Cisco CMTS Router Layer 3 and Bundle Interface Features Configuration Guide

First Published: 2008-02-11

Last Modified: 2016-01-28

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-27609-04

CONTENTS

CHAPTER 1

DOCSIS 3.0 Multicast Support on the CMTS Routers

First Published: December 18, 2008

Last Updated: May 27, 2013

Cisco IOS Release 12.2(33)SCB introduces multicast improvements based on Data-over-Cable Service Interface Specifications (DOCSIS) 3.0 for the Cisco cable modem termination system (CMTS) routers. DOCSIS 3.0 multicast support improves bandwidth efficiency and allows service providers to offer differentiated quality of service for different types of traffic.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for the DOCSIS 3.0 Multicast Support

- DOCSIS 3.0-compliant Cisco CMTS and DOCSIS 3.0-enabled cable modems are required.
- Cisco CMTS must be MDF-enabled by default.
- Quality of service (QoS) parameters must be configured for various multicast sessions.
- Multicast Baseline Privacy Interface Plus (BPI+) profile must be configured before adding a Multicast BPI+ profile to a Multicast BPI+ multicast group.

Table below shows the Cisco CMTS hardware compatibility prerequisites for this feature.

Table 1: DOCSIS 3.0 Multicast Support Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCC and later releases** • PRE2 • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	**Cisco IOS Release 12.2(33)SCC and later releases** • Cisco UBR-MC20X20V[1] **Cisco IOS Release 12.2(33)SCE and later releases** • Cisco UBR-MC3GX60V[2]
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCB and later releases** • NPE-G2	**Cisco IOS Release 12.2(33)SCD and later releases** • Cisco uBR-MC88V[3]
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCB and later releases** • NPE-G2	**Cisco IOS Release 12.2(33)SCD and later releases** • Cisco uBR-MC88V

[1] The Cisco UBR-MC20X20V cable interface line card has three variants: Cisco UBR-MC20X20V-0D, Cisco UBR-MC20X20V-5D, and Cisco UBR-MC20X20V-20D. The Cisco UBR-MC20X20V-0D line card supports 20 upstreams and zero (no) downstreams. The Cisco UBR-MC20X20V-5D line card supports 20 upstreams and 5 downstreams, and the Cisco UBR-MC20X20V-20D line card supports 20 upstreams and 20 downstreams.

[2] The Cisco uBR-MC3GX60V line card is not compatible with PRE2.

[3] The Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Restrictions for the DOCSIS 3.0 Multicast Support

- You cannot disable explicit tracking.

- For multicast QoS, you must define three objects and templates, Service-Class, Group-QoS-Config (GQC), and Group-Config, and associate them to a particular bundle or forwarding interface.
- You must define a default service class and GQC before defining objects and templates.
- Multicast authorization is disabled by default and you should enable and configure it properly.
- Static multicast feature is always enabled and you cannot disable it.
- The service flow attribute-based selection will be ignored if the group configuration is configured on the default forwarding interface.
- A profile group cannot be deleted when it is applied to any forwarding or bundle interface. However, the same restriction does not apply to the global profile group. A global profile group can be deleted even when it is assigned to a forwarding or bundle interface.
- The multicast DSID feature is supported only on DOCSIS 3.0-compliant cable modems.
- The cable multicast mdf-disable wb-incapable-cm command disables multicast downstream service identifier (DSID) forwarding capability on the cable modem, which impacts the DSID capability between the Cisco CMTS and the cable modem.
- The multicast traffic to CPE increases two-fold after changing the multicast QoS configuration or the service-flow attribute during an active session. The traffic replication will continue till the default session timeout period (180 seconds). After the session timeout, the multicast DSID is removed from both Cisco CMTS and CM, and normal multicast traffic flow is resumed.
- For the DOCSIS 3.0 Multicast support feature to function properly, the CPE and the CM must be in the same virtual routing and forwarding (VRF) interface.

Information About the DOCSIS 3.0 Multicast Support

IP multicast, an integral technology in networked applications, is the transmission of the same information to multiple recipients. Any network application, including cable networks, can benefit from the bandwidth efficiency of multicast technology. Two new technologies—Channel Bonding and Single Source Multicast (SSM)—are expected to dramatically accelerate multicast deployment.

The channel bonding and SSM technologies dramatically increase the operational efficiency of the existing hybrid fiber-coaxial (HFC) network. Using the multicast improvements, the cable operators can seamlessly deliver advanced services like video on demand (VoD), internet protocol television (IPTV), and facilitate interactive video and audio, and data services.

The following sections explain the benefits of DOCSIS 3.0 Multicast Support:

Multicast DSID Forwarding

DOCSIS 3.0 multicast support introduces centralized control at the Cisco CMTS to provide flexibility and scalability to support a large array of multicast protocols. It replaces the Internet Group Management Protocol (IGMP), version 2 snooping infrastructure, which was part of the DOCSIS 1.1 and 2.0 models. Now, the Cisco CMTS allocates an unique Downstream Service Identifier (DSID) to identify every multicast stream. These DSIDs are sent to the CMs that use these DSIDs to filter and forward Multicast traffic to the CPEs.

The multicast DSID forwarding (MDF) provides the following benefits:

- Unique identification of packet stream across bonding group within a MAC domain.

- Designation of packet stream as either Any Source Multicast (ASM) or Source Specific Multicast (SSM) per multicast channel.
- Implementation of multicast DSID management on the Route Processor (RP) makes it operate on a standalone basis.
- Snooping of all upstream signal control packets by the Cisco CMTS to find the customer premises equipment (CPE) on the Multicast DSID-based Forwarding (MDF) enabled CM and allocates DSID from the pool.
- Transmission of allocated DSIDs to the CM through Dynamic Bonding Change (DBC) message.
- Reuse of DSIDs on other MDF-enabled CMs in the same bonding group, joining the multicast session.
- Removal of DSIDs from the CM through a DBC message by the Cisco CMTS after a multicast session leave event.
- Release of DSID to the pool by the Cisco CMTS when the last member leaves the bonding group.
- The following DSIDs are preallocated for each primary downstream (modular and integrated cable interfaces) to forward general query messages. These DSIDs form part of the multicast group signaling protocol. Other multicast groups, do no use these DSIDs.
    - IGMPv2 general query (IPv4)
    - IGMPv3 general query (IPv4)
    - MLDv1 general query (IPv6)
    - MLDv2 general query (IPv6)
    - Preregistration of DSID (IPv6)
- Allocation of DSID ensures traffic segregation between virtual private networks (VPNs) for DOCSIS 3.0 MDF-enabled CMs. For example, two clients from two VPNs joining the same multicast will get two distinct DSIDs.

Multicast Forwarding on Bonded CM

Multicast packets to the DOCSIS 3.0-enabled CMs are transmitted as bonded packets with DSID extension header on the primary bonding group if the Secondary Multicast Bonding Group is disabled. Multicast packets for MDF-disabled or pre-DOCSIS 3.0 CMs are transmitted as non-bonded without DSID extension header. For more information on this feature, refer to Multicast Secondary Bonding Group, on page 9.

In a network, where only MDF-enabled or MDF-disabled CMs exist, the traffic is segregated using field types. The MDF-enabled CM forwards the frame with the field type and the MDF-disabled CM drops it. The DSID labeling ensures that MDF-enabled CM gets a copy of the multicast session to prevent “cross talk”.

For hybrid CMs (MDF-enabled and MDF-disabled CMs) that do not support field type forwarding, you should configure per session encryption or security association identifier (SAID) isolation to ensure traffic segregation. DOCSIS 3.0 mandates that if the hybrid CM fails to forward field type frames, the Cisco CMTS should employ multicast security association identifier (MSAID) isolation. This isolation is achieved by assigning different MSAID to each replication, one to bonded CM and another to the non-bonded or hybrid CM. This helps to prevent CMs from receiving duplicate traffic.

Static TLV Forwarding

As per DOCSIS 3.0 specifications, the Cisco CMTS must support Static Multicast. When the CM tries to register with the Cisco CMTS, the Cisco CMTS checks whether Static Multicast Encoding is present in the CM configuration file. If the Static Multicast Encoding is present, the Cisco CMTS sends a DSID corresponding to each Static Multicast channel in the Registration-Response (REG-RSP) message.

The Multicast DSID management is located at RP and the cable line card (CLC) has to contact the RP for proper DSID assignment. The CLC also caches the response from RP to eliminate the need to communicate to the RP for subsequent Static Multicast encoding. Refer BPI+ Support, on page 5 for more details on SAID assignment for Static Multicast functionality.

IPv6 Multicast

The Cisco CMTS routers support both IPv4 and IPv6 protocol stacks. The basic multicast character of IPv6 is similar to that of IPv4 multicast. Multicast in IPv6 can be either a Multicast Listener Discovery (MLD), version 1 that supports ASM or MLDv2 that supports SSM. DOCSIS 3.0 specifications demand support for both MLDv1 and MLDv2.

The MLD component uses the protocol descriptor block (PDB) for the multicast. The PDB contains all information about the session, including source, group, and number of sources. IPv6 mandates that all information, such as source MAC and Cisco CMTS service identifier (SID), should be accessed from the PDB. The packet header in IPv6 contains the correct forwarding interface and DSID information. When the packet arrives at the Cisco CMTS, it is identified as an IPv6 packet and sent to the correct bundle.

For more details on IPv6, refer to the IPv6 on Cable document available at the following location: http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_ipv6.html

Explicit Tracking

The Cisco CMTS can perform explicit tracking with IGMPv3 support. The IGMPv3 removes the report suppression feature associated with the IGMPv2 specification enabling the Cisco CMTS to get the complete information on session and host information. This benefits the IGMP Fast Leave processing and DSID management for each CM.

A host or session database is used to track hosts (IP/MAC) joining a particular multicast session. From the host, you can track the CM based on the SID and cable downstream interface. This database also helps to determine whether the Cisco CMTS should remove the DSID from a particular CM when the multicast session is over.

BPI+ Support

The DOCSIS Baseline Privacy Interface (BPI) feature is based on the DOCSIS BPI Specification (SP-BPI-I02-990319 or later revision). It provides data privacy across the HFC network by encrypting traffic flows between the router and the cable operator's CMTS.

The BPI+ (BPI Plus) feature is an enhancement to the BPI feature and is based on the DOCSIS BPI+ Specification (SP-BPI+-I04-000407 or later revision). In addition to the regular BPI features, BPI+ provides more secure authentication of cable modems through the use of digital certificates. Also, a cable modem can use a digital signature to verify that the software image it has downloaded has not been altered or corrupted in transit.

Dynamic Multicast Encryption

The Cisco CMTS encrypts downstream multicast traffic to the CMs with a security association (SA), which is previously signaled to the CM. The security association identifier is defined per session and communicated in a SA encoding through the MAC management message sent to the CM. The Cisco CMTS uses dynamic SA mechanism for DSID multicast forwarding in MDF-disabled CMs.

During a dynamic multicast join event, through IGMP or Multicast Listener Discovery (MLD), the Cisco CMTS checks the configuration table to see whether the session must be encrypted. If it requires encryption, the Cisco CMTS creates a multicast security association identifier (MSAID) and includes it in SA encoding with an add action in the Dynamic Bonding Change Request (DBC-REQ).

Static Multicast Encryption

During a static multicast encoding of Registration Request (REG-REQ), Cisco CMTS checks the configuration table at the RP through the Inter-Process Communication (IPC) to ascertain the need for encryption. If it requires encryption, the Cisco CMTS creates an MSAID and includes it in the SA encoding with an add action in the REG-RSP. The cable line card (CLC) can also cache the MSAID mapping for subsequent requests.

Multicast Join Authorization

DOCSIS 3.0 introduces the IP Multicast Join Authorization feature to control the IP multicast sessions joined by the IP multicast clients. The set of IP multicast clients reached through the CM includes the CM IP host stack itself. This feature controls only the joining of downstream IP multicast sessions and not the ability of any client to transmit IP multicast traffic upstream.

General guidelines for multicast join authorization are as follows:

- Cisco CMTS should authorize the IP multicast sessions joined by the IP multicast clients.
- IPv6 solicited node multicast sessions should be routed to IPv6 addresses through the Source Address Verification (SAV) feature.
- IP multicast sessions identified by static IP multicast encoding should be in the registration request of the CM.
- IPv6 or IPv4 multicast sessions which map to Layer 2 Ethernet multicast MAC address should be identified using the static multicast MAC address encoding in the registration request of the CM.
- For an IP multicast session, the CM should have a “permit” action for the highest priority matching rule “IP Multicast Join Authorization Session.”
- When the management object “Default IP Multicast Join Authorization Action” is set to “permit”, the IP multicast session should not match any “IP Multicast Join Authorization” rule.

With the above guidelines, static MAC multicast and static IP multicast are authorized by default. The Cisco CMTS enforces IP multicast join authorization by signaling or not signaling multicast DSIDs and /or SAs. For a pre-DOCSIS 3.0 CM, multicast BPI+ must be used.

The cable multicast auth enable default-action command is used to enable or disable Multicast Join Authorization feature.

Multicast Session Limits

DOCSIS 3.0 supports per CM multicast session where you can configure Multicast Session Encoding in the CM configuration file as specified in the DOCSIS 3.0 specifications.

The Cisco CMTS receives the encoding of REG-REQ from the CLC and the CLC would notify the Route Processor through Inter-Process Communication about CM registration.

The Cisco CMTS supports a session limit between 0 and 65535 per CM. If the CM does not include encoding, the Cisco CMTS uses the default Maximum Multicast Sessions. The multicast session limit only enforces the dynamic join session and does not restrict Static Multicast sessions.

IP Multicast Profile

In an IP multicast profile, the Cisco CMTS provides the capability to store 16 profiles, each with 256 session rules. Each session rule consists of the Source prefix, Group prefix, Priority, and “Permit” or “Deny” action. The rule priority is used to determine the best matching rule.

The CM can store up to 16 IP multicast profiles and the Cisco CMTS makes use of them to configure a multicast profile for the CM. If the CM does not have any IP multicast profile defined, the Cisco CMTS uses the Default IP multicast profile name. If the IP multicast profile defined in the CM configuration file is not available in the Cisco CMTS, an empty multicast profile with the same name is created by the Cisco CMTS, which can be configured later by the operator.

If the join request of a CM to a multicast session does not match any of the session rules, the Cisco CMTS uses the default IP multicast join authorization action, which can be either “Permit” or “Deny.” When the session rules are changed, the Cisco CMTS reapplies the latest rules on all subsequent join requests.

Default Multicast Authorization Profiles

Cisco IOS Release 12.2(33)SCC introduces the option to create default multicast authorization profiles. These profiles are used to register modems without an authorization profile in their configuration file. Like other profiles, the default profile group can store up to 16 default multicast authorization profiles. The default profile group also maintains a sorted list of session rules from all default profiles, based on priority. Each configured default profile can store up to 256 session rules.

The session rules are used to authorize modems without a profile name in their configuration file. When an IGMP join for a group is received from such a modem, it is matched against the rules in the default profile group. If the rules match, the join action is permitted, else the globally configured default action is taken.

When a session rule is created, the Cisco CMTS assigns an ID to that rule. These session rule IDs are assigned sequentially and are unique per profile. If there are 5 session rules in a profile, they are assigned IDs ranging from 0 to 4. If a session rule is deleted, the next rule in the profile is assigned with that ID. For example, when a session rule with ID 3 is deleted, the next rule in the profile will be assigned ID 3.

The DOCSIS 3.0 operations support system (OSS) specification mandates that the session rules have to be identified within a profile using an identifier value that has a range of 1 to 4,294,967,295 (32 bit).

The **cable multicast auth profile-name** command is used to define a cable multicast authorization profile and to set it as the default profile.

MDF-Disabled CM

To enforce multicast authorization in MDF-disabled and pre-DOCSIS 3.0 CMs, the Cisco CMTS should configure per-session encryption based on Security Association-Multicast Authorization Profile (SA-MAP) authorization. The Cisco CMTS should check the SA-MAP request against the multicast authorization profile of the CM to verify if it is an authorized flow and reply with a SAID accordingly.

Multicast Quality of Service Enhancement

DOCSIS 3.0 mandates that the CMTS should not admit any flow exceeding the session limit. Though the current Multicast QoS (MQoS) session limit admits the session, it fails to provide any QoS for sessions exceeding the session limit.

Note Multicast packets are sent using the default Group Service Flows (GSF) when the Multicast QoS feature is disabled.

As part of DOCSIS 3.0 requirements for Multicast QoS, Cisco IOS Release 12.2(33)SCC provides support for Group Classifier Rules (GCR). The Cisco CMTS determines the set of Group Configurations (GCs) whose session range matches the multicast group address. For SSM, the source address is also used to identify the matching GCs. A GCR is created for each matching GC and linked to the multicast session. The GCR is assigned also with an unique identifier, SAID, and Group Service Flow (GSF).

The following conditions are used to select the GC entries:

- The GC entry with the highest rule priority is selected, if more than one GC entry matches.
- All matching GC entries are selected, when multiple GCs have the same highest rule priority.

The GCR classification is done based on type of service (TOS) fields. The TOS specifier in the GCR is used to choose the correct GCR when multiple GCRs match a single multicast session.

Note When two multicast group configurations (GCs) have the same session range and configuration (under global or bundle configuration), then the same forwarding interface selection is not guaranteed.

Non-IP multicasts and broadcast packets use GSF. They are similar to individual service flows and are shared by all the CMs on a particular Digital Command Signal (DCS) matching the same GCR. A single GSF is used for multicast sessions matching different GCs using the same aggregate GQC.

The legacy multicast QoS **cable match address** command is replaced from Cisco IOS Release 12.2(33)SCB onwards to allow multiple system operators (MSOs) to move to the new multicast QoS model. The old command is automatically translated to the new command during system bootup while parsing the startup configuration. After system configuration, the old command is disabled from the parser chain.

For details on DOCSIS QoS support, refer to the DOCSIS QoS Support section of the DOCSIS WFQ Scheduler on the Cisco CMTS Routers guide.

Multicast Secondary Bonding Group

The DOCSIS 3.0-compliant CM can receive multicast packets from non-primary (or bonded) channels using the MDF support at the CMTS.

The multicast secondary bonding group is defined as a shared bonding group or RF channel that feeds more than one fiber node through an optical split. This allows CMs from different primary bonding groups and channels to listen to one or more shared sets. The multicast packets are replicated only to the shared downstream channel set, which helps conserve the downstream bandwidth.

DOCSIS 3.0 defines attribute-based service flow creation, which allows the Cisco CMTS to make more “intelligent” decisions on the selection of bonding group or individual channel for unicast and multicast forwarding.

The Multicast Secondary Bonding Group provides the following benefits:

- New MQoS and attribute-based forwarding for Multicast Secondary Bonding Group.
- The primary downstream interface acts as a forwarding interface for narrowband CMs.
- The following algorithm is used to select a forwarding interface for wideband CMs:
    - A primary bonding group is selected if a group-config matching the session is present in it. MQoS parameters are taken from the group-config.
    - A primary bonding group is selected if a group-config is not present at the bundle level or at the global level.
    - A group-config found at the bundle level or global level is used to find the Group-QoS-Config (GQC) and eventually the attribute and forbidden bit-masks, which are then used to find the interface.
    - All Wideband Cable Modems (WCMs) in a bundle use the same secondary bonding group if a bundle-level group-config or global-level group-config is configured.
- The IGMP report ignores a source if the given source address fails to find a matching interface.
    - If a matching interface is found, that interface is used for forwarding and the MQoS parameters are taken from the matching group-config from the forwarding interface or bundle interface or global level.
    - If a matching interface is not found, then the IGMP report is ignored.
- For a static join, attribute-based forwarding is not supported, and only the primary downstream is used.

Multicast Replication Session Cache

Cisco IOS Release 12.2(33)SCH introduces the multicast replication session cache feature to improve CPU utilization on the Cisco uBR10012 router. In Cisco IOS releases before Cisco IOS Release 12.2(33)SCH, the Cisco uBR10012 router supported multicast replication session creation and deletion, and IGMP leave and join operations of existing multicast replication sessions. By caching the existing multicast replication sessions and reusing them when an IGMP join is received and matched, the CPU performance of the Cisco uBR10012 router improves.

This feature is supported for dynamic IPv4 group join operations on single type multicast sessions. When a new IGMP join is received, the session cache is searched for an existing replication session. If a match is found, the session is reused.

Note The multicast replication session cache is *not* supported for IPv6 multicast sessions and aggregate multicast sessions.

The multicast replication session cache can be configured globally for all the interfaces on the Cisco uBR10012 router or can be configured at the interface level for the forwarding interface. The cache size value can be configured using the **cable multicast ses-cache** command.

The **clear cable multicast cache ses-cache** command clears the multicast cache counters on the forwarding interface as well as the cached entry. The **show cable multicast ses-cache** command displays the multicast replication session information, both at the global level and the interface level.

The multicast replication cache session is enabled only on the active RP and not on the standby RP.

Load Balancing

The Load Balancing feature modified in Cisco IOS Release 12.2(33)SCB will not load balance a CM while a multicast stream is going on for that particular CM. It utilizes the Explicit Tracking Database, which holds complete information on the CM subscription to achieve this. For more information on Load Balancing, refer to the Configuring Load Balancing and Dynamic Channel Change on the Cisco CMTS Routers document.

Bonded DS Admission Control

Multiple MAC domains may share a single DS bonding group. Similarly, CPEs from multiple MAC domains could listen to a Wideband multicast service flow. The devices could join or leave the multicast group in any order.

The bonded multicast service flows are admitted and created on the Guardian line card rather than on a specific host line card.

The admission control for Wideband DS interfaces should also take into account the multicast service flow bandwidth usage. The entire DS bonding group bandwidth is available for every single MAC domain and the multicast traffic for committed information rate (CIR) reservations is based on the current CIR bandwidth usage of the sharing MAC domains.

The aggregate use of CIR bandwidth is limited by the bonding group definition. However, a single MAC domain could reserve the entire bandwidth if other MAC domains are not using it for CIR purposes.

The following criteria is used for DS bonding group bandwidth distribution:

- The Guardian line card can use 50 percent of the available bandwidth for multicast. The rest of the bandwidth is equally distributed to other MAC domain hosts sharing the bonding group.
- If any of the MAC domain or Guardian line card exceeds 90 percent of the bandwidth reservation of the entire bonding group, the remaining bandwidth is given to the same MAC domain or Guardian line card to effectively utilize the small unusable fragments.

When the number of MAC domains sharing the DS bonding group increases, the available bandwidth decreases proportionally. It also limits the service flow CIR that can be admitted on the Guardian line card or MAC domain host.

Based on the example given in Table below, three MAC domain hosts are sharing a DS bonded interface with 60 Mbps bandwidth. Initially, the Guardian line card is getting 30 Mbps and the other MAC domain hosts are getting 10 Mbps each. If the multicast usage goes up by 30 Mbps, the available bandwidth will be 60 – 30 = 30 Mbps. This new bandwidth will be shared between the Guardian line card and MAC domain hosts. Now, the Guardian line card would get 15 Mbps and the MAC domains would get 5 Mbps each. This limits the highest CIR service flow that can be admitted to MAC domain hosts to 5 Mbps, although the available bandwidth is still 30 Mbps. If any of the MAC domain hosts keeps admitting service flows much smaller (for example, 100 Kbps) compared to 5 Mbps, it could reserve close to 30 Mbps provided the service flow admission is spaced apart by 3 seconds.

Table 2: Sharing a DS Bonded Interface Between Guardian Line Card and Three MAC Domains

WB Interface Bandwidth		**Guardian Bandwidth**		**MAC Domain Host 1 Bandwidth**		**MAC Domain Host 2 Bandwidth**		**MAC Domain Host 3 Bandwidth**	
Available	**Reserved**	**Available**	**Reserved**	**Available**	**Reserved**	**Available**	**Reserved**	**Available**	**Reserved**
60	0	30	0	10	0	10	0	10	0
30	30	15	30	5	0	5	0	5	0
0.6	59.4	0.3	30	0.1	29.4	0.1	0	0.1	0

Multicast DSID Forwarding Disabled Mode

For any application that needs the cable modem to perform IGMP snooping, the MDF on the cable modem must be disabled. Cable modems registered in MDF-enabled mode by the Cisco CMTS do not perform IGMP snooping because MDF forwarding is based on DSID filtering. In Cisco IOS Release 12.2(33)SCD3, the **cable multicast mdf-disable** command is introduced in global configuration mode to disable the MDF capability on the cable modem.

This command is configured on the route processor and is downloaded to the cable line card via the configuration update. The configuration does not change the Cisco CMTS forwarding mechanism or DSID allocation. The Cisco CMTS allocates the DSID and the multicast packet is encapsulated with the DSID header. This does not affect traffic forwarding on the MDF-disabled cable modem. According to DOCSIS3.0 specification, pre-DOCSIS2.0 or MDF-disabled cable modems ignore the DSID header and continue multicast forwarding based on the Group Media Access Control (GMAC) from IGMP snooping. When the cable modem runs in MDF-disabled mode, only IGMPv2 is supported and the Cisco CMTS drops IGMPv3 and MLD messages.

Multicast encryption based on BPI+ is not supported on non-MDF cable modems, if IGMP SSM mapping is used. A non-MDF cable modem is either a pre-DOCSIS 3.0 cable modem or a DOCSIS 3.0 cable modem running in MDF-disabled mode.

MDF1 Support for DOCSIS 2.0 Hybrid Cable Modems

Starting with Cisco IOS Release 12.2(33)SCE4, the Cisco CMTS router enables MDF capability for DOCSIS 2.0 hybrid cable modems, IPv6, and other cable modems that advertise MDF capability to allow IPv6 packet forwarding. In earlier releases, MDF capability was disabled for wideband incapable cable modems and cable modems that were not DOCSIS 3.0-compliant. The **wb-incapable-cm** keyword was added to the cable multicast mdf-disable command to disable MDF on all DOCSIS 2.0 hybrid cable modems including DOCSIS Set-Top Gateway (DSG) hybrid embedded cable modems to support IGMP snooping.

DSG Disablement for Hybrid STBs

In Cisco IOS Release 12.2(33)SCE4 and later, the **cable multicast mdf-disable** command with the wb-incapable-cm keyword prevents all DOCSIS 2.0 DSG embedded cable modems from receiving DSG multicast traffic besides disabling MDF support. In Cisco IOS Release 12.2(33)SCF2, the wb-incapable-cm keyword was modified to supersede the restriction on DSG multicast traffic.

In Cisco IOS Release 12.2(33)SCF2 and later, the wb-incapable-cm keyword disables MDF capability only on non-DSG DOCSIS 2.0 hybrid cable modems. To disable MDF capability on all DSG embedded cable modems (DOCSIS 3.0 DSG and DOCSIS 2.0 DSG hybrid), a new keyword, DSG, was introduced in Cisco IOS Release 12.2(33)SCF2.

Note After disabling MDF capability, you must run **clear cable modem reset** command to bring all DSG embedded cable modems online.

Table below provides details of the cable multicast mdf-disable command behavior in Cisco IOS Release 12.2(33)SCF2 and later.

Table 3: cable multicast mdf-disable Command Behavior in Cisco IOS Release 12.2(33)SCF2

Command	Behavior
cable multicast mdf-disable	Disables MDF capability of all cable modems connected to the Cisco CMTS router.
cable multicast mdf-disable wb-incapable-cm	Disables MDF capability of all non-DSG DOCSIS 2.0 hybrid cable modems.
cable multicast mdf-disable dsg	Disables MDF capability of all DSG embedded cable modems, including DOCSIS 3.0 DSG and DOCSIS 2.0 DSG hybrid modems.

Benefits of MDF1 Support

- Supports IPv6 on different known cable modem firmware types.
- Disables the MDF capability on the Cisco CMTS.
- Supports In-Service Software Upgrade (ISSU) and line card high availability.

How to Configure the DOCSIS 3.0 Multicast Support

This section describes the following tasks that are required to implement DOCSIS 3.0 Multicast Support on Cisco CMTS Routers:

Configuring Basic Multicast Forwarding

To configure a basic multicast forwarding profile that can be applied to a DOCSIS 3.0 multicast configuration, use the **ip multicast-routing** command. You must configure a multicast routing profile before you can proceed with a multicast group.

DETAILED STEPS

	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`	Enters global configuration mode.
Step 3	**IP multicast-routing** [**vrf**] **Example:** `Router(config)# IP multicast-routing vrf`	Enables multicast routing globally or on a particular virtual routing and forwarding (VRF) interface. • *vrf* —(Optional) Specifies the name of the VRF instance.
Step 4	**interface bundle** *number* **Example:** `Router(config)# interface bundle 1`	Configures the interface bundle and enters interface configuration mode. • *number*—Bundle interface number. The valid range is from 1 to 255.
Step 5	**IP pim sparse-mode** **Example:** `Router(config-if)# IP pim sparse-mode`	Configures sparse mode of operation. **Note** In Cisco IOS Release 12.2(33)SCA and later releases, a Cisco CMTS router must have a Protocol Independent Multicast (PIM) rendezvous point (RP) configured for the PIM sparse mode. The RP is configured using the ip pim rp-address command or Auto-RP configuration protocol.

	Command or Action	Purpose
Step 6	**IP pim sparse-dense-mode** **Example:** `Router(config-if)# IP pim sparse-dense-mode`	Configures the interface for either sparse mode or dense mode of operation, depending on the mode in which the multicast group is operating.
Step 7	**IP igmp version version-number** **Example:** `Router(config-if)# IP igmp version 3`	Configures the interface to use IGMP version 3. • *version-number* —IGMP version number used on the router.

Configuring Multicast DSID Forwarding

The multicast DSID forwarding is enabled by default. You cannot configure this feature.

Configuring Explicit Tracking

The Explicit Tracking feature is enabled by default. You cannot configure it.

Configuring Multicast QoS

To configure a Multicast QoS profile that can be applied to a DOCSIS 3.0 configuration, use the **cable multicast group-qos** command. You must configure a Multicast QoS profile before you can add a Multicast QoS profile to a QoS multicast group.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable service class** *class-index* **name** *service-class-name*	Configures the name of the cable service class.

	Command or Action	Purpose
	Example: `Router(config)# cable service class 1 name MQOS_DEFAULT`	• *class-index* —Class ID for the class to be modified. Valid range is from 1 to 255. • *service-class-name*—Service class name.
Step 4	**cable service class** *class-index* **downstream** **Example:** `Router(config)# cable service class 1 downstream`	Configures the downstream for the cable service class.
Step 5	**cable service class** *class-index* **max-rate** *maximum-bandwidth-allowed* **Example:** `Router(config)# cable service class 1 max-rate 10000000`	Configures the maximum allowed bandwidth for the cable service class.
Step 6	**cable service class** *class-index* **min-rate** *cir* **Example:** `Router(config)# cable service class 1 min-rate 1000000`	Configures the minimum committed information rate for the cable service class.
Step 7	**cable multicast group-qos default scn** *service-class-name* **aggregate** **Example:** `Router(config)# cable multicast group-qos default scn MQOS_DEFAULT aggregate`	Specifies the default service class name for the QoS profile. • *default*—Specifies the default QoS profile number for the cable multicast QoS group. • *service class name*—Service class name for the QoS profile.
Step 8	**cable multicast qos group** *number* **priority** *value* **Example:** `Router(config)# cable multicast qos group 20 priority 1`	Configures a multicast QoS group and enters multicast QoS configuration mode, and specifies the priority of the cable multicast QoS group. • *number*—QoS profile number for the cable multicast QoS group. The valid range is from 1 to 255. • *value*—Cable multicast QoS group priority. The valid range is from 1 to 255.
Step 9	**application-id** *app-id* **Example:** `Router(config-mqos)# application-id 10`	Specifies the application identification number of the multicast QoS group. This value is configured to enable admission control to the multicast QoS group. The valid range is from 1 to 65535.

	Command or Action	Purpose
Step 10	**session-range ip-address ip-mask** **Example:** `Router(config-mqos)# session-range 230.0.0.0 255.0.0.0`	Specifies the session range IP address and IP mask of the multicast QoS group. You can configure multiple session ranges.
Step 11	**tos** *tos-value-low tos-value-high tos-mask* **Example:** `Router(config-mqos)# tos 1 6 15`	Specifies the minimum type of service (ToS) data bytes, maximum ToS data bytes, and mask for a multicast QoS group. The valid range for each is from 0 to 255. • *tos-value-low*—MQoS Group ToS low value. • *tos-value-high*—MQoS Group ToS high value. • *tos-mask*—MQoS Group ToS mask value.
Step 12	**cable multicast qos group** *number priority value* [**global**] **Example:** `Router(config)#cable multicast qos group 20 priority 63 global`	Specifies the multicast QoS group identifier. • *number*—Cable multicast QoS group number. The valid range is from 1 to 255. • *priority value*—Specifies the priority of the cable multicast QoS group. The valid range is from 1 to 255. • **global**—(Optional) Specifies that the multicast QoS group configuration is applied to all cable interfaces.

Configuring a Multicast BPI+ Support

To configure a multicast BPI+ profile that can be applied to a QoS group configuration, use the **cable multicast qos group** command.

DETAILED STEPS

	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`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	**cable multicast group-encryption** *number* **algorithm** {**128bit-aes** | **40bit-des** | **56bit-des**}
	Example:
	`Router(config)# cable multicast group-encryption 30 algorithm 56bit-des`
		Configures a group encryption profile.
		• *number*—Number of a specific cable multicast QoS group encryption profile. The valid range is from 1 to 255.
		• **algorithm**—Specifies that the data encryption standard (DES) as either 128, 56 or 40 bits.

Step 4	**cable multicast qos group** *gc-id* priority value [global] **Example:** `Router(config)# cable multicast qos group 20 priority 63 global`	Configures a multicast QoS group and enters multicast QoS configuration mode. • *gc-id* —Cable multicast QoS group number. The valid range is from 1 to 255. • *priority value*—Specifies the priority of the cable multicast QoS group. The valid range is from 1 to 255. • *global* —(Optional) Specifies that the multicast QoS group configuration is applied to all cable interfaces.
Step 5	**session-range ip-address ip-mask** **Example:** `Router(config-mqos)# session-range 230.0.0.0 255.0.0.0`	Specifies the session range IP address and IP mask of the multicast QoS group. You can configure multiple session ranges.
Step 6	**group-encryption** *group-encrypt-id* **Example:** `Router(config-mqos)# group-encryption 30`	Specifies a group encryption number.

Configuring a Multicast Join Authorization

To configure a multicast join authorization to control the IP multicast sessions joined by the IP multicast clients, use the **cable multicast authorization** command.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable multicast auth enable default-action** { *permit* | *deny* } **max-sessions** *limit* **Example:** `Router(config)#` **`cable multicast auth enable default-action deny max-sessions 10`**	Enables multicast authorization and sets the maximum sessions limit. • *permit* —Enables multicast authorization by default. • *deny* —Denies multicast authorization by default. • *limit* —Maximum number of dynamic multicast sessions allowed per CM. Maximum value allowed is 65535.
Step 4	**cable multicast auth profile-name** *profile-name* [**default**] **Example:** `Router(config-mauth)#` **`cable multicast auth profile-name GOLD default`**	Configures the multicast authorization profile, and (optionally) sets it as the default profile. • *profile-name* —Name of the authorization profile to be used. • *default* —Specifies that the profile name should be treated as the default profile.

Step 5	**match rule** { *ipv4* | *ipv6* } *source-prefix group-prefix priority-value* {*permit* | *deny* }
	Example:
	`Router(config-mauth)#` **`match rule ipv4 source 0.0.0.0/0 230.0.0.0/16 128 permit`**
		Configures the match rule, rule priority, and its related action.
		• *ipv4*—Matching IPv4 group address or prefix length (for example, 224.1.1.1/16).
		• *ipv6*—Matching IPv6 group address or prefix length (for example, FEDC:BA98:7654:3210::/<prefix-length>).
		• *source-prefix* —Matching source address prefix.
		• *group-prefix* —Matching group address prefix.
		• *priority-value* —Cable multicast authorization profile priority.
		• *permit* —Specifies whether to allow specified packets to be forwarded.
		• *deny* —Specifies whether to allow specified packets to be rejected.

Selecting a Forwarding Interface Based on Service Flow Attribute

The Service Flow Attribute feature allows a bonded CM to listen to multiple bonding groups, and using the interface-specific bit-masks, the CM can select the best route to receive multicast traffic.

Service Flow Attribute

The Service Flow Attribute feature allows selection of a forwarding interface based on the DOCSIS 3.0 construct named “service flow attribute mask.” Every interface has an attribute bit-mask depicting attributes of that interface. The multicast service class specified in the group QoS configuration contains required and forbidden attribute bit-masks. If a bonded CM can listen to multiple bonding groups (wideband interfaces), using specific bit-masks in the service class as well as on the bonding group, then one of these bonding groups can be selected for forwarding of multicast traffic.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable service class** *class-index* **Example:** `Router(config)# cable service class 10`	Configures the service class name. • *class-index* —Class index. Valid range is from 1 to 255.
Step 4	**cable service class** *class-index* **downstream** **Example:** `Router(config)# cable service class 10 downstream`	Configures the downstream for the selected service class. • *downstream* —Specifies the downstream for the service class.
Step 5	**cable service class** *class-index* **max-rate** *maximum-rate* **Example:** `Router(config)# cable service class 10 max-rate 1000000`	Configures the maximum rate for the selected service class. • *max-rate* —Configures the maximum rate for the service class. • *maximum-rate* —Maximum reserved rate. Valid range is from 0 to 4,294,967,295.
Step 6	**cable service class** *class-index* **min-rate** *minimum-rate* **Example:** `Router(config)#  cable service class 10 min-rate 100000`	Configures the minimum rate for the selected service class. • *min-rate* —Configures the minimum rate for the service class. • *minimum-rate* —Minimum reserved rate. Valid range is from 0 to 4,294,967,295.

	Command or Action	Purpose
Step 7	**cable service class** *class-index* **req-attr-mask** *required-attribute-mask* **Example:** `Router(config)# cable service class 10 req-attr-mask 8000000F`	Configures the required attribute mask for the selected service class. • *req-attr-mask* —Configures the required attribute mask for the service class. • *required-attribute-mask* —Required attribute mask value. Valid range is from 0 to FFFFFFFF.
Step 8	**cable service class** *class-index* **forb-attr-mask** *forbidden-attribute-mask* **Example:** `Router(config)# cable service class 10 forb-attr-mask 7FFFFFF0`	Configures the forbidden attribute mask for the selected service class name. • *forb-attr-mask* — Configures the forbidden attribute mask for the service class. • *forbidden-attribute-mask* —Forbidden attribute mask value. Valid range is from 0 to FFFFFFFF.
Step 9	**cable multicast group-qos** *number* **scn** *service-class-name* **aggregate** **Example:** `Router(config)# cable multicast group-qos 1 scn 10 mcast10 aggregate`	Configures the cable multicast group QoS identifier, service class name, and multicast value. • *number* —Cable multicast QoS group profile number. Valid range is from 1 to 255. • *scn* —Configures a service class name. • *service-class-name* —Service class name. • *aggregate* —Specifies aggregate service flow for sessions in the same MQoS group.
Step 10	**cable multicast qos group** *group* **priority** *priority* **Example:** `Router(config)# cable multicast qos group 1 priority 1`	Configures the cable MQoS group configuration on the bundle interface. • *group* —Cable MQoS group number. Valid range is from 1 to 255. • *priority priority* —Specifies the cable MQoS group priority.
Step 11	**session-range** *session-range mask* **group-qos** *qos* **Example:** `Router(config-mqos)# session-range 230.1.1.1 255.255.255.255 group-qos 1`	Enters MQoS configuration mode and specifies session range and group QoS. • *session-range session-range* —Configures the MQoS group session range. • *mask* —Session range group prefix mask. • *group-qos* —Specifies the MQoS group QoS identifier. • *qos* —MQoS group QoS number. Valid range is from 1 to 255.

	Command or Action	Purpose

Step 12	**interface bundle** *number* **ip address** *ip mask* **ip pim sparse-mode ip helper-address** *helper-address* **cable multicast qos group** *group*
	Example:
	`Router(config)#` **`interface Bundle1`**
	`ip address 40.1.1.1 255.255.255.0`
	`ip pim sparse-mode`
	`ip helper-address 2.39.16.1`
	`cable multicast-qos group 1`
		Configures the interface bundle with the IP address, helper address, and MQoS group.
		• *number* —Bundle interface number. Valid range is from 1 to 255.
		• *ip address* —Specifies the IP address range and mask.
		• *ip* —IP address range.
		• *mask* —IP address subnet mask.
		• *ip pim sparse-mode* —Enables PIM sparse mode operation.
		• *ip helper-addressv* —Specifies a destination address for UDP broadcasts.
		• *helper-address* —Destination IP address.

Step 13	**interface wideband-cable {slot/port |** *slot*/*subslot*/*bay*:*port-number}* **description cable rf-channel** *rf-channel* **bandwidth-percent** *percent-value* **cable bundle** *number* **cable bonding-group-id** *id-num* **cable rf-channel** *rf-port* **bandwidth-percent** *percent-value* **cable downstream attribute-mask attribute-***mask* **Example:** `Router(config)#` **`interface Wideband-Cable1/0/0:0`** **Example:** **`description cable rf-channel 0 bandwidth-percent 40`** **Example:** **`cable bundle 1`** **Example:** **`cable bonding-group-id 1`** **Example:** **`cable rf-channel 0 bandwidth-percent 10`** **Example:** **`cable rf-channel 1 bandwidth-percent 10`**	Selects the interface for forwarding based on the bit-masks specified in the service class and on the wideband interface. • On the Cisco uBR7246VXR router, the valid values are: ◦ slot—3 to 6 ◦ port—0 or 1 (depending on the cable interface) • On the Cisco uBR7225VXR router, the valid values are: ◦ slot—1 and 2 ◦ port—0 or 1 (depending on the cable interface) • On the Cisco uBR10012 router, the valid values are: ◦ slot—Wideband SPA interface processor (SIP) slot. Valid values are 1 to 3. ◦ subslot—Wideband SIP subslot. Valid value is 0. ◦ bay—Wideband SIP bay where the wideband shared port adapter (SPA) is located. Valid values are 0 (upper bay) and 1 (lower bay). • *rf-channel*—Specifies RF channel associated with the wideband interface. • *rf-channel*—RF channel number. • *bandwidth-percent*—Specifies the percentage of bandwidth from this RF channel that is reserved for the wideband interface.

	Command or Action	Purpose

	Example:
	`cable rf-channel 2 bandwidth-percent 10`
	Example:
	`cable downstream attribute-mask 8000FF00`
		• *percent-value*—Bandwidth percentage value.
		• *cable bundle*—Specifies the bundle number for bundling of cable interfaces.
		• *number*—Cable bundle number.
		• *cable bonding-group-id*—Specifies the cable interface bonding group.
		• *id-num*—Cable bonding group identifier.
		• *cable downstream attribute-mask*—Specifies the attribute mask for the downstream channel.
		• *attribute-mask*—Cable downstream interface attribute mask.

Step 14	**interface wideband-cable** {*slot*/*port* | *slot*/*subslot*/*bay*:*port-number*} **cable bundle** *number* **cable bonding-group-id** *id-num* **secondary**
	Example:
	cable rf-channel *rf-port* **bandwidth-percent** *percent-value* **cable downstream attribute-mask** [**attribute-***mask*]
	Example:
	`Router(config)# interface wideband-cable1/0/0:1`
	`cable bundle 1`
	`cable bonding-group-id 2 secondary`
	`cable rf-channel 0 bandwidth-percent 40`
	`cable downstream attribute-mask 8000FFF0`
		Selects the required attributes from the service class that match the interface attribute bit-mask.

Step 15	**interface wideband-cable** {*slot*/*port* | *slot*/*subslot*/*bay*:*port-number*} **cable bundle** *number* **cable bonding-group-id** *id-num* **secondary**
	Example:
	cable rf-channel *rf-port* **bandwidth-percent** *percent-value* **cable rf-channel** *rf-channel* **bandwidth-percent** *percent-value* **cable downstream attribute-mask** [*mask*]
	Example:
	`Router(config)# interface wideband-cable1/0/0:2`
	`cable bundle 1`
		Selects the required attributes from the service class that match the interface attribute bit-mask; and the forbidden attributes that do not match.

	Command or Action	Purpose

	`cable bonding-group-id 3 secondary`
	`cable rf-channel 1 bandwidth-percent 40`
	`cable rf-channel 2 bandwidth-percent 40`
	`cable downstream attribute-mask 8000000F`	

Configuring Multicast DSID Forwarding Disabled Mode

To disable MDF on the cable modem, use the **cable multicast mdf-disable** command in global configuration mode.

Note Multicast encryption based on BPI+ is not supported on non-MDF cable modems, if IGMP SSM mapping is used.

DETAILED STEPS

	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`	Enters global configuration mode.
Step 3	**cable multicast mdf-disable [wb-incapable-cm]** **Example:** `Router(config)#` **cable multicast mdf-disable**	Disables MDF capability on the cable modem. • wb-incapable-cm—(Optional) Turns off the MDF capability on the wideband incapable cable modems.

Step 4	exit
	Example:
	`Router(config)#` **`exit`**
	`Router#`
		Exits the global configuration mode.

Configuring Multicast Replication Session Cache at the Forwarding Interface

This section describes the multicast replication session cache configuration for a wideband interface on the Cisco uBR10012 router.

To configure multicast replication session cache at the interface level on the Cisco uBR10012 router, first configure a forwarding interface: modular, integrated or wideband.

Note The multicast replication cache can be configured globally for all interfaces on the Cisco uBR10012 router using the **cable multicast ses-cache** command**.**

DETAILED STEPS

	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`	Enters global configuration mode.
Step 3	**interface wideband-cable** *slot*/*subslot*/*port*:*wideband-channel* **Example:** `Router(config)# **interface wideband-cable 6/0/1:22**`	Enters cable interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS software release. For details, see the Cisco IOS CMTS Cable Command Reference . • *slot*—Slot where a SPA interface processor (SIP) or a line card resides. • *subslot*—Secondary slot for a shared port adapter (SPA) or a line card. • *bay*—Bay in a SIP where a SPA is located. • *port*—Downstream port number. • *wideband-channel*—Wideband channel number.
Step 4	**cable multicast ses-cache***value* **Example:** `Router(config-if)# **cable multicast ses-cache 100**`	Configures the multicast replication session cache on wideband cable interface. • *value*—Multicast replication session cache size limit. The valid range is from 0 to 500. The default value is 0.

	Command or Action	Purpose

Step 5	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

How to Monitor the DOCSIS 3.0 Multicast Support

To monitor the DOCSIS 3.0 Multicast Support feature, use the following procedures:

Verifying the Basic Multicast Forwarding

To verify the configuration parameters for basic multicast forwarding, use the **show ip mroute** command as shown in the following example:

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 230.1.1.1), 00:00:03/00:02:55, RP 30.1.1.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Bundle1, Forward/Sparse, 00:00:03/00:02:55, H
(*, 224.0.1.40), 00:12:02/00:02:19, RP 30.1.1.1, flags: SJCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Bundle1, Forward/Sparse, 00:12:02/00:02:19
```

Note During parallel express forwarding (PXF) reload, all the dynamic multicast route (mroute) entries in the IP multicast routing table are deleted. Only the IGMP static group entries are retained. After the PXF reload, dynamic mroutes are populated in the IP multicast routing table only when next IGMP join is received.

To verify the multicast information for the specified virtual interface bundle, based on IGMPv3, use the **show cable bundle multicast** command as shown in the following example:

```
Router# show cable bundle 1 multicast

CableBundle Interface Source IP  Multicast IP    MAC Address
1    Bundle1.1 *       230.1.1.1    0100.5e00.0001
```

To verify the MAC forwarding table for the specified virtual interface bundle, based on IGMPv3, use the **show cable bundle forwarding** command as shown in the following example:

```
Router# show cable bundle 1 forwarding

MAC address Interface Flags Location link sublink
00c0.5e01.0203 Cable8/0/0 3 64E5BF60 0 64E5BE00
00c0.5e01.0203 Cable7/0/0 3 64E5BE00 0 0
00c0.5e01.0101 Cable8/0/0 3 64E5BEE0 0 64E5BE40
```

To verify the multicast routing table in the PXF processor for a specified group, use the **show pxf cpu mroute** command as shown in the following example:

Note The show pxf cpu command is supported only on Cisco uBR10012 universal broadband routers.

```
Router# show pxf cpu mroute 0.0.0.0

Shadow G/SG[5624]: s: 0.0.0.0 g: 224.0.1.40 uses: 0 bytes 0 flags: [D ] LNJ
Interface vcci offset rw_index mac_header
In : 0 0x000004
Shadow G/SG[3195]: s: 0.0.0.0 g: 234.5.6.7 uses: 0 bytes 0 flags: [5 ] NJ
Interface vcci offset rw_index mac_header
In : 0 0x000008
Out: Cable5/1/0 5 0x00002C 1B 00000026800001005E05060700010
Out: Cable6/1/1 9 0x000028 1A 00000026800001005E05060700010
Out: Cable6/0/0 6 0x000024 19 00000026800001005E05060700010
Out: Cable5/0/0 3 0x000020 18 00000026800001005E05060700010
Out: Cable7/0/0 A 0x00001C 17 00000026800001005E05060700010
Out: Cable7/1/1 C 0x000018 16 00000026800001005E05060700010
Out: Cable7/1/0 B 0x000014 15 00000026800001005E05060700010
Out: Cable6/1/0 8 0x000010 14 00000026800001005E05060700010
Out: Cable6/0/1 7 0x00000C 13 00000026800001005E05060700010
Out: Cable5/0/1 4 0x000008 12 00000026800001005E05060700010
```

To verify the multicast routes (mroutes) in the PXF processor for a specified group, use the **show pxf cable multicast** command as shown in the following example:

```
Router# show pxf cable multicast 0.0.0.0

MDB Flags: L - Local, F - Register flag, T - SPT-bit set, J - Join SPT
           Z - Multicast Tunnel, N- No FastSwitching
OIF Flags: P - Prune Flag, A - Assert Flag
PXF multicast switching for vrf default is enabled.
Mdb at index= 3 hash= 0xE9F7:
 next_mdb_idx: 0, fib_root: 0x0001, source_addr: 0.0.0.0, group_addr: 230.1.1.1
 uses: 0, bytes: 0, vcci_in: 0, oif: 0x000002
 rpf_failed: 0, drop_others: 0
 rp_bit_mask:0x00,  flags: [0xA0]
 Ref Count=0, MDB Flags=0x0082, MDB FastFlags=0x10
```

Verifying the Multicast DSID Forwarding

To verify the entire DSID database content, use the **show cable multicast dsid** command as shown in the following example:

```
Router# show cable multicast dsid
Multicast Group    : 230.1.2.3
         Source    : *
         IDB       : Bu2         Interface: Mo1/1/0:0   Dsid: 0x1F078
         StatIndex : 2           SAID: DEFAULT
Multicast Group    : 230.1.2.3
         Source    : *
         IDB       : Bu2         Interface: Mo1/1/0:0   Dsid: 0x1F078
         StatIndex : 3           SAID: 8196
Multicast Group    : 230.1.2.3
```

```
         Source    : *
         IDB       : Bu2         Interface: Mo1/1/0:0   Dsid: 0x1F078
```

StatIndex : 4 SAID: 8197

To verify the entire database content, use the **show cable multicast db** command as shown in the following example:

Router# **show cable multicast db**

```
interface : Bundle1
Session (S,G) : (*,230.1.1.1)
Fwd Intfc Sub Intfc Host Intfc CM Mac Hosts
Wi1/1/0:0 Bundle1 Ca5/0/0 0018.6852.8056 1
```

To verify the information for the registered and unregistered CMs, use the **show cable modem verbose** command as shown in the following example:

Router# **show cable modem 0010.7bb3.fcd1 verbose**

```
MAC Address : 00C0.7bb3.fcd1
IP Address : 10.20.113.2
Prim Sid : 1
QoS Profile Index : 6
Interface : C5/0/U5
sysDescr : Vendor ABC DOCSIS 2.0 Cable Modem
Upstream Power : 0 dBmV (SNR = 33.25 dBmV)
Downstream Power : 0 dBmV (SNR = ----- dBmV)
Timing Offset : 1624
Initial Timing Offset : 2812
Received Power : 0.25
MAC Version : DOC1.0
Qos Provisioned Mode : DOC1.0
Enable DOCSIS2.0 Mode : Y
Phy Operating Mode : atdma
Capabilities : {Frag=N, Concat=N, PHS=N, Priv=BPI}
Sid/Said Limit : {Max Us Sids=0, Max Ds Saids=0}
Optional Filtering Support : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support : {Taps/Symbol= 0, Num of Taps= 0}
Number of CPE IPs : 0(Max CPEs = 1)
CFG Max-CPE : 1
Flaps : 373(Jun 1 13:11:01)
Errors : 0 CRCs, 0 HCSes
Stn Mtn Failures : 0 aborts, 3 exhausted
Total US Flows : 1(1 active)
Total DS Flows : 1(1 active)
Total US Data : 1452082 packets, 171344434 bytes
Total US Throughput : 0 bits/sec, 0 packets/sec
Total DS Data : 1452073 packets, 171343858 bytes
Total DS Throughput : 0 bits/sec, 0 packets/sec
Active Classifiers : 0 (Max = NO LIMIT)
DSA/DSX messages : reject all
Dynamic Secret : A3D1028F36EBD54FDCC2F74719664D3F
Spoof attempt : Dynamic secret check failed
Total Time Online : 16:16
```

Verifying the Explicit Tracking Feature

To verify explicit tracking information, use the **show cable multicast db** command as shown in the following example:

Router# **show cable multicast db**

```
Interface : Bundle1
Session (S,G) : (*,230.1.1.1)
Fwd Intfc  Sub Intfc  Host Intfc   CM Mac           Hosts
Mo1/1/0:0  Bundle1    Ca5/0/0      0018.6852.8056       1
```

Verifying the Multicast QoS Feature

To verify the cable MQoS details, use the **show cable multicast qos** commands as shown in the following example:

```
Router# show cable multicast qos ?
group-config Display Multicast Group Config information
group-encryption Display Multicast Group Encryption information
group-qos Display Multicast Group QOS information
Router# show cable multicast qos group-config
Multicast Group Config 1 : Priority 1
Group QOS - 1
Group Encryption - 1
Session Range - Group Prefix 230.0.0.0 Mask 255.0.0.0 Source Prefix 0.0.0.0 Mask 0.0.0.0
Router# show cable multicast qos group-encryption
Multicast Group Encryption 1 : Algorithm 56bit-des
Router# show cable multicast qos group-qos
Group QOS Index Service Class Control Igmp Limit Override
DEFAULT MQOS_DEFAULT Aggregate NO-LIMIT 1 MQOS Aggregate NO-LIMIT
```

To verify the DOCSIS service flows on a given cable interface, use the **show interface service-flow** command as shown in the following example:

```
Router# show interface cable 6/0 service-flow

Sfid  Sid   Mac Address     QoS Param Index Type    Dir    Curr   Active
BG/CH
                             Prov  Adm  Act                 State  Time
4     8193  ffff.ffff.ffff   3     3    3   sec(S)  DS     act    21h57m
5     8196  ffff.ffff.ffff   4     4    4   sec(S)  DS     act    00:17
```

To verify the parallel express forwarding (PXF) queueing and link queue statistics, use the **show pxf cpu queue** command as shown in the following example:

Note The show pxf cpu command is supported only on Cisco uBR10012 universal broadband routers.

```
Router# show pxf cpu queue

FP queue statistics for Cable5/0/0
FP queue statistics for Cable6/0/0
Queue algorithm 0x0
Queue number 0 Shared
wq_avg_qlen 0 wq_flags_pd_offset 18A0001
wq_drop_factor 40
wq_buffer_drop 0 wq_limit_drop 0
wq_invalid_enq_wqb_drop 0 wq_invalid_deq_wqb_drop 0
wq_rnd_pkt_drop 0 wq_rnd_byte_drop 0
wq_static_qlen_drop 0
wq_len 0
Packet xmit 56414 Byte xmit 14322357
Queue number 15 Shared High priority
wq_avg_qlen 0 wq_flags_pd_offset 18A8001
wq_drop_factor 1000
wq_buffer_drop 0 wq_limit_drop 0
wq_invalid_enq_wqb_drop 0 wq_invalid_deq_wqb_drop 0
wq_rnd_pkt_drop 0 wq_rnd_byte_drop 0
wq_static_qlen_drop 0
wq_len 0
Packet xmit 0 Byte xmit 0
```

Verifying the Multicast BPI+ Support Feature

To verify information about the multicast sessions on a specific virtual forwarding interface, use the **show interface multicast-sessions** command as shown in the following example:

Router# **show interface wideband-Cable 5/1/2:0 multicast-sessions**

```
Default Multicast Service Flow 9 on Wideband-Cable5/1/2:0
Multicast Group    : 230.1.2.3
         Source    : N/A
         Act GCRs  : 2
         Interface : Bu123                 State: A      GI: Wi5/1/2:0   RC: 0
         GCR       : GC   SAID    SFID    Key   GQC    GEn
                     2    8244    14      27    2      1
                     1    8245    15      28    1      1
Aggregate Multicast Sessions on Wideband-Cable5/1/2:0
Multicast Group    : 230.1.2.3
         Source    : N/A
         GCRs      : 2
         Interface : Bu123                 State: A      GI: Wi5/1/2:0   RC: 0
         GCR       : GC   SAID    SFID    Key   GQC    GEn
                     2    8244    14      27    2      1
                     1    8245    15      28    1      1
```

To verify the service identifier (SID) information of the multicast sessions on a specific virtual forwarding interface, use the **show interface cable sid** command as shown in the following example:

Router# **show interface cable 5/1/0:0 sid 1**

```
Wideband SPA: 1/0    total index assigned: 0      multicast: 0
Wideband SPA: 1/1    total index assigned: 1      multicast: 1
SID : 8197      Latest : 2      Current : 1
  Wideband SPA:  WB channel : 0     blaze_index: 1
  Status[0] : 1  DES Key[0] : 1C7619321C8F0D73   DES IV[0]  :
166D1A291375011A
  Key Life[0]: 43171 sec
  Status[1] : 1  DES Key[1] : E5B0B2C23EA07B6    DES IV[1]  :
209E105D13E91F73
  Key Life[1]: 21571 sec
  Req : 0        Rply : 0        Rej : 0 Inv : 0 RxErr : 0
```

Verifying the Multicast Join Authorization

To verify the multicast profile information, use the **show cable modem auth-profile** command as shown in the following example:

```
Router# show cable modem 0019.474a.d518 auth-profile
Multicast Profile Information for  0019.474a.d518  IP: 20.1.2.3
Multicast Profile Group #           : 0
This CM's Session Limit             : 5
Profile Id          Profile
   0                goldservice
   1                platinumservice
   2                silverservice
```

To verify the multicast profile group, use the **show cable** multicast authorization profile-group command as shown in the following example:

```
Router# show cable multicast authorization profile-group 0
   ProfileGroup:  0,    CMs using this group: 4
   ProfileId   CMs        Profile
   ------------------------------
     0         4         goldservice
     1         4         platinumservice
     2         4         silverservice
   Auth Rule List for prof_group_index: 0
           Src                     Grp            Priority     Action
   ----------------------------------------------------------------------
           0.0.0.0/0            230.1.1.1/24        255       permit
```

To verify multicast profile list, use the **show cable** multicast authorization profile-list command as shown in the following example:

```
Router# show cable multicast authorization profile-list 0
       CMTS Authorization Profile List
       -------------------------------
   Profile Name: goldservice at index: 0
   Number of CMs using this Profile: 4
           Src                     Grp            Priority     Action
   ----------------------------------------------------------------------
           0.0.0.0/0            230.1.1.1/24        255       permit
```

Verifying the Service Flow Attributes

To verify the configuration of service flow attributes on the service class configuration, use the show cable service-class verbose command as shown in the following example:

```
Router# show cable service-class 10 verbose
Index:                                  10
Name:                                   mcast10
Direction:                              Downstream
Traffic Priority:                       0
Maximum Sustained Rate:                 1000000 bits/sec
Max Burst:                              3044 bytes
Minimum Reserved Rate:                  1000000 bits/sec
Minimum Packet Size                     0 bytes
Admitted QoS Timeout                    200 seconds
Active QoS Timeout                      0 seconds
Required Attribute Mask                 8000000F
Forbidden Attribute Mask                7FFFFFF0
Scheduling Type:                        Undefined
Max Latency:                            0 usecs
Parameter Presence Bitfield:            {0x3148, 0x0}
```

To verify the configuration of SF attributes on the Wideband interface configuration, use the **show running-config interface** command as shown in the following example:

```
Router# show running-config interface Wideband-Cable 1/0/0:2
interface Wideband-Cable1/0/0:2
 cable bundle 1
 cable bonding-group-id 3
 cable rf-channel 3
 cable downstream attribute-mask 8000000F
end
```

Verifying the Multicast Group Classifiers

To verify the details of the Group Classifier Rule, use the **show interface wideband-cable multicast-gcr** command as shown in the following example:

```
Router# show interface wideband-cable 1/1/0:0 multicast-gcr
Group Classifier Rules on Wideband-Cable1/1/0:0:
Classifier_id  Group_id  Group_Qos_id  Sid   SFID   ref_count
7              1         1             8196  10     1
8              2         1             8197  11     1
```

Troubleshooting Tips

Make sure that CM can listen to the RF-frequencies specified for the Wideband interfaced chosen for forwarding multicast traffic.

Verifying Multicast Replication Session Cache

To verify the cable multicast replication session cache information at the wideband interface, use the **show cable multicast ses-cache** command with the interface keyword as shown in the following example:

```
Router# show cable multicast ses-cache interface wi7/1/0:1
Fwd Intfc           Sub Intfc              Session (S,G)
Wi7/1/0:1          Bundle1               (30.30.30.30,226.0.0.20)
                   Bundle1               (30.30.30.30,226.0.0.22)
                   Bundle1               (30.30.30.30,226.0.0.23)
                   Bundle1               (30.30.30.30,226.0.0.21)
```

To verify the cable multicast replication session cache information at the modular-cable interface, use the **show cable multicast ses-cache** command with the interface keyword as shown in the following example:

```
Router# show cable multicast ses-cache int Mo6/0/1:0
Fwd Intfc            Sub Intfc              Session (S, G)
Mo6/0/1:0            Bundle1                (*, 230.0.8.138)
```

To verify the cable multicast replication session cache information at the global level, use the **show cable multicast ses-cache** command with the global keyword as shown in the following example:

```
Router# show cable multicast ses-cache global

Fwd Intfc           Sub Intfc               Session (S,G)
Wi7/1/0:0          Bundle1               (30.30.30.30,227.0.0.20)
                   Bundle1               (30.30.30.30,227.0.0.22)

Wi7/1/0:1          Bundle1               (30.30.30.30,226.0.0.20)
                   Bundle1               (30.30.30.30,226.0.0.22)
                   Bundle1               (30.30.30.30,226.0.0.23)
                   Bundle1               (30.30.30.30,226.0.0.21)
Mo6/0/1:0            Bundle1                (*, 230.0.8.138)
```

Configuration Examples for DOCSIS 3.0 Multicast Support

This section provides the following configuration examples:

Example: Configuring Basic Multicast Forwarding

Note The commands given below are required to enable the Cisco CMTS to forward multicast packets. However, Multicast QoS, BPI+, and Authorization features are all optional for multicast packets to be forwarded correctly.

In the following example, a basic multicast forwarding profile is configured.

```
ip multicast-routing
int g1/0/0
```

```
  ip pim sparse-dense-mode
int Bundle 1
  ip pim sparse-mode
  ip igmp version 3
```

Example: Configuring Multicast QoS

Note A default service class and GQC must be defined before proceeding with configuring Multicast QoS.

In the following example, Multicast QoS is configured. You should define three objects and templates and then associate these to a particular bundle or forwarding interface. The objects are Service-Class, Group-QoS-Config (GQC), and Group-Config.

```
cable service class 1 name MQOS_DEFAULT
cable service class 1 downstream
cable service class 1 max-rate 10000000
cable service class 1 min-rate 1000000
cable multicast group-qos default scn MQOS_DEFAULT aggregate
cable multicast group-qos 10 scn MQOS single
cable multicast qos group 20 priority 1
application-id 10
session-range 230.0.0.0 255.0.0.0
tos 1 6 15
vrf name1
cable multicast qos group 20 priority 63 global
```

Example: Configuring Multicast BPI+

In the following example, Multicast BPI+ is configured. The Multicast BPI+ basically reuses the Multicast QoS CLI model under Group-Config object.

```
cable multicast group-encryption 30 algorithm 56bit-des
cable multicast qos group 40 priority 2 global
  session-range 230.0.0.0 255.0.0.0
  group-encryption 30
interface Cable5/0/0
  cable multicast-qos group 40
```

Example: Configuring Multicast Join Authorization

In the following example, multicast join authorization is configured:

```
cable multicast auth enable default-action  deny  max-sessions 10
cable multicast auth profile GOLD
   match rule ipv4 source 0.0.0.0/0 230.0.0.0/16 128 permit
   match rule ipv4 source 10.1.1.1/8 232.0.0.0/8 128 permit
end
```

Example: Configuring Forwarding Interface Selection Based on Service Flow Attribute

In the following example, the service flow attribute-based Forwarding Interface Selection is configured. To send multicast traffic for group 230.1.1.1, interface W1/0/0:2 is selected. The multicast QoS parameters are taken from group qos 1 (effectively from service class “mcast10”).

```
cable service class 10 name mcast10
cable service class 10 downstream
cable service class 10 max-rate 1000000
cable service class 10 min-rate 1000000
cable service class 10 req-attr-mask 8000000F
cable service class 10 forb-attr-mask 7FFFFFF0
cable multicast group-qos 1 scn mcast10 aggregate
cable multicast qos group 1 priority 1
session-range 230.1.1.1 255.255.255.255
 group-qos 1
interface Bundle1
 ip address 40.1.1.1 255.255.255.0
 ip pim sparse-mode
 ip helper-address 2.39.16.1
 cable multicast-qos group 1
end
interface Wideband-Cable1/0/0:0
 description cable rf-channel 0 bandwidth-percent 40
 cable bundle 1
 cable bonding-group-id 1
 cable rf-channel 0 bandwidth-percent 10
 cable rf-channel 1 bandwidth-percent 10
 cable rf-channel 2 bandwidth-percent 10
 cable downstream attribute-mask 8000FF00
interface Wideband-Cable1/0/0:1
 cable bundle 1
 cable bonding-group-id 2 secondary
 cable rf-channel 0 bandwidth-percent 40
 cable rf-channel 1 bandwidth-percent 40
 cable downstream attribute-mask 8000FFF0
interface Wideband-Cable1/0/0:2
 cable bundle 1
 cable bonding-group-id 3 secondary
 cable rf-channel 1 bandwidth-percent 40
 cable rf-channel 2 bandwidth-percent 40
 cable downstream attribute-mask 8000000F
```

Where to Go Next

For further information on the commands required to configure, maintain, and troubleshoot Cisco uBR7200 series universal broadband routers, the Cisco uBR10012 universal broadband routers, and Cisco cable modems, see the *Cisco IOS CMTS Cable Command Reference* at http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

Additional References

The following sections provide references related to the DOCSIS 3.0 Multicast Support on the CMTS Routers.

Related Documents

Related Topic	Document Title
CMTS cable commands	http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.htmlCisco IOS CMTS Cable Command Reference
Multicast VPN and DOCSIS 3.0 Multicast QoS	Multicast VPN and DOCSIS 3.0 Multicast QoS Support
DOCSIS 3.0 QoS Support	DOCSIS WFQ Scheduler on the Cisco CMTS Routers

Standards

Standard	Title
CM-SP-CMCIv3-I01-080320	Cable Modem to Customer Premise Equipment Interface Specification
CM-SP-MULPIv3.0-I08-080522	MAC and Upper Layer Protocols Interface Specification
CM-SP-OSSIv3.0-I07-080522	Operations Support System Interface Specification
CM-SP-PHYv3.0-I07-080522	Physical Layer Specification
CM-SP-SECv3.0-I08-080522	Security Specification

MIBs

MIB[4]	MIBs Link
• DOCS-MCAST-AUTH-MIB • DOCS-MCAST-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

[4] Not all supported MIBs are listed.

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

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 3.0 Multicast Support on the CMTS Routers

Table below lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Note Table below lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 4: Feature Information for DOCSIS 3.0 Multicast Support on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Multicast DSID Forwarding	12.2(33)SCB	The Multicast DSID Forwarding makes use of the DSID to identify the CMs intended to join the Cisco CMTS for the multicast session. It filters and forwards the multicast packets from the CM to the Cisco CMTS. The following sections provide information about this feature: Multicast DSID Forwarding, on page 3 Configuring Basic Multicast Forwarding, on page 13 Configuring Multicast DSID Forwarding, on page 14 The following command was introduced or modified: • **show cable multicast dsid**
Multicast Forwarding on Bonded CM	12.2(33)SCB	Multicast packets are sent to the CM on the primary bonding group it has registered, if Secondary Multicast Bonding Group feature is disabled. The following sections provide information about this feature: Multicast Forwarding on Bonded CM, on page 4 The following command was introduced or modified: • **show cable modem verbose**

Feature Name	Releases	Feature Information
Explicit Tracking	12.2(33)SCB	IGMPv3 support removes report suppression enabling the Cisco CMTS to get the complete session and host information. The following sections provide information about this feature: Explicit Tracking, on page 5 Configuring Multicast QoS, on page 14 The following command was introduced or modified: • **show cable multicast db**
BPI+ Support	12.2(33)SCB	The BPI feature provides data privacy across the HFC network by encrypting traffic flows between the router and the cable operator's CMTS. The BPI+ (BPI Plus) feature provides more secure authentication of cable modems through the use of digital certificates. The following sections provide information about this feature: BPI+ Support, on page 5 Configuring a Multicast BPI+ Support, on page 16 Configuring a Multicast Join Authorization, on page 17

Feature Name	Releases	Feature Information
Multicast Join Authorization	12.2(33)SCB	The Multicast Join Authorization feature allows control of the IP multicast sessions joined by the IP multicast clients. The following sections provide information about this feature: Multicast Join Authorization, on page 6 Configuring a Multicast Join Authorization, on page 17 The following commands were introduced or modified: - **cable multicast authorization** - **cable multicast authorization profile** - **match rule**
Multicast Quality of Service Enhancement	12.2(33)SCB	DOCSIS 3.0 mandates that the CMTS should not admit any flow exceeding the session limit. The current Multicast QoS session limit admits the session, however, it fails to provide any QoS for sessions exceeding the session limit. The following sections provide information about this feature: Multicast Secondary Bonding Group, on page 9 The following command was introduced or modified: - **cable multicast group-qos**

Feature Name	Releases	Feature Information
Multicast Secondary Bonding Group	12.2(33)SCB	The Multicast Secondary Bonding Group is defined as a shared bonding group or RF channel that feeds more than one fiber node through an optical split. This allows CMs from different primary bonding groups and channels to listen to one or more shared sets. The following sections provide information about this feature: Multicast Secondary Bonding Group, on page 9
Default Multicast Authorization Profile	12.2(33)SCC	The Default Multicast Authorization Profile feature allows to create default multicast authorization profile group to authorize modems without a profile name in their configuration file. The following sections provide information about this feature: Default Multicast Authorization Profiles, on page 7 The following command was introduced or modified: • **cable multicast auth profile-name**
Group Classifier Rules	12.2(33)SCC	Group Classifier Rules allows the Cisco CMTS to determine the set of GC entries whose session range matches the new SSM session. The following sections provide information about this feature: Multicast Quality of Service Enhancement, on page 8 Verifying the Multicast Group Classifiers, on page 30 The following command was introduced or modified: • **show interface multicast-gcr**

Feature Name	Releases	Feature Information
DOCSIS 3.0 Multicast	12.2(33)SCD	Support was added for the Cisco uBR7246VXR and Cisco uBR7225VXR routers. The following commands were introduced or modified: • **show cable multicast dsid** • **show cable modem auth-profile**
Multicast DSID Forwarding Disabled Mode	12.2(33)SCD3	A global CLI is introduced to disable MDF on the cable modem. The following sections provide information about this feature: Multicast DSID Forwarding Disabled Mode, on page 11 Configuring Multicast DSID Forwarding Disabled Mode, on page 23 The following command was introduced or modified: • **cable multicast mdf-disable**
MDF1 Support for DOCSIS 2.0 Hybrid Cable Modems	12.2(33)SCE4	The Cisco CMTS router enables the MDF capability in a DOCSIS 2.0 hybrid CM to allow IPv6 packet forwarding. The following sections provide information about this feature: • Multicast DSID Forwarding Disabled Mode, on page 11 • Configuring Multicast DSID Forwarding Disabled Mode, on page 23 The following command was modified: • **cable multicast mdf-disable**

Feature Name	Releases	Feature Information
DSG Disablement for Hybrid STBs	12.2(33)SCF2	In Cisco IOS Release 12.2(33)SCF2 and later, MDF capability can be disabled on all DSG embedded cable modems using the **cable multicast mdf-disable** command with the DSG keyword. For details about this functionality, see the DSG Disablement for Hybrid STBs, on page 12. The **cable multicast mdf-disable** command was modified to support this feature.
Multicast replication session cache	12.2(33)SCH	The following sections provide information about this feature: • Multicast Replication Session Cache, on page 9 • Configuring Multicast Replication Session Cache at the Forwarding Interface, on page 24 The following commands were introduced or modified: • **cable multicast ses-cache** • **clear cable multicast ses-cache** • **show cable multicast ses-cache** {**global** | **interface**}[**summary** | **verbose**]

CHAPTER 2

IPv6 on Cable

First Published: February 18, 2008

Last Updated: January 28, 2016

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Support for the IPv6 on Cable feature is introduced in Cisco IOS Release 12.2(33)SCA for the Cisco uBR7225VXR, Cisco uBR7246VXR, and Cisco uBR10012 universal broadband routers to extend IP addressing functionality on these Cisco cable modem termination system (CMTS) routers to include support for both IPv4 and IPv6 protocol stacks.

Note Starting with Cisco IOS Release 12.2(33)SCC and later releases, Cisco CMTS routers also support dual stack on the customer premises equipment (CPE) and IPv6 over subinterfaces.

The IPv6 feature support available in the Cisco IOS software and for Cisco CMTS routers is extensive. This document provides a comprehensive overview of all of the IPv6 features supported on the Cisco CMTS routers, and their restrictions.

However, the details of every feature are not covered in this document. The areas of IPv6 protocol support for the Cisco CMTS routers discussed in this document are classified by platform-independence or by platform-specific feature support.

- Platform-independent IPv6 features—Describes IPv6 features that are supported in the Cisco IOS software for several other Cisco platforms, and which generally do not have any platform-specific behavior or configuration differences on the Cisco CMTS routers.
  - Documentation about the restrictions for these platform-independent features can be found in the Restrictions for IPv6 on Cable, on page 46.
  - Detailed information about these features, including conceptual and task-based configuration information, is documented outside of this feature and in the Cisco IOS software documentation. Detailed information about the location of this related documentation in the Cisco IOS software documentation is described in the Feature Information for IPv6 on Cable, on page 95.

- Platform-specific IPv6 features—Describes IPv6 features that are specific to the cable technology area and that only apply to the supported Cisco CMTS routers. The cable-specific IPv6 feature support includes new or modified cable features supporting IPv6, and any transparent support of the IPv6 protocol in existing (legacy) cable features on the CMTS router platforms.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for IPv6 on Cable

- MDF capable line cards are required for DOCSIS 3.0 cable modems (CMs) to support IPv6 CPEs.

Table below shows the hardware compatibility prerequisites for the IPv6 on Cable feature.

Table 5: IPv6 on Cable Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards and SPA
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • PRE2 **Cisco IOS Release 12.2(33)SCB and later** • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR10-MC5X20S/U[5] • Cisco Wideband SPA 2 **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V[6] **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V 2 **Cisco IOS Release 12.2(33)SCH and later** • Cisco Next Generation Wideband SPA
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later** • NPE-G2[7]	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-MC28U/X 1 **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V 2
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later** • NPE-G2 3	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-MC28U/X 1 **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V 2

[5] Supports only DOCSIS 2.0 and IPv6 cable modems.

[6] Supports only DOCSIS 3.0 and IPv6 cable modems.

[7] Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2

Note In a typical customer configuration, the IPv6 requires an additional pass through the PRE4. For example, if a packet with a given set of configured features takes one pass through PXF for IPv4 processing, it requires two passes for IPv6 processing.

Restrictions for IPv6 on Cable

The following capabilities are not supported by IPv6 on the Cisco CMTS routers:

- IPv6 support for SCF releases—Cisco IOS SCF releases do not support IPv6 related features

Note Do not enable IPv6 on Cisco IOS SCF releases.

- Access Control List (ACL) extensions for mobile IPv6
- Alternative Provisioning Mode (APM) and Dynamic Provisioning Mode (DPM) (Supported from Cisco IOS Release 12.3(33)SCB onwards)
- Cable Intercept (PacketCable Communications Assistance for Law Enforcement Act [CALEA])
- Cable monitoring based on IPv6 ACL
- Configuration file generation for Dynamic Message Integrity Check (DMIC) for IPv6 cable modems
- DOCSIS Set-top Gateway (DSG) for IPv6
- Hot Standby Router Protocol (HSRP) for IPv6
- Internet Control Message Protocol for IPv6 (ICMPv6) filtering and policing (ICMPv6 is subject to Divert Rate Limit [DRL] in PRE4 punt path.)
- IPv6 anycast addressing
- IPv6 default router preference (DRP)
- IPv6 high availability (HA)
- IPv6 Policy Based Routing (PBR)
- IPv6 VPNs
- Load balancing used with Hot Standby Connection-to-Connection Protocol (HCCP)
- Mobile IPv6 home agent
- Multiple Dynamic Host Configuration Protocol for IPv6 (DHCPv6) addresses

Note Starting with Cisco IOS Release 12.2(33)SCG1, assignment of multiple IPv6 addresses and IPv6 prefixes via DHCP to a single CPE is supported.

- Multi protocol Label System-Virtual Private Network (MPLS-VPN)
- Netflow for IPv6
- Network Address Translation-Protocol Translation (NAT-PT)
- PacketCable and PacketCable Multimedia

Note Starting with Cisco IOS Release 12.2(33)SCJ, IPv6 PacketCable Multimedia Voice is supported.

- Quality of Service (QoS) for IPv6
- Scalable differential IP address assignment (DOCSIS 3.0 assignment of different prefixes to CM and CPE based on DHCPv6 MAC address)

Note Starting with Cisco IOS Release 12.2(33)SCF4, DOCSIS 3.0 assignment of different prefixes to CM and CPE is supported.

- Service Independent Intercept (SII) or Packet Intercept IPv6 address tapping

Note Starting with Cisco IOS Release 12.2(33)SCE, IPv6 HA is supported.

Other restrictions for IPv6 on cable:

DHCPv6 Restrictions for IPv6 on Cable

- Deploy IPv6 source verification only with DHCPv6 leasequery to recover lost CPE data and ensure that traffic from legitimate CPEs can continue to be forwarded.
- DHCPv6 leasequery does not support CPEs that use only prefix delegation (PD) addresses.

The following DHCPv6 areas are not supported by the Cisco CMTS routers:

- DHCP leasequeries
- The following DHCPv6 relay agent options are not supported by the Cisco CMTS routers:
    - Syslog server address option
    - CableLabs client configuration
    - DHCPv6 relay agent subscriber-ID option
    - DHCPv6 relay agent RADIUS attribute option
    - RAAN option

IPv6 Access Services Restrictions for IPv6 on Cable

The following areas of IPv6 access services are not supported by the CMTS routers:

- Authorization, authentication, and accounting (AAA) support for Cisco IPv6 vendor-specific attributes (VSA)
- AAA support for RFC 3162 IPv6 Remote Access Dial-In User Service (RADIUS) attributes
- DHCPv6 prefix delegation via AAA
- Point-to-Point Protocol (PPP) over ATM (PPPoA)
- PPP over Ethernet (PPPoE)
- Prefix pools
- Remote bridged encapsulation

IPv6 Data Link Layer Restrictions for IPv6 on Cable

The following areas of the IPv6 Data Link Layer are not supported by the Cisco CMTS routers:

- Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC) and ATM LAN emulation (LANE)
- Fiber Distributed Data Interface (FDDI)
- Frame Relay PVC13
- Cisco High-Level Data Link Control (HDLC)
- PPP service over Packet over SONET (POS)
- Integrated Services Digital Network (ISDN)
- Serial (synchronous and asynchronous)
- Virtual LANs (VLANs) using Cisco Inter-Switch Link (ISL)
- Dynamic Packet Transport (DPT)

Multicast Restrictions

IPv6 multicast has the following behavior restrictions on the Cisco CMTS routers:

- IPv6 multicast packets on the Cisco uBR10012 universal broadband router are process-switched by the Performance Routing Engines (PRE).
- IPv6 multicast support complies with DOCSIS 2.0 for Cisco uBR10-MC5X20U and Cisco uBR-MC28U cable interface line cards only.
- IPv6 multicast support complies with DOCSIS 3.0 for Cisco uBR-MC3GX60V, Cisco uBR-MC88V, Cisco UBR-MC20X20V interface line cards, and Cisco Wideband SPA only.
- ICMP redirects are not sent to the originating host if the packet is destined for another CPE behind the same CM. All CPE-to-CPE traffic is processed by the Cisco CMTS router.
- IPv6 multicast forwarding is not supported in Parallel Express Forwarding (PXF), therefore, the IPv6 multicast forwarding performance is limited by the Router Processor (RP).

The following areas of IPv6 multicast are not supported by the Cisco CMTS routers:

- Address family support for Multiprotocol Border Gateway Protocol (MBGP)
- Bidirectional Protocol Independent Multicast (PIM)
- Bootstrap router (BSR)
- DOCSIS 3.0 encrypted multicast
- Explicit tracking of receivers
- IPv6 multicast echo
- Multicast Forwarding Information Base (MFIB) display enhancements
- Multicast use authentication and profile support
- PIM embedded rendezvous point
- Protocol Independent Multicast sparse mode (PIM-SM) accept register feature
- Reverse path forwarding (RPF) flooding of bootstrap router (BSR) packets
- Routable address hello option
- Source Specific Multicast (SSM) mapping for Multicast Listener Device (MLD) version 1 SSM
- IPv6 multicast forwarding on the Cisco uBR10012 universal broadband router in Parallel Express Forwarding (PXF)

Provisioning Restrictions for IPv6 on Cable

The following areas of IPv6 provisioning are not supported on the Cisco CMTS routers:

- Preregistration downstream service ID (DSID) notification
- Bonded-Downstream Channel Descriptor (B-DCD) messages
- Multiple DHCPv6 IPv6 addresses per CM or CPE
- Static IP address assignment for CPEs
- Stateless address auto-configuration (SLAAC) address assignment

Note In Cisco IOS Release 12.2(33)SCC and later, static IPv6 addressing for CPE is supported using Source Address Verification (SAV). For more information about SAV, see the Source Address verification section in the *DOCSIS 3.0 Security Specification* guide.

Note Starting with Cisco IOS Release 12.2(33)SCG1, Multiple IAPDs in a Single Advertise feature supports assignment of multiple IPv6 addresses to a Cable Modem (CM) subscriber.

Note Due to restrictions with DSID and B-DCD messaging support in Cisco IOS Release 12.2(33)SCA, DOCSIS 3.0 CMs must operate with DOCSIS 2.0-level functionality.

QoS Restrictions

Effective with , the following fields are supported for theIPv6 downstream classification:

- IPv6 dest addr
- ipv6 src addr
- IPv6 next header
- IPv6 traffic class

Note IPv6 flow label field is not supported.

The following areas of DOCSIS QoS are not supported by the Cisco CMTS routers:

- Upstream IPv6 Type of Service (ToS) overwrite
- Downstream IPv6 classification

Note ToS overwrite, DOCSIS classification, and Modular QoS CLI (MQC) on Gigabit Ethernet are supported on PRE4 from Cisco IOS Release 12.2(33)SCE onwards.

Routing Restrictions for IPv6 on Cable

The following areas of IPv6 routing are not supported by the Cisco CMTS routers:

- Authenticate route injection via Routing Information Protocol (RIP) for IPv6 (RIPng)
- Differential address/prefix assignment for CM and the CPE behind CM

Note Starting with Cisco IOS Release 12.2(33)SCF4, differential prefix assignment for CM and the CPE behind CM is supported.

- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPFv3) cannot operate with IPv6 multicast routing. To use OSPF, you must disable the **ipv6 multicast-routing** command on the Cisco CMTS routers.

Services and Management Restrictions for IPv6 on Cable

The following areas of IPv6 services and management are not supported by the Cisco CMTS routers:

- IPv6 general prefixes
- IPv6 IOS firewall, including IOS firewall and FTP application support

Switching Restrictions for IPv6 on Cable

The following areas of IPv6 switching services are not supported by the Cisco CMTS routers:

- Automatic 6to4 tunnels
- Provider edge router over Multiprotocol Label Switching (MPLS) (6PE)
- CEFv6 switched Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels
- CEFv6 switched automatic IPv4-compatible tunnels
- Parallel Express Forwarding (PXF) switching on the Cisco uBR10012 router

Note PXF switching is supported on the Cisco CMTS routers from Cisco IOS Release 12.2(33)SCE onwards.

Tunneling Restrictions for IPv6 on Cable

The following areas of IPv6 tunneling services are not supported by the Cisco CMTS routers:

- Automatic 6to4 tunnels
- Automatic IPv4-compatible tunnels
- IPv6 over Universal Transport Interface (UTI) using a Tunnel Line Card
- ISATAP tunnel support
- IPv6 over IPv6 tunnels
- IP over IPv6 Generic Routing Encapsulation (GRE) tunnels
- IPv6 GRE tunnels in Connectionless Network Service (CLNS) networks

Restrictions for IPv6 Dual Stack CPE Support on the CMTS

The IPv6 Dual Stack CPE Support on the CMTS feature in Cisco IOS Release 12.2(33)SCC has the following limitations:

Note These limitations are not applicable for Cisco IOS Release 12.2(33)SCE. PXF acceleration support is available only on PRE4 from Cisco IOS Release 12.2(33)SCE and later releases.

- The CMTS must use DHCPv4 and DHCPv6 to assign both IPv4 and IPv6 addresses to a dual stack CPE client.
- The IPv6 functionality on the Cisco uBR10012 router manages the CM and tests the infrastructure for CPE deployment. Cisco IOS Release 12.2(33)SCC does not support PXF acceleration of IPv6 data packets on the Cisco uBR10012 router platform. IPv6 data packets from CPE devices are handled by the control processor. Hence, the packets per second (pps) rate is limited to a few kpps per CMTS. IPv6

traffic of 3 kpps on PRE2 and 12 kpps on PRE4 produces an acceptable load on the Cisco uBR10012 control processor.

Restrictions for Implementing IPv6 VPN over MPLS

- The maximum number of IPv6 virtual routing and forwarding instances (VRF) that can be supported is 2038 (including the global routing instances).
- Each subinterface on the CMTS requires an address range from the ISP and from the MSO that will will be used to assign addresses for cable modems. These two address ranges must not overlap and must be extensible to support an increased number of subscribers for scalability.
- This feature does not support DHCPv6 over MPLS and IPv6 multicast.

Note Starting with Cisco IOS Release 12.2(33)SCF4, DHCPv6 over MPLS is supported.

Restrictions for Multiple IAPDs in a Single Advertise

- The cable modem can have only one Identity Association for Non-temporary Address (IA_NA). The IA_NA can either be static or assigned via the DHCP.
- The CPE can have multiple Identity Association for Prefix Delegations (IAPDs) via a DHCP.
- The CPE cannot have multiple IA_NAs and IAPDs, both static and assigned via a DHCP at the same time.
- The default maximum number of IPv6 addresses per CPE is 16.
- The router displays all IA_NA and IAPD requests when CPEs send them together in a single request, or IA_NAs are received first followed by IAPDs. If CPEs send IA_NA and IAPD requests separately to the router and IAPD requests are received first followed by IA_NAs, then only IA_NA addresses are visible on the router. All IAPD addresses are automatically cleared.

Information About IPv6 on Cable

This section includes the following topics:

Features Supported from Cisco IOS Release 12.2(33)SCE

The following features are supported on the Cisco CMTS routers from Cisco IOS Release 12.2(33)SCE onwards:

- PXF switching
- PXF acceleration of IPv6 data packets
- Source verification of IPv6 packets in PXF

- ACL support for PXF
- ToS overwrite
- DOCSIS classification
- Modular QoS CLI (MQC) on Gigabit Ethernet
- IPv6 DOCSIS RP and LC HA and DCC
- MAC tapping of IPv6 packets
- Equal cost route load balancing of IPv6 packets destined to the backhaul
- IPv6 over IPv4 GRE tunnels

Features Supported from Cisco IOS Release 12.2(33)SCF4

The following features are supported on the Cisco CMTS routers from Cisco IOS Release 12.2(33)SCF4 onwards:

- Assignment of different prefixes to CM and CPE
- DHCPv6 over MPLS-VPN
- DHCPv6 relay prefix delegation VRF awareness

Features Supported from Cisco IOS Release 12.2(33)SCG1

The following features are supported on Cisco CMTS routers from Cisco IOS Release 12.2(33)SCG1 onwards:

- Assignment of multiple IAPDs in a single advertise for each CPE.
- Assignment of multiple IA_NA and IAPD combinations to multiple CPEs behind a CM.
- The default maximum number of IA_NA and IAPD combinations for each cable modem is 16, including link-local addresses.

Features Supported from Cisco IOS Release 12.2(33)SCI1

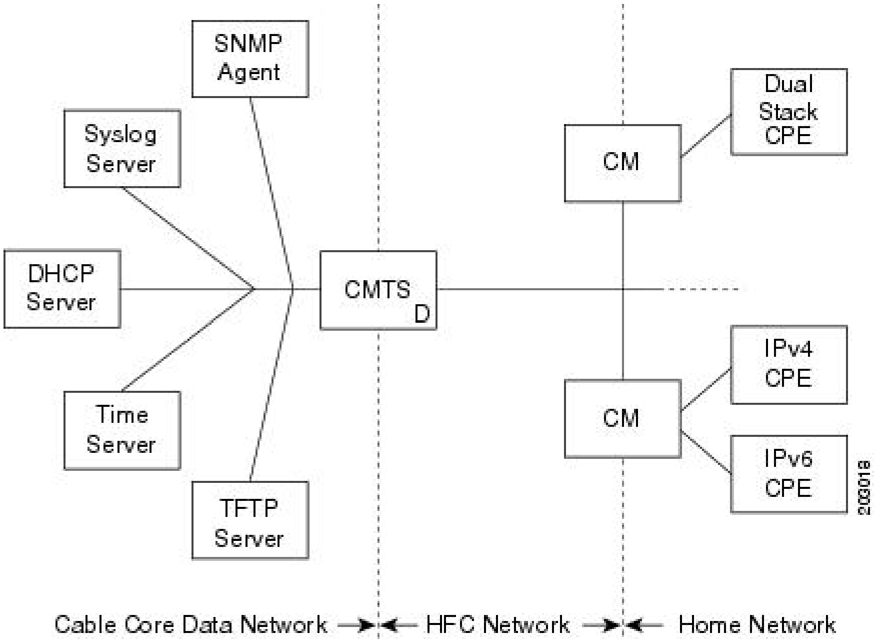
The following features are supported on Cisco CMTS routers from Cisco IOS Release 12.2(33)SCI1 onwards:

- IPv4 and IPv6 Downstream ToS overwrite.
- DHCPv6 Client Link-Layer Address Option (RFC 6939).

Overview of the DOCSIS 3.0 Network Model Supporting IPv6

Figure below illustrates the network model described by the *DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification*.

Figure 1: DOCSIS 3.0 Network Model



In this model, the different devices support the following functions and services:

- Customer premises equipment (CPE)—Supports IPv4, IPv6, or dual stack operation.

Note In Cisco IOS Release 12.2(33)SCC and later releases, Cisco CMTS routers support CPE devices provisioned for dual stack operation.

- Cable modem (CM)—Functions as a bridging device and supports IPv4, IPv6, or dual stack operation.
- Cable modem termination system (CMTS) router—Works with the CM over the hybrid fiber coaxial cable (HFC) network to provide IPv4 and IPv6 network connectivity to the provisioning servers and the core data network behind the CMTS router.

The CMTS router supports IPv6 address assignment, routing, and forwarding of IPv6 multicast and unicast packets.

Note In Cisco IOS Release 12.2(33)SCA and later releases, the Cisco CMTS router supports only a single DHCPv6 IPv6 address per client CM or CPE. This restriction also applies to DHCPv6 Prefix Delegation prefixes. The reason for blocking more than one DHCPv6 address or prefix for a client is because the end-to-end network requires Source Address Selection (SAS) and all nodes in the end-to-end network may not support the correct SAS. Moreover, the SAS specification (RFC 3484) is being revised by the IETF to define the correct SAS behavior.

- Simple Network Management Protocol (SNMP) agent—Provides management tools to configure and query devices on the network.
- Syslog server—Collects messages from the CM to support its functions.
- Dynamic Host Control Protocol (DHCP) server—The DOCSIS 3.0 network model supports both DHCPv4 and DHCPv6 servers to control the assignment of IP addresses.
- Time server—Provides the current time to the CM.
- Trivial File Transport Protocol (TFTP) server—Provides the CM configuration file.

Note In Cisco IOS Release 12.2(33)SCG1, the Cisco CMTS router supports multiple IPv6 addresses per client CPE via DHCP. The *Multiple IAPDs in a Single Advertise* feature supports assignment of multiple IA_NA and IAPD to a client CPE. This feature removes the restriction introduced in Cisco IOS Release 12.2(33)SCA to enable allocation of multiple globally-reachable IPv6 addresses to home devices of the cable modem subscriber.

Note The Cisco CMTS router supports multiple IPv6 addresses per client CPE via DHCP. The *Multiple IAPDs in a Single Advertise* feature supports assignment of multiple IA_NA and IAPD to a client CPE. This feature removes the restriction introduced in Cisco IOS Release 12.2(33)SCA to enable allocation of multiple globally-reachable IPv6 addresses to home devices of the cable modem subscriber.

Overview of Cable Modem IPv6 Address Provisioning

Prior to cable modem registration with a CMTS router, the CMTS router sends a MAC Domain Descriptor (MDD) message to provide information to the cable modem about its supported IP provisioning mode. You configure the CMTS router provisioning mode using the **cable ip-init** interface configuration command. For more information, see the Implementing IPv6 Addressing and Basic Connectivity for Cable Interfaces and Bundles, on page 66.

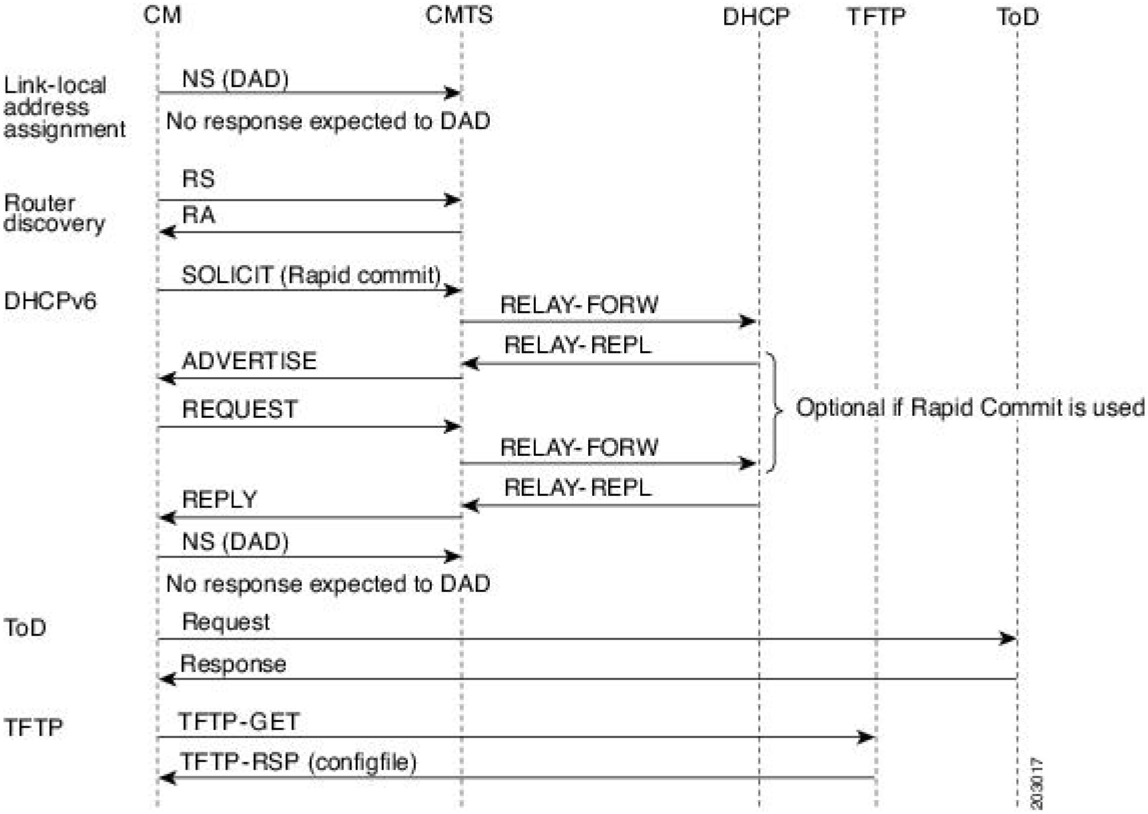
The MDD contains an IP initialization parameters type length value (TLV) that defines the IP version, management and alternate provisioning mode, and pre-registration downstream service ID (DSID) that is used by cable modems that are capable of downstream traffic filtering.

Note In Cisco IOS Release 12.2(33)SCA, the Cisco CMTS routers do not support alternate provisioning mode or pre-registration DSID.

To support the MULPIv3.0 I04 or later version of the *DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification*, the cable modem must attempt IPv6 address acquisition first.

Figure below illustrates the message flow between a cable modem, the CMTS router, and the DHCP server when the cable modem is requesting an IPv6 address.

Figure 2: Message Flow for CM Provisioning of DHCP IPv6 Address Assignment



1 Link-local address assignment—The cable modem sends a Neighbor Solicit (NS) message with its link-local address (LLA) to the CMTS router, which starts the duplicate address detection (DAD) process for that LLA. The cable modem expects no response to the NS message.

2 Router discovery—The cable modem listens to the downstream to detect periodical Router Advertise (RA) messages. When an RA message is detected, the cable modem uses the data in the RA message to configure the default route. If an RA is not detected in a specified period, the cable modem sends a Router Solicit (RS) message to find the router on the link (all nodes multicast). The CMTS router responds with a Router Advertise (RA) message with theM and O bits set to 1 to instruct the CM to perform stateful address configuration.

Note Cisco CMTS routers do not support SLAAC address assignment.

- DHCPv6—The cable modem sends a DHCPv6 Solicit message to the CMTS router to request an IPv6 address. The CMTS router relays this message to the DHCPv6 servers. The DHCPv6 servers send an Advertise message indicating the server's availability.

If the Rapid-Commit option is not used by the cable modem, then the cable modem responds to the Advertise message of the server with a Request message to select the server that the CMTS router relays to the DHCPv6 server. If the Rapid-Commit option is used, then multiple DHCPv6 servers that could assign different addresses to the same CPE must not be used.

The cable modem starts the DAD process to verify the uniqueness of the IPv6 address that the DHCPv6 server assigns to it.

- TFTP and Time of Day (ToD)—Once the CM establishes IP connectivity, it sends a request to the TFTP server to download a configuration file and requests the current time from the ToD server to complete its boot process.

Overview of IPv6 Dual Stack CPE Support on the CMTS

In Cisco IOS Release 12.2(33)SCA and later releases, IPv6 was added to the CMTS. Most operating systems (OS) deployed at homes support dual stack operation. In Cisco IOS Release 12.2(33)SCC and later releases, CMTS also supports dual stack, which is both IPv4 and IPv6 addressing on the CPE.

Overview of IPv6 over Subinterfaces

In Cisco IOS Release 12.2(33)SCC, CMTS supports IPv6 over bundle subinterfaces. To configure IPv6 on bundle subinterfaces, see the Implementing IPv6 Addressing and Basic Connectivity for Cable Interfaces and Bundles, on page 66 section. For a CMTS bundle configuration example, see the Example: IPv6 over Subinterfaces , on page 81 section.

To enable IPv6 on subinterfaces, configure IPv6 on bundle subinterfaces and not the bundle. Reset the CMs after the subinterface is configured.

Note In Cisco IOS Release 12.2(33)SCC, MPLS VPN over subinterfaces for IPv6 is not supported.

Overview of High Availability on IPv6

In Cisco IOS Release 12.2(33)SCE, CMTS supports HA features on IPv6. IPv6 HA is supported on PRE2 with IPv6 punt path forwarding and on PRE4 with IPv6 PXF forwarding.

Note IPv6 DOCSIS HA and HCCP is supported on the Cisco CMTS routers from Cisco IOS Release 12.2(33)SCE onwards.

The IPv6 HA feature support in Cisco CMTS routers covers the following capabilities:

- DOCSIS PRE HA
- DOCSIS line card HA
- Dynamic Channel Change (DCC)

DOCSIS PRE HA

The DOCSIS PRE HA has the following behavior restrictions and prerequisites on the Cisco CMTS routers:

- The CMs and CPEs should not go offline after a PRE switchover.
- The data structures of the IPv6 CM and CPE should be synchronized to the standby PRE before the PRE switchover. Both dynamic and bulk synchronization is supported.
- Single stack, dual stack, and APM are supported for the CM.
- Single stack and dual stack provisioning modes are supported on the CPE.
- After a PRE switchover, the IPv6 neighbor entries are rebuilt by Neighbor Discovery (ND) messages on the standby PRE, and the IPv6 routes are rebuilt after converging the routing protocol.

DOCSIS Line Card HA

The DOCSIS line card HA has the following behavior restrictions and prerequisites on the Cisco CMTS routers:

- The data structures of the IPv6 CM and CPE should be synchronized to the standby line card before the line card switchover. Both dynamic and bulk synchronization is supported.
- The CMs and CPEs should not fall offline after a line card switches over and reverts; the CMs and CPEs should behave the same as before the switchover.
- The DOCSIS line card HA supports both 4+1 and 7+1 redundancy.
- Traffic outages in IPv6 may be longer because traffic recovery occurs only after converging the routing protocol.

Dynamic Channel Change

The Dynamic Channel Change (DCC) feature is supported on Cisco CMTS routers.

Note The behavior of the DCC for single stack IPv6 CM and CPE, or dual stack CM and CPE is the same as that of a single stack IPv4 CM and CPE.

The IPv6 and IPv4 DCC functionality has the following behavior restrictions and prerequisites on the Cisco CMTS routers:

Narrowband Cable Modem

- If the source and destination MAC domains of the CM are on the same line card, DCC initialization techniques 0, 1, 2, 3, and 4 are used to move the CM and its associated CPE from one upstream or downstream to another; or move the CM and CPE from one upstream and downstream combination to another.
- If the source and destination MAC domains of the CM are on different line cards, you can use only the DCC initialization technique 0 to move the CM and its associated CPE across line cards.

Wideband Cable Modem

- If the source and destination MAC domains of the CM are on the same line card, DCC initialization techniques 0, 1, 2, 3, and 4 are used to move the CM and its associated CPE from one upstream to another.
- If the primary downstream of a CM is changed after DCC, you can use only the DCC initialization technique 0 to move the CM and its associated CPE across line cards.

Overview of IPv6 VPN over MPLS

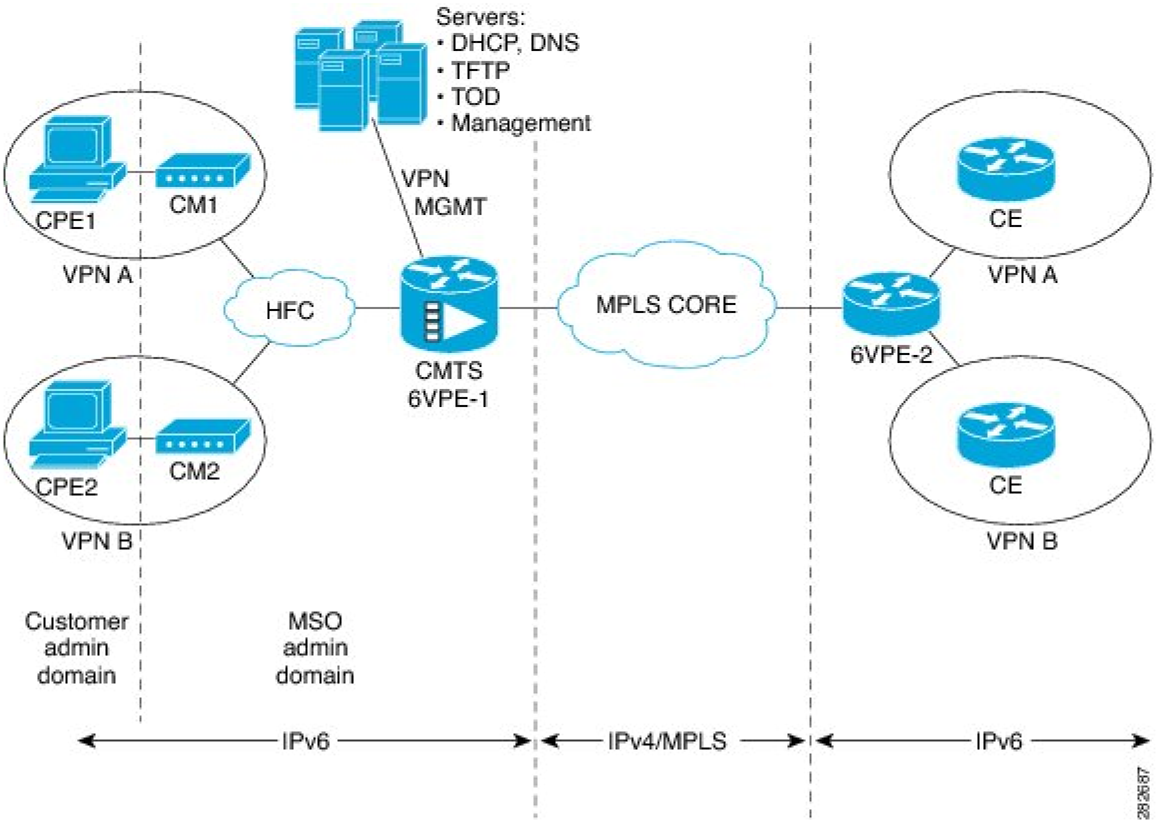
The Multiprotocol Label Switching (MPLS) VPN feature represents an implementation of the provider edge (PE) based VPN model. This document describes the IPv6 VPN over MPLS (6VPE) feature.

The 6VPE feature allows Service Providers to provide an IPv6 VPN service that does not require an upgrade or reconfiguration of the PE routers in the IPv4 MPLS Core. The resulting IPv6 VPN service has a configuration and operation which is virtually identical to the current IPv4 VPN service.

In principle, there is no difference between IPv4 and IPv6 VPNs. In both IPv4 and IPv6, the multiprotocol BGP is the core of the MPLS VPN for IPv6 (VPNv6) architecture. It is used to distribute IPv6 routes over the service provider backbone using the same procedures to work with overlapping addresses, redistribution policies, and scalability issues.

Figure below illustrates the 6PE/6VPE reference architecture diagram.

Figure 3: 6PE/6VPE Reference Architecture



For more information about these tasks, see the Implementing IPv6 VPN over MPLS chapter in the Cisco IOS IPv6 Configuration Guide, Release 12.2SR.

Cable Monitor

The Cable Monitor and Intercept features for Cisco CMTS routers provide a software solution for monitoring and intercepting traffic coming from a cable network. These features give service providers Lawful Intercept capabilities.

For more information, see Cable Monitor and Intercept Features for the Cisco CMTS Routers guide at: http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_mon_intrcpt.html

Overview of IPv6 CPE Router Support on the Cisco CMTS

In Cisco IOS Release 12.2(33)SCF and later releases, the IPv6 CPE router support is provided on the Cisco CMTS. The IPv6 CPE router is a node primarily for home or small office use that connects the end-user network to a service provider network. It is also referred to as the home router.

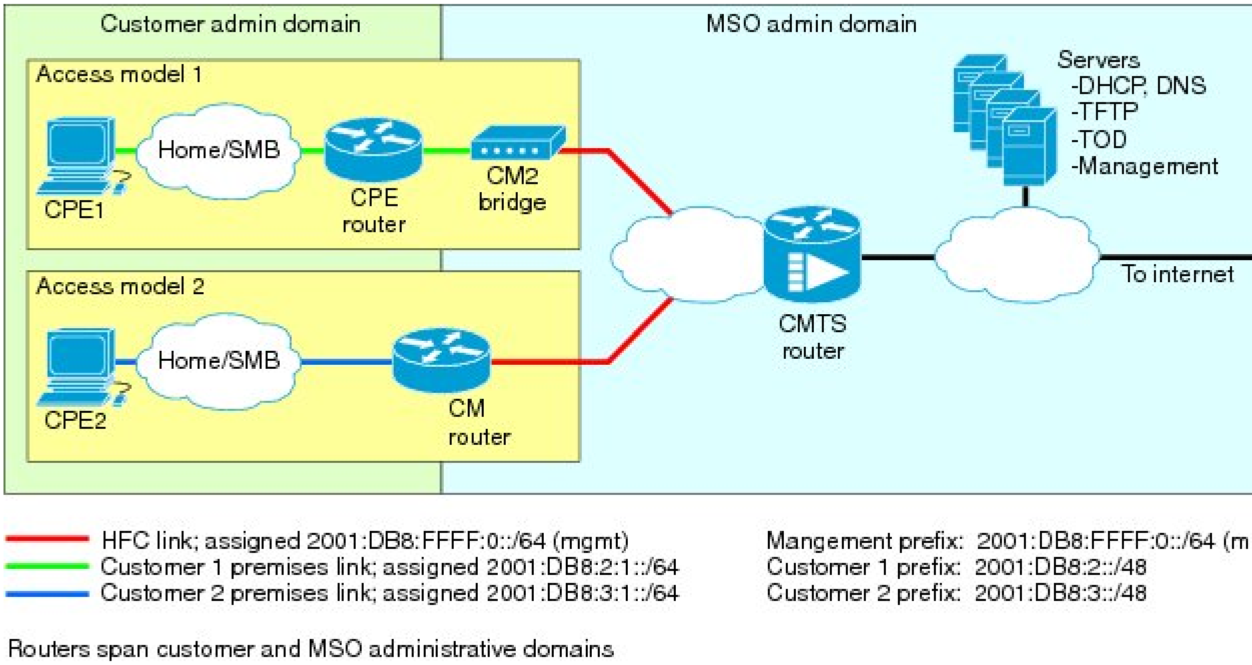
The IPv6 CPE router is responsible for implementing IPv6 routing; that is, the IPv6 CPE router looks up the IPv6 destination address in its routing table and decides to which interface the packet should be sent.

The IPv6 CPE router performs the following functions:

- Provisions its WAN interface automatically.
- Acquires IP address space for provisioning of its LAN interfaces.
- Fetches other configuration information from the service provider network.

Figure below illustrates the CPE router reference architecture diagram between the CPE router, the CMTS, and the DHCPv6 server (CNR) when the CM is requesting an IPv6 address.

Figure 4: IPv6 CPE Router Reference Architecture


Customer admin domain
MSO admin domain
Access model 1
Home/SMB
CPE1
CPE router
CM2 bridge
Access model 2
Home/SMB
CPE2
CM router
CMTS router
Servers
-DHCP, DNS
-TFTP
-TOD
-Management
To internet
HFC link; assigned 2001:DB8:FFFF:0::/64 (mgmt)
Customer 1 premises link; assigned 2001:DB8:2:1::/64
Customer 2 premises link; assigned 2001:DB8:3:1::/64
Mangement prefix: 2001:DB8:FFFF:0::/64 (m
Customer 1 prefix: 2001:DB8:2::/48
Customer 2 prefix: 2001:DB8:3::/48
Routers span customer and MSO administrative domains

As part of the IPv6 CPE Router Support feature, the following enhancements are introduced:

- Support to IPv6 router devices.
- IPv6 Prefix Delegation (PD) High Availability.
- Prefix awareness support in IPv6 cable source-verify, Cable DOCSIS filters code, and packet intercepts.

Support for IPv6 Prefix Stability on the CMTS

Cisco IOS Release 12.2(33)SCF1 supports IPv6 prefix stability on the Cisco CMTS as specified in DOCSIS 3.0 MULPI CM-SP-MULPIv3.0-I15-110210 standard. The IPv6 prefix stability allows an IPv6 home router to move from one Cisco CMTS to another while retaining the same prefix.

The multiple service operators (MSOs) can use this feature to allow their business customers (with IPv6 routers) to retain the same IPv6 prefix during a node split.

Configurable DHCPv6 Relay Address

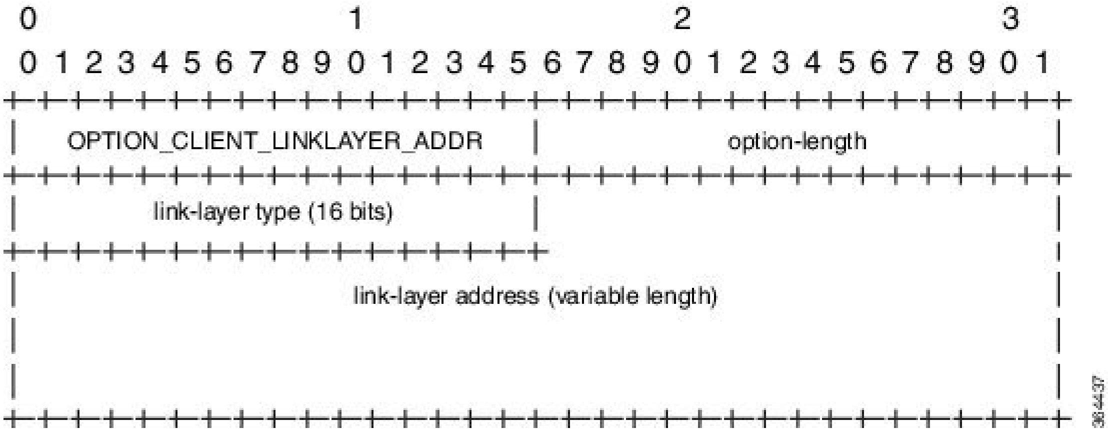
The DHCPv6 Cisco IOS relay agent on the Cisco CMTS router sends relay-forward messages from a source address to all configured relay destinations. The source address is either an IPv6 address provisioned on the network interface or a Cisco CMTS WAN IPv6 address. The relay destination can be a unicast address of a server, another relay agent, or a multicast address. The relay-forward messages contain specific DHCPv6 link-addresses.

A DHCP relay agent is used to relay messages between the client and server. A client locates a DHCP server using a reserved, link-scoped multicast address.

DHCPv6 Client Link-Layer Address Option (RFC 6939)

Cisco IOS Release 12.2(33)SCI1 supports DHCPv6 Client Link-Layer Address Option (RFC 6939). It defines an optional mechanism and the related DHCPv6 option to allow first-hop DHCPv6 relay agents (relay agents that are connected to the same link as the client) to provide the client's link-layer address in the DHCPv6 messages being sent towards the server.

The format of the DHCPv6 Client Link-Layer Address option is shown below.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| OPTION_CLIENT_LINKLAYER_ADDR  |          option-length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   link-layer type (16 bits)   |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
|            link-layer address (variable length)               |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Name	Description
option-code	OPTION_CLIENT_LINKLAYER_ADDR (79)
option-length	2 + length of MAC address
link-layer type	CPE or CM MAC address type. The link-layer type MUST be a valid hardware type assigned by the IANA, as described in RFC0826.
link-layer address	MAC address of the CPE or CM.

Note Starting with Cisco IOS Release 12.2(33)SCI1, RFC6939 is enabled by default. It can not be enabled/disabled by any CLI command.

To configure DHCPv6 Relay Address on the Cisco CMTS bundle subinterfaces, see the Configuring DHCPv6 Relay Agent, on page 77 section.

For more information about the DHCPv6 client, server, and relay functions, see the “Implementing DHCP for IPv6” chapter in the Cisco IOS IPv6 Configuration Guide, Release 12.2SR .

Unitary DHCPv6 Leasequery

The Cisco IOS Release 12.2(33)SCF1 introduces support for unitary DHCPv6 leasequery protocol (RFC 5007) on the Cisco CMTS routers for upstream IPv6 source verification. This protocol verifies the authenticity of the IPv6 CPE behind a home or small office cable deployment.

For more information on unitary DHCPv6 leasequery, see the Unitary DHCPv6 Leasequery feature guide.

Support for Multiple IAPDs in a Single Advertise

Cisco IOS Release 12.2(33)SCG1supports assignment of multiple IA_NA and IAPD to CPEs behind a CM. This feature includes support for link-local addresses and IA_NA and IAPD. However, a CM can be assigned only one IA_NA. This IA_NA can be either static or DHCP-assigned.

The CPEs behind the CM can request for multiple DHCPv6 IA_NAs and IAPDs. Each CPE is assigned multiple IA_NAs and IAPDs in a single Advertise/Reply message. Each CPE request for IA_NA and IAPD is treated as a separate Advertise/Reply message.

IPv6 Neighbor Discovery Gleaning

The IPv6 Neighbor Discovery (ND) Gleaning feature enables Cisco CMTS routers to automatically recover lost IPv6 CPE addresses and update the CPE records in the Cisco CMTS subscriber database. The Cisco CMTS router gleans only the solicited neighbor advertise (NA) messages transmitted in the upstream direction. IPv6 ND gleaning is similar to Address Resolution Protocol (ARP) gleaning for IPv4 CPE recovery.

The IPv6 ND Gleaning feature is configured by default on Cisco CMTS routers. To disable this feature, use the **no** form of the **cable nd** command in bundle interface configuration mode. The **cable nd** command adds a CPE (host behind a cable modem) to the Cisco CMTS subscriber database. This command does not impact the IPv6 ND protocol operation on the router.

Note The IPv6 ND Gleaning feature does not support gleaning of NA messages transmitted in the downstream direction.

IPv6 Address Packet Intercept

The IPv6 Address Packet Intercept feature provides lawful intercept of cable modems and CPEs provisioned with IPv6 addresses. This feature taps all the packets received and sent from the system. The intercepted packets are sent to the MD with the content connection identifier (CCCID) specified by the tapping rule.

For more information on IPv6 Address Packet Intercept, see the IPv6 Address Packet Intercept feature guide.

How to Configure IPv6 on Cable

This section includes the following tasks:

Configuring IPv6 Switching Services

The CMTS routers support forwarding of unicast and multicast IPv6 traffic using either Cisco Express Forwarding for IPv6 (CEFv6) or distributed CEFv6 (dCEFv6):

- CEFv6—All CMTS platforms
- dCEFv6—Cisco uBR10012 universal broadband router only

The CMTS routers also support Unicast Reverse Path Forwarding (RPF), as long as you enable Cisco Express Forwarding switching or distributed Cisco Express Forwarding switching globally on the router. There is no need to configure the input interface for Cisco Express Forwarding switching. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.

To configure forwarding of IPv6 traffic using Cisco Express Forwarding or distributed Cisco Express Forwarding (supported on the Cisco uBR10012 universal broadband router only) on the CMTS routers, you must configure forwarding of IPv6 unicast datagrams using the **ipv6 unicast-routing** global configuration command, and you must configure an IPv6 address on the bundle interface using the **ipv6 address** command.

The **show ipv6 cef platform** command is supported on the Cisco CMTS platform from Cisco IOS Release 12.2(33)SCE onwards. You can use the **show ipv6 cef platform** command for debugging purposes.

Before You Begin

- You must enable Cisco Express Forwarding for IPv4 globally on the router by using the **ip cef** or **ip cef distributed** command before configuring Cisco Express Forwarding v6 or distributed Cisco Express Forwarding v6.

Note The **ip cef** command is enabled by default on all Cisco CMTS routers. Therefore, you only must configure the command if it has been disabled. However, you must explicitly configure the **ip cef distributed** command on a Cisco uBR10012 universal broadband router if you want to run distributed CEF switching services for IPv4 or IPv6.

- You must configure forwarding of IPv6 unicast datagrams using the **ipv6 unicast-routing** global configuration command.
- You must configure IPv6 addressing on the cable bundle interface.
- CEF switching is required for Unicast RPF to work.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	Do one of the following:
	• **ip cef**
	• **ip cef distributed**
	Example:
	`Router(config)# ip cef`
	`or`
	`Router(config)# ip cef distributed`
		Enables Cisco Express Forwarding.
		or
		Enables distributed Cisco Express Forwarding for IPv4 datagrams.
		Note For CMTS routers, distributed Cisco Express Forwarding is supported only on a Cisco uBR10012 universal broadband router.

Step 4	Do one of the following:
	• **ipv6 cef**
	• **ipv6 cef distributed**
	Example:
	`Router(config)# ipv6 cef`
	`or`
	`Router(config)# ipv6 cef distributed`
		Enables Cisco Express Forwarding v6.
		or
		Enables distributed Cisco Express Forwarding v6 for IPv6 datagrams.
		Note For CMTS routers, distributed Cisco Express Forwarding v6 is supported only on a Cisco uBR10012 universal broadband router.

Step 5	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.

What to Do Next

- (Optional) Enable IPv6 multicast routing using the **ipv6 multicast-routing** command in global configuration mode and configure other multicast features.

Note In Cisco IOS Release 12.2(33)SCA, the Cisco CMTS routers do not support OSPF with IPv6 multicast routing.

Implementing IPv6 Addressing and Basic Connectivity for Cable Interfaces and Bundles

Configuring the Cable Virtual Bundle Interface

The only required IPv6 configuration on a cable line card interface is the IP provisioning mode. The remainder of the IPv6 features are configured at the virtual bundle interface, which is then associated with a particular cable line card interface to establish its configuration.

Most of the IPv6 features that are supported in interface configuration mode (both cable-specific as well as platform-independent IPv6 features) are configured at a cable bundle interface.

The Cisco CMTS routers support IPv6 routing on the bundle interface and map both IPv6 unicast and multicast addresses into the cable bundle forwarding table, for packet forwarding.

Each bundle interface has a unique link-local address (LLA) to support link-local traffic when IPv6 is enabled. Cisco CMTS routers can support a maximum of 40 active bundle interfaces, which also translates to a maximum of 40 active IPv6-enabled bundle interfaces.

Starting with Cisco IOS Release 12.3(33)SCB10, IPv6 commands can be configured on multiple bundle subinterfaces.

Before You Begin

The **cable ipv6 source-verify** and **cable nd** commands are not compatible with each other in Cisco IOS release 12.2(33)SCE and later. You must disable IPv6 ND gleaning using the **no** form of the **cable nd** command before using the **cable ipv6 source-verify** command to ensure that only DHCPv6 and SAV-based CPEs can send traffic on the router.

Restriction All multicast traffic is flooded onto bundle member interfaces.

DETAILED STEPS

	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`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface bundle** *n* **Example:** `Router(config)# interface bundle 1`	Specifies the cable bundle interface and enters interface configuration mode, where *n* specifies the number of the bundle interface.
Step 4	**ipv6 address***ipv6-prefix*/*prefix-length* [**eui-64**] **Example:** `Router(config-if)# ipv6 address 2001:DB8::/32 eui-64`	Specifies an IPv6 network assigned to the interface and enables IPv6 processing on the interface. The ipv6 address eui-64 command configures site-local and global IPv6 addresses with an interface identifier (ID) in the low-order 64 bits of the IPv6 address. You need to specify only the 64-bit network prefix for the address; the last 64 bits are automatically computed from the interface ID.
Step 5	**ipv6 address***ipv6-prefix* /*prefix-length* **link-local** **Example:** `Router(config-if)# ipv6 address 2001:DB8::/32 link-local`	(Optional) Specifies an IPv6 address assigned to the interface and enables IPv6 processing on the interface. The **ipv6 address link-local** command configures a link-local address on the interface that is used instead of the link-local address that is automatically configured, when IPv6 is enabled on the interface (using the **ipv6 enable** command).
Step 6	**ipv6 enable** **Example:** `Router(config-if)# ipv6 enable`	Automatically configures an IPv6 link-local address on the interface while also enabling the interface for IPv6 processing. The link-local address can be used only to communicate with nodes on the same link.
Step 7	cable ipv6 source-verify **Example:** `Router(config-if)# cable ipv6 source-verify`	(Optional) Enables source verification of MAC address-MD-SID-IPv6 address binding packets received by a cable interface upstream on Cisco CMTS routers. **Note** DHCPv6 leasequery is not supported in Cisco IOS release 12.2(33)SCE.

What to Do Next

- Configure the desired platform-independent IPv6 features on the bundle interface, such as Neighbor Discovery and DHCPv6 features.
- Configure the IP provisioning mode and bundle on the cable interface.

Configuring the IP Provisioning Mode and Bundle on the Cable Interface

The CMTS routers allow you to configure cable interfaces to support cable modems provisioned for both IPv4 and IPv6 addressing support (known as “dual stack”), only IPv4 addressing, or only IPv6 addressing. Prior to cable modem registration, the CMTS router sends its supported provisioning mode to the cable modem in the MDD message.

In addition to configuring the provisioning mode on the cable interface, you must also associate the cable interface with a cable bundle. You perform most of the other IPv6 feature configuration at the bundle interface.

Note This section describes only the commands associated with establishing IPv6 support on a CMTS router. Other cable interface commands that apply but are optional are not shown, such as to configure upstream and downstream features.

Before You Begin

Configuration of a bundle interface is required.

Restriction APM is not supported in Cisco IOS Release 12.2(33)SCA. Support for APM feature is provided from Cisco IOS Release 12.2(33)SCC onwards.

Note Starting from Cisco IOS Release 12.2(33)SCC onwards, the port parameter of the interface cable was changed to *cable-interface-index* to indicate the MAC domain index for the Cisco UBR-MC and Cisco uBR-MC3GX60V cable interface line cards.

DETAILED STEPS

	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`	Enters global configuration mode.

Step 3	**interface cable** {*slot* / *port* | *slot* / *subslot* /*port* }
	Example:
	`Router(config)# interface cable 5/0/1`
		Specifies the cable interface line card, where:
		The valid values for these arguments are dependent on your CMTS router and cable interface line card. Refer to the hardware documentation for your router chassis and cable interface line card for supported slot and port numbering.

Step 4	**cable ip-init** {**apm** | **dual-stack** | **ipv4** | **ipv6**}
	Example:
	`Router(config-if)# cable ip-init ipv6`
		Specifies the IP provisioning mode supported by the cable interface, where:

Step 5	**cable bundle***n* **Example:** `Router(config)# cable bundle 1`	Associates the cable interface with a configured virtual bundle interface, where *n* specifies the number of the bundle interface.

What to Do Next

- Proceed to configuring any other cable interface features that you want to support, such as upstream and downstream features. For more information about the other cable interface features, refer to the *Cisco IOS CMTS Cable Software Configuration Guide* .
- Proceed to configure other optional IPv6 cable features.

Configuring IPv6 Cable Filter Groups

Cisco IOS Release 12.2(33)SCA extends the CMTS router IPv4 cable filter group capability to add support for IPv6 filter options.

Cable Filter Groups and the DOCSIS Subscriber Management MIB

Cable subscriber management is a DOCSIS 1.1 specification, which can be established using the following configuration methods:

- CMTS router configuration (via CLI)
- SNMP configuration
- DOCSIS 1.1 configuration file (TLVs 35, 36, and 37)

This section describes the IPv6 cable filter group feature support of the packet filtering portion of the DOCSIS Subscriber Management MIB (DOCS-SUBMGMT-MIB) using configuration commands on the CMTS routers. This IPv6 cable filter group support extends filter classifiers with IPv6 addressing options for CM and CPE traffic, but is independent of DOCSIS IPv6 classifiers, which are used to match packets to service flows.

Configuration of IPv6 cable filter groups on the CMTS routers is supported according to the following guidelines:

- A cable filter group consists of a set of **cable filter group** commands that share the same group ID.
- Separate indexes can be used to define different sets of filters for the same group ID. This can be used to define both IPv4 and IPv6 filters to the same filter group.
- CMs can be associated with one upstream and one downstream filter group.
    - ◦ Upstream traffic—All traffic coming from CMs is evaluated against the assigned upstream filter group that is configured by the **cable submgmt default filter-group cm upstream** command.
    - ◦ Downstream traffic—All traffic going to CMs is evaluated against the assigned downstream filter group that is configured by the **cable submgmt default filter-group cm downstream** command.
- CPEs can be associated with one upstream and one downstream filter group.
    - ◦ Upstream traffic—All traffic coming from CPEs is evaluated against the assigned upstream filter group that is configured by the **cable submgmt default filter-group cpe upstream** command.

- ◦ Downstream traffic—All traffic going to CPEs is evaluated against the assigned downstream filter group that is configured by the **cable submgmt default filter-group cpe downstream** command.

Note Because TLVs 35, 36, and 37 do not apply to DOCSIS 1.0 CM configuration files, the only way to enable cable subscriber management for a DOCSIS 1.0 CM is to configure it explicitly on the Cisco CMTS router and activate it by using the **cable submgmt default active** global configuration command.

Before You Begin

You must create the cable filter group before you assign it to a CM or CPE upstream or downstream.

Restriction

- Chained IPv6 headers are not supported.
- An individual filter group index cannot be configured to support both IPv4 and IPv6 versions at the same time. If you need to support IPv4 and IPv6 filters for the same filter group, then you must use a separate index number with the same filter group ID, and configure one index as **ip-version ipv4**, and the other index as **ip-version ipv6**.
- Only a single upstream and a single downstream filter group can be assigned for CM traffic.
- Only a single upstream and a single downstream filter group can be assigned to CPEs attached to a CM such that all CPEs behind a CM share a common filter group.
- For the filter group to work for CMs, a CM must re-register after the CMTS router is configured for the filter group.
- If parallel eXpress forwarding (PXF) is configured on the Cisco uBR10012 router, either the **cable filter group** commands or the interface ACL (**ip access-list**) command can be configured.
- If you do not provision TLVs 35, 36, and 37 in the DOCSIS CM configuration file, then you must activate the functionality by specifying the **cable submgmt default active** global configuration command on the CMTS router.

DETAILED STEPS

	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`	Enters global configuration mode.
Step 3	**cable filter group***group-id* **index***index-num***dest-port***port-num*	(Optional) Specifies the TCP/UDP destination port number that should be matched. The valid range is from 0 to 65535.

	Command or Action	Purpose
	Example: `Router(config)# cable filter group 1 index 1 dest-port 69`	The default value matches all TCP/UDP port numbers (IPv4 and IPv6 filters).
Step 4	**cable filter group** *group-id* **index** *index-num* **ip-proto** *proto-type* **Example:** `Router(config)# cable filter group 1 index 1 ip-proto 17`	(Optional) Specifies the IP protocol type number that should be matched. The valid range is from 0 to 256, with a default value of 256 that matches all protocols (IPv4 and IPv6 filters). Some commonly used values are:
Step 5	**cable filter group** *group-id* **index** *index-num* **ip-tos** *tos-mask tos-value* **Example:** `Router(config)# cable filter group 1 index 1 ip-tos 0xff 0x80`	(Optional) Specifies a ToS mask and value to be matched (IPv4 and IPv6 filters): The *tos-mask* is logically ANDed with the *tos-value* and compared to the result of ANDing the *tos-mask* with the actual ToS value of the packet. The filter considers it a match if the two values are the same. The default values for both parameters matches all ToS values.
Step 6	**cable filter group** *group-id* **index** *index-num* **ip-version ipv6** **Example:** `Router(config)# cable filter group 1 index 1 ip-version ipv6`	Specifies that this filter group is an IPv6 filter group.

Step 7	**cable filter group** *group-id* **index** *index-num* **match-action** {**accept** | **drop**}
	Example:
	`Router(config)# cable filter group 1 index 1 match-action drop`
		(Optional) Specifies the action that should be taken for packets that match this filter (IPv4 and IPv6 filters):

Step 8	**cable filter group** *group-id* **index** *index-num* **src-port** *port-num* **Example:** `Router(config)# cable filter group 1 index 1 src-port 50`	(Optional) Specifies the TCP/UDP source port number that should be matched. The valid range is from 0 to 65535. The default value matches all TCP/UDP port numbers (IPv4 and IPv6 filters).

Step 9	**cable filter group** *group-id* **index** *index-num* **status** {**active** | **inactive**}
	Example:
	`Router(config)# cable filter group 1 index 1 status inactive`
		(Optional) Enables or disables the filter (IPv4 and IPv6 filters):
		Note You must create a filter group using at least one of the other options before you can use this command to enable or disable the filter.

	Command or Action	Purpose
Step 10	**cable filter group** *group-id* **index** *index-num* **tcp-flags** *flags-mask flags-value* **Example:** `Router(config)# cable filter group 1 index 1 tcp-flags 0 0`	(Optional) Specifies the TCP flag mask and value to be matched (IPv4 and IPv6 filters):
Step 11	**cable filter group** *group-id* **index** *index-num* **v6-dest-address** *ipv6-address* **Example:** `Router(config)# cable filter group 1 index 1 v6-dest-address 2001:DB8::/32`	(Optional) Specifies the IPv6 destination address that should be matched using the format X:X:X:X::X (IPv6 filters only).
Step 12	**cable filter group** *group-id* **index** *index-num* **v6-dest-pfxlen** *prefix-length* **Example:** `Router(config)# cable filter group 1 index 1 v6-dest-pfxlen 64`	(Optional) Specifies the length of the network portion of the IPv6 destination address. The valid range is from 0 to 128.
Step 13	**cable filter group** *group-id* **index** *index-num* **v6-src-address** *ipv6-address* **Example:** `Router(config)# cable filter group 1 index 1 v6-src-address 2001:DB8::/32`	(Optional) Specifies the IPv6 source address that should be matched using the format X:X:X:X::X (IPv6 filters only).
Step 14	**cable filter group** *group-id* **index** *index-num* **v6-src-pfxlen** *prefix-length* **Example:** `Router(config)# cable filter group 1 index 1 v6-src-pfxlen 48`	(Optional) Specifies the length of the network portion of the IPv6 source address. The valid range is from 0 to 128 (IPv6 filters only).
Step 15	**cable submgmt default filter-group** {**cm** | **cpe**} {**downstream** | **upstream**} *group-id* **Example:** `Router(config)# cable submgmt default filter-group cm upstream 1`	Applies a defined filter group (by specifying its *group-id)* to either a CM or its CPE devices, for downstream or upstream traffic.
Step 16	**cable submgmt default active** **Example:** `Router(config)# cable submgmt default active`	(Required if you do not provision TLVs 35, 36, and 37 in the DOCSIS 1.1 CM configuration file) Enables filters and allows the CMTS to manage the CPE devices for a particular CM (sets the docsSubMgtCpeActiveDefault attribute to TRUE).

The following example shows how to create an IPv6 filter group with ID 254 and an index number of 128. The **ip-version ipv6** keywords must be configured to create the IPv6 filter group; otherwise, the default is an IPv4 filter group:

```
configure terminal
cable filter group 254
 index 128 v6-src-address 2001:DB8::/32
cable filter group 254
 index 128 v6-src-pfxlen 48
cable filter group 254
 index 128 v6-dest-address 2001:DB8::/32
cable filter group 254
 index 128 v6-dest-pfxlen 64
cable filter group 254
 index 128 ip-version ipv6
cable filter group 254
 index 128 match-action drop
cable submgmt default filter-group cm upstream 254
```

This group filters CM upstream traffic and drops any packets with an IPv6 source address of 2001:33::20B:BFFF:FEA9:741F (with network prefix of 128) destined for an IPv6 address of 2001:DB8::/32 (with network prefix of 128).

All of the **cable filter group** commands are associated by their group ID of 254 (and index of 128), and the **cable submgmt default filter-group** command applies the corresponding filter group ID of 254 to CM upstream traffic.

To monitor your cable filter group configuration, use forms of the **show cable filter** command as shown in the following examples. In these output examples, the output from the **show cable filter**, **show cable filter group 254**, and **show cable filter group 254 index 128** commands all display the same information because there is currently only a single filter group and index defined.

Note The "Use Verbose" string appears in the output area of the SrcAddr/mask and DestAddr/Mask fields suggesting use of the **show cable filter group verbose** form of the command to display the complete IPv6 address.

```
Router# show cable filter
Filter    SrcAddr/Mask       DestAddr/Mask      Prot ToS  SPort DPort TCP   Action Status
Grp Id v6                                                             Flags
254 128Y  Use Verbose
        Use Verbose
                                    drop   active
Router# show cable filter group 254
Filter    SrcAddr/Mask       DestAddr/Mask      Prot ToS  SPort DPort TCP   Action Status
Grp Id v6                                                             Flags
254 128Y  Use Verbose        Use Verbose                                    drop   active
Router# show cable filter group 254 index 128
Filter    SrcAddr/Mask       DestAddr/Mask      Prot ToS  SPort DPort TCP   Action Status
Grp Id v6                                                             Flags
254 128Y  Use Verbose        Use Verbose                                    drop   active
Router# show cable filter group 254 index 128 verbose
Filter Group                         : 254
Filter Index                         : 128
Filter Version                       : IPv6
Matches                              : 0
    Source IPv6 address              : 2001:DB8::/32
    Destination IPv6 address         : 2001:DB8::/32
    Match action                     : drop
    Status                           : active
```

Troubleshooting Tips

You should configure the **cable filter group** commands prior to applying a filter group using the **cable submgmt default filter-group** command. Failure to do so results in the following message, and an association to a filter group that is undefined:

```
Router(config)# cable submgmt default filter-group cm upstream 100
Default value set to a nonexistent filter-group 100.
```

Configuring IPv6 Domain Name Service

Cisco IOS Release 12.2(33)SCA introduces the domain name service (DNS) capability for devices using IPv6 addressing on the Cisco CMTS routers.

Cisco IOS Release 12.2(33)SCA introduces the domain name service (DNS) capability for devices using IPv6 addressing on the Cisco CMTS routers.

DNS simplifies the identification of cable devices by associating a hostname with what can often be a complex 128-bit IPv6 address. The hostname can then be used in place of the IPv6 address within the CMTS router CLI that supports use of hostnames.

There are two separate DNS caches supported on a CMTS router—an IOS DNS cache and a cable-specific DNS cache that stores IPv6 addresses learned by the CMTS router for CMs and CPEs.

In this phase of the IPv6 DNS service on cable, the DNS server is queried for domain name information as needed when you use the **show cable modem domain-name** command. When you use this command, the following actions take place:

1. The CMTS router checks whether CMs are online. If a CM is online, the CMTS router uses the corresponding IPv6 address assigned to the CM and looks up its domain name from the IOS DNS cache.
2. If no match is found, the CMTS router sends a DNS-QUERY message with the IPv6 address of the CM to the DNS server, which tries to resolve the domain name.
3. When the DNS reply is received, the CMTS router stores the domain name in the IOS DNS cache for each IPv6 address.
4. The CMTS router also stores the fully-qualified domain name (FQDN) that is replied by the DNS server in the cable-specific DNS cache.

Note Running the **no ip domain lookup** command turns off the DNS resolution.

The following platform-independent Cisco IOS software commands are supported using host names by the CMTS router for IPv6 DNS on cable:

- **connect**
- **ping ipv6**
- **show hosts**
- **telnet**
- **traceroute**

Before You Begin

- A DNS server must be configured.
- You must identify and assign the host names to the IPv6 addresses. If you are using the Cisco DNS server, use the **ip host** global configuration command to map hostnames to IP addresses.
- You must configure the DNS server using the **ip name-server** global configuration command before use of DNS host names (or domains) are available in the supported commands.
- The **show cable modem domain-name** command must be run first on the Route Processor (RP) of the CMTS router before any domain name can be used as part of a cable command.

For more information about configuring these prerequisites and related IP domain configuration options, refer to the *Mapping Host Names to IP Addresses* section in the *Cisco IOS IP Configuration Guide* at: http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfipadr.html#wp1001317

Restriction

- DNS for cable devices using IPv4 addressing is not supported.
- Due to column size limitations within the command-line interface (CLI), the domain name display is limited to 32 characters. Therefore, the entire domain name cannot always be seen in CMTS router command output.
- Only those cable devices where IPv6 address learning takes place are supported, such as acquiring an IPv6 address through DHCPv6 or the IPv6 (ND) process.
- The cable-specific DNS cache is only updated when you use the **show cable modem domain-name** command on the Route Processor (RP). A DNS-QUERY can only be sent on the RP using this command, therefore the DNS cache cannot update if you use the **show cable modem domain-name** command on a line card console. The output is displayed on the RP only.
- The cable-specific DNS cache does not store partially qualified domain names, only FQDNs are stored.
- The cable-specific DNS cache is not associated with the timeouts that apply to the IOS DNS cache. Therefore, a cable-specific DNS cache entry is not removed when an IOS DNS cache timeout occurs for that device. The cable-specific DNS cache is only updated when you use the **show cable modem domain-name** command.
- The CMTS router supports storage of only one domain name per IPv6 address in the cable-specific DNS cache.
- Domain names for the link local address are not supported.
- The **no ip domain-name** command disables DNS lookup.

DETAILED STEPS

	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`	Enters global configuration mode.
Step 3	**ip name-server** [**vrf** *vrf-name*] *server-address1* [*server-address2*...*server-address6*] **Example:** `Router(config)# ip name-server 2001:DB8::/32`	Specifies the address of one or more name servers to use for name and address resolution.
Step 4	**exit** **Example:** `Router(config)# exit`	Leaves global configuration mode and enters privileged EXEC mode.
Step 5	**show cable modem domain-name** **Example:** `Router# show cable modem domain-name`	Updates the cable-specific DNS cache and displays the domain name for all CMs and the CPE devices behind a CM.

Configuring IPv6 Source Verification

Typically, the IPv6 source verification feature is enabled on a cable bundle interface. From there, the cable interface is associated with the virtual bundle interface to acquire its configuration.

When you enable IPv6 source verification on a cable line card interface, the source verification routine verifies the MAC address-MD-SID-IP binding of the packet. If the source verification succeeds, the packet is forwarded. If the verification fails, the packet is dropped.

When a CM is operating as a bridge modem device, then the CMTS router verifies all the IPv6 addresses related to that CM and the CPEs behind that CM.

The **cable ipv6 source-verify** command controls only the source verification of IPv6 packets. For IPv4-based source verification, use the **cable source-verify** command, which also supports different options.

For more information about how to configure IPv6 source verification on a bundle interface, see the Configuring the Cable Virtual Bundle Interface, on page 66.

Restrictions

Source verification of IPv6 packets occurs only on packets in the process-switched path of the Route Processor (RP).

Note Source verification of IPv6 packets in PXF is supported on the Cisco CMTS routers from Cisco IOS Release 12.2(33)SCE onwards.

Configuring IPv6 VPN over MPLS

Starting with Cisco IOS Release 12.2(33)SCF, the Cisco CMTS routers support the IPv6 VPN over MPLS (6VPE) feature. Implementing this feature includes the following configuration tasks.

- Configuring a VRF instance for IPv6
- Binding a VRF to an interface
- Creating a subinterface
- Configuring a static route for PE-to-CE-routing
- Configuring eBGP PE-to-CE routing sessions
- Configuring the IPv6 VPN address family for iBGP
- Configuring route reflectors for improved scalability
- Configuring Internet access

For detailed information about these tasks, see the Implementing IPv6 VPN over MPLS chapter in the Cisco IOS IPv6 Configuration Guide, Release 12.2SR at: http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sr/ip6-ov-mpls-6vpe.html.

For detailed information about the configuration examples, see Configuration Examples for IPv6 on Cable, on page 81.

Note Starting from Cisco IOS Release 12.2(33)SCF2, the IPv6 address of the sub-bundle interface (to which the CM is connected) is used in the DHCPv6 relay packet of the CPE DHCPv6 request. If the DHCPv6 packet has to go from one VRF interface to another, the IPv6 address of each VRF interface should be configured on the Cisco CMTS to establish connectivity.

Configuring DHCPv6 Relay Agent

Starting with Cisco IOS Release 12.2(33)SCE5, the Cisco CMTS router supports DHCPv6 relay agent to forward relay-forward messages from a specific source address to client relay destinations.

Perform the steps given below to enable the DHCPv6 relay agent function and specify relay destination addresses on an interface.

Before You Begin

The relay-forward messages should contain specific source IPv6 address. This is required because the firewall deployed between the Cisco CMTS DHCPv6 relay agent and the DHCPv6 server expects only one source address for one Cisco CMTS bundle interface.

Restriction If you change one or more parameters of the **ipv6 dhcp relay destination** command, you have to disable the command using the **no** form, and execute the command again with changed parameters.

DETAILED STEPS

	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`	Enters global configuration mode.
Step 3	**interface type** *number* **Example:** `Router(config)# interface ethernet 4/2`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 dhcp relay destination** *ipv6-address*[*interface*] [**link-address** *link-address*] [**source-address** *source-address*] **Example:** `Router(config-if) ipv6 dhcp relay destination 2001:db8:1234::1 ethernet 4/2 link-address 2001:db8::1 source-address 2001:db8::2`	Specifies a destination address to which client packets are forwarded and enables DHCPv6 relay service on the interface.

Step 5	**end**
	Example:
	`Router(config-if) end`
		Exits interface configuration mode and enters privileged EXEC mode.

Disabling IPv6 ND Gleaning

You must disable IPv6 ND gleaning before configuring IPv6 source verification using DHCPv6 leasequery.

DETAILED STEPS

	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`	Enters global configuration mode.
Step 3	**interfacebundle** *bundle-no* **Example:** `Router(config)# interface bundle 1`	Specifies a bundle interface number and enters bundle interface configuration mode. - *bundle-no* —Bundle interface number. The valid range is from 1 to 255.
Step 4	**no cable nd** **Example:** `Router(config-if) no cable nd`	Disables IPv6 ND gleaning on the Cisco CMTS router.

Step 5	**end**
	Example:
	`Router(config-if) end`
		Returns to privileged EXEC mode.

How to Verify IPv6 Dual Stack CPE Support

This section describes how to use **show** commands to verify the configuration of the IPv6 Dual Stack CPE Support on the CMTS feature in Cisco IOS Release 12.2(33)SCC.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose

Step 2	**show cable modem** [*ip-address* | *mac-address*] **ipv6**[**cpe** | **prefix** | **registered** | **unregistered]**
	Example:
	`Router# show cable modem ipv6 registered`
	Example:
	`Router# show cable modem 0019.474a.c14a ipv6 cpe`
		Displays IPv6 information for specified CMs and CPEs behind a CM on a Cisco CMTS router. You can specify the following options:

Step 3	**show cable modem** [ip-address | mac-address] **registered** **Example:** `Router# show cable modem 0019.474e.e4DF registered`	Displays a list of the CMs that have registered with the Cisco CMTS. You can specify the following options:
Step 4	**show cable modem** {ip-address | mac-address} **cpe** **Example:** `Router# show cable modem 0019.474a.c14a cpe`	Displays the CPE devices accessing the cable interface through a particular CM. You can specify the following options:

Examples

Use the **show cable modem ipv6** command to display the IPv6 portion of a dual stack CPE and use the **show cable modem cpe** command to display the IPv4 mode of a dual stack CPE. Both **show cable modem ipv6 registered** and **show cable modem registered** commands display CPE count as one for a dual stack CPE.

The following example shows the output of the **show cable modem ipv6** command:

```
Router# show cable modem ipv6 registered
Interface   Prim Online       CPE IP Address                              MAC Address
            Sid  State
C4/0/U2     1    online       0   ---                                     0019.474a.c18c
C4/0/U2     3    online(pt)   1   2001:420:3800:809:EDA4:350C:2F75:4779   0019.474a.c14a
Router# show cable modem 0019.474a.c14a ipv6 cpe
MAC Address    IP Address                              Domain Name
0005.0052.2c1d 2001:420:3800:809:48F7:3C33:B774:9185
```

Starting from Cisco IOS Release 12.2(33)SCG1, the output of the show cable modem ipv6 command for keyword cpe is changed.

The following example shows the output of the **show cable modem ipv6** command:

```
Router# show cable modem
 0023.bed9.4c8e ipv6 cpe
Load for five secs: 0%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *06:37:20.439 UTC Thu Aug 2 2012
MAC Address    IP Address
0023.bed9.4c91 2001:40:3:4:200:5EB7:BB6:C759
2001:40:3:4:210:D73B:7A50:2D05
```

The following example shows the output of the **show cable modem registered** command:

```
Router# show cable modem registered
```

```
Interface   Prim Online      Timing Rec   QoS CPE IP address      MAC address
            Sid  State       Offset Power
C4/0/U2     3    online      1022   0.00  2   1   50.3.37.12      0019.474a.c14a
```

The following example shows the output of the **show cable modem cpe** command:

```
Router# show cable modem 0019.474a.c14a cpe

IP address        MAC address      Dual IP
```

50.3.37.3 0005.0052.2c1d Y

Configuration Examples for IPv6 on Cable

This section includes the following examples:

Example: IPv6 over Subinterfaces

The following example shows the CMTS bundle configuration that can be used with subinterfaces:

```
Router# show cable modem ipv6
Device Type: B - CM Bridge, R - CM Router
IP Assignment Method: D - DHCP
MAC Address    Type Interface    Mac State    D/IP IP Address
0019.474a.c18c B/D  C4/0/U2      online        Y  2001:420:3800:809:4C7A:D518:91
C6:8A18
Router# show run interface bundle2
Building configuration...
Current configuration : 138 bytes
!
interface Bundle2
 no ip address
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
 no cable ip-multicast-echo
end
Router#

show run interface bundle2.1
Building configuration...
Current configuration : 382 bytes
!
interface Bundle2.1
 ip address 50.3.37.1 255.255.255.0
 no cable ip-multicast-echo
 cable helper-address 10.10.0.12
 ipv6 address 2001:DB8::/32
 ipv6 enable
 ipv6 nd prefix default no-advertise
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd ra interval msec 2000
 ipv6 dhcp relay destination 2001:420:3800:800:203:BAFF:FE11:B644
 arp timeout 240
end
```

Example: Basic IPv6 Cable Filter Groups

The following example shows the configuration of an IPv6 filter group that drops traffic from a specific IPv6 host (with source address 2001:DB8::1/48) behind a cable router to an IPv6 host on the network (with destination address 2001:DB8::5/64):

```
configure terminal
!
! Specify the filter group criteria using a common group ID
!
cable filter group 254 index 128 v6-src-address 2001:DB8::1
cable filter group 254 index 128 v6-src-pfxlen 128
cable filter group 254 index 128 v6-dest-address 2001:DB8::5
cable filter group 254 index 128 v6-dest-pfxlen 128
!
! Specify that the filter group is IP version 6
!
cable filter group 254 index 128 ip-version ipv6
!
! Specify the drop action for matching packets
!
cable filter group 254 index 128 match-action drop
!
! Apply the filter group with ID 254 to all CM upstream traffic
!
cable submgmt default filter-group cm upstream 254
```

Example: Complete Cable Configuration with IPv6

The following example shows a complete cable configuration example; it also displays the configuration of multiple cable filter groups using both IPv4 and IPv6 and separate indexes to associate the filter definitions with the same group ID.

```
Router# show running-config
Building configuration...
Current configuration : 15010 bytes
!
! Last configuration change at 08:32:14 PST Thu Nov 8 2007
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service compress-config
!
hostname router
!
boot-start-marker
boot-end-marker
!
enable password password1
!
no aaa new-model
clock timezone PST -9
clock summer-time PDT recurring
clock calendar-valid
facility-alarm core-temperature major 53
facility-alarm core-temperature minor 45
facility-alarm core-temperature critical 85
facility-alarm intake-temperature major 49
facility-alarm intake-temperature minor 40
facility-alarm intake-temperature critical 67
```

```
!
!
card 1/0 2jacket-1
card 1/0/0 24rfchannel-spa-1
card 5/0 5cable-mc520h-d
cable admission-control preempt priority-voice
cable modem vendor 00.18.68 SA-DPC2203
cable modem vendor 00.19.47 SA-DPC2505
no cable qos permission create
no cable qos permission update
cable qos permission modems
!
cable filter group 1 index 1 src-ip 0.0.0.0
cable filter group 1 index 1 src-mask 0.0.0.0
cable filter group 1 index 1 dest-ip 0.0.0.0
cable filter group 1 index 1 dest-mask 0.0.0.0
cable filter group 2 index 1 src-ip 0.0.0.0
cable filter group 2 index 1 src-mask 0.0.0.0
cable filter group 2 index 1 dest-ip 0.0.0.0
cable filter group 2 index 1 dest-mask 0.0.0.0
cable filter group 3 index 1 src-ip 0.0.0.0
cable filter group 3 index 1 src-mask 0.0.0.0
cable filter group 3 index 1 dest-ip 0.0.0.0
cable filter group 3 index 1 dest-mask 0.0.0.0
cable filter group 4 index 1 src-ip 0.0.0.0
cable filter group 4 index 1 src-mask 0.0.0.0
cable filter group 4 index 1 dest-ip 0.0.0.0
cable filter group 4 index 1 dest-mask 0.0.0.0
cable filter group 5 index 1 src-ip 0.0.0.0
cable filter group 5 index 1 src-mask 0.0.0.0
cable filter group 5 index 1 dest-ip 0.0.0.0
cable filter group 5 index 1 dest-mask 0.0.0.0
cable filter group 6 index 1 src-ip 0.0.0.0
cable filter group 6 index 1 src-mask 0.0.0.0
cable filter group 6 index 1 dest-ip 0.0.0.0
cable filter group 6 index 1 dest-mask 0.0.0.0
cable filter group 7 index 1 src-ip 0.0.0.0
cable filter group 7 index 1 src-mask 0.0.0.0
cable filter group 7 index 1 dest-ip 0.0.0.0
cable filter group 7 index 1 dest-mask 0.0.0.0
cable filter group 8 index 1 src-ip 0.0.0.0
cable filter group 8 index 1 src-mask 0.0.0.0
cable filter group 8 index 1 dest-ip 0.0.0.0
cable filter group 8 index 1 dest-mask 0.0.0.0
cable filter group 9 index 1 src-ip 0.0.0.0
cable filter group 9 index 1 src-mask 0.0.0.0
cable filter group 9 index 1 dest-ip 0.0.0.0
cable filter group 9 index 1 dest-mask 0.0.0.0
cable filter group 10 index 1 src-ip 0.0.0.0
cable filter group 10 index 1 src-mask 0.0.0.0
cable filter group 10 index 1 dest-ip 0.0.0.0
cable filter group 10 index 1 dest-mask 0.0.0.0
cable filter group 12 index 1 src-ip 0.0.0.0
cable filter group 12 index 1 src-mask 0.0.0.0
cable filter group 12 index 1 dest-ip 0.0.0.0
cable filter group 12 index 1 dest-mask 0.0.0.0
cable filter group 16 index 1 src-ip 0.0.0.0
cable filter group 16 index 1 src-mask 0.0.0.0
cable filter group 16 index 1 dest-ip 0.0.0.0
cable filter group 16 index 1 dest-mask 0.0.0.0
ip subnet-zero
ip domain name cisco.com
ip host host1 239.192.254.254
ip host host2 239.192.254.253
ip name-server 10.39.26.7
ip name-server 2001:0DB8:4321:FFFF:0:800:20CA:D8BA
!
!
!
!
ipv6 unicast-routing
ipv6 cef
packetcable multimedia
```

```
packetcable
!
!
!
redundancy
 mode sso
!
!
controller Modular-Cable 1/0/0
 annex B modulation 64qam 0 23
 ip-address 10.30.4.175
 modular-host subslot 5/0
 rf-channel 0 cable downstream channel-id 24
 rf-channel 1 cable downstream channel-id 25
 rf-channel 2 cable downstream channel-id 26
 rf-channel 3 cable downstream channel-id 27
 rf-channel 4 cable downstream channel-id 28
 rf-channel 5 cable downstream channel-id 29
 rf-channel 6 cable downstream channel-id 30
 rf-channel 7 cable downstream channel-id 31
 rf-channel 8 cable downstream channel-id 32
 rf-channel 9 cable downstream channel-id 33
 rf-channel 10 cable downstream channel-id 34
 rf-channel 11 cable downstream channel-id 35
 rf-channel 12 cable downstream channel-id 36
 rf-channel 13 cable downstream channel-id 37
 rf-channel 14 cable downstream channel-id 38
 rf-channel 15 cable downstream channel-id 39
 rf-channel 16 cable downstream channel-id 40
 rf-channel 17 cable downstream channel-id 41
 rf-channel 18 cable downstream channel-id 42
 rf-channel 19 cable downstream channel-id 43
 rf-channel 20 cable downstream channel-id 44
 rf-channel 21 cable downstream channel-id 45
 rf-channel 22 cable downstream channel-id 46
 rf-channel 23 cable downstream channel-id 47
!
!
policy-map foo
policy-map 1
policy-map cos
policy-map qpolicy
policy-map shape
policy-map dscp
!
!
!
!
!
!
interface Loopback0
 ip address 127.0.0.1 255.255.255.255
!
interface FastEthernet0/0/0
 ip address 10.39.21.10 255.255.0.0
 speed 100
 half-duplex
 ipv6 address 2001:DB8::/32
 ipv6 enable
!
interface Wideband-Cable1/0/0:0
 no cable packet-cache
 cable bonding-group-id 1
!
interface Wideband-Cable1/0/0:1
 no cable packet-cache
 cable bonding-group-id 2
!
interface Wideband-Cable1/0/0:2
 no cable packet-cache
 cable bonding-group-id 3
!
interface Wideband-Cable1/0/0:3
```

```
 no cable packet-cache
 cable bonding-group-id 4
!
interface Wideband-Cable1/0/0:4
 no cable packet-cache
 cable bundle 1
 cable bonding-group-id 5
 cable rf-channel 1 bandwidth-percent 60
!
interface Wideband-Cable1/0/0:5
 no cable packet-cache
 cable bundle 1
 cable bonding-group-id 6
 cable rf-channel 0 bandwidth-percent 40
 cable rf-channel 2
 cable rf-channel 3
!
interface Wideband-Cable1/0/0:6
 no cable packet-cache
 cable bonding-group-id 7
!
interface Wideband-Cable1/0/0:7
 no cable packet-cache
 cable bonding-group-id 8
!
interface Wideband-Cable1/0/0:8
 no cable packet-cache
 cable bonding-group-id 9
!
interface Wideband-Cable1/0/0:9
 no cable packet-cache
 cable bonding-group-id 33
!
interface Wideband-Cable1/0/0:10
 no cable packet-cache
 cable bonding-group-id 34
!
interface Wideband-Cable1/0/0:11
 no cable packet-cache
 cable bonding-group-id 35
!
interface Cable5/0/0
 no cable packet-cache
 cable bundle 1
 cable downstream channel-id 119
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 99000000
 no cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 0
 cable upstream 0 frequency 6000000
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 3
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Cable5/0/1
 cable ip-init ipv6
 no cable packet-cache
 cable bundle 1
 cable downstream channel-id 120
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 705000000
 no cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 4
 cable upstream 0 frequency 6000000
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 no cable upstream 0 shutdown
 cable upstream 1 connector 5
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 6
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 7
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Cable5/0/2
 no cable packet-cache
 cable downstream channel-id 121
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 8
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 cable upstream 0 shutdown
 cable upstream 1 connector 9
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 10
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 11
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Cable5/0/3
 no cable packet-cache
 cable downstream channel-id 122
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 12
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 cable upstream 0 shutdown
 cable upstream 1 connector 13
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 14
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 15
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Cable5/0/4
 no cable packet-cache
 cable downstream channel-id 123
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 16
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 cable upstream 0 shutdown
 cable upstream 1 connector 17
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 18
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 19
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Bundle1
 ip address 10.46.2.1 255.255.0.0 secondary
 ip address 10.46.1.1 255.255.0.0
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
 cable dhcp-giaddr policy strict
 cable helper-address 10.39.26.8
 ipv6 address 2001:DB8::/32
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd ra interval 5
 ipv6 dhcp relay destination 2001:0DB8:4321:FFFF:0:800:20CA:D8BA
!
ip default-gateway 10.39.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.39.26.12
ip route 192.168.254.253 255.255.255.255 10.39.0.1
ip route 192.168.254.254 255.255.255.255 10.39.0.1
!
!
no ip http server
no ip http secure-server
!
logging cmts cr10k log-level errors
cpd cr-id 1
nls resp-timeout 1
cdp run
!
tftp-server bootflash:docs10.cm alias docs10.cm
tftp-server bootflash:rfsw_x373.bin alias rfsw_x373.bin
snmp-server community private RW
snmp-server enable traps cable
snmp-server manager
!
!
control-plane
!
!
```

```
line con 0
 logging synchronous
 stopbits 1
line aux 0
line vty 0 4
 password lab
 login
!
!
cable fiber-node 1
  downstream Modular-Cable 1/0/0 rf-channel 1
  upstream Cable 5/0 connector 0
!
cable fiber-node 2
  downstream Modular-Cable 1/0/0 rf-channel 0 2-3
  upstream Cable 5/0 connector 4
!
end
```

Example: BGP Configuration for 6VPE

The following example shows a sample BGP configuration on CMTS 6VPE.

```
Router# router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 11.1.1.5 remote-as 1
 neighbor 11.1.1.5 update-source Loopback1
 no auto-summary
 !
 address-family vpnv6               --- Enable vpnv6 AF
  neighbor 11.1.1.5 activate       --- Activate neighbor 6VPE-2
  neighbor 11.1.1.5 send-community extended
 exit-address-family
 !
 address-family ipv6 vrf vrf_mgmt
  redistribute connected            ---- Publish directly connected route
  redistribute static
  no synchronization
 exit-address-family
!
 address-family ipv6 vrf vrfa   --- Enable IPv6 vrf AF for each VRF
  redistribute connected
  no synchronization
 exit-address-family
 !
 address-family ipv6 vrf vrfb --- Enable IPv6 vrf AF for each VRF
  redistribute connected
  no synchronization
 exit-address-family
!
```

Example: Subinterface Configuration for 6VPE

The following example shows how to define a subinterface on virtual bundle interface 1.

When configuring IPv6 VPNs, you must configure the first subinterface created as a part of the management VRF. In the following example, Bundle 1.10 is the first sub-interface, which is configured into management VRF. Make sure the CNR server is reachable in management VRF.

```
interface Bundle1.10                --- Management VRF
 vrf forwarding vrf_mgmt
 cable dhcp-giaddr primary
 ipv6 address 2001:40:3:110::1/64
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination 2001:10:74:129::2
interface Bundle1.11          --- VRF A
 vrf forwarding vrfa
 cable dhcp-giaddr primary
 ipv6 address 2001:40:3:111::1/64
 ipv6 enable
 ipv6 dhcp relay destination 2001:10:74:129::2
interface Bundle1.12          --- VRFB
 vrf forwarding vrfb
 cable dhcp-giaddr primary
 ipv6 address 2001:40:3:112::1/64
 ipv6 enable
 ipv6 dhcp relay destination 2001:10:74:129::2
```

Example: Cable Interface Bundling

The following example shows how to bundle a group of physical interfaces.

```
int C5/0/4 and int c5/0/3 are bundled.
int c5/0/4
cable bundle 1
int c5/0/3
cable bundle 1
```

Example: VRF Configuration for 6VPE

The following example shows how to create VRFs for each VPN.

```
vrf definition vrf_mgmt
 rd 1:1
 !
 address-family ipv4
 route-target export 1:1
 route-target import 1:1
 route-target import 2:2
 route-target import 2:1
 exit-address-family
 !
 address-family ipv6
 route-target export 1:1
 route-target import 1:1
 route-target import 2:1  -- import route of vrfa
 route-target import 2:2  -- import route of vrfb
 exit-address-family
```

Verifying IPv6 on Cable

This section explains how to verify IPv6 on cable configuration and it contains the following topics:

Verifying IPv6 VRF Configuration

To verify the IPv6 VRF configuration, use the show vrf ipv6 command in privileged EXEC mode.

```
Router# show vrf ipv6 vrfa
  Name                             Default RD          Protocols   Interfaces
  vrfa                             2:1                 ipv4,ipv6   Bu1.11
Router# show vrf ipv6 interfaces
Interface              VRF                              Protocol   Address

Bu1.10                 vrf_mgmt                         up         2001:40:3:110::1

Fa0/0/0                vrf_mgmt                         up         2001:20:4:1::38

Bu1.11                 vrfa                             up         2001:40:3:111::1

Bu1.12                 vrfb                             up         2001:40:3:112::1

CMTS#
```

Verifying IPv6 BGP Status

To verify the IPv6 BGP status, use the show ip bgp command in privileged EXEC mode.

```
Router# show ip bgp vpnv6 unicast all neighbors

BGP neighbor is 11.1.1.5,  remote AS 1, internal link
  BGP version 4, remote router ID 11.1.1.5
  Session state = Established, up for 00:35:52
  Last read 00:00:37, last write 00:00:14, hold time is 180, keepalive interval is 60 seconds

  BGP multisession with 2 sessions (2 established), first up for 00:40:07
  Neighbor sessions:
    2 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new) on session 1, 2
    Address family IPv4 Unicast: advertised and received
    Address family VPNv6 Unicast: advertised and received
......
```

Verifying MPLS Forwarding Table

To verify the output of the MPLS forwarding table, use the show mpls forwarding-table command in the privileged EXEC mode.

```
Router# show mpls forwarding-table

Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id      Switched      interface
......
19     No Label      2001:40:3:110::/64[V]   \                              ---Route in
vrf_mgmt
                                       0             aggregate/vrf_mgmt
21     No Label      2001:40:3:111::/64[V]   \                              ---Route in
vrfa
                                       0             aggregate/vrfa
22     No Label      2001:40:3:112::/64[V]   \                              ---Route in
vrfb
                                       0             aggregate/vrfb
......
```

Verifying IPv6 Cable Modem and its Host State

To verify IPv6 addresses and connected host states of cable modems and CPEs, use the **show interface cable modem** command in the privileged EXEC mode:

```
Router# show interface cable 7/0/0 modem ipv6
SID  Type State         IPv6 Address                            M MAC address
11   CM  online         2001:420:3800:809:3519:5F9C:B96A:D31    D 0025.2e2d.743a
11   CPE unknown        2001:420:3800:809:3DB2:8A6C:115F:41D8   D 0011.2544.f33b
```

Verifying Multiple IAPDs in a Single Advertise

To verify the multiple IPv6 prefixes assigned to devices on a network, use the show cable modem ipv6 prefix command in privileged EXEC mode:

```
Router# show cable modem ipv6 prefix
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *06:36:53.075 UTC Thu Aug 2 2012
Device Type: B - CM Bridge, R - CM Router
IP Assignment Method: D - DHCP
MAC Address    Type IPv6 prefix
0023.bed9.4c91 R/D  2001:40:1012::/64
               R/D  2001:40:2012:1::/64
0000.002e.074c R/D  2001:40:1012:8::/64
               R/D  2001:40:2012:1D::/64
0000.002e.074b R/D  2001:40:1012:23::/64
               R/D  2001:40:2012:1C::/64
0000.002e.074a R/D  2001:40:1012:22::/64
               R/D  2001:40:2012:1B::/64
```

To verify the multiple IPv6 prefixes assigned to CPEs behind a CM with a specific MAC address, use the **show cable modem** *mac-address* **ipv6 prefix** command in privileged EXEC mode:

```
Router# show cable modem 0023.bed9.4c8e ipv6 prefix
Load for five secs: 0%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *06:37:22.335 UTC Thu Aug 2 2012
Device Type: B - CM Bridge, R - CM Router
IP Assignment Method: D - DHCP
MAC Address    Type IPv6 prefix
0023.bed9.4c91 R/D  2001:40:1012::/64
               R/D  2001:40:2012:1::/64
```

To verify the IPv6 information of CPEs behind a CM with a specific MAC address, use the show cable modem *mac-address* ipv6 **cpe** command in privileged EXEC mode:

```
Router# show cable modem 0023.bed9.4c8e ipv6 cpe
Load for five secs: 0%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *06:37:20.439 UTC Thu Aug 2 2012
MAC Address    IP Address
0023.bed9.4c91 2001:40:3:4:200:5EB7:BB6:C759
               2001:40:3:4:210:D73B:7A50:2D05
```

Additional References

The following sections provide references related to the IPv6 on Cable feature.

Related Documents

Related Topic	Document Title
Commands on the Cisco CMTS (universal broadband) routers	Cisco IOS CMTS Cable Command Reference
Platform-independent IPv6 configuration guide	Cisco IOS IPv6 Configuration Guide, Release 12.2SR
Platform-independent IPv6 commands	Cisco IOS IPv6 Command Reference
Platform-independent IPv6 concepts and feature configuration	Cisco IOS IPv6 Configuration Library

Standards

Standard	Title
CM-SP-MULPIv3.0-I04-070518	*DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification*
CM-SP-MULPIv3.0-I15-110210	*DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification*

MIBs

MIB	MIBs Link
CISCO-IP-FORWARD-MIB CISCO-IP-MIB CISCO-DOCS-EXT-MIB DOCS-CABLE-DEVICE-MIB DOCS-IF-MIB DOCS-SUBMGT-MIB DOCS-SUBMGT3-MIB IF-MIB (Interface counters) TCP-MIB UDP-MIB	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

RFCs

RFC	Title
draft-ietf-isis-ipv6-06.txt	*Routing IPv6 with IS-IS*

RFC	Title
RFC 2460	*Internet Protocol, Version 6 (IPv6) Specification*
RFC 2461	*Neighbor Discovery for IP version 6 (IPv6)*
RFC 2462	*IPv6 Stateless Address Autoconfiguration*
RFC 2463	*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
RFC 2464	*Transmission of IPv6 Packets over Ethernet Networks*
RFC 2710	*Multicast Listener Discovery (MLD) for IPv6*
RFC 2740	*OSPF for IPv6*
RFC 2893 (Dual stack mode of operation)	*Transition Mechanisms for IPv6 Hosts and Routers*
RFC 3315 (Relay Agent)	*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
RFC 3513	*Internet Protocol Version 6 (IPv6) Addressing Architecture*
RFC 3587	*IPv6 Global Unicast Address Format*
RFC 3596 (AAAA records)	*DNS Extensions to Support IP Version 6*
RFC 3810	*Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
RFC 4022	*Management Information Base for the Transmission Control Protocol (TCP)*
RFC 4113	*Management Information Base for the User Datagram Protocol (UDP)*
RFC 4659	BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
RFC 4861	*Neighbor Discovery for IP version 6 (IPv6)*
RFC 4862	*IPv6 Stateless Address Autoconfiguration*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for IPv6 on Cable

Table below lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

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

Table 6: Feature Information for IPv6 on Cable

Feature Name	Releases	Feature Information
IPv6 on Cable	12.2(33)SCA	This feature is introduced on the Cisco uBR7225VXR, Cisco uBR7246VXR, and Cisco uBR10012 Universal Broadband Routers. The following new commands are supported: • **cable ip-init** • **cable ipv6 source-verify** • **clear cable modem name** • **debug cable ipv6** • **show cable modem classifiers** • **show cable modem domain-name** • **show cable modem ipv6** • **show cable modem type**
	12.2(33)SCA	The following modified commands are supported: • **cable event syslog-server** • **cable filter group** • **clear cable host** • **clear cable modem reset** • **ping docsis** • **show cable filter** • **show cable modem** • **show cable modem access-group**

Feature Name	Releases	Feature Information
IPv6 on Cable (continued)	12.2(33)SCA	• **show cable modem calls** • **show cable modem classifiers** • **show cable modem cnr** • **show cable modem connectivity** • **show cable modem counters** • **show cable modem cpe** • **show cable modem errors** • **show cable modem flap** • **show cable modem mac** • **show cable modem maintenance** • **show cable modem offline** • **show cable modem phy** • **show cable modem qos** • **show cable modem registered** • **show cable modem rogue** • **show cable modem unregistered** • **show interface cable modem** • **show interface cable sid**

Feature Name	Releases	Feature Information
	12.2(33)SCA	The following existing cable features support the IPv6 protocol stack without any other modification to the configuration of the cable feature on the Cisco CMTS routers: • Baseline Privacy Plus (BPI+) • Cable Monitor (Except cable monitoring based on IPv6 ACL) • Cable Transport LAN Service (TLS) • CM configuration files • DHCP Relay Agent option for DOCSIS 3.0, Annex J (See also DHCPv6 Restrictions for IPv6 on Cable, on page 47)
IPv6 on Cable	12.2(33)SCA	• DMIC (except configuration file generation for DMIC IPv6 CMs) • Dynamic Channel Change (DCC) • DOCSIS Dynamic Service Addition (DSA) and Dynamic Service Change (DSC) operations • DOCSIS load balancing (except load balancing with HCCP) • Flap list • IPv6 L2VPN • Spectrum management • Virtual bundles (See the Configuring the Cable Virtual Bundle Interface, on page 66)
IPv6 Access Services		

Feature Name	Releases	Feature Information
IPv6 Access Services: DHCP for IPv6 Relay Agent	12.2(33)SCA	A DHCP relay agent, which may reside on the client's link, is used to relay messages between the client and server. **Platform-Independent Cisco IOS Software Documentation** The " http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dhcp.html " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature.
IPv6 Access Services: Source Verification	12.2(33)SCA	Enabling IPv6 source verification on a cable line card interface allows the source verification routine to verify the MAC address-MD-SID-IP binding of the packet. If the source verification succeeds, the packet is forwarded. If the verification fails, then the packet is dropped. **Platform-Specific Documentation for the Cisco CMTS Routers** For information about configuring IPv6 source verification, see the Configuring IPv6 Source Verification, on page 76.

Feature Name	Releases	Feature Information
IPv6 Access Services: Stateless DHCPv6	12.2(33)SCA	Stateless DHCP for IPv6 allows DHCP for IPv6 to be used for configuring a node with parameters that do not require a server to maintain any dynamic state for the node. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing DHCP for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Configuring the Stateless DHCPv6 Function • Configuring the Stateless DHCPv6 Function: Example
IPv6 Basic Connectivity		
Syslog over IPv6	12.2(33)SCA	The Cisco IOS syslog process in IPv6 allows users to log syslog messages to external syslog servers and hosts with IPv6 addresses. **Platform-Independent Cisco IOS Software Documentation** The Simplified IPv6 Packet Header section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter and the Configuring Syslog over IPv6 section of the " Implementing IPv6 for Network Management " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature.

Feature Name	Releases	Feature Information
IPv6 Unicast	12.2(33)SCA	An IPv6 unicast address is an identifier for a single interface, on a single node. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IPv6 Address Formats • IPv6 Address Type: Unicast • IPv6 Address Type: Multicast • IPv6 Neighbor Solicitation Message • IPv6 Router Advertisement Message • Configuring IPv6 Addressing and Enabling IPv6 Routing

Feature Name	Releases	Feature Information
IPv6 Unicast Reverse Path Forwarding (uRPF)	12.2(33)SCA	The Unicast RPF feature mitigates problems caused by malformed or forged (spoofed) IPv6 source addresses that pass through an IPv6 router. Malformed or forged source addresses can indicate denial-of-service (DoS) attacks based on source IPv6 address spoofing. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Prerequisites for Implementing IPv6 Addressing and Basic Connectivity • Cisco Express Forwarding and distributed Cisco Express Forwarding Switching for IPv6
IPv6 Cable Filter Groups		

Feature Name	Releases	Feature Information
IPv6 Cable Filter Groups: IPv6 Filter Classifiers for CM and CPE traffic	12.2(33)SCA	The IPv6 cable filter group feature support of the packet filtering portion of the DOCSIS Subscriber Management MIB (DOCS-SUBMGMT-MIB) using configuration commands on the CMTS routers. This IPv6 cable filter group support extends filter classifiers with IPv6 addressing options for CM and CPE traffic, but is independent of DOCSIS IPv6 classifiers which are used to match packets to service flows. **Platform-Specific Documentation for the Cisco CMTS Routers** For information about configuring IPv6 cable filter groups, see the Configuring IPv6 Cable Filter Groups, on page 69.
IPv6 Data Link Layer		
IPv6 Data Link: Ethernet, Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet	12.2(33)SCA	In IPv6 networks, a data link is a network sharing a particular link-local prefix. Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet are data links supported for IPv6. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature: • IPv6 Data Links

Feature Name	Releases	Feature Information
IPv6 Data Link: VLANs Using IEEE 802.1q Encapsulation	12.2(33)SCA	In IPv6 networks, a data link is a network sharing a particular link-local prefix. VLANs using IEEE 802.1Q encapsulation is a type of data link supported for IPv6. **Platform-Independent Cisco IOS Software Documentation** The “IPv6 Data Links” section of the “ Implementing IPv6 Addressing and Basic Connectivity ” chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature.
IPv6 ICMPv6		
ICMPv6	12.2(33)SCA	ICMP for IPv6 generates error messages, such as ICMP destination unreachable messages, and informational messages, such as ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process, path MTU discovery, and the MLD protocol for IPv6. **Platform-Independent Cisco IOS Software Documentation** The following sections of the “ Implementing IPv6 Addressing and Basic Connectivity ” chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • ICMP for IPv6 • IPv6 Neighbor Discovery • IPv6 Neighbor Solicitation Message • IPv6 Router Advertisement MessageConfiguring IPv6 ICMP Rate Limiting • IPv6 ICMP Rate Limiting Configuration: Example

Feature Name	Releases	Feature Information
ICMPv6 Redirect	12.2(33)SCA	A value of 137 in the Type field of the ICMP packet header identifies an IPv6 neighbor redirect message. Routers send neighbor redirect messages to inform hosts of better first-hop nodes on the path to a destination. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IPv6 Neighbor Redirect Message • IPv6 Redirect Messages
IPv6 Multicast		

Feature Name	Releases	Feature Information
IPv6 Multicast	12.2(33)SCA	An IPv6 multicast address is an identifier for a set of interfaces that typically belong to different nodes. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about the supported IPv6 multicast features on the Cisco CMTS routers: • Prerequisites for Implementing IPv6 Multicast • Restrictions for Implementing IPv6 Multicast • Information about Implementing IPv6 Multicast • Enabling IPv6 Multicast Routing • Configuring the MLD Protocol • Configuring PIM • Configuring Static Mroutes • Disabling Default Features in IPv6 Multicast • Configuration Examples for Implementing IPv6 Multicast • Additional References

Feature Name	Releases	Feature Information
IPv6 Multicast: MLD Access Group	12.2(33)SCA	The MLD access group provides receiver access control in Cisco IOS IPv6 multicast routers. The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • MLD Access Group • Customizing and Verifying MLD on an Interface
IPv6 Multicast: MLD Group Limits	12.2(33)SCA	The MLD group limits feature provides protection against denial of service (DoS) attacks caused by MLD packets. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Multicast Listener Discovery Protocol for IPv6 • Implementing MLD Group Limits

Feature Name	Releases	Feature Information
IPv6 Multicast: PIM Sparse Mode (PIM-SM)	12.2(33)SCA	PIM-SM uses unicast routing to provide reverse-path information for multicast tree building. PIM-SM is used in a multicast network when relatively few routers are involved in each multicast and these routers do not forward multicast packets for a group, unless there is an explicit request for the traffic. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Restrictions for Implementing IPv6 Multicast • IPv6 Multicast Routing Implementation • Protocol Independent Multicast

Feature Name	Releases	Feature Information
IPv6 Multicast: PIM Source Specific Multicast (PIM-SSM)	12.2(33)SCA	PIM-SSM supports the implementation of SSM and is derived from PIM-SM. The SSM feature forwards datagram traffic to receivers from only those multicast sources that the receivers have explicitly joined, optimizing bandwidth utilization and denying unwanted Internet broadcast traffic. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IPv6 Multicast Routing Implementation • Protocol Independent Multicast • PIM-Source Specific Multicast • IPv6 Multicast Process Switching and Fast Switching • Configuring PIM
IPv6 Multicast: Scope Boundaries	12.2(33)SCA	IPv6 includes support for global and nonglobal addresses. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IPv6 Multicast Addressing • Scoped Address Architecture • IPv6 BSR • Configuring a BSR

Feature Name	Releases	Feature Information
IPv6 Multicast: Static Multicast Routing (Mroute)	12.2(33)SCA	IPv6 static mroutes share the same database as IPv6 static routes and are implemented by extending static route support. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Multicast " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Restrictions for Implementing IPv6 Multicast • Static Mroutes • Configuring Static Mroutes
IPv6 Neighbor Discovery		
IPv6 Neighbor Discovery	12.2(33)SCA	The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring routers. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Link-Local Address • ICMP for IPv6 • IPv6 Neighbor Discovery • IPv6 Multicast Groups

Feature Name	Releases	Feature Information
IPv6 Neighbor Discovery Duplicate Address Detection	12.2(33)SCA	IPv6 neighbor discovery duplicate address detection is performed first on a new, link-local IPv6 address before the address is assigned to an interface (the new address remains in a tentative state while duplicate address detection is performed). **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IPv6 Neighbor Solicitation Message • IPv6 Stateless Autoconfiguration
IPv6 Neighbor Discovery Static Cache Entry	12.2(33)SCA	The IPv6 static cache entry for neighbor discovery feature allows static entries to be made in the IPv6 neighbor cache. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature: • IPv6 Neighbor Discovery
IPv6 Routing		

Feature Name	Releases	Feature Information
IPv6 Routing: IS-IS Support for IPv6	12.2(33)SCA	IPv6 enhancements to IS-IS allow IS-IS to advertise IPv6 prefixes in addition to IPv4 and OSI routes. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IS-IS for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IS-IS Enhancements for IPv6 • Configuring Single-Topology IS-IS for IPv6 • Customizing IPv6 IS-IS • Redistributing Routes into an IS-IS Routing Process • Redistributing IPv6 IS-IS Routes Between IS-IS Levels
IPv6 Routing: IS-IS Multitopology Support for IPv6	12.2(33)SCA	IS-IS multitopology support for IPv6 allows IS-IS to maintain a set of independent topologies within a single area or domain. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IS-IS for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • IS-IS Enhancements for IPv6 • IS-IS Multitopology Support for IPv6 • Transition from Single-Topology to Multitopology Support for IPv6 • Configuring Multitopology IS-IS for IPv6

Feature Name	Releases	Feature Information
IPv6 Routing: Multiprotocol BGP Extensions for IPv6	12.2(33)SCA	Multiprotocol BGP extensions for IPv6 supports the same features and functionality as IPv4 BGP. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing Multiprotocol BGP for IPv6" chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Multiprotocol BGP Extensions for IPv6 • How to Implement Multiprotocol BGP for IPv6
IPv6 Routing: Multiprotocol BGP Link-local Address Peering	12.2(33)SCA	IPv6 on Cable supports multiprotocol BGP link-local address peering. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing Multiprotocol BGP for IPv6" chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Configuring an IPv6 Multiprotocol BGP Peer Using a Link-Local Address • Multiprotocol BGP Peering Using Link-Local Addresses

Feature Name	Releases	Feature Information
IPv6 Routing: OSPF for IPv6 (OSPFv3)	12.2(33)SCA	OSPF version 3 for IPv6 expands on OSPF version 2 to provide support for IPv6 routing prefixes and the larger size of IPv6 addresses. **Platform-Independent Cisco IOS Software Documentation** The " Implementing OSPF for IPv6" chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature.
IPv6 Routing: OSPF for IPv6 Authentication Support with IPSec	12.2(33)SCA	OSPF for IPv6 uses the IPSec secure socket API to add authentication to OSPF for IPv6 packets. **Note** In Cisco IOS Release 12.2(33)SCA, the Cisco CMTS routers do not support OSPF with IPv6 multicast routing. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing OSPF for IPv6" chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • OSPF for IPv6 Authentication Support with IPSec • Configuring IPSec on OSPF for IPv6 • Defining Authentication on an Interface • Defining Authentication in an OSPF Area

Feature Name	Releases	Feature Information
IPv6 Routing: RIP for IPv6 (RIPng)	12.2(33)SCA	RIP enhancements for IPv6 include support for IPv6 addresses and prefixes, and the use of the all-RIP-routers multicast group address FF02::9 as the destination address for RIP update messages. **Platform-Independent Cisco IOS Software Documentation** The “ Implementing RIP for IPv6 ” chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature.
IPv6 Routing: Route Redistribution for RIPng	12.2(33)SCA	Routes may be specified by prefix, using a route-map prefix list, or by tag, using the route-map "match tag" function. **Platform-Independent Cisco IOS Software Documentation** The following sections of the “ Implementing RIP for IPv6 ” chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Redistributing Routes into an IPv6 RIP Routing Process • Configuring Tags for RIP Routes • IPv6 RIP Configuration: Example

Feature Name	Releases	Feature Information
IPv6 Routing: Route Redistribution for IS-IS	12.2(33)SCA	IS-IS for IPv6 supports redistributing routes into an IPv6 IS-IS routing process and redistributing IPv6 IS-IS routes between IS-IS levels. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IS-IS for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Information about Implementing IS-IS for IPv6 • Redistributing Routes into an IS-IS Routing Process • Redistributing IPv6 IS-IS Routes Between IS-IS Levels
IPv6 Routing: Static Routes	12.2(33)SCA	Static routes are manually configured and define an explicit path between two networking devices. **Platform-Independent Cisco IOS Software Documentation** The " Implementing Static Routes for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature.
IPv6 Services and Management		

Feature Name	Releases	Feature Information
IPv6 Services: AAAA DNS Lookups over an IPv4 Transport	12.2(33)SCA	IPv6 basic connectivity can be enhanced by configuring support for AAAA record types in the DNS name-to-address and address-to-name lookup processes. **Platform-Independent Cisco IOS Software Documentation** The " DNS for IPv6 " section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature.
IPv6 Services: Cisco Discovery Protocol—IPv6 Address Family Support for Neighbor Information	12.2(33)SCA	The Cisco Discovery Protocol IPv6 address support for neighbor information feature adds the ability to transfer IPv6 addressing information between two Cisco devices. **Platform-Independent Cisco IOS Software Documentation** The " Cisco Discovery Protocol IPv6 Address Support " section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature.
IPv6 Services: CISCO-IP-FORWARD-MIB	12.2(33)SCA	A MIB is a database of the objects that can be managed on a device. The managed objects, or variables, can be set or read to provide information on the network devices and interfaces. **Platform-Independent Cisco IOS Software Documentation** The " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature.

Feature Name	Releases	Feature Information
IPv6 Services: CISCO-IP-MIB Support	12.2(33)SCA	A MIB is a database of the objects that can be managed on a device. The managed objects, or variables, can be set or read to provide information on the network devices and interfaces. **Platform-Independent Cisco IOS Software Documentation** The " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature.
IPv6 Services: DNS Lookups over an IPv6 Transport	12.2(33)SCA	IPv6 supports DNS record types that are supported in the DNS name-to-address and address-to-name lookup processes. **Platform-Independent Cisco IOS Software Documentation** The " DNS for IPv6 " section of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provides information about this feature. **Platform-Specific Documentation for the Cisco CMTS Routers** For information about configuring DNS for IPv6 on the Cisco CMTS routers, see the Configuring IPv6 Domain Name Service, on page 74.

Feature Name	Releases	Feature Information
IPv6 Services: IPv6 IPSec VPN	12.2(33)SCA	**Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPSec in IPv6 Security " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Information About Implementing IPSec for IPv6 Security • How to Implement IPSec for IPv6 Security
IPv6 Services: Secure Shell (SSH) Support over IPv6	12.2(33)SCA	SSH in IPv6 functions the same and offers the same benefits as SSH in IPv4—the SSH Server feature enables an SSH client to make a secure, encrypted connection to a Cisco router and the SSH Client feature enables a Cisco router to make a secure, encrypted connection to another Cisco router or to any other device running an SSH server. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 for Network Management " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • SSH over an IPv6 Transport • Enabling SSH on an IPv6 Router

Feature Name	Releases	Feature Information
IPv6 Services: SNMP over IPv6	12.2(33)SCA	SNMP can be configured over IPv6 transport so that an IPv6 host can perform SNMP queries and receive SNMP notifications from a device running Cisco IOS IPv6. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 for Network Management " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • SNMP over an IPv6 Transport • Configuring an SNMP Notification Server over IPv6 • Configuring an SNMP Notification Server over IPv6: Examples

Feature Name	Releases	Feature Information
IPv6 Services: Standard Access Control Lists	12.2(33)SCA	Access lists determine what traffic is blocked and what traffic is forwarded at router interfaces and allow filtering based on source and destination addresses, inbound and outbound to a specific interface. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing Traffic Filters and Firewalls for IPv6 Security " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Restrictions for Implementing Traffic Filters and Firewalls for IPv6 Security • Access Control Lists for IPv6 Traffic Filtering • PAM in Cisco IOS Firewall for IPv6 • How to Implement Traffic Filters and Firewalls for IPv6 Security • Configuration Examples for Implementing Traffic Filters and Firewalls for IPv6 Security
IPv6 Switching		

Feature Name	Releases	Feature Information
IPv6 Switching: CEF/dCEF Support	12.2(33)SCA	Cisco Express Forwarding for IPv6 is advanced, Layer 3 IP switching technology for the forwarding of IPv6 packets. Distributed Cisco Express Forwarding for IPv6 performs the same functions as CEFv6 but for distributed architecture platforms. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing IPv6 Addressing and Basic Connectivity " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Cisco Express Forwarding and distributed Cisco Express Forwarding Switching for IPv6 • Configuring Cisco Express Forwarding and distributed Cisco Express Forwarding Switching for IPv6 **Platform-Specific Documentation for the Cisco CMTS Routers** For information about configuring IPv6 switching on the Cisco CMTS routers, see the Configuring DHCPv6 Relay Agent, on page 77.
IPv6 Tunneling		

Feature Name	Releases	Feature Information
IPv6 Tunneling: Manually Configured IPv6 over IPv4 Tunnels	12.2(33)SCA	A manually configured tunnel is equivalent to a permanent link between two IPv6 domains over an IPv4 backbone. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing Tunneling for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Overlay Tunnels for IPv6 • IPv6 Manually Configured Tunnels • Configuring Manual IPv6 Tunnels • Configuring Manual IPv6 Tunnels: Example
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels	12.2(33)SCA	GRE tunnels are links between two points, with a separate tunnel for each link. The tunnels are not tied to a specific passenger or transport protocol, but in this case carry IPv6 as the passenger protocol with the GRE as the carrier protocol and IPv4 or IPv6 as the transport protocol. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing Tunneling for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Library* provide information about this feature: • Overlay Tunnels for IPv6 • GRE/IPv4 Tunnel Support for IPv6 Traffic • Configuring GRE IPv6 Tunnels • Configure GRE Tunnels: Examples

Feature Name	Releases	Feature Information
IPv6 Tunneling: IPv4 over IPv6 Tunnels	12.2(33)SCA	**Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing Tunneling for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Guide* provide information about this feature: • IPv6 Manually Configured Tunnels • Configuring Manual IPv6 Tunnels
IPv6 Dual Stack CPE Support on the CMTS	12.2(33)SCC	Cisco IOS Release 12.2(33)SCC introduced this feature on the Cisco CMTS routers. The following sections provide information about this feature: • Restrictions for IPv6 Dual Stack CPE Support on the CMTS, on page 51 • Overview of IPv6 Dual Stack CPE Support on the CMTS, on page 57 • How to Verify IPv6 Dual Stack CPE Support , on page 79
IPv6 over Subinterfaces	12.2(33)SCC	Cisco IOS Release 12.2(33)SCC introduced this feature on the Cisco CMTS routers. The following sections provide information about this feature: • Overview of IPv6 over Subinterfaces , on page 57 • Example: IPv6 over Subinterfaces , on page 81

Feature Name	Releases	Feature Information
IPv6 ND Gleaning	12.2(33)SCC	The IPv6 ND Gleaning feature enables Cisco CMTS routers to automatically recover lost IPv6 CPE addresses. This feature is configured by default on routers. The **cable nd** command was introduced to support this feature. The following sections provide information about this feature: • IPv6 Neighbor Discovery Gleaning, on page 63 • Disabling IPv6 ND Gleaning, on page 78
IPv6 Support on Multiple Subinterfaces	12.2(33)SCB10	Starting with Cisco IOS Release 12.2(33)SCB10, IPv6 commands are supported on multiple CMTS bundle subinterfaces.
IPv6 HA	12.2(33)SCE	Cisco IOS Release 12.2(33)SCE introduced this feature on the Cisco CMTS routers.

Feature Name	Releases	Feature Information
IPv6 Access Services: DHCPv6 Prefix Delegation	12.2(33)SCE3	The DHCP for IPv6 prefix delegation feature can be used to manage link, subnet, and site addressing changes. DHCP for IPv6 can be used in environments to deliver stateful and stateless information. **Platform-Independent Cisco IOS Software Documentation** The following sections of the " Implementing DHCP for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Guide* provide information about this feature: • DHCPv6 Prefix Delegation • Configuring the DHCP for IPv6 Server Function • Configuring the DHCP for IPv6 Client Function • Configuring the DHCP for IPv6 Server Function: Example • Configuring the DHCP for IPv6 Client Function: Example
IPv6: 6PE & 6VPE	12.2(33)SCF	The Multiprotocol Label Switching (MPLS) virtual private network (VPN) feature represents an implementation of the provider edge (PE)-based VPN model. The 6VPE feature allows Service Providers to provide an IPv6 VPN service that does not require an upgrade or reconfiguration of the PE routers in the IPv4 MPLS core. The following sections provide information about this feature: • Overview of IPv6 VPN over MPLS, on page 59 • Services and Management Restrictions for IPv6 on Cable, on page 50

Feature Name	Releases	Feature Information
IPv6 CPE Router Support on the Cisco CMTS	12.2(33)SCF	The IPv6 CPE router is a node for home or small office use that connects the end-user network to a service provider network. The following section provides information about this feature: • Overview of IPv6 CPE Router Support on the Cisco CMTS, on page 60 The following commands were introduced or modified: • show ipv6 route • **show ipv6 cef platform**
Support for IPv6 Prefix Stability on the Cisco CMTS	12.2(33)SCF1	The IPv6 prefix stability on the Cisco CMTS allows an IPv6 home router to move from one Cisco CMTS to another while retaining the same prefix. The following section provides information about this feature: • Overview of IPv6 CPE Router Support on the Cisco CMTS, on page 60
Unitary DHCPv6 Leasequery protocol (RFC 5007)	12.2(33)SCF1	Added support for RFC 5007 compliant DHCPv6 leasequery protocol. The following commands were introduced or modified: **cable ipv6 source-verify, cable ipv6 source-verify leasequery-filter downstream, show cable leasequery-filter, and debug cable ipv6 lq**.

Feature Name	Releases	Feature Information
Configurable DHCPv6 Relay Address	12.2(33)SCE5	The Cisco CMTS router supports the DHCPv6 relay agent to send relay-forward messages from a specific source address to client relay destinations. The following sections provide information about this feature: **Platform-Specific Documentation for the Cisco CMTS Routers** • Configurable DHCPv6 Relay Address, on page 61 • Configuring DHCPv6 Relay Agent, on page 77 The ipv6 dhcp relay destination command was modified for this feature. **Platform-Independent Cisco IOS Software Documentation** The following section of the " Implementing DHCP for IPv6 " chapter of the *Cisco IOS IPv6 Configuration Guide* provides more information about this feature. • DHCPv6 Client, Server, and Relay Functions

Feature Name	Releases	Feature Information
DHCPv6 with Full 6VPE Support	12.2(33)SCF4	Starting with Cisco IOS Release 12.2(33)SCF4, the following capabilities are supported by IPv6 on the Cisco CMTS routers: • Assignment of different prefixes to CM and CPE • DHCPv6 over MPLS-VPN • DHCPv6 relay Prefix Delegation (PD) VRF awareness The following commands were modified: • **clear ipv6 dhcp relay binding** • **show ipv6 dhcp relay binding** **Platform-Independent Cisco IOS Software Documentation** For more information on the modified commands, see Cisco IOS IPv6 Command Reference .
IPv6 Address Packet Intercept	12.2(33)SCG	The IPv6 Address Packet Intercept feature supports lawful intercept of CMs and CPEs provisioned with IPv6 addresses. The following sections provide information about this feature: • IPv6 Address Packet Intercept • Provisioning IPv6 Taps Using SNMPv3.

Feature Name	Releases	Feature Information
Multiple IAPDs in a Single Advertise	12.2(33)SCG1	The Multiple IAPDs in a Single Advertise feature supports assignment of multiple IA_NAs and IAPDs for a CPE in a single advertise. The output of the **show cable modem ipv6** command was modified to support this feature. The following sections provide more information about this feature: • Restrictions for Multiple IAPDs in a Single Advertise, on page 52 • Support for Multiple IAPDs in a Single Advertise, on page 63 • Verifying Multiple IAPDs in a Single Advertise, on page 92

CHAPTER 3

Multicast VPN and DOCSIS 3.0 Multicast QoS Support

First Published: February 14, 2008

Last Updated: November 29, 2010

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

The CMTS enhanced multicast new features are consistent with DOCSIS 3.0 specifications and include:

- Enhanced multicast echo in which the Layer 3 multicast switching path uses a parallel express forwarding (PXF) multicast routing table.
- Enhanced multicast quality of service (MQoS) framework that specifies a group configuration (GC) to define a session range of multicast addresses and rule priorities and its associated multicast VPN (MVPN).
- Intelligent multicast admission control to include multicast service flows.
- Enhanced multicast VPN feature to configure and support multicast traffic in a multiprotocol label switching (MPLS)-VPN environment.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for the Multicast VPN and DOCSIS 3.0 Multicast QoS Support

DOCSIS 1.1 or 2.0 modems are required for multicast encryption.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 7: Multicast VPN and DOCSIS 3.0 Multicast QoS Support Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	Cisco IOS Release 12.2(33)SCB and later • Cisco uBR10-MC5X20U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [8]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [9]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

[8] Cisco uBR3GX60V cable interface line card is not compatible with PRE2.

[9] Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1. You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for the Multicast VPN and DOCSIS 3.0 Multicast QoS Support

You can only configure type of service (ToS) for Cisco uBR7200 series universal broadband routers. This parameter is not recognized by the Cisco uBR10012 universal broadband router.

Information About the Multicast VPN and DOCSIS 3.0 Multicast QoS Support

IP multicast—transmission of the same information to multiple cable network recipients—improves bandwidth efficiency and allows service providers to offer differentiated quality of service for different types of traffic. Enhanced multicast introduces multicast improvements as mandated by the introduction of DOCSIS 3.0 specifications.

Note DOCSIS 3.0 standards retain backwards compatibility with the DOCSIS 2.0 multicast mode of operation.

The following are the benefits of CMTS enhanced multicast are:

Improved Multicast Echo

In the enhanced multicast echo feature, the Layer 3 multicast switching path uses a parallel express forwarding (PXF) multicast routing table instead of the existing multicast echo path. Therefore, upstream packets are echoed using the Layer 3 switching path and all upstream data packets are treated similarly to the ingress packets from a WAN interface, in which they pass through existing classifiers and service flows.

The advantages of improved multicast echo are the following:

- Each outgoing interface has its own DSJIB/DSBlaze header to satisfy baseline privacy interface plus (BPI+) and downstream session identifier (DSID) requirements.
- The echoing decision is based on the PXF multicast routing table with packets forwarded only to interfaces that have existing clients.
- There is independent control of echoing multicast traffic for a single cable interface within a defined cable bundle.
- Bandwidth consumption is reduced because the upstream multicast data packets are not echoed to physical interfaces within the same cable bundle group that do not have an existing client.
- The Internet Group Management Protocol (IGMP) control packets echo functionality is retained allowing the ability to selectively enable or disable multicast echo for IGMP reports and data.
- Multicast QoS is supported because packets are following the same forwarding path as downstream multicast packets.

Enhanced Quality of Service

In the new multicast QoS (MQoS) framework, you can specify a group configuration (GC) that defines a session range of multicast addresses and rule priorities and its associated multicast VPN (MVPN). For every GC, there is attached a group QoS configuration (GQC) and a group encryption rule.

Based on the session range, rule priority, and MVPN, a multicast service flow is admitted into a GC and the associated GQC and group encryption rule are applied to the flow. In MQoS implementation, the source address of the multicast session is not checked because the current implementation for cable-specific multicast supports IGMP Version 2 but not IGMP Version 3. The downstream service flow, service identifier (SID), and MAC-rewrite string are created at the time of a new IGMP join (or static multicast group CLI on the interface) and MQoS is applied to the new multicast group join.

The benefits of enhanced QoS are the following:

- Group classifiers can be applied at cable interface level and also at bundle interface level.
- Group service flow (GSF) definition is based on service class names. The GSF is similar to individual service flows and commonly includes the minimum rate and maximum rate parameters for the service class. GSF is shared by all cable modems on a particular downstream channel set (DCS) that is matched to the same group classifier rule (GCR). A default service flow is used for multicast flows that do not match to any GCR. A GSF is always in the active state.
- CMTS replicates multicast packets and then classifies them.
- Single-stage replication and two-stage replication are supported.
- Enhanced QoS is compatible and integrated with DOCSIS Set-Top Gateway (DSG).

Intelligent Multicast Admission Control

Admission control allows you to categorize service flows into buckets. Examples of categories are the service class name used to create the service flow, service flow priority, or the service flow type such as unsolicited grant service (UGS). Bandwidth limits for each bucket can also be defined. For example, you can define bucket 1 for high priority packet cable service flows and specify that bucket 1 is allowed a minimum of 30 percent and a maximum of 50 percent of the link bandwidth.

Intelligent multicast admission control includes additional features such as the inclusion of multicast service flows using the GSF concept. GSFs are created based on the rules as defined in the GQC table. The rules link the multicast streams to a GSF through the session range. The service class name in the rule defines the QoS for that GSF. Additionally, another attribute is added to the rules and the group configuration table to specify the application type to which each GSF belongs. In this way, the QoS associated with each GSF is independent of the bucket category for the GSF.

The benefits of intelligent multicast admission control are the following:

- There is explicit acknowledgment of the establishment of each multicast session.
- Admission control does not consume additional bandwidth for multicast flows once the first flow is established.
- Service flows are cleaned up as the multicast session is torn down.

Multicast Session Limit Support

In a multicast video environment, you can limit the number of multicast sessions admitted onto a particular service flow. The multicast session limit feature—which adds functionality on top of the multicast QoS infrastructure—enables you to specify the number of multicast sessions to be admitted on a particular service flow. If the current number of sessions has reached the defined limit, new sessions will be forwarded but they will make use of the default multicast service flow until a session ends to free up a slot for new sessions.

Multicast Virtual Private Network

The new multicast VPN (MVPN) feature allows you to configure and support multicast traffic in a multiprotocol label switching (MPLS)-VPN environment. This feature supports routing and forwarding of multicast packets for each individual VPN virtual routing and forwarding (VRF) instance, and also provides a mechanism to transport VPN multicast packets across the service provider backbone.

MVPN allows you to connect multiple remote sites or devices over either a Layer 3 or Layer 2 VPN. A Layer 3 VPN enables the routing of traffic inside the VPN. A Layer 2 VPN provides a bridging transport mechanism for traffic between remote sites belonging to a customer. To support multicast over Layer 3 VPNs, each VPN receives a separate multicast domain with an associated MVPN routing and forwarding (mVRF) table maintained by the provider edge (PE) router. In a cable environment, the PE router is a routing CMTS. The provider network builds a default multicast distribution tree (default-MDT) for each VPN between all the associated mVRF-enabled PE routers. This tree is used to distribute multicast traffic to all PE routers.

To enable maximum security and data privacy in a VPN environment, the CMTS distinguishes between multicast sessions on the same downstream interface that belong to different VPNs. To differentiate multicast traffic between different VPNs, the CMTS implements a per-VRF subinterface multicast security association identifier (MSAID) allocation feature that is BPI+ enabled. The MSAID is allocated for each cable bundle group for each subinterface. A multicast group has a specific MSAID for each VRF instance.

How to Configure the Multicast VPN and DOCSIS 3.0 Multicast QoS Support

This section contains the following procedures:

Configuring a QoS Profile for a Multicast Group

To configure a QoS profile that can be applied to a QoS group configuration, use the **cable multicast group-qos** command. You must configure a QoS profile before you can add a QoS profile to a QoS multicast group.

DETAILED STEPS

	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`	Enters global configuration mode.

Step 3	**cable multicast group-qos** *number* **scn** *service-class-name* **control**{ **single** | **aggregate** [**limit** *max-sessions*]}
	Example:
	`Router(config)#: cable multicast group-qos 2 scn name1 control single`
		Configures a QoS profile that can be applied to a multicast QoS group.
		Note If a number is not specified, a default QoS profile is applied. The default group qos configuration creates a default multicast service flow for each cable interface that is used when a multicast session does not match any classifiers of a GC on the interface.

Configuring Encryption for a Multicast Group

To configure and enable an encryption profile that can be applied to a QoS group configuration (GC), use the **cable multicast group-encryption** command. You must configure an encryption profile before you can add an encryption profile to a QoS multicast group.

DETAILED STEPS

	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`	Enters global configuration mode.
Step 3	**cable multicast group-encryption** *number* **algorithm 56bit-des** **Example:** `Router(config)#: cable multicast group-encryption 35 algorithm 56bit-des`	Specifies an encryption number and encryption type of a specific cable multicast QoS group encryption profile. - *number*—Enables encryption and specifies the encryption number that can be applied to a specific cable multicast QoS group. The valid range is 1–255. - **algorithm 56bit-des**—Specifies that the data encryption standard (DES) is 56 bits.

Configuring a Multicast QoS Group

You can specify a group configuration (GC) that defines a session range of multicast addresses and rule priorities and its associated multicast VPN (MVPN). For every GC, there is attached a group QoS configuration and a group encryption rule.

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**cable multicast group-encryption** *number***algorithm56bit-des** **Example:** `Router(config-mqos)# cable multicast group-encryption 12 algorithm 56bit-des`	(Optional) Specifies an encryption number and encryption type of a specific cable multicast QoS group encryption profile.

Step 4	**cable multicast group-qos** *number* **scn** *service-class-name* **control** {**single** | **aggregate** [limit *max-sessions*]}
	Example:
	`Router(config-mqos)# cable multicast group-qos 5 scn name1 control single`
		(Optional) Configures a QoS profile that can be applied to a multicast QoS group.
		Note If a number is not specified, a default QoS profile is applied. The default group qos configuration creates a default multicast service flow for each cable interface that is used when a multicast session does not match any classifiers of a GC on the interface.

Step 5	**cable multicast qos group** *id* **priority** *value* [**global**] **Example:** `Router(config)# cable multicast qos group 2 priority 6`	Configures a multicast QoS group and enters multicast QoS configuration mode.
Step 6	**session-range** *ip-address ip-mask* **Example:** `Router(config-mqos)# session-range 224.10.10.10 255.255.255.224`	Specifies the session range IP address and IP mask of the multicast QoS group. You can configure multiple session ranges.
Step 7	**tos** *low-byte high-byte mask* **Example:** `Router(config-mqos)# tos 1 6 15`	(Optional) Specifies the minimum type of service (ToS) data bytes, maximum ToS data bytes, and mask for a multicast QoS group.
Step 8	**vrf***name* **Example:** `Router(config-mqos)# vrf name1`	(Optional) Specifies the name for the virtual routing and forwarding (VRF) instance. **Note** If a multicast QoS (MQoS) group is not defined for this VRF, you will see an error message. You must either define a specific MQoS group for each VRF, or define a default MQoS group that can be assigned in those situations where no matching MQoS group is found. See the Configuring a Default Multicast QoS Group for VRF, on page 139.
Step 9	**application-id***number* **Example:** `Router(config-mqos)# application-id 25`	(Optional) Specifies the application identification number of the multicast QoS group. This value is configured to enable admission control to the multicast QoS group.

Configuring a Default Multicast QoS Group for VRF

Each virtual routing and forwarding (VRF) instance that is defined must match a defined MQoS group to avoid multicast stream crosstalk between VRFs. To avoid potential crosstalk, define a default MQoS group that is assigned to the VRF whenever the multicast traffic in the VRF does not match an existing MQoS group.

DETAILED STEPS

	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`	Enters global configuration mode.
Step 3	**cable multicast group-encryption** *number***algorithm56bit-des** **Example:** `Router(config-mqos)# cable multicast group-encryption 12 algorithm 56bit-des`	(Optional) Specifies an encryption number and encryption type of a specific cable multicast QoS group encryption profile. The algorithm keyword and 56bit-des argument specify that the data encryption standard (DES) is 56 bits.

Step 4	**cable multicastgroup-qos***number* **scn***service-class-name* **control** {**single** | **aggregate** [**limit** *max-sessions*]}
	Example:
	`Router(config-mqos)# cable multicast group-qos 5 scn name1 control single`
		(Optional) Configures a QoS profile that can be applied to a multicast QoS group.

Step 5	**cable multicast qos group** *id* **priority 255 global** **Example:** `Router(config)# cable multicast qos group 2 priority 255 global`	Configures a default multicast QoS group and enters multicast QoS configuration mode.
Step 6	**session-range 224.0.0.0 224.0.0.0** **Example:** `Router(config-mqos)# session-range 224.0.0.0 224.0.0.0`	Specifies the session-range IP address and IP mask of the default multicast QoS group. By entering 224.0.0.0 for the IP address and the IP mask you cover all possible multicast sessions.

	Command or Action	Purpose
Step 7	**tos**_low-byte high-byte mask_ **Example:** `Router(config-mqos)# tos 1 6 15`	(Optional) Specifies the minimum type of service (ToS) data bytes, maximum ToS data bytes, and mask for the default multicast QoS group.
Step 8	**vrf**_name_ **Example:** `Router(config-mqos)# vrf name1`	Specifies the name of the virtual routing and forwarding (VRF) instance.
Step 9	**application-id**_number_ **Example:** `Router(config-mqos)# application-id 5`	(Optional) Specifies the application identification number of the multicast QoS group. This value is configured to enable admission control to the multicast QoS group.

Verifying Configuration of the Multicast VPN and DOCSIS 3.0 Multicast QoS Support

To verify the configuration of the Multicast VPN and DOCSIS 3.0 Multicast QoS Support feature, use the **show** commands described below.

- To show the configuration parameters for multicast sessions on a specific bundle, use the **show interface bundle** *number* **multicast-sessions** command as shown in the following example:

```
Router# show interface bundle 1 multicast-sessions
Multicast Sessions on Bundle1
 Group            Interface    GC  SAID SFID  GQC GEn RefCount GC-Interface State
 234.1.1.45       Bundle1.1    1   8193  ---   1   5   1        Bundle1     ACTIVE
 234.1.1.46       Bundle1.1    1   8193  ---   1   5   1        Bundle1     ACTIVE
 234.1.1.47       Bundle1.1    1   8193  ---   1   5   1        Bundle1     ACTIVE
Aggregate Multicast Sessions on Bundle1
 Aggregate Sessions for SAID 8193 GQC 1 CurrSess 3
 Group            Interface    GC  SAID SFID AggGQC GEn RefCount GC-Interface
 234.1.1.45       Bundle1.1    1   8193  ---   1      5   1        Bundle1
 234.1.1.46       Bundle1.1    1   8193  ---   1      5   1        Bundle1
 234.1.1.47       Bundle1.1    1   8193  ---   1      5   1        Bundle1
```

- To show the configuration parameters for multicast sessions on a specific cable, use the **show interface cable** *ip-addr* **multicast-sessions** command as shown in the following example:

```
Router# show interface cable 7/0/0 multicast-sessions
Default Multicast Service Flow 3 on Cable7/0/0
Multicast Sessions on Cable7/0/0
 Group            Interface    GC  SAID SFID  GQC GEn RefCount GC-Interface State
 234.1.1.45       Bundle1.1    1   8193 24     1   5   1        Bundle1     ACTIVE
 234.1.1.46       Bundle1.1    1   8193 24     1   5   1        Bundle1     ACTIVE
 234.1.1.47       Bundle1.1    1   8193 24     1   5   1        Bundle1     ACTIVE
Aggregate Multicast Sessions on Cable7/0/0
 Aggregate Sessions for SAID 8193 SFID 24 GQC 1 CurrSess 3
 Group            Interface    GC  SAID SFID AggGQC GEn RefCount GC-Interface
 234.1.1.45       Bundle1.1    1   8193 24     1      5   1        Bundle1
 234.1.1.46       Bundle1.1    1   8193 24     1      5   1        Bundle1
 234.1.1.47       Bundle1.1    1   8193 24     1      5   1        Bundle1
```

- To show the MSAID multicast group subinterface mapping, use the **show interface cable** *address* **modem** command as shown in the following example:

```
Router# show interface cable 6/1/0 modem
SID   Priv Type      State          IP address      method  MAC address     Dual
      bits                                                                  IP
9     11   modem     online(pt)     101.1.0.6       dhcp    0006.28f9.8c79  N
9     11   host      unknown        111.1.1.45      dhcp    0018.1952.a859  N
10    10   modem     online(pt)     101.1.0.5       dhcp    0006.5305.ac19  N
10    10   host      unknown        111.1.0.3       dhcp    0018.1952.a85a  N
13    10   modem     online(pt)     101.1.0.3       dhcp    0014.f8c1.fd1c  N
8195  10   multicast unknown        224.1.1.51      static  0000.0000.0000  N
8195  10   multicast unknown        224.1.1.49      static  0000.0000.0000  N
8195  10   multicast unknown        224.1.1.50      static  0000.0000.0000  N
```

Configuration Examples for the Multicast VPN and DOCSIS 3.0 Multicast QoS Support

This section provides the following configuration examples:

Example: Configuring Group QoS and Group Encryption Profiles

Note To add group QoS and group encryption profiles to a QoS group, you must configure each profile first before configuring the QoS group.

In the following example, QoS profile 3 and encryption profile 35 are configured.

```
configure terminal
cable multicast group-qos 3 scn name1 control single
cable multicast group-encryption 35 algorithm 56bit-des
```

Example: Configuring a QoS Group

In the following example, QoS group 2 is configured with a priority of 6 and global application. To QoS group 2, QoS profile 3 and encryption profile 35 are applied. Other parameters are configured for QoS group 2 including application type, session range, ToS, and VRF.

```
cable multicast qos group 2 priority 6 global
group-encryption 35
group-qos 3
session-range 224.10.10.01 255.255.255.254
tos 1 6 15
vrf vrf-name1
application-id 44
```

Where to Go Next

For further information on the commands required to configure, maintain, and troubleshoot Cicso uBR7200 series universal broadband routers, Cisco uBR10012 series universal broadband routers, and Cisco cable modems, see the *Cisco IOS CMTS Cable Command Reference* at:

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

Additional References

The following sections provide references related to the Multicast VPN and DOCSIS 3.0 Multicast QoS Support.

Related Documents

Related Topic	Document Title
CMTS cable commands	*Cisco CMTS Cable Command Reference* http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2236	*Internet Group Management Protocol, Version 2*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Multicast VPN and DOCSIS 3.0 Multicast QoS Support

Table below lists the release history for this feature.

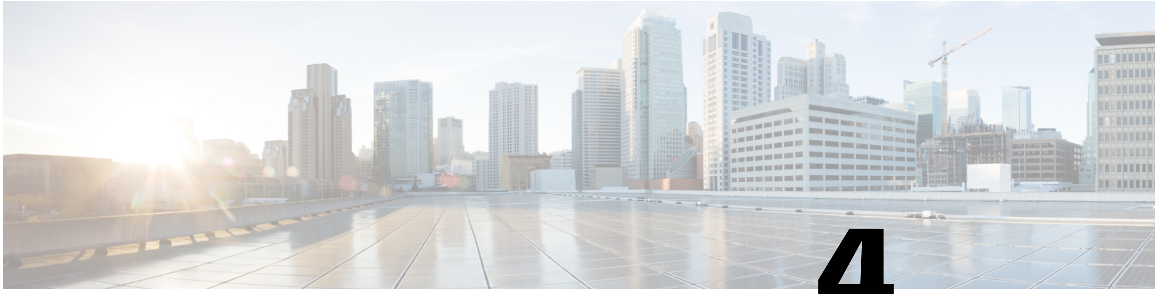
Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

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

Table 8: Feature Information for Multicast VPN and DOCSIS 3.0 Multicast QoS Support

Feature Name	Releases	Feature Information
Multicast VPN and DOCSIS 3.0 Multicast QoS Support	12.2(33)SCA	Enhanced multicast new features include configuration of a QoS group to include QoS, encryption, VRF, ToS, application type, and session range parameters. The following commands were introduced or modified by this feature: • **application-id** • **cable application-type include** • **cable multicast group-encryption** • **cable multicast group-qos** • **cable multicast qos group** • **session-range** • **show interface bundle multicast-sessions** • **show interface cable modem** • **show interface cable multicast-sessions** • **tos (multicast qos)** • **vrf (multicast qos)**



CHAPTER 4

Virtual Interface Bundling for the Cisco CMTS

First Published: February 11, 2008

> **Note** Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

This document describes how to combine multiple cable interfaces in a Cisco Cable Modem Termination System (CMTS) universal broadband router into a single logical bundle, so as to conserve IP address space and simplify network management.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Virtual Interface Bundling

The Virtual Interface Bundling feature is supported on the Cisco CMTS routers in Cisco IOS Release 12.3BC and 12.2SCA. Table below shows the hardware compatibility prerequisites for the Admission Control feature.

Table 9: Virtual Interface Bundling Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	Cisco IOS Release 12.2(33)SCA • Cisco uBR10-MC5X20S/U/H Cisco IOS Release 12.2(33)SCC and later • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [10]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

[10] Cisco uBR-MC88V cable interface line card is not compatible with NPE-G1.

Information About Virtual Interface Bundling

This section describes the Virtual Interface Bundling feature in Cisco IOS 12.3(13a)BC and later releases, to include configuration, guidelines, examples and additional information in these topics:

Overview of Virtual Interface Bundling

Note In Cisco IOS Release 12.3(21)BC and later releases, all cable bundles are automatically converted and configured to virtual interface bundles. Any standalone cable interfaces must be manually configured to be in a virtual bundle to operate properly.

Cisco IOS Release 12.3(13a)BC first introduced support for virtual interface bundling on the Cisco uBR10012 universal broadband router and the Cisco uBR10-MC5X20S/U/H Broadband Processing Engine (BPE), and the Cisco uBR7246VXR router.

In prior Cisco IOS releases, cable interface bundling was limited to physical interfaces as master or slave interfaces, and **show** commands did not supply bundle information.

Virtual interface bundling removes the prior concepts of master and slave interfaces, and introduces these additional changes:

- Virtual interface bundling uses *bundle interface* and *bundle members* instead of master and slave interfaces.
- A virtual bundle interface is virtually defined, as with IP loopback addresses.
- Virtual interface bundling supports bundle information in multiple **show** commands.

Virtual interface bundling prevents loss of connectivity on physical interfaces should there be a failure, problematic online insertion and removal (OIR) of one line card in the bundle, or erroneous removal of configuration on the master interface.

Virtual interface bundling supports and governs the following Layer 3 settings for the bundle member interfaces:

- IP address
- IP helper-address
- source-verify and lease-timer functions
- cable dhcp-giaddr (The giaddr field is set to the IP address of the DHCP client.)
- Protocol Independent Multicast (PIM)
- Access control lists (ACLs)
- Sub-interfaces

Note This virtual interface for the bundle should always remain on (enabled with **no shutdown**). Prior to Cisco IOS Release 12.3(13a)BC, the Cisco CMTS displays a warning message prior to execution of the **shutdown** command. In Cisco 12.3(13a)BC and later releases, no warning message displays.

Guidelines for Virtual Interface Bundling

The following guidelines describe virtual interface bundling, with comparison to the previous Cable Interface Bundling feature, where applicable:

- The former rules for bundle *master* are applicable to the new *virtual bundle interface* .
- The former rules for bundle *slaves* are applicable to the new virtual bundle *members* .
- With Cisco IOS Release 12.3(13a)BC, initial configuration of the first virtual bundle *member* automatically creates a virtual bundle interface.
- Beginning with Cisco IOS Release 12.3(21)BC, all cable bundles are automatically converted and configured to be in a virtual bundle after loading the software image.
- Beginning with Cisco IOS Release 12.3(21)BC, standalone cable interfaces must be manually configured to be in a virtual bundle to operate properly.
- The virtual bundle interface accumulates the counters from members; counters on member links are not cleared when they are added to the bundle. If a bundle-only counter is desired, clear the bundle counter on the members before adding them to the bundle, or before loading the image (for Cisco IOS Release 12.3(21)BC and later).
- Cisco IOS Release 12.3(13a)BC and later releases support a maximum of 40 virtual interface bundles, with the numeric range from 1 to 255.
- In releases prior to Cisco IOS Release 12.3(21)BC, if you delete the virtual bundle interface, the virtual bundle disappears.
- The virtual bundle interface remains configured unless specifically deleted, even if all members in the bundle are deleted.
- This feature supports subinterfaces on the virtual bundle interface.
- *Bundle-aware* configurations are supported on the virtual bundle interface.
- *Bundle-unaware* configurations are supported on each bundle member.
- While creating the virtual bundle interface, if the bundle interface existed in earlier Cisco IOS releases, then the earlier cable configurations re-appear after upgrade.

Virtual Interface Bundle-aware and Bundle-unaware Support

Virtual interface bundling uses two configurations: the virtual *bundle* itself, and the interfaces in that virtual bundle, known as *bundle members* . The virtual interface bundle and bundle members are either aware of the bundle, or unaware of the bundle, as follows.

- Bundle-aware features are maintained on the virtual *bundle* . These include:
    - IP Address
    - IP helper, cable helper
    - Dhcp-giaddr
    - Sub-interface
    - Source verify

    - Lease-query
    - Address Resolution Protocol (Cable ARP filtering, which also bundles cable interfaces, and Proxy ARP)
    - Cable match
    - Access Control Lists (ACLs)
    - Protocol Independent Multicast (PIM)
    - Cable Intercept (supported on the Cisco uBR10012 router with PRE2 module, only)

- Bundle-unaware features are maintained on the *bundle members* . These include:
    - DS/US configurations
    - HCCP redundancy
    - Load balancing
    - DMIC, tftp-enforce, shared-secret
    - Spectrum management
    - Admission control
    - Max-host
    - Intercept (supported on the Cisco uBR7200 series router and Cisco uBR10012 router with PRE1 module, only)

Multicast Support for IGMPv3 SSM and Virtual Interface Bundling

Cisco IOS Release 12.3(13a)BC introduces support for Internet Group Management Protocol (IGMPv3) Source Specific Multicast (SSM). This enhancement provides support for virtual interface bundling on the Cisco CMTS.

IGMP is used by IPv4 systems to report their IP multicast group memberships to any neighboring multicast routers. The latest IGMPv3 enables an individual member to join a particular channel. This is a new per-channel function, in addition to group-based functions (per-group). This channel based membership is known as Source Specific Multicast (SSM). IGMPv3 SSM allows a multicast client to specify the IP source from which they intend to receive, in addition to normal per-group multicast traffic.

For additional information about using IGMPv3 and virtual interface bundling, refer to enhanced show commands in this document, and to the following document on Cisco.com:

- *Virtual Interfaces and Frequency Stacking Configuration on MC5x20S and MC28U Line Cards*

http://www.cisco.com/en/US/tech/tk86/tk804/technologies_white_paper09186a0080232b49.shtml

- *Configuring Virtual Interfaces on the Cisco uBR10-MC5X20S/U Card*

http://www.cisco.com/en/US/docs/interfaces_modules/cable/broadband_processing_engines/ubr10_mc5x20s_u_h/feature/guide/mc5x2vif.html

Migrating Bundle Information During a Cisco IOS Upgrade

Migration to virtual interface bundling is automatic the first time a supporting Cisco IOS image is loaded onto the Cisco CMTS.

- Previously configured cable masters and slaves are converted to be members of a new virtual bundle interface.

For cable interface bundling configured in releases prior to Cisco IOS Release 12.3(13a)BC, a new virtual bundle is created with bundle numbers ranging from 1 to 255. However, only a maximum of 40 virtual bundles are supported.

- Bundle-aware configurations are transferred to the virtual bundle interface.
- In releases prior to Cisco IOS Release 12.3(21)BC, you can save new changes, however copying the startup-config to running-config does not translate cable interface bundling to virtual interface bundling, of itself.

Note In Cisco IOS Release 12.3(21)BC and later releases, standalone cable interfaces must be manually configured to be a member of a virtual bundle interface to operate properly.

Configuring Virtual Interface Bundling

Note When upgrading to Cisco IOS Release 12.3(21)BC or later from an earlier release, virtual bundles and bundle members are created and configured automatically. Standalone cable interfaces must be manually configured to be in a virtual bundle to operate properly.

When upgrading to Cisco IOS Release 12.3(13a)BC from an earlier release, it may be necessary to reconfigure all cable interface bundling information after loading the Cisco IOS software image. In this circumstance, cable modems do not receive an IP address from the Cisco CMTS until cable interfaces and cable interface bundling is reconfigured.

To enable virtual interface bundling, and to reconfigure interface information on the Cisco CMTS as required, you first configure the virtual interface bundle, then add additional bundle members for the specified virtual bundle. Perform these steps on each interface, as needed for all virtual interface bundles.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface bundle** *n* **Example:** `Router(config-if)# interface bundle 1`	Adds the selected interface to the virtual bundle. If this is the first interface on which the virtual bundle is configured, this command enables the bundle on the specified interface. The previous **master** keyword, as supported in the **cable bundle master** command for prior Cisco IOS releases, is not used for virtual interface bundling in Cisco IOS release 12.3(13a)BC, and later releases. As many as 40 virtual interface bundles can be configured on the Cisco CMTS. Numeric identifiers may range from 1 to 255.
Step 4	**ip address** *address mask* **Example:** `Router(config-if)# ip address 7.7.7.7 255.255.255.0`	Use as needed after Cisco IOS upgrade. Configures the IP address for the specified interface and virtual bundle.

Step 5	**interface cable** {*slot* /*port* |*slot* /*subslot* / *port* }
	Example:
	`Router#`
	`Router(config-if)#`
		Enters interface configuration mode for the selected interface, on which virtual interface bundling is to be enabled.
		• *slot* /*port* —Cable interface on the Cisco uBR7100 Series or Cisco uBR7200 Series. On the Cisco uBR7100 series router, the only valid value is 1/0. On the Cisco uBR7200 series router, slot can range from 3 to 6, and port can be 0 or 1, depending on the cable interface.
		• *slot* /*subslot* / *port* — Cable interface on the Cisco uBR10012 router. The following are the valid values:
		◦ *slot* —5 to 8
		◦ *subslot* — 0 or 1
		◦ *port* — 0 to 4 (depending on the cable interface)

Step 6	**cable bundle** *n* **Example:** `Router(config-if)# cable bundle 1`	Configures a cable interface to belong to an interface bundle, where *n* is the bundle number.
Step 7	**cable upstream max-ports** *n* **Example:** `Router(config-if)# cable upstream max-ports 6`	Use as needed after Cisco IOS upgrade. Configures the maximum number of upstreams on a downstream (MAC domain) on a Cisco cable interface line card. To reset the card to its default value of 4 upstreams per downstream, use the **no** form of this command. • *n* —Number of upstreams, ranging from 1 to 8, with a default of 4.

	Command or Action	Purpose
Step 8	**cable upstream***logical-port* **connector***physical-port* **Example:** `Router(config-if)# cable upstream 4 connector 16`	Use as needed after Cisco IOS upgrade. Maps an upstream port to a physical port on the Cisco cable interface line card for use with a particular downstream. To remove the mapping and shut down the upstream port, use the **no** form of this command. • *logical-port* —Specifies the upstream port number for the logical port assignment. The number of logical ports is configured with the cable modulation-profile command, and the valid range is from 0 to one less than the current value set with the cable modulation-profile command. **Tip** The default value for max-ports command is 4, which means the default range for logical-port is 0 to 3. • *physical-port* —Specifies the upstream port number for the actual physical port to be assigned. The valid range is 0 to 19, with no default.
Step 9	**cable upstream***n***frequency***up-freq-hz* **Example:** `Router(config-if)# cable upstream 4 frequency 15000000`	Use as needed after Cisco IOS upgrade. Enters a fixed frequency of the upstream radio frequency (RF) carrier for an upstream port. To restore the default value for this command, use the **no** form of this command. • *n* —Specifies the upstream port number on the cable interface line card for which you want to assign an upstream frequency. Valid values start with 0 for the first upstream port on the cable interface line card. • *up-freq-hz* —The upstream center frequency is configured to a fixed Hertz (Hz) value. The valid upstream frequency range is 5 MHz (5000000 Hz) to 42 MHz (42000000 Hz), 55 MHz (55000000 Hz), or 65 MHz (65000000 Hz), depending on the cable interface line card being used. If you wish to have the Cisco CMTS dynamically specify a center frequency for the given upstream interface, do not enter any frequency value.
Step 10	**no cable upstream** *n* **shut** **Example:** `Router(config-if)# no cable upstream 4 shut`	Use as needed after Cisco IOS upgrade. The cable interface must be enabled using the no shutdown command for the specified cable interface. *n* —Specifies the cable interface to enable for the virtual bundle.

Step 11	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

What to Do Next

To remove a virtual bundle from the interface, use the **no interface bundle** command in interface configuration mode, where *n* specifies the bundle identifier:

no interface bundle *n*

If you remove a member from a bundle, the bundle remains on the interface (even if empty) until the bundle itself is specifically removed.

In releases prior to Cisco IOS Release 12.3(21)BC, if you remove a bundle from an interface that still has active members, the bundle is removed.

Monitoring Virtual Interface Bundling

Cisco IOS Release 12.3(13a)BC introduces support for several enhanced show commands that display virtual bundle information.

Example: Virtual Interface Bundling

The following example illustrates a virtual interface bundle with the **show ip interface brief** command:

```
Router# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0/0          1.8.44.1        YES NVRAM  up                    up
POS1/0/0                   unassigned      YES NVRAM  up                    up
GigabitEthernet2/0/0       11.0.0.2        YES NVRAM  up                    up
GigabitEthernet3/0/0       10.1.1.101      YES NVRAM  up                    up
GigabitEthernet4/0/0       1.1.1.1         YES NVRAM  down                  down
Cable8/1/0                 unassigned      YES NVRAM  up                    up
Cable8/1/1                 unassigned      YES NVRAM  up                    up
Cable8/1/2                 unassigned      YES NVRAM  up                    up
Cable8/1/3                 unassigned      YES NVRAM  up                    up
Cable8/1/4                 unassigned      YES NVRAM  up                    up
Bundle1                    10.44.50.1      YES TFTP   up                    up
Router#
```

The following example illustrates virtual bundle information for the specified bundle:

```
Router# show running-config interface Bundle 1
Building configuration...
Current configuration : 189 bytes
!
interface Bundle1
 ip address 10.44.51.1 255.255.255.0 secondary
 ip address 10.44.50.1 255.255.255.0
 ip access-group 130 in
 ip helper-address 1.8.35.200
 cable source-verify dhcp
end
```

The following examples illustrate subinterface information for the specified bundle on a Cisco uBR10012 router:

```
Router# sh ip int br | include Bundle
Bundle1                    10.44.50.1      YES TFTP   up                    up
Bundle150                  unassigned      YES unset  up                    up
Bundle150.1                30.0.0.1        YES manual up                    up
Bundle200                  unassigned      YES unset  up                    up
Bundle255                  unassigned      YES unset  up                    up
Router# sh run int Bundle150.1
Building configuration...
```

```
Current configuration : 93 bytes
!
interface Bundle150.1
 ip address 30.0.0.1 255.0.0.0
 cable helper-address 1.8.35.200
end
```

Additional References

Related Documents

Related Topic	Document Title
CMTS Command Reference	Cisco IOS CMTS Cable Command Reference Guide

Standards and RFCs

Standards	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1
SP-RFIv2.0-I03-021218	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 2.0
SP-OSSIv2.0-I03-021218	Data-over-Cable Service Interface Specifications Operations Support System Interface Specification, version 2.0
SP-BPI+-I09-020830	Data-over-Cable Service Interface Specifications Baseline Privacy Plus Interface Specification, version 2.0

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Cable Interface Bundling and Virtual Interface Bundling for the Cisco CMTS

Table below lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

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

Table 10: Feature Information for Bundling on the Cisco CMTS

Feature Name	Releases	Feature Information
Virtual Interface Bundling	12.3(13a)BC	Cable bundling was updated to virtual interface bundling, so that cable bundles are automatically converted to virtual interface bundles. Cable bundling concepts, such as master and slave linecards, are no longer supported. See the Information About Virtual Interface Bundling, on page 147. In Cisco IOS Release 12.3(21)BC, all cable bundles are now automatically converted and configured to be in a virtual bundle, and standalone cable interfaces must be manually configured to be in a virtual bundle to operate properly. Previously, new virtual interface bundles and bundle members required reconfiguration, and there could also be standalone interfaces not part of a bundle at all.

Feature Name	Releases	Feature Information
Automatic Virtual Interface Bundling	12.2(33)SCA	Support for the Cisco uBR7225VXR Universal Broadband Router was added.

CHAPTER 5

Layer 3 CPE Mobility

First Published: February 18, 2014

Cisco IOS 12.2(33)SCH2 introduces the Layer 3 CPE Mobility feature, which allows the mobility CPE devices to move between cable modems with as less disruption of traffic as possible.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Prerequisites for Layer 3 CPE Mobility

Table below shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 11: Layer3 CPE Mobility for the Cisco CMTS Routers Hardware Compatibility Matrix

Cisco CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCH2 and later releases • PRE4 • PRE5	**Cisco IOS Release 12.2(33)SCC and later releases** • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR-MC3GX60V [11]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V [12]
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCB and later releases • NPE-G2	Cisco IOS Release 12.2(33)SCD and later releases • Cisco uBR-MC88V

[11] Cisco uBR3GX60V cable interface line card is compatible with PRE4.

[12] Cisco uBR-MC88V cable interface line card is compatible with NPE-G2.

Restrictions for Layer 3 CPE Mobility

- Layer 3 CPE Mobility feature allows CPE devices to move only in the same bundle or sub-bundle interface.
- The IPv4 or IPv6 subnets that are configured with mobility must match with the IPv4 or IPv6 subnets already configured on bundle or sub-bundle interface. Otherwise, configuration will not be accepted and the following message will be displayed:

```
Please remove the previous online CPEs or reset CMs,
```

- If you remove the IPv4 or IPv6 address on bundle or sub-bundle interface, it also removes the relative mobility subnets at the same time.
- Multicast packets will not trigger the Layer 3 CPE Mobility feature.
- VRF configured under bundle or sub-bundle interface is not supported for CPE mobility feature.

- On Cisco uBR72000 series platform, Layer3 CPE Mobility may fail if cable filter is configured.
- On uBR10k series platform, if PXF is disabled, Layer3 CPE Mobility function may not be fully supportd and some behavior may not be consistent with PXF enabled scenario.
- In Layer 3 CPE Mobility feature, the packet lost time period during mobility will be unpredictable, depending on how many CPE devices move at the same time and system loading conditions.
- For CPE devices, which have multiple IPv4 or IPv6 addresses, all of IPv4 or IPv6 addresses will be rebuilt with new source information.
- Layer 3 CPE Mobility may be failed during line card or PRE HA and the trigger upstream packet will be dropped.
- If CPE mobility is turned on, mobility behavior will become effective before cable Ipv4 or IPv6 source verify.
- If Layer 3 CPE Mobility is enabled, some of the security checks will be skipped for the mobility subnets to achieve faster movement of the CPE devices.

Information About Layer 3 CPE Mobility

The Layer 3 CPE Mobility feature allows CPE devices to move from cable modem to other by trigger of any unicast upstream packets of IPv4 or IPV6.

Each cable modem would be situated at a business hotspot location and the CPE devices move from one business location to another, where the service provider is the same and the head end CMTS is the same. This mobility is allowed for selected IP subnets.

The maximum number of subnets supported is 2 IPv6 and 6 IPv4 subnets per bundle or sub-bundle interface. To support more subnets, configure more bundle or sub-bundle interfaces.

The IPv4 or IPv6 subnets that are configured with mobility must match with the IPv4 or IPv6 subnets already configured on bundle or sub-bundle interface. Otherwise, configuration will not be accepted and the following message will be displayed:

```
Please remove the previous online CPEs or reset CMs,
```

When you remove mobility subnets under bundle or sub-bundle interface. The following warning message will be displayed after mobility subnets is configured or removed.

```
Warning: Please remove the previous online CPEs or reset CMs, to make the mobility scope
change works for every device !!!
```

Note If you have enabled mobility configuration for a subnet, the existing online CPE devices will not be aware of the mobility subnets. So after mobility subnets is configured, in order to make the mobility feature work for every CPE device, remove the online CPE devices or reset cable modem.

Benefits of Layer 3 CPE Mobility

The feature provides the movement of CPE devices from one cable modem to another without change in the IP address and the TCP or UDP sessions established are maintained.

How to Configure Layer 3 Mobility

Configuring CPE Mobility

This section describes how to enable mobility on a particular IP subnet on a interface or subinterface bundle.

Before You Begin

Mobility subnets should match the IPv4 or IPv6 address configured on the bundle or sub-bundle interface.

DETAILED STEPS

	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`	Enters global configuration mode.

Step 3	**interface bundle bundle number| bundle-subif-number**
	Example:
	`Router(config)# interface bundle 1`
	`or`
	`Router(config)# interface Bundle 1.1`
		Enters interface configuration or subinterface mode.

Step 4	**cable l3-mobility** *IP-address mask | IPv6 prefix*
	Example:
	`Router(config-if)# cable l3-mobility 2001:DB:22:1::1/64`
	Example:
	`Router(config-subif)# cable l3-mobility 192.0.3.1 255.255.255.0`
	Example:
	`Router(config-subif)#cable l3-mobility 2001:DB:22:1::1/64`
		Enables mobility for a particular IPv4 or IPv6 subnet.
		Note This command can be configured on a interface or a subinterface bundle.

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

What to Do Next

Troubleshooting Tips

If the mobility IP address does not match with the mobility subnet, the following warning message is displayed:

```
Mobility IP should match the IDB subnet!
```

If you remove the IPv4 or IPv6 address from the interface, the mobility scope is removed for the IP address and the following warning message is displayed.

```
IPv6 2001:DBB:3:111::1 removed from Mobility subnets on Bundle1
.
```

Configuring PXF Divert-Limit

This section describes how to configure or modify the PXF divert limit. This procedure is optional and if not configured, will set the value to the default value.

Note If **cable l3 mobility** command on the bundle or sub-bundle interface is enabled, the PXF divert limit is also enabled by default. So this configuration is optional.

Before You Begin

Ensure that the **cable l3 mobility** command is enabled on the bundle or sub-bundle interface. If disabled, the **service divert-limit l3-mobility** function does not work.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**service divert-limit l3-mobility-counter** *limit* | **l3-mobility-timeslot** *timeslot*
	Example:
	`Router(config-if)# service divert-limit l3-mobility-counter 1`
	`Router(config-if)# service divert-limit l3-mobility-timeslot 1`
		Configures the PXF threshold limit and timslot.
		• **l3-mobility-counter —** Configures the layer 3 CPE mobility counter threshold limit.
		• *limit*— Specifies the mobility counter threshold limit in packets. The default is 16.
		• **l3-mobility-timeslot —** Configures the layer 3 CPE mobility timeslot in ms. The default is 300.
		• *timeslot* — Specifies the mobility timeslot in milliseconds. The range is from 1 to 4095. The range is from 1 to 127.

Step 4	**exit** **Example:** `Router(config-if)# exit`	Exits global configuration mode.

Disabling CPE Mobility

This section describes how to disable mobility on a particular IP subnet.

Before You Begin

The CPE mobility should be enabled on a particular IP subnet before you complete this procedure.

DETAILED STEPS

	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`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	**interface bundle** *bundle number* | *bundle-subif-number*
	Example:
	`Router(config)# interface bundle 1`
	`or`
	`Router(config)# interface Bundle 1.1`
		Enters interface configuration or subinterface mode.

Step 4	**no cable l3-mobility** *IP-address mask* | *IPv6 prefix*
	Example:
	`Router(config-if)# cable l3-mobility 192.0.3.1 255.255.255.0`
	`Router(config-if)# cable l3-mobility 2001:DB:22:1::1/64`
		Disbles mobility for a particular IPv4 or IPv6 subnet.
		Note This command can be configured on a interface or a subinterface bundle

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

Verifying Layer 3 Mobility Configuration

To verify the layer 3 mobility configuration, use the **show cable bundle** command.

```
Router# show cable bundle 1 mobility Interface                    IP/IPv6 Subnet

-------------------------------------------------------------------------------
Bundle1                  ---
Bundle1.1              192.0.3.0/16
                               192.0.3.1/16
                               192.0.4.1/16
                               2001:DB:5:4:100::1/32
                               2001:DB:5:4:101::1/32
Bundle1.2             192.0.3.1/16
```

Configuration Examples for Layer 3 Mobility

This section provides the following configuration examples:

Example: Configuring CPE Layer 3 Mobility

The following example shows how to configure the layer 3 CPE mobility on a interface bundle:

```
Router#show running interface bundle 10
Building configuration...
Current configuration : 1247 bytes
```

```
!
interface Bundle10
ip address 192.0.3.1 255.255.255.0 secondary
ip address 192.2.21.1 255.255.255.0 secondary
ip address 192.3.23.1 255.255.255.0
ip pim sparse-dense-mode
ip igmp static-group 231.1.1.1
no cable arp filter request-send
no cable arp filter reply-accept
cable l3-mobility 192.0.3.1 255.255.255.0
cable l3-mobility 192.2.21.1 255.255.255.0
cable l3-mobility 192.3.23.1 255.255.255.0
cable l3-mobility 2001:DB:26:1::1/64
cable l3-mobility 2001:DB:27:1::1/96
cable dhcp-giaddr primary
cable helper-address 20.1.0.3
ipv6 address 2001:DB:26:1::1/64
ipv6 address 2001:DB:27:1::1/96
ipv6 enable
ipv6 nd reachable-time 3600000
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp relay destination 2001:DB:1:1:214:4FFF:FEA9:5863
end
```

Example: Configuring PXF Divert-Rate-Limit

The following example shows how to configure the PXF divert rate limit mobility counter and mobility timeslot:

```
Router# show run | in divert-limit
service divert-limit l3-mobility-counter 127
service divert-limit l3-mobility-timeslot 100
```

Additional References

The following sections provide references related to Spectrum Management and Advanced Spectrum Management for the Cisco CMTS routers.

Related Documents

Related Topic	Document Title
CMTS Command Reference	http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html Cisco Broadband Cable Command Reference Guide.

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

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 Layer 3 CPE Mobility

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

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

Table 12: Feature Information for Layer 3 CPE Mobility

Feature Name	Releases	Feature Information
Layer 3 Mobility	12.2(33)SCH2	This feature was introduced for the Cisco uBR10012 and Cisco uBR7200 series universal broadband routers.