DOCSIS 1.1 for the Cisco CMTS Routers

This document describes how to configure the Cisco CMTS router for Data-over-Cable Service Interface Specifications (DOCSIS) 1.1 operations.

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Contents

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 1
- Prerequisites for DOCSIS 1.1 Operations, on page 3
- Restrictions for DOCSIS 1.1 Operations, on page 3
- Information about DOCSIS 1.1, on page 5
- How to Configure the Cisco CMTS for DOCSIS 1.1 Operations, on page 18
- Monitoring DOCSIS Operations, on page 30
- Configuration Examples for DOCSIS 1.1 Operations, on page 36
- Additional References, on page 40
- Feature Information for DOCSIS 1.1 for Cisco CMTS Routers, on page 40

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Note Do not use DPICs (8X10G and 2x100G) to forward IP traffic, as it may cause buffer exhaustion, leading to line card reload.

The only allowed traffic on a DPIC interface is DEPI, UEPI, and GCP traffic from the Cisco cBR-8 router to Remote PHY devices. Other traffic such as DHCP, SSH, and UTSC should flow via another router, since DPICs cannot be used for normal routing.

Prerequisites for DOCSIS 1.1 Operations

To support DOCSIS 1.1 operations, the cable modem must also support the DOCSIS 1.1 feature set. In addition, before you power on and configure the Cisco CMTS, check the following points:

- Ensure that your network supports reliable broadband data transmission. Your plant must be swept, balanced, and certified, based on NTSC or appropriate international cable plant recommendations. Ensure that your plant meets all DOCSIS downstream and upstream RF requirements.
- Ensure that your Cisco CMTS is installed according to the instructions provided in the appropriate Hardware Installation Guide. The chassis must contain at least one port adapter to provide backbone connectivity and one Cisco cable line card to serve as the RF cable TV interface.
- 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 virtual private networks (VPNs); and dialup access servers, telephone circuits and connections and other equipment if supporting telco return.
- Ensure that DHCP and DOCSIS 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 configuration files. Optionally, ensure that your servers can also download updated software images to DOCSIS 1.0 and DOCSIS 1.1 cable modems.
- 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.
- Ensure that the system clocks on the Cisco 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 Cisco CMTS, which could interfere with BPI+ operations. In particular, this could prevent the proper verification of the digital certificates on the cable modem (CM).

After these prerequisites are met, you are ready to configure the Cisco CMTS. This includes, at a minimum, configuring a host name and password for the Cisco CMTS and configuring the Cisco CMTS to support IP over the cable plant and network backbone.

Caution If you plan to use service-class-based provisioning, the service classes must be configured at the Cisco CMTS before cable modems attempt to make a connection. Use the **cable service class** command to configure service classes.

Restrictions for DOCSIS 1.1 Operations

DOCSIS 1.1 operations includes the following restrictions:

Baseline Privacy Interface Plus Requirements

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

Also, 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.

Note 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.

BPI+-Encrypted Multicast Not Supported with Bundled Subinterfaces on the Cisco cBR-8 Router

The current Cisco IOS-XE releases do not support using BPI+ encrypted multicast on bundled cable subinterfaces on the Cisco cBR-8 router. Encrypted multicast is supported on bundled cable interfaces or on non-bundled cable subinterfaces, but not when a subinterface is bundled on the Cisco cBR-8 router.

BPI+ Not Supported with High Availability Configurations

The current Cisco IOS-XE releases do not support using BPI+ encrypted multicast on a cable interface when the interface has also been configured for N+1 (1:n) High Availability or Remote Processor Redundancy Plus (RPR+) High Availability redundancy.

In addition, BPI+ is not automatically supported after a switchover from the Working cable interface to the Protect cable interface, because the cable interface configurations that are required for BPI+ encryption are not automatically synchronized between the two interfaces. A workaround for this is to manually configure the Protect cable interfaces with the required configurations.

DOCSIS Root Certificates

The Cisco CMTS supports only one DOCSIS Root CA certificate.

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.

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.

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 must handle the existing registration Type/Length/Value parameters 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 the 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 1.0 cable modem registers with a DOCSIS 1.1 CMTS, the registration request explicitly requests all nondefault service-class parameters in the registration. The absence of an indirect service class reference eliminates the need for the DOCSIS 1.1 TLVs and eliminates the need to establish a local registration acknowledge wait state.

When a DOCSIS 1.1 CMTS receives a registration request from a DOCSIS 1.0 cable modem, it responds with the DOCSIS 1.0 style registration response and does not expect the cable modem to send the registration-acknowledge MAC message.

Information about DOCSIS 1.1

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.

The DOCSIS 1.1 specification provides the following feature enhancements over DOCSIS 1.0 networks:

Baseline Privacy Interface Plus

DOCSIS 1.0 introduced 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. DOCSIS 1.1 enhances these security features with BPI Plus (BPI+), which includes the following enhancements:

- X.509 Digital certificates provide secure user identification and authentication. The Cisco CMTS supports both self-signed manufacturer's certificates and certificates that are chained to the DOCSIS Root CA certificate.
- Key encryption uses 168-bit Triple DES (3DES) encryption that is suitable for the most sensitive applications.
- 1024-bit public key with Pkcs#1 Version 2.0 encryption.
- Support for encrypted multicast broadcasts, so that only authorized service flows receive a particular multicast broadcast.
- Secure software download allows a service provider to upgrade a cable modem's software remotely, without the risk of interception, interference, or alteration.

Concatenation

Concatenation allows a cable modem to make a single time-slice request for multiple upstream packets, sending all of the packets in a single large burst on the upstream. Concatenation can send multiple upstream packets as part of one larger MAC data frame, allowing the cable modem to make only one time-slot request for the entire concatenated MAC frame, reducing the delay in transmitting the packets on the upstream channel. This avoids wasting upstream bandwidth when sending a number of very small packets, such as TCP acknowledgement packets.

Dynamic MAC Messages

Dynamic Service MAC messages allow the cable modem to dynamically create service flows on demand. These messages are DOCSIS link layer equivalents of the higher layer messages that create, tear down, and modify a service flow.

The DOCSIS 1.1 dynamic services state machine supports the following messages:

- Dynamic Service Add (DSA)—This message is used to create a new service flow.
- Dynamic Service Change (DSC)—This message is used to change the attributes of an existing service flow.
- Dynamic Service Deletion (DSD)—This message is used to delete an existing service flow.

Note These messages are collectively known as DSX messages.

Enhanced Quality of Service

DOCSIS 1.1 provides enhanced quality of service (QoS) capabilities 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 and service class 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.
- Upstream service flows can be assigned one of the following QoS scheduling types, depending on the type of traffic and application being used:
  - Best-effort—Data traffic sent on a non-guaranteed best-effort basis. This type of service flow is similar to the method used in DOCSIS 1.0 networks.
  - Real-time polling (rtPS)—Real-time service flows, such as video, that produce unicast, variable size packets at fixed intervals.
  - Non-real-time polling service (nrtPS)—Similar to the rtPS type, in that the cable modem is guaranteed regular opportunities to request data bursts of varying length, except that the CMTS can vary the time between its polling of the cable modem depending on the amount of traffic and congestion on the network.
  - Unsolicited grants (UGS)—Constant bit rate (CBR) or committed information rate (CIR) traffic, such as voice, that is characterized by fixed-size packets at fixed intervals, providing a guaranteed minimum data rate.
  - 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.

Fragmentation

DOCSIS fragmentation allows the upstream MAC scheduler to slice large data requests to fit into the scheduling gaps between UGS (voice slots). This prevents large data packets from affecting real-time traffic, such as voice and video.

Fragmentation reduces the run-time jitter experienced by the UGS slots when large data grants preempt the UGS slots. Disabling fragmentation increases the run-time jitter, but also reduces the fragmentation reassembly overhead for fragmented MAC frames.

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.

Interoperability

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

Payload Header Suppression

Payload header suppression (PHS) conserves link-layer bandwidth by suppressing repetitive or redundant packet headers on both upstream and downstream service flows. PHS is enabled or disabled per service flow, and each service flow can support a separate set of PHS rules that determine which parts of the header are suppressed. This ensures that PHS is done in the most efficient manner for each service flow and its particular type of application.

Downstream ToS Overwrite

Downstream ToS Overwrite is supported in DOCSIS 1.1. It can be used in IPv4 and IPv6 environment. You can use CLI command **cable service class** *class-index* **tos-overwrite** *and-mask or-mask* or the cable modem configuration file to configure downstream ToS overwrite.

To display the ToS value, use the **show cable modem qos verbose** command as shown in the following example:

```
Router# show cable modem 30.140.0.41 qos verbose
Load for five secs: 5%/0%; one minute: 4%; five minutes: 4%
Time source is NTP, 15:22:46.911 CST Wed Apr 25 2018

Sfid: 29
Current State: Active
Sid: 8
Service Class Name:
Traffic Priority: 0
Maximum Sustained rate: 0 bits/sec
Maximum Burst: 3044 bytes
Minimum Reserved rate: 0 bits/sec
Minimum Packet Size: 0 bytes
Admitted QoS Timeout: 200 seconds
Active QoS Timeout: 0 seconds
Maximum Concatenated Burst: 1522 bytes
Scheduling Type: Best Effort
Request/Transmission policy: 0x0
IP ToS Overwrite[AND-mask, OR-mask]: 0xFF, 0x0
Peak Rate: 0 bits/sec
Current Throughput: 545 bits/sec, 0 packets/sec

Sfid: 30
Current State: Active
Sid: N/A
Low Latency App: No
Service Class Name:
Traffic Priority: 0
Maximum Sustained rate: 0 bits/sec
Maximum Burst: 3044 bytes
Minimum Reserved rate: 0 bits/sec
Minimum Packet Size: 0 bytes
Admitted QoS Timeout: 200 seconds
Active QoS Timeout: 0 seconds
Maximum Latency: 0 usecs
IP ToS Overwrite[AND-mask, OR-mask]: 0xFF, 0x0
```

```
Peak Rate: 0 bits/sec
Current Throughput: 446 bits/sec, 0 packets/sec
```

DOCSIS 1.1 Quality of Service

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

- Service flow—A unidirectional sequence of packets on the DOCSIS link. Separate service flows are used for upstream and downstream traffic, and define the QoS parameters for that traffic.
- 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 associated with that service class.
- Packet classifier—A set of packet header fields used to classify packets onto a service flow to which the classifier belongs. The CMTS uses the packet classifiers to match the packet to the appropriate service flow.
- Payload header suppression (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. PHS increases the bandwidth efficiency by removing repeated packet headers before transmission.

See the following sections for more information on these components.

Service Flow

In DOCSIS 1.1, the basic unit of QoS is the service flow, which is a unidirectional sequence of packets transported across the RF interface between the cable modem and CMTS. A service flow defines a set of QoS parameters such as latency, jitter, and throughput assurances, and these parameters can be applied independently to the upstream and downstream traffic flows. This is a major difference from DOCSIS 1.0 networks, where the same QoS parameters were applied to both the downstream and upstream flows.

Note DOCSIS 1.0 networks used service IDs (SIDs) to identify the QoS parameter set for a particular flow. DOCSIS 1.1 networks use the service flow ID (SFID) to identify the service flows that have been assigned to a particular upstream or downstream. DOCSIS 1.1 networks still use the term SID, but it applies exclusively to upstream service flows.

Every cable modem establishes primary service flows for the upstream and downstream directions, with a separate SFID for the upstream and the downstream flows. The primary flows maintain connectivity between the cable modem and CMTS, allowing the CMTS to send MAC management messages at all times to the cable modem.

In addition, a DOCSIS 1.1 cable modem can establish multiple secondary service flows. The secondary service flows either can be permanently created (by configuring them in the DOCSIS configuration file that is downloaded to the cable modem), or the service flows can be created dynamically to meet the needs of the on-demand traffic, such as voice calls. Permanent service flows remain in effect, even if they are not being used, while dynamic service flows are deleted when they are no longer needed.

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 network. Every service flow is identified by an SFID, while upstream service 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.

Service Class

Each service flow is associated with a service class, which defines a particular class of service and its QoS characteristics, such as the maximum bandwidth for the service flow and the priority of its traffic. The service class attributes can be inherited from a preconfigured CMTS local service class (class-based flows), or they can be individually specified when a cable modem dynamically requests a service flow and the CMTS creates it.

The DOCSIS 1.1 service class also defines the MAC-layer scheduling type for the service flow. The schedule type defines the type of data burst requests that the cable modem can make, and how often it can make those requests. The following types of schedule types are supported:

- Best-effort (BE)—A cable modem competes with the other cable modems in making bandwidth requests and must wait for the CMTS to grant those requests before transmitting data. This type of service flow is similar to the method used in DOCSIS 1.0 networks.
- Real-time polling service (rtPS)—A cable modem is given a periodic time slot in which it can make bandwidth requests without competing with other cable modems. This allows real-time transmissions with data bursts of varying length.
- Non-real-time polling service (nrtPS)—A cable modem is given regular opportunities to make bandwidth requests for data bursts of varying size. This type of flow is similar to the rtPS type, in that the cable modem is guaranteed regular opportunities to request data bursts of varying length, except that the CMTS can vary the time between its polling of the cable modem, depending on the amount of traffic and congestion on the network.
- Unsolicited grant service (UGS)—A cable modem can transmit fixed data bursts at a guaranteed minimum data rate and with a guaranteed maximum level of jitter. This type of service flow is suitable for traffic that requires a Committed Information Rate (CIR), such as Voice-over-IP (VoIP) calls.
- Unsolicited grant service with activity detection (UGS-AD)—Similar to the UGS type, except that the CMTS monitors the traffic to detect when the cable modem is not using the service flow (such as voice calls when nobody is speaking). When the CMTS detects silence on the service flow, the CMTS temporarily switches the service flow to an rtPS type. When the cable modem begins using the flow again, the CMTS switches the flow back to the UGS type. This allows the CMTS to more efficiently support VoIP calls.

Each service flow is assigned a single service class, but the same service class can be assigned to multiple service flows. Also, a cable modem can be assigned multiple service flows, allowing it to have multiple traffic flows that use different service classes.

Packet Classifiers

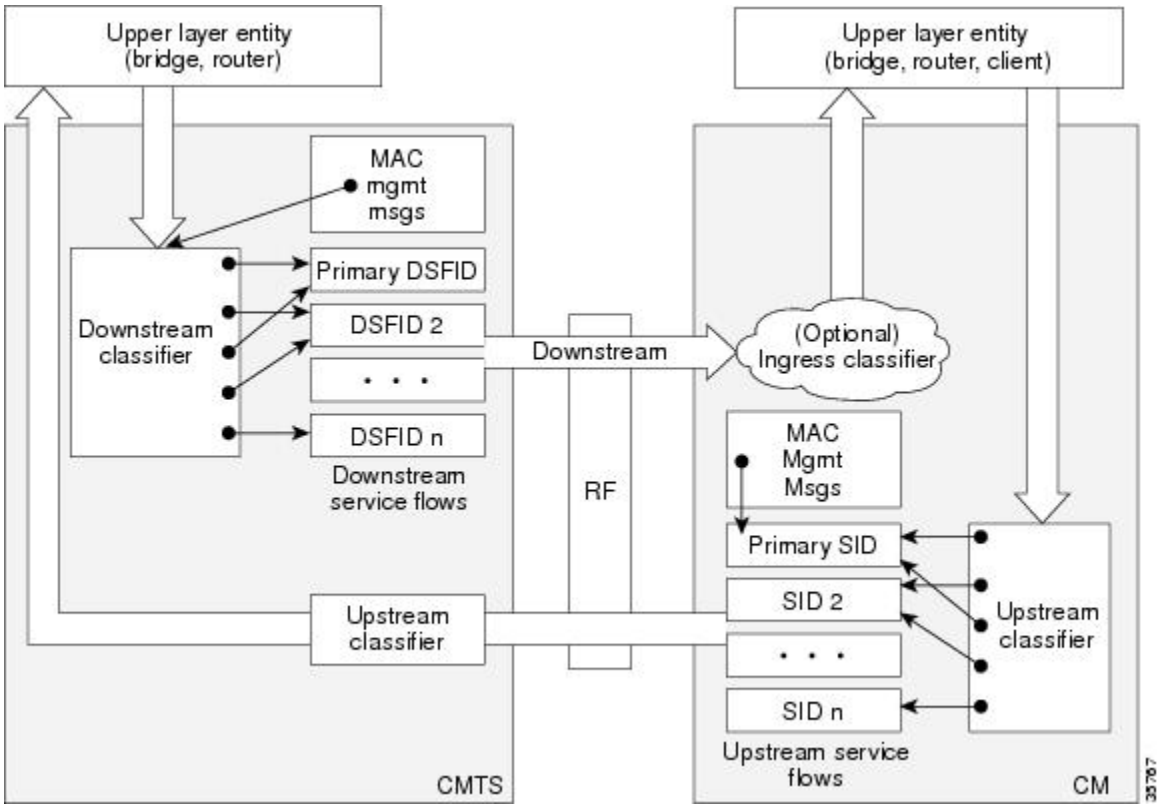
In DOCSIS 1.0 networks, a cable modem used only one set of QoS parameters for all of its traffic, so the CMTS simply had to route packets to and from the appropriate cable modems. In DOCSIS 1.1 networks, however, cable modems can be using multiple service flows, and each service flow can be given a different level of service. To quickly assign upstream and downstream packets to their proper service flows, the CMTS uses the concept of packet classifiers.

Each packet classifier specifies one or more packet header attributes, such as source MAC address, destination IP address, or protocol type. The classifier also specifies the service flow to be used when a packet matches this particular combination of headers. Separate classifiers are used for downstream and upstream service flows.

When the CMTS receives downstream and upstream packets, it compares each packet's headers to the contents of each packet classifier. When the CMTS matches the packet to a classifier, the CMTS then assigns the proper SFID to the packet and transmits the packet to or from the cable modem. This ensures that the packet is assigned its proper service flow, and thus its proper QoS parameters.

Figure below illustrates the mapping of packet classifiers.

Figure 1: Classification Within the MAC Layer



Packet Header Suppression Rules

Because many data and real-time applications may use fixed values in their packet header fields, DOCSIS 1.1 supports PHS to suppress the duplicate portions of the packet headers when a group of packets is transmitted during a session. Each service flow can support a separate set of PHS rules that determine which parts of the header are suppressed.

When PHS is being used, the transmitting CMTS suppresses the specified headers in all the packets for that service flow. The receiving CMTS then restores the missing headers before forwarding the packets on to their ultimate destination.

Proper use of PHS can increase the efficiency of packetized transmissions, especially for real-time data that is encapsulated by other protocols, such as VoIP traffic.

Quality of Service Comparison

This section summarizes the differences in QoS between DOCSIS 1.0, DOCSIS 1.0+, and DOCSIS 1.1 networks.

Note Cisco CMTS routers can transparently interoperate with cable modems running DOCSIS 1.0, DOCSIS 1.0+ extensions, or DOCSIS 1.1. If a cable modem indicates at system initialization that it is DOCSIS 1.1-capable, the Cisco CMTS router uses the DOCSIS 1.1 features. If the cable modem is not DOCSIS 1.1-capable, but does support the DOCSIS 1.0+ QoS extensions, the Cisco CMTS automatically supports the cable modem's requests for dynamic services. Otherwise, the cable modem is treated as a DOCSIS 1.0 device.

DOCSIS 1.0

DOCSIS1.0 uses a static QoS model that is based on a class of service (CoS) that is preprovisioned in the DOCSIS configuration file that is downloaded to the cable modem. The CoS is a bidirectional QoS profile that applies to both the upstream and downstream directions, and 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 identifies the cable modems that are allowed to transmit on the network. In DOCSIS 1.0 networks, each cable modem is assigned only one SID for both the upstream and downstream directions, creating a one-to-one correspondence between a cable modem and its SID. All traffic originating from, or destined for, a cable modem is mapped to that particular 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, has a limited ability to 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+

In response to the limitations of DOCSIS 1.0 networks 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’s 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 uBR925 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 and CMTS 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.

Interoperability with Different Versions of DOCSIS Networks

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 CMTS, nor will they interfere with operation of DOCSIS 1.1 features.

Table below shows the interoperability of a DOCSIS 1.1 CMTS with different versions of cable modems.

Table 2: DOCSIS 1.1 Interoperability

For this configuration...	The result is...
DOCSIS 1.1 CMTS with DOCSIS 1.0 cable modems	DOCSIS 1.0 cable modems receive DOCSIS 1.0 features and capabilities. BPI is supported if available and enabled on the CMTS.
DOCSIS 1.1 CMTS with DOCSIS 1.0+ cable modems	DOCSIS 1.0+ cable modems receive basic DOCSIS 1.0 support. BPI is supported if available and enabled on the CMTS. In addition, DOCSIS 1.0+ 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 CMTS with DOCSIS 1.1 cable modems	DOCSIS 1.1 cable modems receive all the DOCSIS 1.1 features listed in this document. BPI+ is supported if available and enabled on the CMTS.

Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems

To define ERBA on the downstream for DOCSIS 1.0 cable modems, use the cable qos promax-ds-burst command in global configuration mode.

The ERBA feature is characterized by the following enhancements:

- Enables support for the DOCSIS1.1 Downstream Maximum Transmit Burst parameter on the Cisco CMTS by using the **cable ds-max-burst** configuration command.
- Allows DOCSIS1.0 modems to support the DOCSIS1.1 Downstream Maximum Transmit Burst parameter by mapping DOCSIS1.0 modems to overriding DOCSIS 1.1 QoS profile parameters on the Cisco CMTS.

ERBA allows DOCSIS1.0 modems to burst their temporary transmission rate up to the full line rate for short durations of time. This capability provides higher bandwidth for instantaneous bandwidth requests, such as those in Internet downloads, without having to make changes to existing service levels in the QoS Profile.

This feature allows you to set the DOCSIS 1.0 cable modems burst transmissions, with mapping to overriding DOCSIS 1.1 QoS profile parameters on the Cisco CMTS. DOCSIS 1.0 cable modems require DOCSIS 1.0 parameters when registering to a matching QoS profile. This feature enables maximum downstream line rates, and the ERBA setting applies to all cable modems that register to the corresponding QoS profile.

Note QoS definitions must previously exist on the Cisco CMTS headend to support this feature.

ERBA for DOCSIS 1.0 cable modems is supported with these new or enhanced commands or keywords:

- cable qos pro max-ds-burst burst-size
- show cable qos profile n [verbose]

DOCSIS 3.0 Downstream Peak Traffic Rate TLV Support for ERBA

The DOCSIS WFQ Scheduler allows each service flow to have one dedicated queue. When ERBA is enabled for the service flow, the peak rate is implemented as the queue shape rate within the scheduler, while the maximum sustained rate is set as the token bucket refill rate. When ERBA is turned off, the burst size and the peak rate value are not used.

The maximum traffic burst parameter is used to control a service flow burst duration, to burst up to the channel line rate or a configured peak rate, when it is within its maximum burst size allowance. On the Cisco cBR-8 Converged Broadband Router, the **cable ds-max-burst** command is used to control this behavior explicitly.

The *peak-rate* keyword is introduced to specify the peak rate an ERBA-enabled service flow can use. The peak rate value is applied to a specific service flow created after the configuration of the **cable ds-max-burst** command.

If the DOCSIS 3.0 TLV 25.27 is specified for a service flow, the *peak rate* value is set as the TLV value. However, if ERBA is not turned on for a service flow, the *peak rate* value is ignored.

During modem registration or Dynamic Service Addition (DSA) operation, the service class name TLV 25.4 is sent to create the static or dynamic downstream service flow that matches the service class template. These downstream service flows are created with a specific *peak rate*.

Some of the DOCSIS 1.x an DOCSIS 2.0 cable modems, which are not fully DOCSIS 1.x or DOCSIS 2.0 compliant, may fail to come online when the downstream peak rate TLV 25.27 is received from the CMTS during registration. To overcome this failure, you can configure the cable service attribute withhold-TLVs command to restrict sending of the peak traffic rate TLVs to DOCSIS1.x and DOCSIS 2.0 cable modems. For more information on how to suppress peak rate TLVs, see Suppressing Upstream and Downstream Peak Rate TLVs for pre DOCSIS 3.0 Cable Modems, on page 15.

Note The ERBA feature is not applicable for high priority service flows and multicast service flows.

Table below summarizes the ERBA support for the Cisco cBR-8 router.

Table 3: Enhanced Rate Bandwidth Allocation Support for the Cisco cBR-8 Router

	Policer Rate	Policer Exceed Action	Policer Token Bucket Size	Queue Shape Rate
Traditional Service Flow	Maximum Sustained Traffic Rate (unused)	Transmit	A value computed internally by CMTS (unused)	Maximum Sustained Traffic Rate
ERBA-Enabled Service Flow	Maximum Sustained Traffic Rate	Drop	Maximum Traffic Burst TLV	Peak Traffic Rate

In Cisco cBR-8 routers, the dual token bucket-based shaper is used to support ERBA on the Cisco cBR-8 CCAP line card (the ERBA feature is always enabled on the Cisco cBR-8 CCAP line card). The dual token bucket shaper has two independent token buckets for each service flow. The maximum rate of one bucket is configured to MSR and the maximum tokens are set to maximum traffic burst. The other bucket is configured with the refilling rate of the *peak rate* and the maximum tokens are set to the default level of 4 milliseconds. Packets are shaped if any of the two buckets are exhausted.

Table below summarizes the ERBA dual token bucket configuration for the Cisco cBR-8 routers.

Table 4: ERBA Dual Token Bucket Configuration

	Token Bucket Rate (One)	Token Bucket Size (One)	Token Bucket Rate (Two)	Token Bucket Size (Two)
Traditional Service Flow	Maximum Sustained Traffic Rate	4ms * MSR	N/A	N/A
ERBA-enabled Service Flow	Maximum Sustained Traffic Rate	Maximum Traffic Burst or 4ms * MSR	Peak Rate	4ms * Peak Rate

Suppressing Upstream and Downstream Peak Rate TLVs for pre DOCSIS 3.0 Cable Modems

The DOCSIS 3.0 upstream (US) peak rate TLV 24.27 and downstream (DS) peak rate TLV 25.27 are enabled on the Cisco CMTS through the cable service class command or the CM configuration file. The DOCSIS 1.x and DOCSIS 2.0 CMs do not support these TLVs. Ideally, if a DOCSIS 1.x or DOCSIS 2.0 CM receives peak rate TLVs during registration, it should ignore these TLVs and proceed with the registration. However there are a few old non-compliant pre DOCSIS 3.0 CMs, which may fail to come online when peak-rate TLVs are received in the registration response from the Cisco CMTS. To overcome this, the Cisco CMTS enables suppression of the DOCSIS 3.0 peak rate TLVs for the pre-DOCSIS3.0 CMs.

To suppress the DOCSIS 3.0 US and DS peak rate TLVs, use the **cable service attribute withhold-TLVs command with the peak-rate** keyword in global configuration mode. When configured, this command restricts the Cisco CMTS from sending US and DS peak rate TLVs to the DOCSIS 1.x and DOCSIS 2.0 CMs. The decision to send the TLVs is based on the DOCSIS version of the CM received during registration. If the registration request is from a pre DOCSIS 3.0 CM, the peak rate TLVs are not sent in the registration response. However this command does not restrict sending of DOCSIS 3.0 peak-rate TLVs to DOCSIS 3.0 CMs.

Downstream Classification Enhancement with MAC Addresses

Downstream classifiers, specified in the cable modem configuration file, are used to map packets to service flows based on DOCSIS specifications. New combinations of downstream classifiers with a destination MAC address are supported. This enhancement enables service providers to better manage high priority service flows associated with a downstream classifier. For example, a single User Datagram Protocol (UDP) port can be shared by high priority and low priority traffic.

Downstream classification is automatically enabled on the Cisco CMTS router. The downstream classifier combinations that are supported on the router are listed below:

Without Combination

- IP (IPv4)
- IPv6
- TCP/UDP
- Destination MAC

With Combination

- IPv4 + TCP/UDP
- IPv6 + TCP/UDP
- Destination MAC + IPv4 (with the exception of a destination IP address)
- Destination MAC + IPv6 (with the exception of a destination IPv6 address)
- Destination MAC + TCP/UDP
- Destination MAC + IPv4 + TCP/UDP (with the exception of a destination IP address)
- Destination MAC + IPv6 + TCP/UDP (with the exception of a destination IPv6 address)

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

Fragmentation

Fragmentation splits large data packets so that they fit into the smaller time slots inbetween UGS slots. This 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.

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 cable modem to suppress repetitive or redundant portions in packet headers before transmitting on the DOCSIS link. This conserves 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 use of the service class provides the following benefits for a DOCSIS 1.1 network:

- 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.

How to Configure the Cisco CMTS for DOCSIS 1.1 Operations

See the following sections for the configuration tasks for DOCSIS 1.1 operations. Each task in the list is identified as either required or optional.

Note This section describes only the configuration tasks that are specific for DOCSIS 1.1 operations.

Configuring Baseline Privacy Interface

BPI+ encryption is by default enabled for 56-bit DES encryption on all cable interfaces. If BPI+ encryption has been previously disabled, or if you want to reconfigure BPI+ encryption on a cable interface on the CMTS, use the following procedure.

Note If you have disabled BPI+ encryption on a cable interface, and a cable modem attempts to register on that interface using BPI+ encryption, the CMTS will reject its registration request, displaying a %CBR-4-SERVICE_PERMANENTLY_UNAVAILABLE error message. The **show cable modem** command will also show that this cable modem has been rejected with a MAC status of reject(c).

Before you begin

BPI+ encryption is supported on all Cisco CMTS images that include “k1”, “k8”, or “k9” in its file name or BPI in the feature set description. All BPI images support 40-bit and 56-bit DES encryption.

By default, BPI+ encryption is enabled for 56-bit DES encryption. Also, when a cable modem is running DOCSIS 1.1 software, BPI+ encryption is enabled by default, unless the service provider has disabled it by setting the Privacy Enable field (TLV 29) in the DOCSIS configuration file to 0. Therefore, both the CMTS and cable modem are set to use BPI+ encryption when using the default configurations.

Procedure

	Command or Action	Purpose

Step 1	**enable**
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose

Step 2	**configure terminal**
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**interface cable***slot /subslot /port*
	Example:
	`Router(config)# interface cable 6/0/0`
	`Router(config-if)#`
		Enters interface configuration mode for the cable interface line card at this particular slot.

Step 4	**cable privacy**
	Example:
	`Router(config-if)# cable privacy`
	`Router(config-if)#`
		(Optional) Enables BPI+ 56-bit DES encryption on the cable interface (default).

Step 5	**cable privacyaccept-self-signed-certificate**
	Example:
	`Router(config-if)# cable privacy accept-self-signed-certificate`
	`Router(config-if)#`
		(Optional) Allows cable modems to register using self-signed manufacturer certificates, as opposed to the default of allowing only manufacturer's certificates that are chained to the DOCSIS root certificate.
		Caution
		Use the above command sparingly, as it bypasses DOCSIS BPI+ certificates. Otherwise, self-signed certificates provide workaround registration for cable modems that are not compliant with DOCSIS BPI+ certificates. This functionality is strictly intended for troubleshooting of a short duration or in the context of additional security measures.
		Note
		By default, the CMTS does not accept self-signed certificates. In the default configuration, if a cable modem attempts to register with self-signed certificates, the CMTS will refuse to allow the cable modem to register.

Step 6	**cable privacy authorize-multicast**
	Example:
	`Router(config-if)# cable privacy authorize-multicast`
	`Router(config-if)#`
		(Optional) Enables BPI+ encryption on the cable interface and uses AAA protocols to authorize all multicast stream (IGMP) join requests.
		Note
		If you use this command to authorize multicast streams, you must also use the **cable privacy authenticate-modem** command to enable AAA services on the cable interface.

	Command or Action	Purpose

Step 7	**cable privacy mandatory**
	Example:
	`Router(config-if)# cable privacy mandatory`
	`Router(config-if)#`
		(Optional) Requires baseline privacy be active for all CMs with BPI/BPI+ enabled in the DOCSIS configuration files, else the CMs are forced to go offline.
		If a CM does not have BPI enabled in its DOCSIS configuration file, it will be allowed to come online without BPI.

Step 8	**cable privacy oaep-support**
	Example:
	`Router(config-if)# cable privacy oaep-support`
	`Router(config-if)#`
		(Optional) Enables BPI+ encryption on the cable interface and enables Optimal Asymmetric Encryption Padding (OAEP). This option is enabled by default. Disabling this option could have a performance impact.

Step 9	**cable privacy kek** {**life-time** *seconds* }
	Example:
	`Router(config-if)# cable privacy kek life-time 302400`
	`Router(config-if)#`
		(Optional) Configures the life-time values for the key encryption keys (KEKs) for BPI+ operations on all cable interfaces.

Step 10	**cable privacy tek** {**life-time** *seconds*}
	Example:
	`Router(config-if)# cable privacy tek life-time 86400`
	`Router(config-if)#`
		(Optional) Configures the life-time values for the traffic encryption keys (TEKs) for BPI+ operations on all cable interfaces.

Step 11	**exit**
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode.
		Note
		Repeat steps Step 3, on page 19 through Step 11, on page 20 for each cable interface.

Step 12	**exit**
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

What to do next

You can also configure the following additional timers for BPI+ operations in the DOCSIS configuration file for each cable modem. As a general rule, you do not need to specify these timers in the DOCSIS configuration file unless you have a specific reason for changing them from their default values.

Table 5: Individual Cable Modem BPI+ Timer Values

Timer	Description
Authorize Wait Timeout	The amount of time a cable modem will wait for a response from a CMTS when negotiating a KEK for the first time.
Reauthorize Wait Timeout	The amount of time a cable modem will wait for a response from a CMTS when negotiating a new KEK because the Authorization Key (KEK) lifetime is about to expire.
Authorize Reject Wait Timeout	The amount of time a cable modem must wait before attempting to negotiate a new KEK if the CMTS rejects its first attempt to negotiate a KEK.
Operational Wait Timeout	The amount of time a cable modem will wait for a response from a CMTS when negotiating a TEK for the first time.
Rekey Wait Timeout	The amount of time a cable modem will wait for a response from a CMTS when negotiating a new TEK because the TEK lifetime is about to expire.

Downloading the DOCSIS Root Certificate to the CMTS

DOCSIS 1.1 allows cable modems to identify themselves using a manufacturer's chained X.509 digital certificate that is chained to the DOCSIS root certificate. The DOCSIS root certificate is already installed on the bootflash of the CMTS router. However, if you want to install another root certificate, for example, the Euro-DOCSIS certificate, download the certificate and save it on the bootflash as "euro-root-cert".

Tip For more information about the DOCSIS root certificate provided by Verisign, see the information at the following URL: http://www.verisign.com/products-services/index.html

Note You may load the DOCSIS root certificate and a EuroDOCSIS or PacketCable root certificate. Cisco recommends that the EuroDOCSIS PacketCable root certificates be copied into bootflash.

To download the DOCSIS root certificate to the Cisco CMTS, which is required if any cable modems on the network are using chained certificates, use the following procedure:

Procedure

Step 1 Download the DOCSIS root certificate from the DOCSIS certificate signer, Verisign. At the time of this document's printing, the DOCSIS root certificate is available for download at the following URL: http://www.verisign.com/products-services/index.html

Step 2 Verisign distributes the DOCSIS root certificate in a compressed ZIP archive file. Extract the DOCSIS root certificate from the archive and copy the certificate to a TFTP server that the CMTS can access.

Tip

To avoid possible confusion with other certificates, keep the file's original filename of "CableLabs_DOCSIS.509" when saving it to the TFTP server.

Step 3 Log in to the Cisco CMTS using either a serial port connection or a Telnet connection. Enter the **enable** command and password to enter Privileged EXEC mode:

Example:

```
Router> enable

Password: <password>
Router#
```

Step 4 Use the **dir bootflash** command to verify that the bootflash has sufficient space for the DOCSIS root certificate (approximately 1,000 bytes of disk space):

Example:

```
Router# dir bootflash:

Directory of bootflash:/
    1  -rw-     3229188   Dec 30 2002 15:53:23  cbrsup-universalk9.2015-03-18_03.30_johuynh.SSA.bin

3407872 bytes total (250824 bytes free)
Router#
```

Tip
If you delete files from the bootflash to make room for the DOCSIS root certificate, remember to use the **squeeze** command to reclaim the free space from the deleted files.

Step 5 Use the **copy tftp bootflash** command to copy the DOCSIS root certificate to the router's bootflash memory. (The file must be named "root-cert" on the bootflash for the CMTS to recognize it as the root certificate.)

Example:

```
Router# copy tftp bootflash:

Address or name of remote host []? tftp-server-ip-address

Source filename []? CableLabs_DOCSIS.509

Destination filename [CableLabs_DOCSIS.509]? root-cert

Loading CableLabs_DOCSIS.509 from tftp-server-ip-address (via FastEthernet0/0): !
[OK - 996/1024 bytes]
996 bytes copied in 4.104 secs (249 bytes/sec)
Router#
```

Tip
You can also copy the root certificate to a PCMCIA Flash Disk (disk0 or disk1). However, because Flash Disks are not secure and easily removed from the router, we recommend that you keep the root certificate in the bootflash for both operational and security reasons.

Step 6 Verify that the DOCSIS root certificate has been successfully copied to the bootflash memory:

Example:

```
Router# dir bootflash:
```

```
Directory of bootflash:/
    1  -rw-     3229188   Dec 30 2002 15:53:23  cbrsup-universalk9.2015-03-18_03.30_johuynh.SSA.bin

    2  -rw-         996   Mar 06 2002 16:03:46  root-cert
3408876 bytes total (248696 zxbytes free)
Router#
```

Step 7 (Optional) After the first cable modem has registered using BPI+, you can use the **show crypto ca trustpoints** command to display the Root certificate that the CMTS has learned:

Note
The **show crypto ca trustpoints** command does not display the root certificate until after at least one cable modem has registered with the CMTS using BPI+ encryption. Alternatively, you can use the unsupported command **test cable generate** in privileged EXEC mode to force the CMTS to register the root certificate.

Example:

```
Router# show crypto ca trustpoints
Root certificate
  Status: Available
  Certificate Serial Number: D54BB68FE934324F6B8FD0E41A65D867
  Key Usage: General Purpose
  Issuer:
    CN = DOCSIS Cable Modem Root Certificate Authority
     OU = Cable Modems
     O = Data Over Cable Service Interface Specifications
     C = US
  Subject Name:
    CN = "BPI Cable Modem Root Certificate Authority "
     OU = DOCSIS
     O = BPI
     C = US
  Validity Date:
    start date: 07:00:00 UTC Mar 27 2001
    end   date: 06:59:59 UTC Jan 1 2007
```

What to do next

Tip To display all certificates (Root, Manufacturers, CM) that the CMTS has learned, use the **show crypto ca certificates** command.

Adding a Manufacturer's Certificate as a Trusted Certificate

The DOCSIS specifications allow operators to control which manufacturer's and CM certificates are allowed on each CMTS by marking them as either trusted or untrusted. You can add a certificate to the list of trusted certificates on the Cisco CMTS using SNMP commands, as described in the following section:

Adding a Certificate as a Trusted Certificate Using SNMP Commands

You can also use an SNMP manager to create and add certificates to the CMTS list of trusted certificates by manipulating the tables and attributes in the DOCS-BPI-PLUS-MIB . To add a manufacturer's certificate, add an entry to the docsBpi2CmtsCACertTable table. Specify the following attributes for each entry:

- docsBpi2CmtsCACertStatus—Set to 4 to create the row entry.
- docsBpi2CmtsCACert—The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate.
- docsBpi2CmtsCACertTrust—An Integer value from 1 to 4 specifying the certificate's trust status: 1=trusted, 2=untrusted, 3= chained, 4=root. Specify 1 for certificates that should be trusted and 3 for chained certificates that should be verified with the root certificate.

Similarly, to add a CM certificate to the list of trusted certificates, add an entry to the docsBpi2CmtsProvisionedCmCertTable table. Specify the following attributes for each entry:

- docsBpi2CmtsProvisionedCmCertStatus—Set to 4 to create the row entry.
- docsBpi2CmtsProvisionedCmCert—The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate.
- docsBpi2CmtsProvisionedCmCertTrust—An Integer value from 1 to 2 specifying the certificate's trust status: 1=trusted, 2=untrusted. Specify 1 for CM certificates that should be trusted.

Tip Always set the CertStatus attributes before loading the actual certificate data, because otherwise the CMTS will assume the certificate is chained and will immediately attempt to verify it with the manufacturers and root certificates.

For example, to use the Unix command-line SNMP utility to add a manufacturer's certificate to the list of trusted certificates on the CMTS at IP address 192.168.100.134, enter the following command (be sure to substitute a valid index pointer for the table entry for the <*index*> value).

```
% setany -v2c 192.168.100.134 private docsBpi2CmtsCACertStatus.
<index>
 -i 4
 docsBpi2CmtsCACert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsCACertTrust.
<index>
 -i 1
```

To do the same thing for a CM certificate, use the following command:

```
% setany -v2c 192.168.100.134 private docsBpi2CmtsProvisionedCmCertStatus.
<index>
 -i 4 docsBpi2CmtsProvisionedCmCert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsProvisionedCmCertTrust.
<index>
 -i 1
```

Tip Most operating systems cannot accept input lines that are as long as needed to input the hexadecimal decimal string that specifies a certificate. For this reason, you should use a graphical SNMP manager to set these attributes. For a number of certificates, you can also use a script file, if more convenient.

Note If you are adding self-signed certificates, you must also use the **cable privacy accept-self-signed-certificate** command before the CMTS will accept the certificates.

Adding a Manufacturer's or CM Certificate to the Hotlist

The DOCSIS specifications allow operators to add a digital manufacturer's or CM certificate to a hotlist (also known as the certificate revocation list, or CRL) on the CMTS, to indicate that this particular certificate should no longer be accepted. This might be done when a user reports that their cable modem has been stolen, or when the service provider decides not to support a particular manufacturer's brand of cable modems.

Adding a Certificate to the Hotlist Using SNMP Commands

You can also use an SNMP manager to create and add certificates to the hotlist by manipulating the tables and attributes in the DOCS-BPI-PLUS-MIB . To add a manufacturer's certificate, add an entry to the docsBpi2CmtsCACertTable table. Specify the following attributes for each entry:

- docsBpi2CmtsCACertStatus—Set to 4 to create the row entry.
- docsBpi2CmtsCACert—The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate.
- docsBpi2CmtsCACertTrust—An Integer value from 1 to 4 specifying the certificate's trust status: 1=trusted, 2=untrusted, 3= chained, 4=root. When adding a certificate to the hotlist, set this attribute to 2 for untrusted.

Similarly, to add a CM certificate to the hotlist, add an entry to the docsBpi2CmtsProvisionedCmCertTable table. Specify the following attributes for each entry:

- docsBpi2CmtsProvisionedCmCertStatus—Set to 4 to create the row entry.
- docsBpi2CmtsProvisionedCmCert—The hexadecimal data, as an X509Certificate value, for the actual X.509 certificate.
- docsBpi2CmtsProvisionedCmCertTrust—An Integer value from 1 to 2 specifying the certificate's trust status: 1=trusted, 2=untrusted. When adding a certificate to the hotlist, set this attribute to 2 for untrusted.

Tip Always set the CertStatus attributes before loading the actual certificate data, because otherwise the CMTS will assume the certificate is chained and will immediately attempt to verify it with the manufacturers and root certificates.

Note This procedure is identical to the one given for adding a certificate as a trusted certificate in the Adding a Certificate as a Trusted Certificate Using SNMP Commands, on page 24, except that the docsBpi2CmtsProvisionedCmCertTrust attribute is set to 2 instead of 1.

For example, to use the Unix command-line SNMP utility to add a manufacturer's certificate to the hotlist on the CMTS at IP address 192.168.100.113, enter the following command (be sure to substitute a valid index pointer for the table entry for the <*index*> value).

```
% setany -v2c 192.168.100.113 private docsBpi2CmtsCACertStatus.
<index>
 -i 4
 docsBpi2CmtsCACert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsCACertTrust.
<index>
 -i 2
```

To do the same thing for a CM certificate, use the following command:

```
% setany -v2c 192.168.100.113 private docsBpi2CmtsProvisionedCmCertStatus.
<index>
 -i 4
 docsBpi2CmtsProvisionedCmCert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsProvisionedCmCertTrust.
<index>
 -i 2
```

Tip Most operating systems cannot accept input lines that are as long as needed to input the hexadecimal decimal string that specifies a certificate. For this reason, you should use a graphical SNMP manager to set these attributes. For a number of certificates, you can also use a script file, if more convenient.

Enabling Concatenation

To enable concatenation for one or more upstreams on a cable interface (which is the default configuration), use the following procedure:

Procedure

	Command or Action	Purpose

Step 1	**enable**
	Example:
	`Router> enable`
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose

Step 2	**configure terminal**
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**interface cable***slot* / *port*
	Example:
	`Router(config)# interface cable 6/0`
	`Router(config-if)#`
		Enters interface configuration mode for the cable interface line card at this particular slot.

Step 4	**cable upstream** *n* **concatenation**
	Example:
	`Router(config-if)# cable upstream 0 concatenation`
	`Router(config-if)# cable upstream 1 concatenation`
	`Router(config-if)#`
		Enables concatenation for the specified upstream on the cable interface.
		Note Repeat this command for each upstream on the interface.

Step 5	**exit**
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode.

Step 6	**exit**
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Enabling DOCSIS Fragmentation

To enable DOCSIS fragmentation for one or more upstreams on a cable interface (which is the default configuration), use the following procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable***slot* /*port*
4. **cable upstream***n* **fragmentation**
5. **cable upstream** *n* **unfrag-slot-jitter** [**limit***jitter* | **cac-enforce**]
6. **exit**
7. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**enable**
	Example:
	`Router> enable`
	Example:
	`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	**interface cable***slot* /*port*
	Example:
	`Router(config)# interface cable 6/0`
	`Router(config-if)#`
		Enters interface configuration mode for the cable interface line card at this particular slot.

Step 4	**cable upstream***n* **fragmentation**
	Example:
	`Router(config-if)# cable upstream 2 fragmentation`
	`Router(config-if)# cable upstream 3 fragmentation`
	`Router(config-if)#`
		Enables fragmentation for the specified upstream on the cable interface.
		Note
		Repeat this command for each upstream on the interface.

Step 5	**cable upstream** *n* **unfrag-slot-jitter** [**limit***jitter* | **cac-enforce**]
	Example:
	`Router(config-if)# cable upstream 0 unfrag-slot-jitter limit 2000 cac-enforce`
	`Router(config-if)#`
		(Optional) Specifies the amount of jitter that can be tolerated on the upstream due to unfragmentable slots. The **limit** option specifies the allowable *jitter* limit in microseconds (0 to 4,294,967,295. The **cac-enforce** option configures the upstream so that it rejects service flows requesting jitter less than the fragmentable slot jitter.
		Note
		By default, *jitter* is set to a limit of 0 microseconds, and the **cac-enforce** option is enabled.

Step 6	**exit**
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode.

	Command or Action	Purpose

Step 7	**exit**
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Example

The following example of the **show cable qos profile** command illustrates that the maximum downstream burst has been defined, and is a management-created QoS profile:

```
Router# show cable qos profile
ID  Prio Max       Guarantee Max        Max   TOS  TOS   Create  B     IP prec.
         upstream  upstream  downstream tx    mask value by      priv  rate
         bandwidth bandwidth bandwidth  burst                     enab  enab
1   0    0         0         0          0     0xFF 0x0   cmts(r) no    no
2   0    64000     0         1000000    0     0xFF 0x0   cmts(r) no    no
3   7    31200     31200     0          0     0xFF 0x0   cmts    yes   no
4   7    87200     87200     0          0     0xFF 0x0   cmts    yes   no
6   1    90000     0         90000      1522  0xFF 0x0   mgmt    yes   no
10  1    90000     0         90000      1522  0x1  0xA0  mgmt    no    no
50  0    0         0         96000      0     0xFF 0x0   mgmt    no    no
51  0    0         0         97000      0     0xFF 0x0   mgmt    no    no
```

The following example illustrates the maximum downstream burst size in sample QoS profile 10 with the **show cable qos profileverbose** command in privileged EXEC mode:

```
Router# show cable qos profile 10 verbose
Profile Index                          10
Name
Upstream Traffic Priority              1
Upstream Maximum Rate (bps)            90000
Upstream Guaranteed Rate (bps)         0
Unsolicited Grant Size (bytes)         0
Unsolicited Grant Interval (usecs)     0
Upstream Maximum Transmit Burst (bytes) 1522
Downstreamam Maximum Transmit Burst (bytes) 100000
IP Type of Service Overwrite Mask      0x1
IP Type of Service Overwrite Value     0xA0
Downstream Maximum Rate (bps)          90000
Created By                             mgmt
Baseline Privacy Enabled               no
```

Enabling DOCSIS 1.1 Downstream Maximum Transmit Burst on the Cisco cBR-8 Router

Perform the following steps to configure ERBA on the Cisco cBR-8 router. This procedure and the associated commands are subject to the guidelines and restrictions cited in this document.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	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	[**no**] **cable ds-max-burst burst-threshold** *threshold* **Example:** `Router(config)# cable ds-max-burst burst-threshold 2048`	Enables the support for DOCSIS 1.1 downstream max burst. To remove this configuration, use the **no** form of this command.
Step 4	**cable service class** *class-index* **peak-rate** *peak-rate* **Example:** `Router(config)# cable service class 1 peak-rate 1000`	Set the peak-rate value of a specific service class.

Step 5	**Ctrl^Z**
	Example:
	`Router(config)# Ctrl^Z`
	`Router#`
		Returns to privileged EXEC mode.

Example

When this feature is enabled, new service flows with burst size larger than the burst threshold are supported. However, the existing service flows are not affected.

When this feature is disabled, no new service flows are configured with the *Downstream Maximum Transmit Burst* parameter—the **cable ds-max-burst** command settings. However, the existing service flows are not affected.

Monitoring DOCSIS Operations

The following sections describe the commands that provide information about the DOCSIS network and its cable modems, the RF network and cable interfaces on the CMTS, and BPI+ operations.

Monitoring the DOCSIS Network

The **show cable modem** command is the primary command to display the current state of cable modems and the DOCSIS network. This command has many options that provide information on different aspects of DOCSIS operations.

Displaying the Status of Cable Modems

To display a list of known cable modems and their current status, use the **show cable modem** command.

You can also display a particular cable modem by specifying its MAC address or IP address with the **show cable modem** command. If you specify the MAC address or IP address for a CPE device, the command will display the information for the cable modem that is associated with that device.

Note If the CPE IP address is no longer associated with a cable modem, the **show cable modem** command might not display information about the cable modem. To display the IP address of the CPE device for the cable modem, use the **clear cable host ip-address** command to clear the IP address of the modem from the router database, and then enter the **ping docsis mac-address** command, which resolves the MAC address by sending the DOCSIS ping to the CM.

To display a list of cable modems sorted by their manufacturer, use the **vendor** option.

The MAC state field in each of these displays shows the current state of the cable modem:

Table 6: Descriptions for the MAC State Field

MAC State Value	Description
Registration and Provisioning Status Conditions	
init(r1)	The CM sent initial ranging.
init(r2)	The CM is ranging. The CMTS received initial ranging from the Cm and has sent RF power, timing offset, and frequency adjustments to the CM.
init(rc)	Ranging has completed.
init(d)	The DHCP request was received. This also indicates that the first IP broadcast packet has been received from the CM.
init(i)	The DHCP reply was received and the IP address has been assigned, but the CM has not yet replied with an IP packet.
init(o)	The CM has begun to download the option file (DOCSIS configuration file) using the Trivial File Transfer Protocol (TFTP), as specified in the DHCP response. If the CM remains in this state, it indicates that the download has failed.
init(t)	Time-of-day (TOD) exchange has started.
resetting	The CM is being reset and will shortly restart the registration process.
Non-error Status Conditions	

MAC State Value	Description
offline	The CM is considered offline (disconnected or powered down).
online	The CM has registered and is enabled to pass data on the network.
online(d)	The CM registered, but network access for the CM has been disabled through the DOCSIS configuration file.
online(pk)	The CM registered, BPI is enabled and KEK is assigned.
online(pt)	The CM registered, BPI is enabled and TEK is assigned. BPI encryption is now being performed.
expire(pk)	The Cm registered, BPI is enabled, KEK was assigned but has since expired.
expire(pt)	The Cm registered, BPI is enabled, TEK was assigned but has since expired.
Error Status Conditions	
reject(m)	The CM attempted to register but registration was refused due to a bad Message Integrity Check (MIC) value. This also could indicate that the shared secret in the DOCSIS configuration file does not match the value configured on the CMTS with the **cable shared-secret** command. It can also indicate that the **cable tftp-enforce** command has been used to require that a CM attempt a TFTP download of the DOCSIS configuration file before registering, but the CM did not do so.
reject(c)	The CM attempted to register, but registration was refused due to a a number of possible errors: • The CM attempted to register with a minimum guaranteed upstream bandwidth that would exceed the limits imposed by the **cable upstream admission-control** command. • The CM has been disabled because of a security violation. • A bad class of service (COS) value in the DOCSIS configuration file. • The CM attempted to create a new COS configuration but the CMTS is configured to not permit such changes.
reject(pk)	KEK key assignment is rejected, BPI encryption has not been established.
reject(pt)	TEK key assignment is rejected, BPI encryption has not been established.
reject(ts)	The CM attempted to register, but registration failed because the TFTP server timestamp in the CM registration request did not match the timestamp maintained by the CMTS. This might indicate that the CM attempted to register by replaying an old DOCSIS configuration file used during a prior registration attempt.
reject(ip)	The CM attempted to register, but registration failed because the IP address in the CM request did not match the IP address that the TFTP server recorded when it sent the DOCSIS configuration file to the CM. IP spoofing could be occurring.

MAC State Value	Description
reject(na)	The CM attempted to register, but registration failed because the CM did not send a Registration-Acknowledgement (REG-ACK) message in reply to the Registration-Response (REG-RSP) message sent by the CMTS. A Registration-NonAcknowledgement (REG-NACK) is assumed.

Displaying a Summary Report for the Cable Modems

The **show cable modem** command also can provide a summary report of the cable modems by using the **summary** and **total** options.

You can also use the **summary** and **total** options to display information for a single interface or a range of interfaces.

Displaying the Capabilities of the Cable Modems

To display the capabilities and current DOCSIS provisioning for cable modems, use the **mac** option.

To get a summary report of the cable modems and their capabilities, use the **mac** option with the **summary** and **total** options.

Displaying Detailed Information About a Particular Cable Modem

Several options for the show cable modem command display detailed information about a particular cable modem (as identified by its MAC address). The **verbose** option displays the most comprehensive output.

The **connectivity** and **maintenance** options also provide information that can be useful in troubleshooting problems with a particular cable modem.

Monitoring the RF Network and Cable Interfaces

You can use the **show interface cable** command to display information about the operation of the RF network and the cable interfaces on the CMTS.

Tip For a complete description of the **show cable interface** command and its options, see the "Cisco Cable Modem Termination System Commands" chapter in the *Cisco Broadband Cable Command Reference Guide* (see http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cmts_quality_of_services/docsis_1_1.html#ref_1239231).

Displaying Information About Cloned Cable Modems

To display the list of cable modems detected as cloned, use the **privacy hotlist** option with the **show interface cable** command.

Denying RF Access For Cable Modems

To deny radio frequency (RF) access for cable modems during ranging, use the **cable privacy hotlist cm** *mac-address* command.

The following example shows how to block cloned cable modems using their own MAC address:

```
Router(config)# cable privacy hotlist cm 00C0.0102.0304
Router(config)#
```

When an operator identifies a modem's MAC address that should not be registered on a specific CMTS, the operator can add this MAC address to the CMTS using the above command. This command ensures that the modem will not be allowed to come online on any interface on that CMTS.

Displaying Information About the Mac Scheduler

To display information about the DOCSIS MAC layer scheduler that is operating on each cable interface, use the **mac-scheduler** option with the **show cable interface** command. You can display information for all of the upstreams on an interface, or you can display information for a single upstream on an interface.

Displaying Information About QoS Parameter Sets

To display information about the DOCSIS 1.1 QoS parameter sets that have been defined on a cable interface, use the **qos paramset** option with the **show cable interface** command.

You can also display detailed information for a particular parameter set by specifying the index number for its Class of Service along with the **verbose** option.

Displaying Information About Service Flows

To display the service flows and their QoS parameter sets that are configured on a cable interface, use the **service-flow** option with the **show interface cable** command.

To display the major QoS parameters for each service flow, add the **qos** option to this command.

To display the complete QoS parameters for a particular service flow, use the **qos** and **verbose** options. You can use these options separately or together.

Displaying Information About Service IDs

To display information about Service IDs (SIDs), which are assigned to only upstreams in DOCSIS 1.1 networks, use the **sid** option with the **show interface cable** command.

Add the **qos** option to display the major QoS parameters associated with each SID.

To display detailed information about a particular SID and its QoS parameters, use both the **qos** and **verbose** options.

Monitoring BPI+ Operations

See the following sections to monitor the state of BPI operations on the CMTS and its connected cable modems:

Displaying the Current BPI+ State of Cable Modems

To display the current BPI+ state of cable modems, use the **show cable modem** command. If used without any options, this command displays the status for cable modems on all interfaces. You can also specify a particular cable interface on the CMTS, or the IP address or MAC address for a specific cable modem:

```
Router# show cable modem
 [ip-address
```

```
| interface
| mac-address
```

The MAC State column in the output of the **show cable modem** command displays the current status of each cable modem. The following are the possible BPI-related values for this field:

Table 7: Possible show cable modem BPI+ States

State	Description
online	A cable modem has come online and, if configured to use BPI+, is negotiating its privacy parameters for the session. If the modem remains in this state for more than a couple of minutes, it is online but not using BPI+. Check that the cable modem is running DOCSIS-certified software and is using a DOCSIS configuration file that enables BPI+.
online(pk)	The cable modem is online and has negotiated a Key Encryption Key(KEK) with the CMTS. If BPI+ negotiation is successful, this state will be shortly followed by online(pt).
online(pt)	The cable modem is online and has negotiated a Traffic Encryption Key (TEK) with the CMTS. The BPI+ session has been established, and the cable modem is encrypting all user traffic with the CMTS using the specified privacy parameters.
reject(pk)	The cable modem failed to negotiate a KEK with the CMTS, typically because the cable modem failed authentication. Check that the cable modem is properly configured for BPI+ and is using valid digital certificates. If the CMTS requires BPI+ for registration, the cable modem will go offline and have to reregister. Check that the cable modem is properly registered in the CMTS provisioning system. **Note** If a cable modem fails BPI+ authentication, a message similar to the following appears in the CMTS log: `%CBR-5-UNAUTHSIDTIMEOUT: CMTS deleted BPI unauthorized Cable Modem 00c0.abcd.ef01` **Note** In cBR-8, if the CM status has a * (asterisk) as prefix, the router does not apply ACL to block the Layer 3 traffic of the CM. While in Cisco uBR10000, the router will apply ACL.
reject(pt)	The cable modem failed to successfully negotiate a TEK with the CMTS. If the CMTS requires BPI+ for registration, the cable modem will have to reregister.

Displaying the BPI+ Timer Values on the CMTS

To display the values for the KEK and TEK lifetime timers on a particular cable interface, use the **show interface cable** *x/y* **privacy** [**kek** | **tek**] command.

Displaying the Certificate List on the CMTS

Use the **show crypt ca certificates** command to display the list of known certificates on the CMTS. For example:

```
Router# show crypto ca certificates

Certificate
```

```
  Status: Available
  Certificate Serial Number: 7DBF85DDDD8358546BB1C67A16B3D832
  Key Usage: General Purpose
  Subject Name
    Name: Cisco Systems
  Validity Date:
    start date: 00:00:00 UTC Sep 12 2001
    end   date: 23:59:59 UTC Sep 11 2021
Root certificate
  Status: Available
  Certificate Serial Number: 5853648728A44DC0335F0CDB33849C19
  Key Usage: General Purpose
    CN = DOCSIS Cable Modem Root Certificate Authority
     OU = Cable Modems
     O = Data Over Cable Service Interface Specifications
     C = US
  Validity Date:
    start date: 00:00:00 UTC Feb 1 2001
    end   date: 23:59:59 UTC Jan 31 2031
```

Configuration Examples for DOCSIS 1.1 Operations

This section lists the following sample configurations for DOCSIS 1.1 operations on the Cisco CMTS:

Example: DOCSIS 1.1 Configuration for Cisco cBR-8 Router (with BPI+)

```
version 12.2
service timestamps log datetime msec localtime
service password-encryption
!
hostname cBR-8
!
redundancy
 main-cpu
  auto-sync standard
logging queue-limit 100
no logging buffered
no logging rate-limit
enable password my-enable-password
!
ipc cache 5000
card 1/1 2cable-tccplus
card 2/0 1gigethernet-1
card 2/1 2cable-tccplus
card 3/0 1gigethernet-1
card 4/0 1oc12pos-1
card 8/0 5cable-mc520s
card 8/1 5cable-mc520s
cable flap-list insertion-time 60
cable flap-list power-adjust threshold 4
cable flap-list aging 86400
cable modem vendor 00.50.F1 TI
cable spectrum-group 2 band 11000000 16000000
cable spectrum-group 21 band 17000000 25000000
cable spectrum-group 32 shared
cable spectrum-group 32 band 5000000 42000000
cable modulation-profile 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
```

```
cable modulation-profile 2 short 6 75 6 8 16qam scrambler 152 no-diff 144 shortened uw8
cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw8
cable modulation-profile 21 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 21 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 21 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 21 short 3 76 12 22 qpsk scrambler 152 no-diff 64 shortened
cable modulation-profile 21 long 7 231 0 22 qpsk scrambler 152 no-diff 64 shortened
cable modulation-profile 22 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 22 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 22 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 22 short 4 76 7 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 22 long 7 231 0 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 23 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 23 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 23 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 23 short 4 76 7 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 23 long 7 231 0 22 16qam scrambler 152 no-diff 128 shortened
cable qos profile 5 max-downstream 10000
cable qos profile 5 max-upstream 1000
cable qos profile 5 priority 7
cable qos profile 5 tos-overwrite 0x3  0x0
cable qos profile 5 name cm_no_priority
cable qos profile 6 max-downstream 10000
cable qos profile 6 max-upstream 5000
cable qos profile 6 priority 7
cable qos profile 6 tos-overwrite 0x3  0x0
cable qos profile 6 name qos6
cable qos profile 7 max-downstream 128
cable qos profile 7 max-upstream 128
cable qos profile 7 priority 7
cable qos profile 8 max-downstream 10000
cable qos profile 8 max-upstream 1000
cable qos profile 8 priority 3
cable qos profile 8 tos-overwrite 0x3  0x0
cable qos profile 8 name qos8
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable event syslog-server 10.10.10.131
ip subnet-zero
!
!
interface FastEthernet0/0/0
 ip address 10.10.32.21 255.255.0.0
 no cdp enable
!
interface GigabitEthernet2/0/0
 ip address 10.10.31.2 255.0.0.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 load-interval 30
 negotiation auto
 no cdp enable
!
interface GigabitEthernet3/0/0
 no ip address
 ip pim sparse-mode
 no ip route-cache cef
 load-interval 30
 shutdown
 negotiation auto
 no cdp enable
!
```

```
interface POS4/0/0
 no ip address
 crc 32
 no cdp enable
 pos ais-shut
!
!
interface Cable8/0/0
 ip address 10.10.10.28 255.255.255.0
 ip helper-address 1.10.10.133
 cable bundle 2 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 669000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable downstream rf-power 45
 cable upstream 0 connector 0
 cable upstream 0 spectrum-group 32
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 data-backoff 0 6
 cable upstream 0 modulation-profile 23
 no cable upstream 0 rate-limit
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
 cable upstream 1 spectrum-group 32
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 data-backoff 0 6
 cable upstream 1 modulation-profile 23
 no cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 spectrum-group 32
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 data-backoff 3 6
 cable upstream 2 modulation-profile 23
 no cable upstream 2 shutdown
 cable upstream 3 connector 3
 cable upstream 3 spectrum-group 32
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 21
 no cable upstream 3 shutdown
 cable source-verify
 cable privacy kek life-time 300
 cable privacy tek life-time 180
 no keepalive
!
interface Cable8/0/1
 ip address 10.10.11.121
 cable bundle 2
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
```

```
 cable upstream max-ports 6
 cable upstream 0 connector 4
 cable upstream 0 spectrum-group 2
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 data-backoff 0 6
 cable upstream 0 modulation-profile 23 21
 no cable upstream 0 rate-limit
 cable upstream 0 shutdown
 cable upstream 1 connector 5
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 6
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 7
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
 cable upstream 4 channel-width 1600000
 cable upstream 4 minislot-size 4
 cable upstream 4 modulation-profile 21
 cable upstream 4 shutdown
 cable upstream 5 channel-width 1600000
 cable upstream 5 minislot-size 4
 cable upstream 5 modulation-profile 21
 cable upstream 5 shutdown
 cable source-verify
 cable privacy kek life-time 300
 cable privacy tek life-time 180
 no keepalive
!
!
ip classless
ip http server
no ip http secure-server
!
!
no cdp run
snmp-server community public RW
snmp-server community private RW
snmp-server enable traps cable
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password my-telnet-password
 login
 length 0
!
end
```

Additional References

For additional information related to DOCSIS 1.1 operations, refer to the following references:

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DOCSIS 1.1 for Cisco CMTS Routers

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 8: Feature Information for DOCSIS 1.1 for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
DOCSIS 1.1 for the Cisco CMTS Routers	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on Cisco cBR Series Converged Broadband Routers.