3 F3 F3 F3
                               F3 F3 F3 F3 F3 F3 F3 F3  F3 F3 F3 F3 33 F7 33 F7
                               88 84 04 4C C4 84 C0 0C  44 08 08 CC 8C 0C 80 48
                               88 40 44 CC 48 4C 00 C4  40 80 8C C8 C0 C8 04 88
Burst Descriptor  0:
  Interval Usage Code:      1
  Modulation Type:          1
  Differential Encoding:    2
  Preamble Length:          64
  Preamble Value Offset:    56
  FEC Error Correction:     0
  FEC Codeword Info Bytes:  16
  Scrambler Seed:           338
  Maximum Burst Size:       1
  Guard Time Size:          8
```

```
  Last Codeword Length:     1
  Scrambler on/off:         1
Burst Descriptor  1:
  Interval Usage Code:      3
  Modulation Type:          1
  Differential Encoding:    2
  Preamble Length:          128
  Preamble Value Offset:    0
  FEC Error Correction:     5
  FEC Codeword Info Bytes:  34
  Scrambler Seed:           338
  Maximum Burst Size:       0
  Guard Time Size:          48
  Last Codeword Length:     1
  Scrambler on/off:         1
Burst Descriptor  2:
  Interval Usage Code:      4
  Modulation Type:          1
  Differential Encoding:    2
  Preamble Length:          128
  Preamble Value Offset:    0
  FEC Error Correction:     5
  FEC Codeword Info Bytes:  34
  Scrambler Seed:           338
  Maximum Burst Size:       0
  Guard Time Size:          48
  Last Codeword Length:     1
  Scrambler on/off:         1
Burst Descriptor  3:
  Interval Usage Code:      5
  Modulation Type:          1
  Differential Encoding:    2
  Preamble Length:          72
  Preamble Value Offset:    48
  FEC Error Correction:     5
  FEC Codeword Info Bytes:  75
  Scrambler Seed:           338
  Maximum Burst Size:       0
  Guard Time Size:          8
  Last Codeword Length:     1
  Scrambler on/off:         1
Config File:
  Network Access:           TRUE
  Concatenation:            Disabled
  Maximum CPEs:             8
  SNMP MIB Object:          0000000000000000000000000000000000000000000000000000
  Vendor ID:                0.240.30
    Baseline Privacy:
    Auth. Wait Timeout:     10
    Reauth. Wait Timeout:   10
    Auth. Grace Time:       600
    Op. Wait Timeout:       1
    Retry Wait Timeout:     1
    TEK Grace Time:         600
    Auth. Reject Wait Time: 60
  COS  1:
    Assigned SID:           5
    Max Downstream Rate:    4000000
    Max Upstream Rate:      2000000
    Upstream Priority:      7
    Min Upstream Rate:      100000
    Max Upstream Burst:     12
    Privacy Enable:         TRUE
Ranging Backoff Start:      0 (at initial ranging)
```

```
Ranging Backoff End:        4 (at initial ranging)
Data Backoff Start:         0 (at initial ranging)
Data Backoff End:           4 (at initial ranging)
IP Address:                 0.0.0.0
Net Mask:                   0.0.0.0

TFTP Server IP Address:     223.255.254.254
Time Server IP Address:     188.188.1.5
Config File Name:           muck/ebuell/tftp/cm_conf
Time Zone Offset:           -28800
Log Server IP Address:      0.0.0.0

Drop Ack Enabled:           TRUE
Piggyback when Ccat On:     Disabled

Mac Sid Status
Max Sids: 4  Sids In Use: 1
 SFid      Sid      State   Type     rxtx Parm State    Idb

   5         2        2       2       F4      7       811C24B0
Router#
```

Table 9 describes the fields shown in the display.

Table 9 show controller cable-modem mac state Field Descriptions

Field	Description
MAC State	Current operational state of the MAC layer of the router.
Ranging SID	Service ID used for ranging requests.
Registered	Whether or not the router is currently registered with the CMTS.
Privacy Established	Whether or not keys for baseline privacy have been exchanged between the router and the CMTS, establishing privacy.
Privacy Version	Whether the router is using BPI or BPI+ baseline privacy.
DOCSIS Operating Mode	DOCSIS revision that the router has been provisioned for (DOCSIS 1.0 or DOCSIS 1.1).
Snmp Operating Mode	Current SNMP operating mode: • Co-existence Mode—SNMPv3 coexistence model • NmAccess Mode—SNMPv2 model
Mac Resets	Number of times the router reset or initialized this interface.
Sync lost	Number of times the router lost synchronization with the downstream channel.
Invalid Maps	Number of times the router received invalid MAP messages.
Invalid UCDs	Number of times the router received invalid upstream channel descriptor (UCD) messages.
Invalid Rng Rsp	Number of times the router received invalid ranging response messages.
Invalid Reg Rsp	Number of times the router received invalid registration response messages.
T1 Timeouts	Number of timeouts caused by the router not receiving a valid UCD from the CMTS within the specified time.

Table 9 show controller cable-modem mac state Field Descriptions (continued)

Field	Description
T2 Timeouts	Number of timeouts caused by the router not receiving a maintenance broadcast for ranging opportunities from the CMTS within a specified time.
T3 Timeouts	Number of timeouts caused by the router not receiving a response within a specified time from the CMTS to a RNG-REQ message during initial maintenance.
T4 Timeouts	Number of timeouts caused by the router not receiving a response within a specified time from the CMTS to a periodic maintenance request.
Range Aborts	Number of times the ranging process was aborted by the CMTS.
DS ID	Identifier of the downstream channel on which this MAC management message has been transmitted. This identifier is arbitrarily chosen by the CMTS and is unique only within the MAC-sublayer domain.
DS Frequency	Downstream frequency acquired by the router during its last initialization sequence.
DS Symbol Rate	Downstream frequency in symbols per second.
DS QAM Mode	Downstream modulation scheme being used by the router.
DS Search	Frequency bands scanned by the router when searching for a downstream channel. The router's default frequency bands correspond to the North American EIA CATV channel plan for 6-MHz channel slots between 90 MHz and 858 MHz.
US ID	Identifier of the upstream channel to which this MAC management message refers. This identifier is arbitrarily chosen by the CMTS and is unique only within the MAC-sublayer domain.
US Frequency	Transmission frequency used by the router in the upstream direction.
US Power Level	Transmit power level of the router in the upstream direction.
US Symbol Rate	Upstream frequency in symbols per second.
Ranging Offset	Delay correction (in increments of 6.25 microseconds/64) applied by the router to the CMTS upstream frame time derived at the router. Used to synchronize the upstream transmissions in the time division multiple access (TDMA) scheme, this value is roughly equal to the round-trip delay of the router from the CMTS.
Mini-Slot Size	Size T of the mini-slot for this upstream channel in units of the timebase tick of 6.25 microseconds. Allowable values are 2, 4, 8, 16, 32, 64, or 128.
Change Count	Incremented by 1 by the CMTS whenever any of the values of this channel descriptor change. If the value of this count in a subsequent upstream channel descriptor (UCD) remains the same, the router can quickly decide that the remaining fields have not changed, and may be able to disregard the remainder of the message.
Preamble Pattern	Byte pattern used for the preamble.
Burst Descriptor:	Compound Type/Length/Value (TLV) encoding that defines, for each type of upstream usage interval, the physical-layer characteristics that are to be used during that interval. Each burst descriptor is given an identifying number.

Table 9 show controller cable-modem mac state Field Descriptions (continued)

Field	Description
Interval Usage Code	Each upstream transmit burst belongs to a class that is given a number called the interval usage code (IUC). Bandwidth MAP messages are used by IUC codes to allocate upstream time slots. The following types are currently defined: 1. Request: bandwidth request slot 2. Request/Data: bandwidth request or data slot 3. Initial Maintenance: initial link registration contention slot 4. Station Maintenance: link keepalive slot 5. Short Data Grant: short data burst slot 6. Long Data Grant: long data burst slot
Modulation Type	Upstream modulation format. (1 = QPSK; 2 = QAM-16)
Differential Encoding	Indicates whether or not differential encoding is used. (1 = yes; 2 = no)
Preamble Length	Length of the preamble in bits. This value must be an integral number of symbols—a multiple of 2 for QPSK; a multiple of 4 for QAM-16.
FEC Error Correction	Length of the forward error correction in bytes. The range is 0 to 10 bytes; a value of 0 implies no forward error correction.
FEC Codeword Info Bytes	Number of information bytes in the FEC codeword.
Scrambler Seed	15-bit seed value loaded at the beginning of each burst after the register has been cleared. Not used if scrambler is off.
Maximum Burst Size	Maximum number of mini-slots that can be transmitted during this burst type. When the interval type is Short Data Grant, this value must be greater than 0. If this value is 0, the burst size is limited elsewhere.
Guard Time Size	Amount of time in symbols between the center of the last symbol of a burst and the center of the first symbol of the preamble of an immediately following burst in an upstream transmission from the router to the CMTS.
Last Codeword Length	Whether or not the length of the last codeword is fixed or shortened. (1 = fixed; 2 = shortened)
Scrambler on/off	Indicates whether or not a scrambler is enabled in the upstream modulator. (1 = on; 2 = off)
Network Access	Whether or not the router has access to the HFC network.
Concatenation	Whether DOCSIS 1.1 concatenation is enabled or disabled.
Maximum CPEs	Maximum number of CPEs supported for this cable modem.
Vendor ID	Unique identifier specifying the CM manufacturer.
Auth. Wait Timeout	Number of seconds the router waits for a reply after sending the Authorization Request message to the CMTS.
Reauth. Wait Timeout	Number of seconds the router waits for a reply after it has sent an Authorization Request message to the CMTS in response to a reauthorization request or an Authorization Invalid message from the CMTS.

Table 9 show controller cable-modem mac state Field Descriptions (continued)

Field	Description
Auth. Grace Time	Number of seconds before the current authorization is set to expire that the grace timer begins, signaling the router to begin the reauthorization process.
Op. Wait Timeout	Number of seconds the TEK state machine waits for a reply from the CMTS after sending its initial Key Request for its SID's keying material.
Retry Wait Timeout	Number of seconds the TEK state machine waits for a replacement key for this SID after the TEK grace timer has expired and the request for a replacement key has been made.
TEK Grace Time	Number of seconds before the current TEK is set to expire that the TEK grace timer begins, signaling the TEK state machine to request a replacement key.
Auth. Reject Wait Time	Number of seconds the router waits before sending another Authorization Request message to the CMTS after it has received an Authorization Reject message.
Assigned SID	Service ID assigned by the CMTS for the corresponding service class.
Max Downstream Rate	Maximum downstream rate in bits per second that the CMTS is permitted to forward to CPE unicast MAC addresses learned or configured as mapping to this router. This rate does not include MAC packets addressed to broadcast or multicast MAC addresses.
Max Upstream Rate	Maximum upstream rate in bits per second that the router is permitted to forward to the RF network. This rate includes packet PDU data packets addressed to broadcast or multicast addresses.
Upstream Priority	Relative priority assigned to this service class for data transmission in the upstream channel. Higher numbers indicate higher priority.
Min Upstream Rate	Data rate in bits per second that are guaranteed to this service class on the upstream channel.
Max Upstream Burst	Maximum transmit burst in bytes allowed for this service class on the upstream channel.
Privacy Enable	Whether or not Baseline Privacy is enabled for this service class.
Ranging Backoff Start	Initial back-off window for initial ranging contention, expressed as a power of 2. Valid values are from 0 to 15.
Ranging Backoff End	Final back-off window for initial ranging contention, expressed as a power of 2. Valid values are from 0 to 15.
Data Backoff Start	Initial back-off window for contention data and requests, expressed as a power of 2. Valid values are from 0 to 15.
Data Backoff End	Final back-off window for contention data and requests, expressed as a power of 2. Valid values are from 0 to 15.
IP Address	IP address of the cable interface.
Net Mask	Subnet mask of the cable interface.
TFTP Server IP Address	IP address of the CMTS TFTP server.
Time Server IP Address	IP address of the CMTS Time-of-Day (TOD) server.

Table 9 show controller cable-modem mac state Field Descriptions (continued)

Field	Description
Config File Name	Name of the configuration file that is downloaded from the TFTP server to provide the router with operational parameters.
Time Zone Offset	Correction received from the DHCP server to synchronize the router time clock with the CMTS.
Log Server IP Address	Displays the IP address for a syslog server, if any has been defined.
Drop Ack Enabled	Whether the TCP drop acknowledge feature is enabled or disabled.
Piggyback when Ccat On	Whether the piggybacking of data onto request packets is enabled when concatenation is also enabled.
Mac Sid Status	Displays the service IDs currently in use.

Tip In Cisco IOS Release 12.2(8)T and later releases, you can add a time stamp to **show** commands using the **exec prompt timestamp** command in line configuration mode.

Related Commands

Command	Description
show controllers cable-modem	Displays high-level controller information about the cable interface.
show controllers cable-modem bpkm	Displays information about the baseline privacy key management exchange between the the cable interface and the CMTS.
show controllers cable-modem des	Displays information about the Data Encryption Standard (DES) engine registers.
show controllers cable-modem filters	Displays the registers in the MAC hardware that are used for filtering received frames.
show controllers cable-modem lookup-table	Displays the mini-slot lookup table for the cable interface.
show controllers cable-modem phy	Displays the contents of the registers used in the downstream physical hardware for the the cable interface.
show controllers cable-modem tuner	Displays the settings for the upstream and downstream tuners used by the cable interface.

show controllers cable-modem manuf-cert

To display the manufacturer's X.509 certificate for the router, use the **show controllers cable-modem manuf-cert** command in privileged EXEC mode.

Cisco uBR905 and Cisco uBR925 Cable Access Routers, and Cisco CVA122 Cable Voice Adapter

show controllers cable-modem *number* **manuf-cert**

Syntax Description

number	Identifies the cable interface (always 0).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)CZ	This command was introduced on the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

Usage Guidelines

This command displays the manufacturing certificate for Cisco Systems, which the Secure Software Download procedure uses to authenticate the software that the router downloads. This command shows the individual X.509 components of the certificate, starting with the DOCSIS restricted X.501 Distinguished Name and ending with the 1024-bit public key.

Tip This command displays the certificate that is incorporated into the Cisco IOS image that the router is currently running. Upgrading the Cisco IOS image could also update the manufacturer's certificate. The **show controllers cable-modem cmcert** command displays the cable-modem certificate that is burned into the router at the factory and is not normally changed.

Examples

The following example shows the starting lines and ending lines of typical output for the **show controllers cable-modem manuf-cert** command:

```
Router# show controllers cable-modem 0 manuf-cert

Cisco Manufacturing Certificate:
SEQ(819)
    SEQ(539)
        Context-specific [A0](3)
            INT(1):2
            END
        INT(16): 0B F5 94 FD 7B 4E E0 79 90 83 5C A9 A4 BE A0 3E
1w3d:         SEQ(13)
            OID(9):SHA Signature 1.2.840.113549.1.1.5
1w3d:               NULL
            END
        SEQ(151)
            SET(11)
                SEQ(9)
```

```
                    OID(3):Country 2.5.4.6
1w3d:                     PRT(2):US
                    END
                END
            SET(57)
                SEQ(55)
                    OID(3):Organization 2.5.4.10
1w3d:                     PRT(48):Data Over Cable Service Interface Specificatis
                    END
                END
            SET(21)
                SEQ(19)
                    OID(3):Organization Unit 2.5.4.11
1w3d:                     PRT(12):Cable Modems
                    END
                END

...

1w3d:          E1 13 05 10 3C F1 F1 A0 CE 43 74 30 9C 59 F5 70
1w3d:          4B C2 71 8E 79 AC 19 3D AB 94 1E B0 BE BC 15 D8
1w3d:          AD A4 79 F5 58 CA 04 25 62 A9 F8 3F E7 40 64 E2
1w3d:          65 B0 D0 53 65 FF F1 12 FF 1B CD DE 1D 47 A2 6E
1w3d:     END

Router#
```

Note You must manually enter a return to redisplay the router prompt after the certificate has been displayed.

Related Commands

Command	Description
show controllers cable-modem cmcert	Displays the router's public key X.509 certificate.

show controllers cable-modem phs

To display the currently defined parameters for Payload Header Suppression (PHS) for the router, use the **show controllers cable-modem phs** command in privileged EXEC mode.

Cisco uBR905 and uBR925 cable access routers, Cisco CVA122 Cable Voice Adapter

show controllers cable-modem *number* **phs** [*rule-index*]

Syntax Description

number	Identifies the cable interface (always **0**).
rule-index	(Optional) Displays information for a specific PHS rule index. The valid range is 1 to 255.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)CZ	This command was introduced for the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

Usage Guidelines

This command displays the PHS parameters that are currently in use for both the upstream and downstream. The information shown corresponds to the PHS parameters that are listed in Appendix C of the DOCSIS 1.1 specification.

Examples

The following example shows typical output for the **show controllers cable-modem phs** command.

```
Router# show controllers cable-modem 0 phs

Upstream PHS Parameters

PHS Parameters
  PHS Classifier Refer:           2
  PHS Classifier ID:              101
  PHS Service Flow Reference:     2
  PHS Service Flow ID:            43
  PHS Dynsrv Change Action:       0
  PHS Fields:                     0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x0a 0x14 0x73 0x21 0x00 0x00 0x00 0x00 0x00 0x00
  PHS Index:                      1
  PHS Mask:                       0x00 0x03 0xc0
  PHS Classifier Size:            24
  PHS Classifier Verification:    0

Downstream PHS Parameters

PHS Parameters
  PHS Classifier Refer:           5
  PHS Classifier ID:              99
  PHS Service Flow Reference:     3
  PHS Service Flow ID:            72
```

```
  PHS Dynsrv Change Action:       0
PHS Fields:                     0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x0a 0x14 0x73 0x21 0x00 0x00 0x00 0x00 0x00 0x00
  PHS Index:                    1
  PHS Mask:                     0x00 0x03 0xc0
  PHS Classifier Size:          24
  PHS Classifier Size:          8
  PHS Classifier Verification:  0

Router#
```

The following shows a typical display for a specific PHS rule:

```
Router# show controllers cable-modem 0 phs 3

Downstream PHS Parameters

PHS Parameters
  PHS Classifier Refer:         15
  PHS Classifier ID:            6
  PHS Service Flow Reference:   6
  PHS Service Flow ID:          1915
  PHS Dynsrv Change Action:     0
  PHS Fields:                   0x08 0x00 0x45 0x00 0x00 0x56 0x00 0x00 0x00 0x00 0x3B
0x00 0x6D 0xA7 0x08 0x00 0x00 0x01 0x0C 0x00 0x00 0x01 0xAB 0xAB 0xAB 0xAB 0xAB 0xAB 0xAB
0xAB 0xAB 0xAB 0xAB 0xAB
  PHS Index:                    3
  PHS Mask:                     0xF0 0x00 0x01 0xFF 0xAB
  PHS Size:                     34
  PHS Verification:             0

Router#
```

Table 10 describes the fields shown in the display.

Table 10 show controllers cable-modem phs Field Descriptions

Field	Description
PHS Classifier Refer	The reference ID for the classifier using this PHS rule.
PHS Classifier ID	The ID for the classifier using this PHS rule.
PHS Service Flow Reference	The reference ID for the service flow using this PHS rule.
PHS Service Flow ID	The ID for the service flow using this PHS rule.
PHS Dynsrv Change Action	The action taken in a dynamic service change request for this PHS rule: • 0 = Add the PHS rule. • 1 = Set the PHS rule. • 2 = Delete the PHS rule. • 3 = Delete all PHS rules.
PHS Fields	The bytes of the headers that must be suppressed and restored during PHS operation. For the upstream, this includes the PDU bytes starting with the first byte after the MAC header checksum. For the downstream, this includes the PDU bytes starting with the 13th byte after the MAC header checksum.

Table 10 show controllers cable-modem phs Field Descriptions

Field	Description
PHS Index	The index that references the suppressed byte string in the PHS Fields. The index is unique per service flow in the upstream direction and unique per the cable modem in the downstream direction.
PHS Mask	The mask used to interpret the bytes in the PHS Fields, where each bit indicates whether the corresponding byte in the PHS Fields should be suppressed (0 = do not suppress, 1 = suppress).
PHS Classifier Size	The total number of bytes in the header to be suppressed.
PHS Classifier Verification	Indicates whether the header bytes are to be verified before suppression (0 = verify, 1 = do not verify).

Related Commands

Command	Description
show controllers cable-modem classifiers	Displays the DOCSIS 1.1 classifiers currently in use on the router.
show controllers cable-modem service-flows	Displays the parameters for each of the service flows defined on the router's upstream and downstream.

show controllers cable-modem qos

To display detailed information about the quality-of-service (QoS) configuration for the router, use the **show controllers cable-modem qos** command in privileged EXEC mode.

Cisco uBR905, Cisco uBR924, and Cisco uBR925 Cable Access Routers, and Cisco CVA122 Cable Voice Adapter

show controllers cable-modem *number* **qos** [**details**]

Syntax Description

number	Identifies the cable interface (always 0).
details	(Optional) Displays detailed information, including classifier information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR and 12.1(1)T	This command was introduced on the Cisco uBR924 cable access router.
12.1(3)XL	Support was added for the Cisco uBR905 cable access router.
12.1(5)XU1	Support was added for the Cisco CVA122 Cable Voice Adapter.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(15)CZ	Support for DOCSIS 1.1 and BPI+ operation was added for the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter. The **details** option was also added.

Usage Guidelines

When the cable modem is operating in DOCSIS 1.0 or DOCSIS 1.0+ mode, this command displays the four possible stream queues, the Service ID (SID) associated with each queue (if the queue is currently in use), and whether the SID is the primary SID, a secondary (static) SID, or a dynamic (on demand) SID. The display also shows the packets and bytes that have been transmitted and received on each stream.

When the cable modem is operating in DOCSIS 1.1 mode, this command also displays the modem's capabilities and packet classifiers.

Examples

The following example shows typical output for a DOCSIS 1.0 or DOCSIS 1.0+ cable modem for the QoS statistics for each of the router's four queues:

```
Router# show controllers cable-modem 0 qos

Queue   SID     SID     SFID    TX      TX              RX      RX
                Type            Pkts    Bytes           Pkts    Bytes

0       2       Primary 0       11377   2721985         12320   983969
1       52      Dynamic 52      116     13608           105     14300
2       0       NA      0       0       0               0       0
3       0       NA      0       0       0               0       0

Router#
```

In Cisco IOS 12.2(15)CZ and later releases, the output for a DOCSIS 1.0 or DOCSIS 1.0+ cable modem also includes the service flow types for each queue:

```
Router# show controllers cable-modem 0 qos

Queue   SID     SID     SFID    TX      TX              RX      RX
                Type            Pkts    Bytes           Pkts    Bytes

0       2       Primary 0       11377   2721985         12320   983969
1       52      Dynamic 52      116     13608           105     14300
2       0       NA      0       0       0               0       0
3       0       NA      0       0       0               0       0


Queue    SF Type
0        BE
1        BE
2        NA
3        NA

Router#
```

Table 11 describes the significant fields shown in the display for a DOCSIS 1.0 or DOCSIS 1.0+ cable modem.

Table 11 show controllers cable-modem qos Field Descriptions

Field	Description
Queue	One of the four possible service flow queues that exist in the router.
SID	Service identifier, a 14-bit integer assigned by the CMTS to each active upstream service flow.
SID Type	Type of SID: • Primary—The service flow used for best-effort data traffic and MAC maintenance messages. • Secondary—Secondary static service flows that are created at power-on provisioning for voice calls when dynamic SIDs are not active. • Dynamic—Secondary service flows that are created for on-demand voice calls when using dynamic SIDs.
SFID	Service flow identifier, a 32-bit integer assigned by the CMTS to each service flow on the router.
TX Pkts	Number of packets the router has transmitted on this service flow.
TX Bytes	Number of bytes the router has transmitted on this service flow.
RX Pkts	Number of packets the router has received on this service flow.
RX Bytes	Number of bytes the router has received on this service flow.
Queue/SF Type	Identifies the type of service flow being used for each queue.

In Cisco IOS Release 12.2(15)CZ and later releases, the QoS statistics include information about the DOCSIS 1.1 operations, including the type of service flow and packet classifiers being used for each queue. The following is a typical default display:

```
Router# show controllers cable-modem 0 qos
```

```
Queue   SID     SF      SF      SFID    TX      TX      RX      RX
                Type    Name            Pkts    Bytes   Pkts    Bytes

0       565     Primary  BE     675     200     34606   518     120321
1       1443    Dynamic  UGS    1911    0       0       0       0
2       1444    Dynamic  UGS_AD 1912    0       0       0       0
3       1445    Dynamic  RTP    1913    0       0       0       0

Queue   Concat  Capabilities
        packets cbr cc fr nbr

0       2       F  T  T  F

1       0       T  T  T  T

2       0       T  T  T  T

3       0       F  T  T  T

Router#
```

The following shows a typical display with the **details** option:

```
Router# show controllers cable-modem 0 qos details

Queue   SID     SF      SF      SFID    TX      TX      RX      RX
                Type    Name            Pkts    Bytes   Pkts    Bytes

0       565     Primary  BE     675     200     34606   529     123351
1       1443    Dynamic  UGS    1911    0       0       0       0
2       1444    Dynamic  UGS_AD 1912    0       0       0       0
3       1445    Dynamic  RTP    1913    0       0       0       0

Queue   Concat  Capabilities
        packets cbr cc fr nbr

0       2       F  T  T  F

1       0       T  T  T  T

2       0       T  T  T  T

3       0       F  T  T  T

Packet Classifiers

Class id   SFID   Pri     valid    Match     SIDT
   1       1913    0        14       0      811EDDE8
   2       1912    0        14       0      811EDBB8
   3       1911    0        14       0      811ED988
   4       675     0        14       0      811ED758
PHS: Inactive
PHS: Active   Index: 1  Size: 34  Suppressed Size: 13
SFID: 1912   Classifier Id: 2
     Verify: TRUE  Packets: 0  Bytes Suppressed: 0
PHS: Active   Index: 1  Size: 34  Suppressed Size: 13
SFID: 1911   Classifier Id: 3
     Verify: TRUE  Packets: 0  Bytes Suppressed: 0
PHS: Active   Index: 1  Size: 34  Suppressed Size: 13
SFID: 675   Classifier Id: 4
     Verify: TRUE  Packets: 0  Bytes Suppressed: 0

Downstream Payload Header Suppression
```

```
PHS: Active   Index: 1  Size: 34  Suppressed Size: 14 (index = 1)
SFID: 676   Classifier Id: 8
     Verify: TRUE  Packets: 0  Bytes Suppressed: 0
PHS: Active   Index: 2  Size: 34  Suppressed Size: 14 (index = 2)
SFID: 1914   Classifier Id: 7
     Verify: TRUE  Packets: 0  Bytes Suppressed: 0
PHS: Active   Index: 3  Size: 34  Suppressed Size: 14 (index = 3)
SFID: 1915   Classifier Id: 6
     Verify: TRUE  Packets: 0  Bytes Suppressed: 0

Router#
```

Table 12 describes the fields shown in the display for a DOCSIS 1.1 cable modem:

Table 12 show controllers cable-modem qos Field Descriptions (DOCSIS 1.1)

Field	Description
Queue	One of the four possible service flow queues that exist in the router.
SID	Service Identifier, a 14-bit integer assigned by the CMTS to each active upstream service flow.
SID Type	The type of SID: • Primary—The service flow used for best-effort data traffic and MAC maintenance messages. • Secondary—Secondary static service flows that are created at power-on provisioning for voice calls when dynamic SIDs are not active. • Dynamic—Secondary service flows that are created for on-demand voice calls when using dynamic SIDs.
SFID	Service Flow Identifier, a 32-bit integer assigned by the CMTS to each service flow on the router.
TX Pkts	Number of packets the router has transmitted on this service flow.
TX Bytes	Number of bytes the router has transmitted on this service flow.
RX Pkts	Number of packets the router has received on this service flow.
RX Bytes	Number of bytes the router has received on this service flow.
Capabilities	These four fields describe whether the following features are enabled.
cbr	Whether committed bit rate traffic (CBR) is supported (T) or not (F). This could indicate either UGS or UGS-AD service flows.
cc	Whether concatenation is supported (T) or not (F).
fr	Indicates whether DOCSIS fragmentation is supported (T) or not (F).
nbr	Not Broadcast status, depending on whether the classifier supports broadcasts (F) or not (T).
Queue/SF Type	Identifies the type of service flow being used for each queue.
Packet Classifiers	Describes the classifiers defined on the router.
Class id	ID used to uniquely identify the classifier in each service flow.
SFID	ID that uniquely identifies the service flow.
Pri	Traffic Priority parameter that was assigned to this classifier. If no value was set, the priority defaults to 0 (lowest priority).

Table 12 show controllers cable-modem qos Field Descriptions (DOCSIS 1.1) (continued)

Field	Description
valid	13-bit bitmask showing which Type/Length/Value (TLV) fields were set on the classifier. The following shows the meaning of each bit, with the least significant bit on the far right. The bit is set to 1 if the corresponding TLV was set for the classifier: • 0x0001—IP Type of Service Range and Mask • 0x0002—IP Protocol • 0x0004—IP Source Address • 0x0008—IP Source Mask • 0x0010—IP Destination Address • 0x0020—IP Destination Mask • 0x0040—TCP/UDP Source Port Start and TCP/UDP Source Port End • 0x0080—TCP/UDP Destination Port Start and TCP/UDP Destination Port End • 0x0100—Destination MAC Address • 0x0200—Source MAC Address • 0x0400—Ethertype/DSAP/MacType • 0x0800—IEEE 802.1P User_Priority • 0x1000—IEEE 802.1Q VLAN_ID For example, a value of D6 translates to the bit-mask “1101 0110”, which indicates that the following fields were set for the classifier: IP Protocol, IP Source Address, IP Destination Address, and the TCP/UDP Source and Destination Port values.
Match	Number of packets matching the classifier.
SIDT	Address for the classifier in the internal SID table (SIDT).
Packet Classifier Details	Detailed description of each packet classifier.
Classifier ID	ID used to uniquely identify the classifier in each service flow.
SFID	ID that uniquely identifies the service flow.
IP source	Matching IP source address.
IP dest	Matching IP destination address.
UDP/TCP source range	Low-end and high-end matching source TCP/UDP port values.
UDP/TCP dest range	Low-end and high-end matching destination TCP/UDP port values.
IP Protocol	Matching IP protocol type, as given in RFC 1700. A value of 256 matches any IP protocol, and a value of 257 matches TCP and UDP traffic.
PHS	Whether payload header suppression (PHS) is active or inactive.
Downstream Payload Header Suppression	Whether PHS is being used on the downstream.

Tip In Cisco IOS Release 12.2(8)T and later releases, you can add a time stamp to **show** commands using the **exec prompt timestamp** command in line configuration mode.

Related Commands

Command	Description
show controllers cable-modem mac	Displays detailed MAC-layer information for the router's cable interface.

show controllers cable-modem service-flows

To display the service flows that are configured on the router, use the **show controllers cable-modem service-flows** command in privileged EXEC mode.

Cisco uBR905, uBR925 cable access routers, Cisco CVA122 Cable Voice Adapter

show controllers cable-modem *number* **service-flows** [*sfid* | **summary**]

Syntax Description

number	Identifies the cable interface (always **0**).
sfid	(Optional) Displays detailed information for a specific service flow, as identified by its service flow ID (SFID). The valid range for *sfid* is 1 to 2147483647.
summary	(Optional) Displays a summary report of all service flows.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)CZ	This command was introduced for the Cisco uBR905 and Cisco uBR924 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

Usage Guidelines

This command displays the Quality of Service (QoS) parameters that make up each of the service flows that are defined on the router for the upstream and downstream. The information shown corresponds to the QoS parameters that are listed in Appendix C of the DOCSIS 1.1 specification.

Examples

The following example shows typical output for the default form of the **show controllers cable-modem service-flows** command.

```
Router# show controllers cable-modem 0 service-flows

Upstream Flow Scheduler Parameters
Flow Type: Primary
  Flow Reference:                 1
  Service Flow ID:                3
  Service ID:                     2
  QoS Set Type:                   7
  QoS Traffic Priority:           0
  QoS Max Sustained Traffic Rate: 0
  QoS Max Traffic Burst:          1522
  QoS Min Reserved Traffic Rate:  0
  QoS Min Reserved Rate Pkt Size: 0
  QoS Timeout For Active Param:   0
  Qos Timeout For Admitted Param: 200
  Max Concatenated Burst:         0
  Scheduling Type:                0x2
  Request/Transmission Policy:    0x0
  Nominal Polling Interval:       0
  Tolerated Poll Jitter:          0
```

```
  Unsolicited Grant Size:         0
  Nominal Grant Interval:         0
  Tolerated Grant Jitter:         0
  Grants Per Interval:            0
  IP TOS Overwrite:               0xFF 0x0

Downstream Flow Scheduler Parameters
Flow Type: Primary
  Flow Reference:                 5
  Service Flow ID:                4
  Service ID:                     0
  QoS Set Type:                   7
  QoS Traffic Priority:           0
  QoS Max Sustained Traffic Rate: 0
  QoS Max Traffic Burst:          1522
  QoS Min Reserved Traffic Rate:  64000
  QoS Min Reserved Rate Pkt Size: 0
  QoS Timeout For Active Param:   0
  Qos Timeout For Admitted Param: 200
  Max DS Latency:                 0

Downstream Flow Scheduler Parameters
Flow Type: Static
  Flow Reference:                 6
  Service Flow ID:                5
  Service ID:                     0
  QoS Set Type:                   7
  QoS Max Sustained Traffic Rate: 10000
  QoS Max Traffic Burst:          1522
  QoS Min Reserved Traffic Rate:  8000
  QoS Min Reserved Rate Pkt Size: 0
  QoS Timeout For Active Param:   0
  Qos Timeout For Admitted Param: 200
  Max DS Latency:                 0

Downstream Flow Scheduler Parameters
Flow Type: Static
  Flow Reference:                 8
  Service Flow ID:                7
  Service ID:                     0
  QoS Set Type:                   7
  QoS Traffic Priority:           0
  QoS Max Sustained Traffic Rate: 30000
  QoS Max Traffic Burst:          1522
  QoS Min Reserved Traffic Rate:  28000
  QoS Min Reserved Rate Pkt Size: 0
  QoS Timeout For Active Param:   0
  Qos Timeout For Admitted Param: 200
  Max DS Latency:                 0

Router#
```

The following example shows typical output for the **summary** option of the **show controllers cable-modem service-flows** command.

```
Router# show controllers cable-modem 0 service-flows summary

Sfid   Sid   Sf        Sf    Service             Direction
             type      Ref   Class name
13     6     Primary   2     -                   upstream
14     N/A   Primary   1     -                   downstream

Router#
```

The following example shows typical output for the **show controllers cable-modem service-flows** command, when displaying information for individual service flows:

```
Router# show controllers cable-modem 0 service-flows 3

Upstream Flow Scheduler Parameters
Flow Type: Primary
  Flow Reference:                1
  Service Flow ID:               3
  Service ID:                    2
  QoS Set Type:                  7
  QoS Traffic Priority:          0
  QoS Max Sustained Traffic Rate: 0
  QoS Max Traffic Burst:         1522
  QoS Min Reserved Traffic Rate:  0
  QoS Min Reserved Rate Pkt Size: 0
  QoS Timeout For Active Param:   0
  Qos Timeout For Admitted Param: 200
  Max Concatenated Burst:        0
  Scheduling Type:               0x2
  Request/Transmission Policy:   0x0
  Nominal Polling Interval:      0
  Tolerated Poll Jitter:         0
  Unsolicited Grant Size:        0
  Nominal Grant Interval:        0
  Tolerated Grant Jitter:        0
  Grants Per Interval:           0
  IP TOS Overwrite:              0xFF 0x0

Router# show controllers cable-modem 0 service-flows 4

Downstream Flow Scheduler Parameters
Flow Type: Primary
  Flow Reference:                5
  Service Flow ID:               4
  Service ID:                    0
  QoS Set Type:                  7
  QoS Traffic Priority:          0
  QoS Max Sustained Traffic Rate: 0
  QoS Max Traffic Burst:         1522
  QoS Min Reserved Traffic Rate:  64000
  QoS Min Reserved Rate Pkt Size: 0
  QoS Timeout For Active Param:   0
  Qos Timeout For Admitted Param: 200
  Max DS Latency:                0

Router#
```

Table 13 describes the significant fields shown by this command. The information shown corresponds to the QoS parameters that are listed in Appendix C of the DOCSIS 1.1 specification.

Table 13 show controllers cable-modem service-flows Field Descriptions

Field	Description
Flow Type, Sf type	Identifies whether the type of service-flow: • Primary—The primary service-flow for the upstream or downstream. • Static—A permanent secondary service-flow. • Dynamic—A dynamically created secondary service-flow.
Flow Reference, Sf Ref	The service flow reference ID that is used to establish the Service Flow ID.

Table 13 show controllers cable-modem service-flows Field Descriptions

Field	Description
Service Flow ID, Sfid	The ID that unique identifies this service flow on the upstream or downstream.
Service ID, Sid	The service identifier (SID) that the CMTS assigns to the service flow.
QoS Set Type	The QoS parameter set type for the service flow. This is a three-bit value, where bit 0 is set for the Provisioned Set, bit 1 is set for the Admitted Set, and bit 2 is set for the Active Set. Multiple bits can be set to produce the following possible values: • 0 = Set Active and Admitted Sets to null. • 1 = Apply to Provisioned Set only. • 2 = Perform admission control and apply to Admitted Set only. • 3 = Perform admission control and apply to Provisioned and Admitted Sets. • 4 = Check against Admitted set in separate Service Flow encoding, perform admission control if needed, activate this service flow, and apply to Active Set. • 5 = Perform admission control, apply to Provisioned and Active Sets, and activate this service flow. • 6 = Perform admission control, activate this service flow, and apply to Admitted and Active Sets. • 7 = Perform admission control, activate this service flow, and apply to Provisioned, Admitted, and Active Sets.
QoS Traffic Priority	The priority assigned to the service flow (0 to 7, where 7 is the highest priority).
QoS Max Sustained Traffic Rate	The maximum traffic rate, in bits, for a token-bucket rate limit for packets.
QoS Max Traffic Burst	The maximum size of a single packet on this service flow.
QoS Min Reserved Traffic Rate	The minimum rate, in bits per second, for traffic on this service flow.
QoS Min Reserved Rate Pkt Size	The minimum packet size, in bytes, for which the minimum rate can be sustained on this service flow.
QoS Timeout For Active Param	The maximum time, in seconds, that resources on a service flow can remain unused before the CMTS sets the flow's Admitted and Active Sets to null. A value of 0 indicates no timeout period.
Qos Timeout For Admitted Param	The maximum time, in seconds, that Admitted resources on a service flow can remain without being activated. After this timeout period, the CMTS will release Admitted resources on a service flow and retain only the activated ones.
Max Concatenated Burst	The maximum burst size, in bytes, for concatenated traffic on the service flow. A value of 0 indicates no limit.

Table 13 show controllers cable-modem service-flows Field Descriptions

Field	Description
Scheduling Type	The type of service used on the upstream for grant requests: • 1 = Undefined • 2 = Best effort • 3 = Non-real-time polling service (NRTPS) • 4 = Real-time polling service (RTPS) • 5 = Unsolicited grant service with activity detection (UGS-AD) • 6 = Unsolicited grant service (UGS)
Request/Transmission Policy	The allowable means of grant request and transmission on the upstream. This value is a 9-bit mask where the bits have the following meanings when set to 1: • Bit 0 = Do not use broadcast request opportunities. • Bit 1 = Do not use priority request multicast request opportunities. • Bit 2 = Do not use Request/Data grants for requests. • Bit 3 = Do not use Request/Data grants for data. • Bit 4 = Do not piggyback data on grant requests. • Bit 5 = Do not use concatenation. • Bit 6 = Do not use DOCSIS fragmentation. • Bit 7 = Do not use payload header suppression (PHS). • Bit 8 = UGS service flows must drop packets that do not fit. See Table 14 for the possible values of each bit for each of the supported flow types.
Nominal Polling Interval	The interval, in microseconds, between successive unicast grant requests for the service flow on the upstream.
Tolerated Poll Jitter	The maximum amount of time, in microseconds, that a unicast request interval may be delayed from the typical polling schedule.
Unsolicited Grant Size	The size of unsolicited grants, in bytes.
Nominal Grant Interval	The interval, in microseconds, between successive data grant opportunities for the service flow on the upstream.
Tolerated Grant Jitter	The maximum amount of time, in microseconds, that transmission opportunities may be delayed from the typical polling schedule.
Grants Per Interval	The actual number of grants per Nominal Grant Interval for UGS service flows, and the maximum number of active grants per Nominal Grant Interval for UGS-AD service flows.
Max DS Latency	The maximum latency, in microseconds, between the reception of a packet by the CMTS on its network interface and the transmission of the packet on its downstream cable interface.

Table 14 Request/Transmission Policy Values

	Drop if Not Fit In UGS Size	Do Not Use...							
		PHS	Frag	Concat	Piggyback Requests	Req/Data for Data	Req/Data for Requests	Priority Multicast Requests	Broadcast Requests
	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Best-Effort	X	X	X	X	X	X	X	X	X
Non-Real Time Polling	X	X	X	X	X	X	X	0 or 1	0 or 1
Real-Time Polling	X	X	X	X	0 or 1	0 or 1	0 or 1	0 or 1	0 or 1
Unsolicited Grant Service	X	X	X	X	1	1	1	1	1
Unsolicited Grant Service with Activity Detection	X	X	X	X	1	1	1	1	1

Tip In Cisco IOS Release 12.2(8)T and later releases, you can add a timestamp to **show** commands using the **exec prompt timestamp** command in line configuration mode.

Related Commands

Command	Description
show controllers cable-modem	Displays high-level controller information about the cable interface.
show controllers cable-modem bpkm	Displays information about the baseline privacy key management exchange between the cable interface and the CMTS.
show controllers cable-modem des	Displays information about the Data Encryption Standard (DES) engine registers.
show controllers cable-modem filters	.Displays the registers in the MAC hardware that are used for filtering received frames.
show controllers cable-modem mac	Displays detailed MAC-layer information for the cable interface.
show controllers cable-modem phy	Displays the contents of the registers used in the downstream physical hardware of the cable interface.
show controllers cable-modem tuner	Displays the settings for the upstream and downstream tuners used by the cable interface.

snmp-server enable traps docsis-cm

To enable one or more Simple Network Management Protocol (SNMP) traps for DOCSIS 1.1 events, use the **snmp-server enable traps docsis-cm** command in global configuration mode. To disable the SNMP traps, use the **no** form of this command.

Cisco uBR905 and Cisco uBR925 Cable Access Routers, and Cisco CVA122 Cable Voice Adapter

snmp-server enable traps docsis-cm [**bpi** | **bpkm** | **dccack** | **dccreq** | **dccrsp** | **dhcp** | **dsack** | **dsreq** | **dsrsp** | **dynsa** | **swupcvc** | **swupfail** | **swupinit** | **swupsucc** | **tlv**]

no snmp-server enable traps docsis-cm [**bpi** | **bpkm** | **dccack** | **dccreq** | **dccrsp** | **dhcp** | **dsack** | **dsreq** | **dsrsp** | **dynsa** | **swupcvc** | **swupfail** | **swupinit** | **swupsucc** | **tlv**]

Syntax Description

bpi	(Optional) Baseline Privacy Interface (BPI) initialization failure traps.
bpkm	(Optional) Baseline Privacy Key Management (BPKM) initialization failure traps.
dccack	(Optional) Dynamic channel change acknowledgement failure traps.
dccreq	(Optional) Dynamic channel change request failure traps.
dccrsp	(Optional) Dynamic channel change response failure traps.
dhcp	(Optional) DHCP failure traps.
dsack	(Optional) Dynamic service acknowledgement failure traps.
dsreq	(Optional) Dynamic service request failure traps.
dsrsp	(Optional) Dynamic service response failure traps.
dynsa	(Optional) Dynamic SA failure traps.
swupcvc	(Optional) Secure software upgrade code verification certificate (CVC) failure traps.
swupfail	(Optional) Secure software upgrade failure traps.
swupinit	(Optional) Enables secure software upgrade initialization failure traps.
swupsucc	(Optional) Secure software upgrade success traps.
tlv	(Optional) Unknown Type/Length/Value (TLV) traps.

Defaults

No traps are enabled. If no options are specified, all DOCSIS-related traps are enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)CZ	This command was introduced on the Cisco uBR905 and Cisco uBR925 cable access routers, and the Cisco CVA122 Cable Voice Adapter.

Usage Guidelines

This command enables the sending of SNMP traps when DOCSIS-related events occur. Multiple traps can be enabled at the same time.

Note The traps are described in the DOCS-CABLE-DEVICE-TRAP-MIB MIB, which is is an extension of the CABLE DEVICE MIB that is defined in RFC 2669.

Examples

The following example shows the BPI+ and secure software download traps being enabled:

```
Router# config terminal
Router(config)# snmp-server enable traps docsis-cm bpi bpkm swupcvc swupfail swupinit
swupsucc
Router(config)#
```

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.
snmp-server manager	Starts the SNMP manager process.