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**]