



## IPv6 on Cable

---

Cisco cBR series Converged Broadband Router supports full IPv6 functionality.

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.
- 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.

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 that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

- [Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 2](#)
- [Restrictions for IPv6 on Cable, on page 3](#)
- [Information About IPv6 on Cable, on page 4](#)
- [How to Configure IPv6 on Cable, on page 13](#)
- [How to Verify IPv6 Dual Stack CPE Support, on page 29](#)
- [Configuration Examples for IPv6 on Cable, on page 30](#)

- [Verifying IPv6 on Cable, on page 41](#)
- [Supported MIBs, on page 43](#)
- [Additional References, on page 43](#)
- [Feature Information for IPv6 on Cable, on page 43](#)

## Hardware Compatibility Matrix for the Cisco cBR Series Routers



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

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

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	<p><b>Cisco IOS-XE Release 16.5.1 and Later Releases</b></p> <p>Cisco cBR-8 Supervisor:</p> <ul style="list-style-type: none"> <li>• PID—CBR-SUP-250G</li> <li>• PID—CBR-CCAP-SUP-160G</li> <li>• PID—CBR-CCAP-SUP-60G</li> </ul>	<p><b>Cisco IOS-XE Release 16.5.1 and Later Releases</b></p> <p>Cisco cBR-8 CCAP Line Cards:</p> <ul style="list-style-type: none"> <li>• PID—CBR-LC-8D30-16U30</li> <li>• PID—CBR-LC-8D31-16U30</li> <li>• PID—CBR-RF-PIC</li> <li>• PID—CBR-RF-PROT-PIC</li> <li>• PID—CBR-CCAP-LC-40G</li> <li>• PID—CBR-CCAP-LC-40G-R</li> <li>• PID—CBR-CCAP-LC-G2-R</li> <li>• PID—CBR-SUP-8X10G-PIC</li> <li>• PID—CBR-2X100G-PIC</li> </ul> <p>Digital PICs:</p> <ul style="list-style-type: none"> <li>• PID—CBR-DPIC-8X10G</li> <li>• PID—CBR-DPIC-2X100G</li> </ul> <p>Cisco cBR-8 Downstream PHY Module:</p> <ul style="list-style-type: none"> <li>• PID—CBR-D31-DS-MOD</li> </ul> <p>Cisco cBR-8 Upstream PHY Modules:</p> <ul style="list-style-type: none"> <li>• PID—CBR-D31-US-MOD</li> </ul>

# Restrictions for IPv6 on Cable

## Multicast Restrictions

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

- 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

## QoS Restrictions

In Cisco IOS-XE Release 16.5.1, the following fields are supported for the IPv6 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.

---

## Information About IPv6 on Cable

This section includes the following topics:

### Features Supported

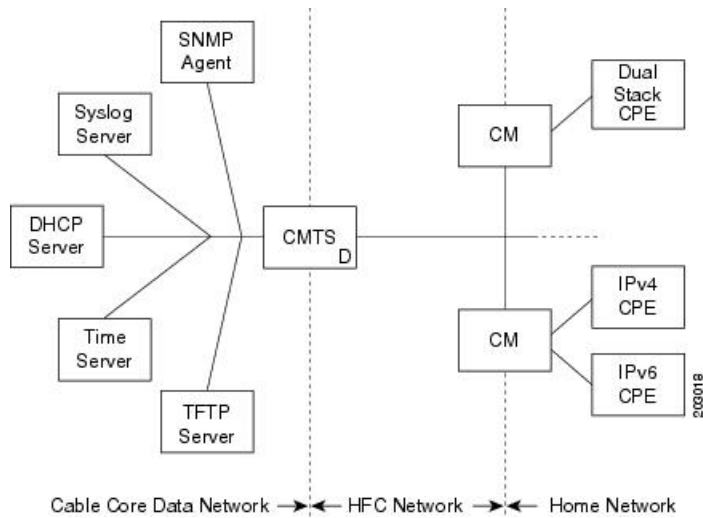
The following features are supported on the Cisco CMTS routers:

- 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
- Assignment of different prefixes to CM and CPE
- DHCPv6 over MPLS-VPN
- DHCPv6 relay prefix delegation VRF awareness
- 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.
- IPv6 Downstream ToS overwrite.
- DHCPv6 Client Link-Layer Address Option (RFC 6939).
- Voice over IPv6. PacketCable Multimedia needs to be enabled before using this feature. For more information, see [http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b\\_pktcbl\\_pktcblmm/packetcable\\_and\\_packetcable\\_multimedia.html](http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_pktcbl_pktcblmm/packetcable_and_packetcable_multimedia.html).

## 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** Cisco cBR 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** The Cisco cBR router supports only a single DHCPv6 IPv6 address per client cable modem 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.

## 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 15.

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.

When IPv6 is configured and active, for transmitting multicast DSID carrying IPv6 ND messages within a MAC domain, the CMTS contains the pre-registration DSID TLV encoding (type 5.2) in the MDD message.

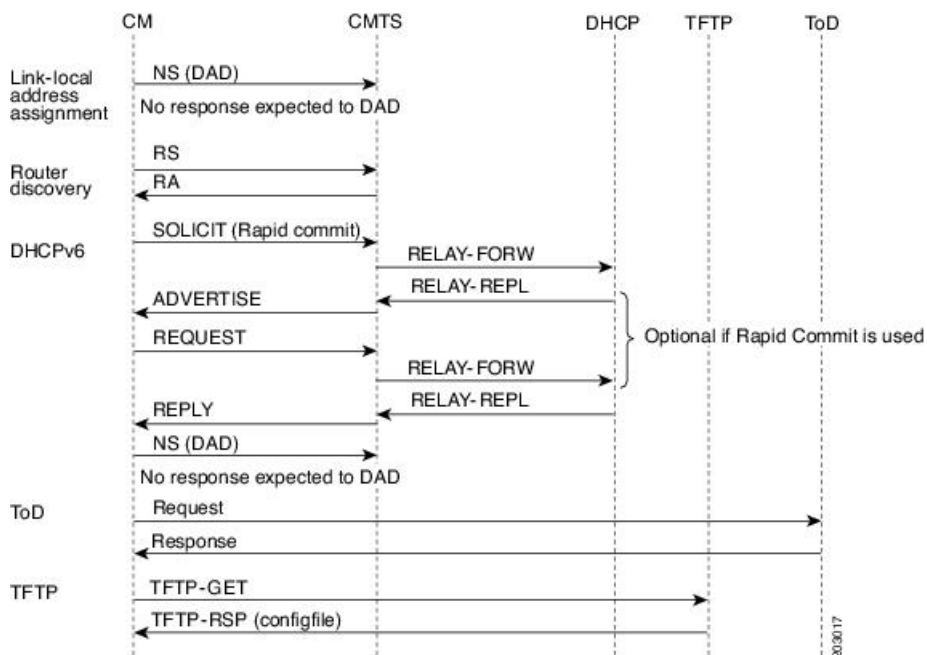


**Note** The Cisco CMTS routers do not support alternate provisioning mode or pre-registration DSID.

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 the M 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

Most operating systems (OS) deployed at homes support dual stack operation. Cisco CMTS supports dual stack, which is both IPv4 and IPv6 addressing on the CPE.

## Overview of IPv6 over Subinterfaces

Cisco 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 15](#) section. For a CMTS bundle configuration example, see the [Example: IPv6 over Subinterfaces, on page 30](#) section.

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



---

**Note** MPLS VPN over subinterfaces for IPv6 is not supported.

---

## Overview of High Availability on IPv6

Cisco cBR Series routers support IPv6 HA for the Supervisor card.




---

**Note** IPv6 DOCSIS HA and HCCP is supported on the Cisco CMTS routers.

---

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**

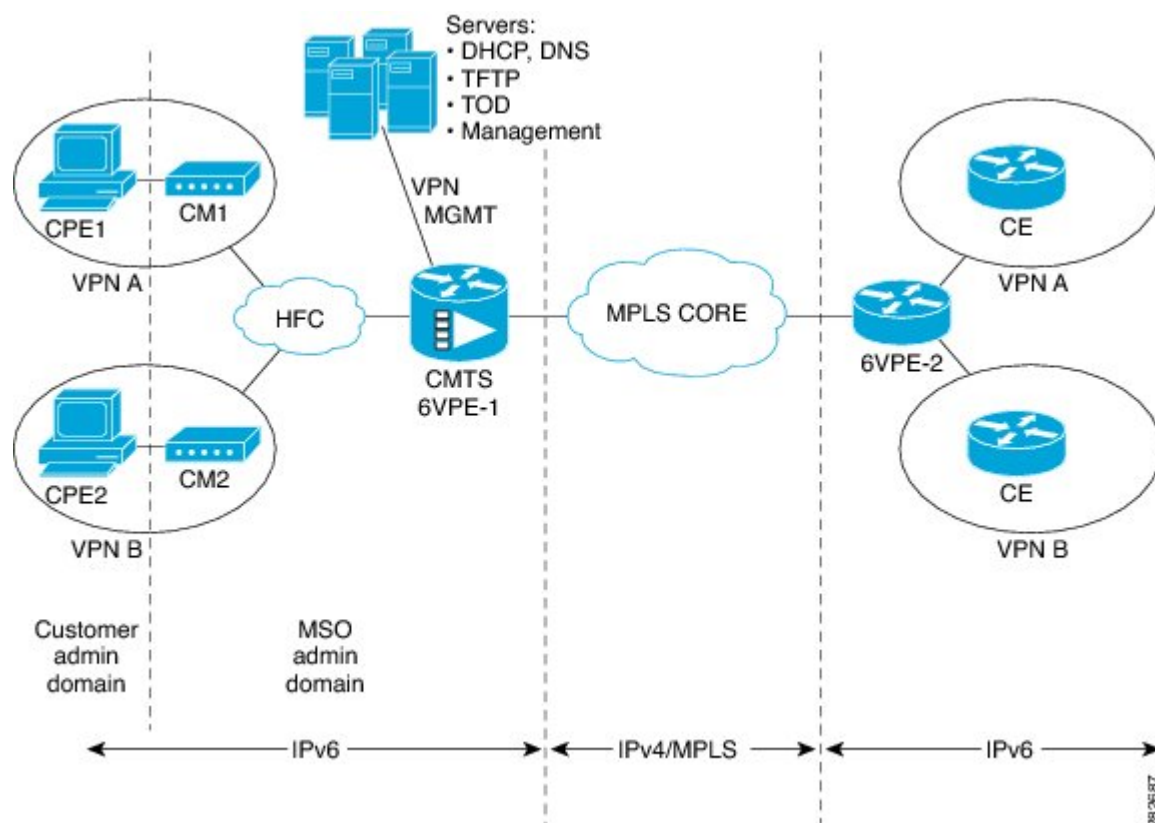
The Multiprotocol Label Switching (MPLS) VPN feature represents an implementation of the provider edge (PE) based VPN model. This document describes the IPv6 VPN over MPLS (6VPE) feature.

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



## 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 the Cable Monitor and Intercept Features for the Cisco CMTS Routers guide.

## Overview of IPv6 CPE Router Support on the Cisco CMTS

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.

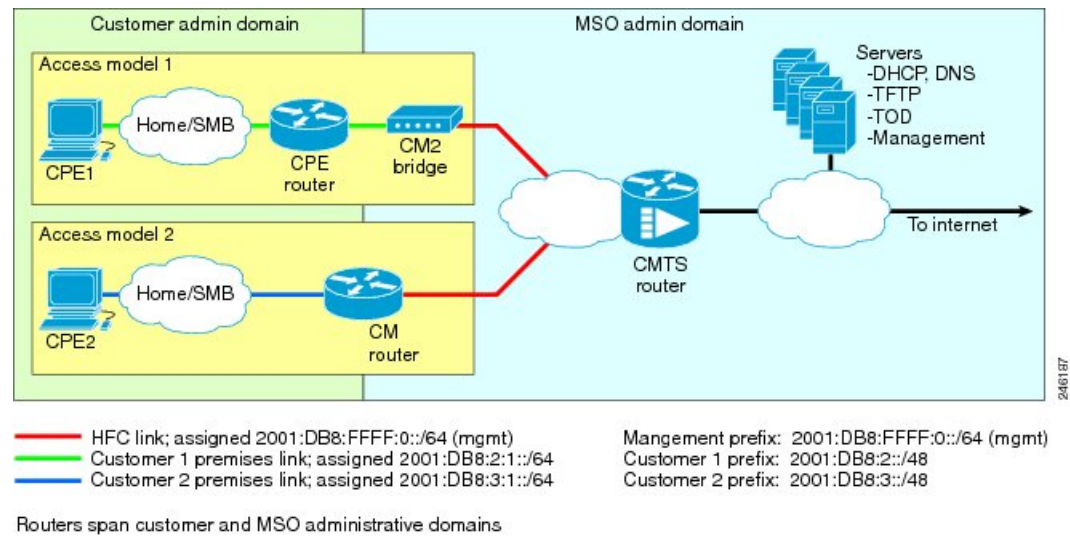
The IPv6 CPE router is responsible for implementing IPv6 routing; that is, the IPv6 CPE router looks up the IPv6 destination address in its routing table and decides to which interface the packet should be sent.

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**



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

IPv6 prefix stability is supported on the Cisco CMTS as specified in DOCSIS 3.0 MULPI CM-SP-MULPIv3.0-115-110210 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.

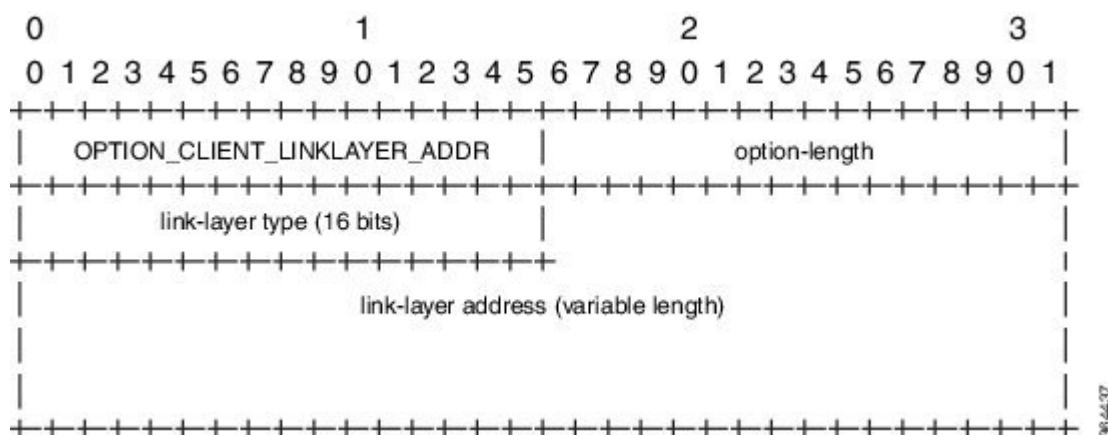
A DHCP relay agent is used to relay messages between the client and server. A client locates a DHCP server using a reserved, link-scoped multicast address.

### DHCPv6 Client Link-Layer Address Option (RFC 6939)

Cisco IOS-XE Releases support 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.



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** 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 26](#) section.

For more information about the DHCPv6 client, server, and relay functions, see the “Implementing DHCP for IPv6” chapter in the [IPv6 Implementation Guide, Cisco IOS XE Release 3S](#).

## Support for Multiple IAPDs in a Single Advertise

Assignment of multiple IA\_NA and IAPD to CPEs behind a CM is supported on Cisco CMTS routers. 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.

---

## 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. 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.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	Do one of the following: <ul style="list-style-type: none"> <li>• <b>ip cef</b></li> <li>• <b>ip cef distributed</b></li> </ul> <b>Example:</b> <pre>Router(config)# ip cef</pre> or <pre>Router(config)# ip cef distributed</pre>	Enables Cisco Express Forwarding. or Enables distributed Cisco Express Forwarding for IPv4 datagrams. <b>Note</b> For CMTS routers, distributed Cisco Express Forwarding is supported only on a Cisco uBR10012 universal broadband router.
<b>Step 4</b>	Do one of the following: <ul style="list-style-type: none"> <li>• <b>ipv6 cef</b></li> <li>• <b>ipv6 cef distributed</b></li> </ul> <b>Example:</b> <pre>Router(config)# ipv6 cef</pre> or <pre>Router(config)# ipv6 cef distributed</pre>	Enables Cisco Express Forwarding v6. or Enables distributed Cisco Express Forwarding v6 for IPv6 datagrams. <b>Note</b> For CMTS routers, distributed Cisco Express Forwarding v6 is supported only on a Cisco uBR10012 universal broadband router.

	Command or Action	Purpose
Step 5	<b>ipv6 unicast-routing</b> <b>Example:</b> Router(config)# <b>ipv6 unicast-routing</b>	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.

## 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.

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.

---

#### Procedure

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b>	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	Router> enable	
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface bundle n</b> <b>Example:</b> Router(config)# interface bundle 1	Specifies the cable bundle interface and enters interface configuration mode, where <i>n</i> specifies the number of the bundle interface.
<b>Step 4</b>	<b>ipv6 address ipv6-prefix /prefix-length [eui-64 ]</b> <b>Example:</b> 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.
<b>Step 5</b>	<b>ipv6 address ipv6-prefix /prefix-length link-local</b> <b>Example:</b> 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 <b>ipv6 address link-local</b> 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 <b>ipv6 enable</b> command).
<b>Step 6</b>	<b>ipv6 enable</b> <b>Example:</b> 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.
<b>Step 7</b>	<b>cable ipv6 source-verify</b> <b>Example:</b> 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.

**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.

---

#### 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.

## Enabling MDD with Pre-Registration DSID

When only IPv4 is configured and active, where the IP provisioning mode is IPv4, for Cable Modems to come online, the pre-registration DSID (TLV 5.2) is required in the MAC Domain Descriptor (MDD) message. To enable this pre-registration DSID, use the following command.

By default, this command is disabled.

```
Router#configure terminal
Router(config)#cable ipv4-prereg-dsid
Router(config)#end
```

## Configuring IPv6 Cable Filter Groups

The Cisco CMTS router supports IPv6 cable filter group capability with IPv6 filter options.

## Configuring IPv6 Cable Filter Groups

The Cisco CMTS router supports IPv6 cable filter group capability with 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.

### Procedure

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

	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>cable filter group</b> <i>group-id</i> <b>index</b> <i>index-num</i> <b>dest-port</b> <i>port-num</i> <b>Example:</b>  Router(config)# cable filter group 1 index 1 dest-port 69	(Optional) Specifies the TCP/UDP destination 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).
<b>Step 4</b>	<b>cable filter group</b> <i>group-id</i> <b>index</b> <i>index-num</i> <b>ip-proto</b> <i>proto-type</i> <b>Example:</b>  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:
<b>Step 5</b>	<b>cable filter group</b> <i>group-id</i> <b>index</b> <i>index-num</i> <b>ip-tos</b> <i>tos-mask</i> <i>tos-value</i> <b>Example:</b>  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 <i>tos-mask</i> is logically ANDed with the <i>tos-value</i> and compared to the result of ANDing the <i>tos-mask</i> 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.
<b>Step 6</b>	<b>cable filter group</b> <i>group-id</i> <b>index</b> <i>index-num</i> <b>ip-version</b> <i>ipv6</i> <b>Example:</b>  Router(config)# cable filter group 1 index 1 ip-version ipv6	Specifies that this filter group is an IPv6 filter group.
<b>Step 7</b>	<b>cable filter group</b> <i>group-id</i> <b>index</b> <i>index-num</i> <b>match-action</b> {accept   drop} <b>Example:</b>  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):
<b>Step 8</b>	<b>cable filter group</b> <i>group-id</i> <b>index</b> <i>index-num</i> <b>src-port</b> <i>port-num</i> <b>Example:</b>  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).

	Command or Action	Purpose
Step 9	<p><b>cable filter group</b> <i>group-id</i> <b>index</b> <i>index-num</i> <b>status</b> {<b>active</b>   <b>inactive</b>}</p> <p><b>Example:</b></p> <pre>Router(config)# cable filter group 1 index 1 status inactive</pre>	<p>(Optional) Enables or disables the filter (IPv4 and IPv6 filters):</p> <p><b>Note</b> 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.</p>
Step 10	<p><b>cable filter group</b> <i>group-id</i> <b>index</b> <i>index-num</i> <b>tcp-flags</b> <i>flags-mask</i> <i>flags-value</i></p> <p><b>Example:</b></p> <pre>Router(config)# cable filter group 1 index 1 tcp-flags 0 0</pre>	<p>(Optional) Specifies the TCP flag mask and value to be matched (IPv4 and IPv6 filters):</p>
Step 11	<p><b>cable filter group</b> <i>group-id</i> <b>index</b> <i>index-num</i> <b>v6-dest-address</b> <i>ipv6-address</i></p> <p><b>Example:</b></p> <pre>Router(config)# cable filter group 1 index 1 v6-dest-address 2001:DB8::/32</pre>	<p>(Optional) Specifies the IPv6 destination address that should be matched using the format X:X:X:X::X (IPv6 filters only).</p>
Step 12	<p><b>cable filter group</b> <i>group-id</i> <b>index</b> <i>index-num</i> <b>v6-dest-pfxlen</b> <i>prefix-length</i></p> <p><b>Example:</b></p> <pre>Router(config)# cable filter group 1 index 1 v6-dest-pfxlen 64</pre>	<p>(Optional) Specifies the length of the network portion of the IPv6 destination address. The valid range is from 0 to 128.</p>
Step 13	<p><b>cable filter group</b> <i>group-id</i> <b>index</b> <i>index-num</i> <b>v6-src-address</b> <i>ipv6-address</i></p> <p><b>Example:</b></p> <pre>Router(config)# cable filter group 1 index 1 v6-src-address 2001:DB8::/32</pre>	<p>(Optional) Specifies the IPv6 source address that should be matched using the format X:X:X:X::X (IPv6 filters only).</p>
Step 14	<p><b>cable filter group</b> <i>group-id</i> <b>index</b> <i>index-num</i> <b>v6-src-pfxlen</b> <i>prefix-length</i></p> <p><b>Example:</b></p> <pre>Router(config)# cable filter group 1 index 1 v6-src-pfxlen 48</pre>	<p>(Optional) Specifies the length of the network portion of the IPv6 source address. The valid range is from 0 to 128 (IPv6 filters only).</p>
Step 15	<p><b>cable submgmt default filter-group</b> {<b>cm</b>   <b>cpe</b>} {<b>downstream</b>   <b>upstream</b>} <i>group-id</i></p> <p><b>Example:</b></p> <pre>Router(config)# cable submgmt default filter-group cm upstream 1</pre>	<p>Applies a defined filter group (by specifying its <i>group-id</i>) to either a CM or its CPE devices, for downstream or upstream traffic.</p>

	Command or Action	Purpose
<b>Step 16</b>	<b>cable submgmt default active</b> <b>Example:</b> Router(config)# <b>cable submgmt default active</b>	(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).

### Example

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
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
254 128Y Use Verbose     Use Verbose
Router# show cable filter group 254 index 128
Filter   SrcAddr/Mask   DestAddr/Mask   Prot ToS   SPort DPort TCP   Action Status
Grp Id v6
254 128Y Use Verbose     Use Verbose
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 releases support 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-xe 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.



---

### 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.
-



## Procedure

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<b>configure terminal</b> <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip name-server</b> [vrf vrf-name] server-address1 [server-address2...server-address6] <b>Example:</b> 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	<b>exit</b> <b>Example:</b> Router(config)# exit	Leaves global configuration mode and enters privileged EXEC mode.
Step 5	<b>show cable modem domain-name</b> <b>Example:</b> 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 15](#).

### Restrictions

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

## Configuring IPv6 VPN over MPLS

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 the configuration examples, see [Configuration Examples for IPv6 on Cable, on page 30](#).



---

**Note** 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

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.

---

## Procedure

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<b>configure terminal</b> <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface type number</b> <b>Example:</b> Router(config)# <b>interface ethernet 4/2</b>	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	<b>ipv6 dhcp relay destination ipv6-address[ interface] [link-address link-address ] [ source-address source-address]</b> <b>Example:</b> Router(config-if) <b>ipv6 dhcp relay destination 2001:db8:1234::1 ethernet 4/2 link-address 2001:db8::1 source-address 2001:db8::2</b>	Specifies a destination address to which client packets are forwarded and enables DHCPv6 relay service on the interface.
Step 5	<b>end</b> <b>Example:</b> Router(config-if) <b>end</b>	Exits interface configuration mode and enters privileged EXEC mode.

## Configuring IPv6 Source Address and Link Address

In some network deployments, there is a firewall between CNR servers and CMTS router. The firewall only allows packets from certain addresses to transmit to CMTS router.

To allow the DHCPv6 message to be sent to CNR server with specific source address, user needs to configure the source address of the relayed forwarded DHCPv6 message in the following 3 ways:

1. In the global configuration mode, use the command **ipv6 dhcp-relay source-interface interface-type interface-number**
2. In the interface configuration mode, use the command **ipv6 dhcp relay source-interface interface-type interface-number**
3. In the interface configuration mode, use the command **ipv6 dhcp relay destination ipv6-address[interface] /link-address link-address ] [source-address source-address]**

If the user does not have any of the above configuration, the DHCPv6 message will be relay forwarded with default source-address, which will be calculated based on relay destination address.

If any one of above is configured, the source-address of the DHCPv6 message will be based on that configuration.

If more than one configuration above is configured, the overriding rule is that more specific configuration wins, i.e., 3>2>1.

## Configurable DOCSIS CMTS Capabilities DHCPv6 Field

According to DOCSIS 3.1 specification, CMTS must support DOCSIS 3.0 cable modems and features. To support the backward compatibility of DOCSIS versions, the DHCPv6 vendor option must change from 30 to 31.

You can now upgrade to any DOCSIS version using the **cable docsis-ver [major version | minor version]** command.

The default value of the command is **cable docsis-ver 3 1**.

## Disabling IPv6 ND Gleaning

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

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interfacebundle <i>bundle-no</i></b> <b>Example:</b>  Router(config)# <b>interface bundle 1</b>	Specifies a bundle interface number and enters bundle interface configuration mode. <ul style="list-style-type: none"> <li><i>bundle-no</i>—Bundle interface number. The valid range is from 1 to 255.</li> </ul>
<b>Step 4</b>	<b>no cable nd</b> <b>Example:</b>  Router(config-if) <b>no cable nd</b>	Disables IPv6 ND gleaning on the Cisco CMTS router.
<b>Step 5</b>	<b>end</b> <b>Example:</b>	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Router(config-if) <b>end</b>	

## 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.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>show cable modem [ip-address   mac-address] ipv6[ cpe   prefix   registered   unregistered]</b> <b>Example:</b> Router# <b>show cable modem ipv6 registered</b> <b>Example:</b> Router# <b>show cable modem 0019.474a.c14a ipv6 cpe</b>	Displays IPv6 information for specified CMs and CPEs behind a CM on a Cisco CMTS router. You can specify the following options:
<b>Step 3</b>	<b>show cable modem [ip-address   mac-address] registered</b> <b>Example:</b> Router# <b>show cable modem 0019.474e.e4DF registered</b>	Displays a list of the CMs that have registered with the Cisco CMTS. You can specify the following options:
<b>Step 4</b>	<b>show cable modem {ip-address   mac-address} cpe</b> <b>Example:</b> Router# <b>show cable modem 0019.474a.c14a cpe</b>	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   ---
C4/0/U2   3   online(pt)  1   2001:420:3800:809:EDA4:350C:2F75:4779  0019.474a.c18c
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

```

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

```

## Example: Complete Cable Configuration with IPv6

```

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

```





```

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 minislots-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 minislots-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 minislots-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 minislots-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 minislots-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 minislots-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 minislots-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 minislots-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 minislots-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 minislots-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 minislots-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 minislots-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 minislots-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 minislots-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 minislots-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 minislots-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

```

## Example: Complete Cable Configuration with IPv6

```

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:rfs_w_x373.bin alias rfs_w_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  ---- Publish directly connected route
  redistribute connected
  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 Label	Outgoing Label or VC	Prefix or Tunnel Id	Bytes Switched	Label	Outgoing interface	Next Hop
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
vrf_a			0		aggregate/vrf_a	
22	No Label	2001:40:3:112::/64[V]	\			---Route in
vrf_b			0		aggregate/vrf_b	

## 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
```

## Supported MIBs

### CISCO-DOCS-EXT-MIB

The CISCO-DOCS-EXT-MIB contains objects that support extensions to the Data-over-Cable Service Interface Specifications (DOCSIS) interface MIB, DOCS-IF-MIB.

- `CdxBundleIpHelperEntry`—Provides a list of cable helper entries on the bundle and sub-bundle interfaces.
- `CdxBundleIPv6DHCPRelayEntry`—Contains the IPv6 DHCP relay option, IPv6 DHCP relay source-interface details, and IPv6 DHCP relay trust configuration on a bundle and sub-bundle interface.
- `CdxBundleIPv6DHCPRelayDestEntry`—Contains a list of IPv6 DHCP relay destination entries on the cable bundle and sub-bundle interfaces.

## Additional References

### Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature Information for IPv6 on Cable

Use Cisco Feature Navigator to find information about the 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 the <https://cfng.cisco.com/> link. An account on the Cisco.com page is not required.



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

**Table 2: Feature Information for Downstream Interface Configuration**

Feature Name	Releases	Feature Information
Enabling MDD with Pre-Registration DSID	Cisco IOS XE Gibraltar 16.12.1x	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.
Configurable DOCSIS CMTS Capabilities DHCPv6 Field	Cisco IOS XE Fuji 16.7.1	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.
IPv6 on cable	Cisco IOS XE Everest 16.6.1	This feature was integrated into the Cisco cBR Series Converged Broadband Routers.