CMTS Router Service Features

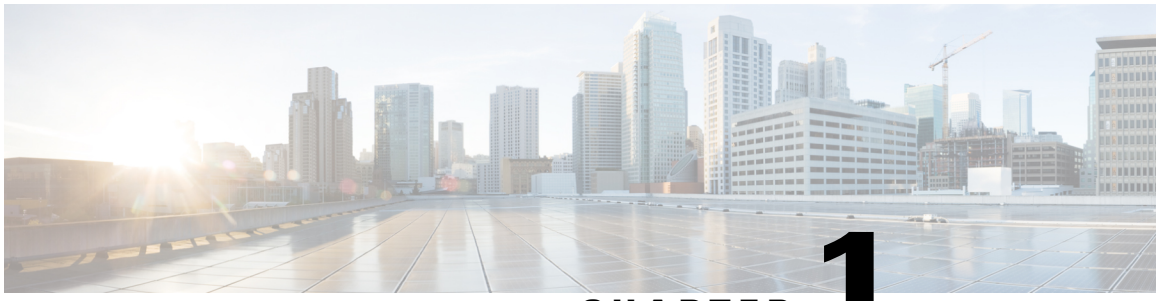
First Published: 2008-02-14

Last Modified: 2014-06-16

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

Text Part Number: OL-27605-02

CONTENTS



CHAPTER 1

Advanced-Mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: February 9, 2009

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

The Advanced-Mode DOCSIS Set-Top Gateway (A-DSG) Issue 1.2 introduces support for the latest DOCSIS Set-Top specification from CableLabs™, to include the following enhancements:

- *DOCSIS Set-top Gateway (DSG) Interface Specification*
- A-DSG 1.2 introduces support for the DOCS-DSG-IF MIB.

Cisco A-DSG 1.2 is certified by CableLabs™, and is a powerful tool in support of latest industry innovations. A-DSG 1.2 offers substantial support for enhanced DOCSIS implementation in the broadband cable environment. The set-top box (STB) dynamically learns the overall environment from the Cisco CMTS router, to include MAC address, traffic management rules, and classifiers.

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 Advanced-Mode DSG Issue 1.2

Table below shows the hardware compatibility prerequisites for the A-DSG for the Cisco CMTS Routers feature.

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

Table 1: A-DSG for the Cisco CMTS Routers Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • PRE2 **Cisco IOS Release 12.2(33)SCB and later** • PRE4	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR10-MC5X20S/U/H **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V[1]
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V[2]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCD and later** • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X • Cisco uBR-MC16U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V[3]

1 Cisco uBR3GX60V cable interface line card is compatible only with PRE4.
2 You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.
3 You must use NPE-G2 with the Cisco uBR-MC88V cable interface line card.

Restrictions for Advanced-Mode DSG Issue 1.2

This section contains restrictions that are specific to A-DSG 1.2 on a Cisco CMTS router.

DSG Configuration File Transfer Operations

DSG 1.2 does not support the copying of a DSG configuration file from a TFTP server, file system, or bootflash to the running configuration.

Previously, with DSG 1.1, when copying the DSG configuration file from a file system or TFTP server to the running configuration, DSG rule error checking may disable a previously configured and valid DSG tunnel configuration. This issue has not been observed in DSG 1.1 when loading the DSG configuration file from the startup configuration, as during a reload.

Multicast Configuration Restrictions

As with earlier versions of DSG Issues 0.9 and 1.0, IP multicasting must be configured for correct operation of A-DSG 1.2. Specifically, IP multicast routing must be set in global configuration. Also, IP PIM must be configured on all bundle interfaces of cable interfaces that are to carry multicast traffic.

See the Configuring the Default Multicast Quality of Service, on page 7 and the Configuring IP Multicast Operations, on page 14 for additional Multicast information and global configurations supporting DSG.

NAT for DSG Unicast-only Mapping

A-DSG 1.2 supports multicast IP addressing. However, it also supports unicast IP destination addresses. On the Cisco uBR7246VXR router, DSG 1.2 support is provided with the configuration of Network Address Translation (NAT) on the router, to include these settings:

- WAN interface(s) are configured with the **ip nat outside** command.
- Cable interface(s) are configured with the **ip nat inside** command.
- For each mapping, additional configuration includes the source static multicast IP address and the unicast IP address.

The unicast IP address is the unicast destination IP address of the DSG packets arriving at the Cisco CMTS router. The multicast IP address is the new destination IP address that is configured to map to one or a set of DSG tunnels.

PIM and SSM for Multicast

When using Source Specific Multicast (SSM) operation in conjunction with A-DSG 1.2, the following system-wide configuration command must be specified:

- **ip pim ssm**

Refer to the Configuring IP Multicast Operations, on page 14.

Subinterfaces

A-DSG 1.2 supports subinterfaces on the Cisco CMTS router starting from Cisco IOS Release 12.2(33)SCB4.

Note Effective with Cisco IOS Release 12.2(33)SCH3, ensure that the DSG downstream configuration is disabled, before you remove a DSG tunnel group from a subinterface.

Information About Advanced-Mode DSG Issue 1.2

A-DSG 1.2 offers substantial upgrades over A-DSG 1.1 and earlier basic DSG on the Cisco CMTS router. A-DSG 1.2 offers these new or enhanced capabilities:

- A-DSG client and agent modes
- Advanced-mode MIBs supporting DSG 1.2, including the DOCS-DSG-IF-MIB
- Advanced-mode tunnels with increased security
- Cable interface bundling through virtual interface bundling
- Downstream Channel Descriptor
- IP multicast support

- Quality of Service (QoS)

DSG 1.2 Clients and Agents

A-DSG 1.2 supports the DSG client and agent functions outlined by the CableLabs™ *DOCSIS Set-top Gateway (DSG) Interface Specification* , CM-SP-DSG-I05-050812.

FQDN Support

Starting with Cisco IOS Release 12.2(33)SCG, you can specify either a fully-qualified domain name (FQDN) or IP address for A-DSG classifier multicast group and source addresses using the **cable dsg cfr** command in global configuration mode. We recommend that you use an FQDN to avoid modification of multicast group and source addresses when network changes are implemented.

This feature allows you to use a hostname (FQDN) in place of the source IP address using the **cable dsg cfr** command. For example, you have two A-DSG tunnel servers, in two locations, sending multicast traffic to the same multicast address. In this scenario, you can specify a hostname for the source IP address and let the DNS server determine which source is sending the multicast traffic.

If you configure an A-DSG classifier with a hostname, the Cisco CMTS router immediately verifies if the hostname can be resolved against an IP address using the local host cache. If not, the router does not enable the classifier until the hostname is resolved. If the hostname cannot be resolved locally, the router performs a DNS query to verify the DSG classifiers.

The FQDN format does not support static Internet Group Management Protocol (IGMP) join requests initiated on the Cisco CMTS router. The IGMP static group IP address created automatically under a bundle interface at the time of A-DSG configuration is not displayed in the **show running-config interface command output i**n Cisco IOS Release 12.2(33)SCG and later. To display the A-DSG static groups configured under a bundle interface, use the **show cable dsg static-group bundle** command in privileged EXEC mode **i**n Cisco IOS Release 12.2(33)SCG and later.

DSG Name Process and DNS Query

Every DNS record contains a time to live (TTL) value set by the server administrator, and this may vary from seconds to weeks. The DSG name process supersedes the TTL value criterion to update A-DSG classifiers on the Cisco CMTS router.

The DSG name process enables the Cisco CMTS router to query the DNS server for faster classifier updates. To enable the Cisco CMTS router to perform a DNS query for an A-DSG classifier verification, you must configure one or more DNS servers using the **ip name-server** command in global configuration mode. You can also specify the DNS query interval using the **cable dsg name-update-interval** command in global configuration mode.

During a Cisco IOS software reload or a route processor switchover, the router may fail to query the DNS server if the interfaces are down, and the router may not wait for the interval specified using the **cable dsg name-update-interval** command to perform a DNS query. In this case, for an unresolved hostname, the router automatically performs a DNS query based on a system-defined (15 seconds) interval to facilitate faster DSG classifier updates. You cannot change the system-defined interval.

A-DSG Forwarding on the Primary Channel

In Cisco IOS Release 12.2(33)SCF and earlier, DSG tunnels are configured globally and applied to all MAC domain interfaces. This automatically creates DSG tunnels for all primary capable interfaces associated with the MAC domain interfaces.

In Cisco IOS Releases earlier to 12.2(33)SCG, you cannot exclude A-DSG forwarding per primary capable interface. However, you can disable A-DSG forwarding for the entire MAC domain by using the no form of the cable dsg tg command.

Starting with Cisco IOS Release 12.2(33)SCG, you can disable A-DSG forwarding per primary capable interface using the **cable downstream dsg disable** command in interface configuration mode. Primary capable interfaces include modular, integrated cable interfaces, and Cisco uBR10-MC5X20 and Cisco uBR-MC28U cable interfaces.

For example, assume the cable interface 7/1/1 has A-DSG enabled and has four modular channels attached to it. However, you want A-DSG forwarding enabled only on two of these four modular channels. You can exclude the channels of your choice using the cable downstream dsg disable command. For details on how to disable modular channels, see the Disabling A-DSG Forwarding on the Primary Channel, on page 21.

Note If A-DSG downstream forwarding is disabled on a primary capable interface, the router does not create multicast service flows on the primary capable interface and stops sending Downstream Channel Descriptor (DCD) messages.

DOCSIS 3.0 DSG MDF Support

Support for DOCSIS 3.0 DSG Multicast DSID Forwarding (MDF) is introduced in Cisco IOS Release 12.2(33)SCG using DSG DA-to-DSID Association Entry type, length, value (TLV 13) in the MAC domain descriptor (MDD) message to communicate the association between a downstream service identifier (DSID) and a group MAC address used for DSG tunnel traffic. This is automatically supported on the Cisco CMTS router.

DOCSIS 2.0 hybrid CMs and DOCSIS 3.0 CMs use Dynamic Bonding Change (DBC) to get DSID information from the Cisco CMTS router, whereas DOCSIS 2.0 DSG hybrid embedded CMs and DOCSIS 3.0 DSG embedded CMs get DSID information from the Cisco CMTS router through MDD messages.

To disable MDF capability on all DSG embedded cable modems, including DOCSIS 3.0 DSG and DOCSIS 2.0 DSG hybrid modems, use the cable multicast mdf-disable command with the dsg keyword in global configuration mode.

Source Specific Multicast Mapping

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments.

The following two Cisco IOS components together support the implementation of SSM:

- Protocol Independent Multicast source-specific mode (PIM-SSM)

- Internet Group Management Protocol Version 3 (IGMPv3)

Starting with Cisco IOS Release 12.2(33)SCG, SSM mapping can be configured on Cisco CMTS routers.

For details on how to configure SSM mapping on a Cisco CMTS router, see the Source Specific Multicast (SSM) Mapping feature guide.

How to Configure Advanced-Mode DSG Issue 1.2

Advanced-mode DSG Issue 1.2 entails support for DSG tunnel configuration, to include global, WAN-side, and interface-level settings in support of Multicast.

Configuring the Default Multicast Quality of Service

According to DOCSIS 3.0, you must configure the default multicast quality of service (MQoS) when using the MQoS. This also applies to the DSG, which uses the MQoS by associating a service class name with the tunnel.

If the default MQoS is not configured, the DSG tunnel service class configuration is rejected. Similarly, if no DSG tunnel uses the MQoS, you are prompted to remove the default MQoS.

The CMTS selects the primary downstream channel to forward the multicast traffic when the default MQoS is configured and there is no matching MQoS group configuration. Otherwise, the wideband interface is used to forward the 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	**configure terminal**
	
	Example:
	
	`Router# configure terminal`
	
	Example:
	
	`Router(config)#`
		Enters global configuration mode.

Step 3	**cable multicast group-qos default scn** *service-class-name* **aggregate** **Example:** `Router(config)# cable multicast group-qos default scn name1 aggregate`	Configures a service class name for the QoS profile.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

What to Do Next

Note If you configure or remove the default MQoS while the CMTS is sending multicast traffic, duplicate traffic is generated for approximately 3 minutes (or 3 times the query interval).

Configuring Global Tunnel Group Settings for Advanced-Mode DSG 1.2

This procedure configures global and interface-level commands on the Cisco CMTS router to enable DSG tunnel groups. A DSG tunnel group is used to bundle some DSG channels together and associate them to a MAC domain interface.

Global A-DSG 1.2 Tunnel Settings

This procedure sets and enables global configurations to support both A-DSG 1.2 clients and agents. Additional procedures provide additional settings for these clients and agents.

Before You Begin

Starting with the Cisco IOS Release 12.2(33)SCC1, when DOCSIS Set-top Gateway (DSG) is configured to have quality of service (QoS) for tunnel, ensure that the default multicast QoS (MQoS) is also configured. For more information, see Configuring the Default Multicast Quality of Service, on page 7.

Note The DSG tunnel service class configuration is rejected, if default MQoS is not configured.

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`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**cable dsg tg***group-id* [**channel***channel-id* |**priority***DSG-rule-priority*] [**enable**|**disable**] **Example:** `Router(config)# cable dsg tg 1 channel 1 priority 1 enable`	Command allows the association of a group of tunnels to one or more downstream interfaces on the Cisco CMTS.
Step 4	**cabledsg tg***group-id* [**channel** *channel-id* [**ucid** *ID1*]] **Example:** `Router(config)# cable dsg tg 1 channel 1 ucid 1`	Sets the upstream channel or channels to which the DSG 1.2 tunnel applies.
Step 5	**cable dsg tg** *group-id* [**channel** *channel-id* [**vendor-param** *vendor-group-id*]] **Example:** `Router(config)# cable dsg tg 1 channel 1 vendor-param 1`	Sets the vendor-specific parameters for upstream DSG 1.2 channels.
Step 6	**cable dsg vendor-param** *group-id* **vendor** *vendor-index* **oui** *oui* **value** *value-in-TLV* **Example:** `Router(config)# cable dsg vendor-param 1 vendor 1 oui ABCDEA value 0101AB`	Configures vendor-specific parameters for A-DSG 1.2. To remove this configuration from the Cisco CMTS, use the no form of this command.
Step 7	**cable dsg chan-list** *list-index* **index** *entry-index* **freq** *freq* **Example:** `Router(config)# cable dsg chan-list 1 index 1 freq 47000000`	Configures the A-DSG 1.2 downstream channel list. The channel list is a list of DSG channels (downstream frequencies) that set-top boxes can search to find the DSG tunnel appropriate for their operation. To remove the A-DSG 1.2 channel list from the Cisco CMTS, us the no form of this command.
Step 8	**cable dsg timer inde** [**Tdsg1** *Tdsg1*] | [**Tdsg2** *Tdsg2*] | [**Tdsg3** *Tdsg3*] | [**Tdsg4** *Tdsg4*] **Example:** `Router(config)# cable dsg timer 1 Tdsg1 1 Tdsg2 2 Tdsg3 3 Tdsg4 4`	Configures the A-DSG 1.2 timer entry to be associated to the downstream channel, and encoded into the Downstream Channel Descriptor (DCD) message. To remove the cable DSG timer from the Cisco CMTS, use the no form of this command.

	Command or Action	Purpose
Step 9	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

What to Do Next

Troubleshooting Tips

Refer to **debug** and **show** commands in the How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature, on page 22.

Adding DSG Tunnel Group to a Subinterface

This procedure adds a DSG tunnel group to a subinterface using the cable dsg tg group-id command. After adding the DSG tunnel-group to a subinterface, appropriate IP Internet Group Management Protocol (IGMP) static joins are created and forwarding of DSG traffic begins, if the downstream DSG is configured.

Note This feature is not supported on Cisco IOS Release 12.2(33)SCC.

Before You Begin

Cisco IOS Release 12.2(33)SCB4 or Cisco IOS Release 12.2(33)SCC1 or future release versions must be installed previously on the Cisco CMTS.

The downstream DSG should exist to create IGMP static joins.

Restriction You can associate a DSG tunnel group to only one subinterface within the same bundle interface.

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

Step 3	**interface bundle***bundle-subif-number*
	
	Example:
	
	`Router(config)# interface bundle 11.2`
	`Router(config-subif)#`
		Specifies the interface bundle and enters the subinterface configuration mode.

Step 4	**cable dsg tg***group-id* **Example:** `Router(config-subif)# cable dsg tg 1`	Adds a DSG tunnel group to a subinterface.
Step 5	end **Example:** `Router(config-subif)# end`	Returns to privileged EXEC mode.

Configuring the DSG Client Settings for Advanced-Mode DSG 1.2

After the global configurations and DSG client configurations are set for DSG 1.2 on the Cisco CMTS, use the following procedure to continue DSG 1.2 client configurations.

Restriction The **in-dcd ignore** option is not supported by DSG-IF-MIBS specification.

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 dsg client-list** *client-list-id* **id-index** *id* {**application-id** *app-id* | **ca-system-id** *sys-id* | **mac-addr** *mac-addr* | **broadcast** [*broadcast-id*]} **Example:** `Router(config)# cable dsg client-list 1 id-index 1 mac-addr abcd.abcd.abcd`	Sets the DSG client parameters. This command is changed from earlier Cisco IOS Releases, and for DSG 1.2, this command specifies the optional broadcast ID to client ID broadcast type and vendor specific parameter index.
Step 4	**cable dsg client-list** *client-list-id* **id-index** *id* [**vendor-param** *vendor-group-id*] **Example:** `Router(config-if)# cable dsg client-list 1 id-index 1 vendor-param 1`	Sets vendor-specific parameters for the DSG client.
Step 5	**cable dsg tunnel** *tunnel id* **mac_addr** *mac addr* **tg** *tunnel-group* **clients** *client-list-id* [**enable** | **disable**] **Example:** `Router(config)# cable dsg tunnel mac-addr abcd.abcd.abcd tg 1 clients 1 enable`	This command is changed to associate a tunnel group and client-list ID to a DSG tunnel. Also, an optional QoS service class name can be associated to the tunnel. **Note** To associate a cable service class with an A-DSG tunnel on a Cisco CMTS router, use the cable dsg tunnel srv-class command in global configuration mode.
Step 6	**cable dsg cfr** *cfr index* [**dest-ip** {*ipaddr* |*hostname}*] [**tunnel** *tunnel-index*][**dest-port** *start end*]| [**priority** *priority*][**src-ip** {*ipaddr* |*hostname}* [**src-prefix-len** *length*]] [**enable** | **disable**] [**in-dcd {yes** | **no** | **ignore}**] **Example:** `Router(config)# cable dsg cfr 1 dest-ip 224.225.225.225 tunnel 1 dest-port 40 50 priority 2 src-ip ciscovideo.com src-prefix-len 24 enable`	Specifies the DSG classifier index, with optional support for the DCD parameter, indicating whether or not to include the classifier in the DCD message. **Note** The **ignore** option was added to the **in-dcd keyword from** Cisco IOS Release 12.2(33)SCD5 onwards. When you use the **ignore** option, the DSG classifier is not included in the DCD message.

Step 7	**end**
	
	Example:
	
	`Router(config)# end`
	`Router#`
		Returns to privileged EXEC mode.

What to Do Next

Troubleshooting Tips

Refer to **debug** and **show** commands in the How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature, on page 22.

Configuring Downstream DSG 1.2 Settings for Advanced-Mode DSG 1.2

When the global and client configurations are set for DSG 1.2 on the Cisco CMTS, use the following procedure to continue with DSG 1.2 downstream configurations.

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	**interface cable** {*slot* /*port* |*slot* /*subslot*/*port* } **Example:** `Router(config)# interface cable 8/1/1`	Enters interface configuration mode.
Step 4	**cable downstream dsg tg** *group-id* **[channel** *channel-id]* **Example:** `Router(config-if)# cable downstream dsg tg 1 channel 1`	Associates the DSG tunnel group to the downstream interface. To remove this setting, use the **no** form of this command.
Step 5	**cable downstream dsg chan-list** *list-index* **Example:** `Router(config-if)# cable downstream dsg chan-list 2`	Associates the A-DSG channel list entry to a downstream channel, to be included in the DCD message. To remove this setting, use the **no** form of this command.
Step 6	**cable downstream dsg timer** *timer-index* **Example:** `Router(config-if)# cable downstream dsg timer 3`	Associates the DSG timer entry to a downstream channel, to be included in the DCD message. To remove this setting, use the no form of this command.
Step 7	**cable downstream dsg vendor-param** *vsif-grp-id* **Example:** `Router(config-if)# cable downstream dsg vendor-param 2`	Associates A-DSG vendor parameters to a downstream to be included in the DCD message. To remove this configuration from the Cisco CMTS, use the no form of this command.

	Command or Action	Purpose
Step 8	**cable downstream dsg** [**dcd-enable** | **dcd-disable**] **Example:** `Router(config-if)# cable downstream dsg dcd-enable`	Enables DCD messages to be sent on a downstream channel. This command is used when there are no enabled rules or tunnels for A-DSG currently on the Cisco CMTS. To disable DCD messages, use the **disable** form of this command.
Step 9	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Configuring IP Multicast Operations

This section describes how to configure the operation of IP multicast transmissions on the cable and WAN interfaces on the Cisco CMTS. You should perform this configuration on each cable interface being used for DSG traffic and for each WAN interface that is connected to a network controller or Conditional Access (CA) server that is forwarding IP multicast traffic.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**ip multicast-routing** **Example:** `Router(config)# ip multicast-routing`	Enables multicast routing on the router.
Step 3	**ip pim ssm** {**default** | **range***{access-list* | *word* }} **Example:** `Router(config)# ip pim ssm range 4`	Defines the Source Specific Multicast (SSM) range of IP multicast addresses. To disable the SSM range, use the no form of this command. **Note** When an SSM range of IP multicast addresses is defined by the **ip pim ssm** command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.
Step 4	ip cef distributed **Example:** `Router(config)# ip cef distributed`	Enables Cisco Express Forwarding (CEF) on the route processor card. To disable CEF, use the no form of this command. For additional information about the **ip cef** command, refer to the following document on Cisco.com:

	Command or Action	Purpose
		• *Cisco IOS Switching Services Command Reference* , Release 12.3 http://www.cisco.com/en/US/docs/ios/12_3/switch/command/reference/swtch_r.html
Step 5	**interface bundle** *bundle-number* **Example:** `Router(config)# interface bundle 10`	Enters interface configuration mode for each interface bundle being used for DSG traffic.
Step 6	**ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**} **Example:** `Router(config-if)# ip pim dense-mode`	Enables Protocol Independent Multicast (PIM) on the cable interface, which is required to use the DSG feature: **Note** You must configure this command on each interface that forwards multicast traffic.
Step 7	Repeat Step 5, on page 15 and Step 6, on page 15 for each cable interface that is being used for DSG traffic. Also repeat these steps on each W AN interface that is forwarding IP multicast traffic from the DSG network controllers and Conditional Access (CA) servers.	
Step 8	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Enabling DNS Query and DSG Name Process

The DSG name process enables the Cisco CMTS router to query the DNS server for faster classifier updates.

Before You Begin

Ensure that the IP DNS-based hostname-to-address translation is configured on the Cisco CMTS router using the **ip domain-lookup** command in global configuration mode. This is configured by default, and the status is not displayed in the running configuration.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**ip domain-name** *name* **Example:** `Router(config)# ip domain-name cisco.com`	Sets the IP domain name that the Cisco IOS software uses to complete unqualified host names
Step 3	r **ip name-serve***server-address*[**multiple-server-addresses**] **Example:** `Router(config)# ip name-server 131.108.1.111`	Sets the server IP address.
Step 4	**cable dsg name-update-interval***minutes* **Example:** `Router(config)# cable dsg name-update-interval 10`	Sets the interval to check the DNS server for any FQDN classifier changes.
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Configuring NAT to Support Unicast Messaging

This section describes how to configure a Cisco CMTS router for Network Address Translation (NAT) to enable the use of IP unicast addresses for DSG messaging. This allows the Cisco CMTS router to translate incoming IP unicast addresses into the appropriate IP multicast address for the DSG traffic.

For the Cisco uBR10012 router, A-DSG 1.2 can use an external router that is close to the Cisco CMTS to support unicast messaging. In this case, the nearby router must support NAT, and then send the address-translated multicast IP packets to the Cisco CMTS.

Tip This procedure should be performed after the cable interface has already been configured for DSG operations, as described in the Configuration Examples for Advanced-Mode DSG, on page 32.

Note The Cisco CMTS router supports NAT only when it is running an "IP Plus" (-i-) Cisco IOS software image. Refer to the release notes for your Cisco IOS release for complete image availability and requirements.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface** *wan-interface* **Example:** `Router(config)# interface FastEthernet0/0`	Enters interface configuration mode for the specified WAN interface.
Step 3	**ip nat outside** **Example:** `Router(config-if)# ip nat outside`	Configures the WAN interface as the "outside" (public) NAT interface.
Step 4	**interface bundle** *bundle-number* **Example:** `Router(config-if)# interface bundle 10`	Enters interface configuration mode for the specified interface bundle. **Note** This interface bundle should have previously been configured for DSG operations.
Step 5	**ip address** *ip-address mask* **secondary** **Example:** `Router(config-if)# ip address 192.168.18.1 255.255.255.0 secondary`	Configures the cable interface with an IP address and subnet that should match the unicast address being used for DSG traffic. This IP address and its subnet must not be used by any other cable interfaces, cable modems, or any other types of traffic in the cable network.
Step 6	**ip nat inside** **Example:** `Router(config-if)# ip nat inside`	Configures the cable interface as the "inside" (private) NAT interface.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 8	**ip nat inside source static** *ip-multicast-address cable-ip-address* **Example:** `Router(config)# ip nat inside source static 224.3.2.1 192.168.18.2`	Maps the unicast IP address assigned to the cable interface to the multicast address that should be used for the DSG traffic.
Step 9	Repeat Step 2, on page 17 and Step 8, on page 18 for each cable interface to be configured for DSG unicast traffic.	
Step 10	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring WAN Interfaces for Multicast Operations

In addition to basic WAN interface configuration on the Cisco CMTS, described in other documents, the following WAN interface commands should be configured on the Cisco CMTS to support IP multicast operations with A-DSG 1.2, as required.

- **ip pim**
- **ip pim ssm**
- **ip cef**

These commands are described in the Configuring IP Multicast Operations, on page 14, and in the following documents on Cisco.com.

For additional information about the **ip pim** command, refer to the following document on Cisco.com:

- *Cisco IOS IP Command Reference, Volume 3 of 4* : Multicast, Release 12.3

http://www.cisco.com/en/US/docs/ios/12_3/ipmulti/command/reference/iprmc_r.html

For additional information about the **ip pim ssm** command, refer to the following document on Cisco.com:

- *Cisco IOS IP Command Reference, Volume 3 of 4: Multicast* , Release 12.3 T

http://www.cisco.com/en/US/docs/ios/12_3t/ip_mcast/command/reference/ip3_i2gt.html

For additional information about the **ip cef** command, refer to the following document on Cisco.com:

- *Cisco IOS Switching Services Command Reference* , Release 12.3

http://www.cisco.com/en/US/docs/ios/12_3/switch/command/reference/swtch_r.html

Configuring a Standard IP Access List for Packet Filtering

This section describes how to configure a standard IP access list so that only authorized traffic is allowed on the cable interface.

Tip This procedure assumes a basic knowledge of how access lists use an IP address and bitmask to determine the range of IP addresses that are allowed access. For full details on configuring access lists, see the documents listed in the Additional References, on page 35.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**access-list** *access-list* **permit** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 permit 228.1.1.1`	Creates an access list specifying that permits access to the specific multicast address that matches the specified *group-ip-address* and *mask* .
Step 3	**access-list** *access-list* **deny** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 deny 224.0.0.0 15.255.255.255`	Configures the access list that denies access to any multicast address that matches the specified *group-ip-address* and *mask* .
Step 4	**access-list** *access-list* **deny any** **Example:** `Router(config)# access-list 90 deny any`	Configures the access list so that it denies access to any IP addresses other than the ones previously configured.
Step 5	**interface bundle** *bundle-number* **Example:** `Router(config)# interface bundle 10`	Enters interface configuration mode for the specified interface bundle.
Step 6	**ip access-group** *access-list* **Example:** `Router(config-if)# ip access-group 90`	(Optional, but recommended) Configures the interface with the access list, so that packets are filtered by the list before being accepted on the interface.

	Command or Action	Purpose
		Note Standard Access lists only allow one address to be specified in the earlier step. If you apply an outbound access-list with only the multicast address of the tunnel denied, then the DSG traffic is not allowed to pass. **Note** On the Cisco uBR10012 router, inbound access lists on the cable interface do not apply to multicast traffic, so they do not apply here. As a result, the Cisco uBR10012 requires that you use extended access lists that are blocked in the outbound direction for packets originating from the cable modem or CPE device on the network, and destined to the multicast group. The multicast group contains the classifiers associated with A-DSG 1.1 rules enabled on the interface.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to Privileged EXEC mode.

Configuring a Standard IP Access List for Multicast Group Filtering

This section describes how to configure a standard IP access list so that non-DOCSIS devices, such as DSG set-top boxes, can access only the authorized multicast group addresses and DSG tunnels.

Tip This procedure assumes a basic knowledge of how access lists use an IP address and bitmask to determine the range of IP addresses that are allowed access. For full details on configuring access lists, see the documents listed in the Additional References, on page 35.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**access-list** *access-list* **permit** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 permit 228.1.1.1`	Creates an access list specifying that permits access to the specific multicast address that matches the specified *group-ip-address* and *mask* .

	Command or Action	Purpose
Step 3	**access-list** *access-list* **deny** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 deny 224.0.0.0 15.255.255.255`	Configures the access list that denies access to any multicast address that matches the specified *group-ip-address* and *mask* .
Step 4	**access-list** *access-list* **deny any** **Example:** `Router(config)# access-list 90 deny any`	Configures the access list so that it denies access to any IP addresses other than the ones previously configured.
Step 5	**interface cable** *interface* **Example:** `Router(config)# interface cable 3/0`	Enters interface configuration mode for the specified cable interface.
Step 6	**ip igmp access-group** *access-list* [*version*] **Example:** `Router(config-if)# ip igmp access-group 90`	(Optional, but recommended) Configures the interface to accept traffic only from the associated access list, so that only authorized devices are allowed to access the DSG tunnels.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Disabling A-DSG Forwarding on the Primary Channel

You can disable A-DSG forwarding per primary capable interface.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface modular-cable** *slot* /*subslot*/*port* :*interface-number*	Specifies the modular cable interface and enters cable interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS

	Command or Action	Purpose
	Example: `Router(config)# interface modular-cable 1/0/0:0`	software release. For details, see the Cisco IOS CMTS Cable Command Reference .
Step 3	**cable downstream dsg disable** **Example:** `Router(config-if)# cable downstream dsg disable`	Disables A-DSG forwarding and DCD messages on the primary capable interface.
Step 4	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature

This section describes the following commands that you can use to monitor and display information about the Advanced-mode DOCSIS Set-Top Gateway feature:

Displaying Global Configurations for Advanced-Mode DSG 1.2

The following commands display globally-configured or interface-level DSG settings, status, statistics, and multiple types of DSG 1.2 tunnel information.

show cable dsg cfr

To verify all DSG classifier details, such as the classifier state, source, and destination IP addresses, use the show cable dsg cfr command as shown in the following example:

```
Router# show cable dsg cfr
cfr id state resolved applied conflict dest-ip           src-ip
------------------------------------ ----------------- -----------------
1000   en    yes      yes     no       232.10.10.0       dsg-server-a
                                                         (40.0.0.30)
1010   en    yes      yes     no       232.10.10.10      dsg-server-b
                                                         (40.0.0.40)
2000   en    yes      yes     no       232.10.11.0       dsg-server-c
                                                         (40.0.0.50)
2010   en    no       no      no       232.10.11.10      non-exist-hostnam
                                                         (----)
3000   en    yes      yes     no       239.10.11.11      0.0.0.0
```

To verify details of a particular DSG classifier, use the **show cable dsg cfr** command as shown in the following example:

```
Router# show cable dsg cfr 1010
cfr id state resolved applied conflict dest-ip           src-ip
------------------------------------ ----------------- ---------------
1010   en    yes      yes     no       232.10.10.10      dsg-server-b
                                                         (40.0.0.40)
```

To verify the detailed output for all DSG classifiers, use the **show cable dsg cfr** command as shown in the following example:

```
Router# show cable dsg cfr verbose
Cfr Id                    : 1000
State                     : enable
Resolved                  : yes
Applied                   : yes
Conflict                  : no
Conflict Cfr Id           : --
Error Code                : 0(DSG_CFR_ERR_NONE)
Tunnel Id                 : 1000
Dest Hostname             : ----
Dest Hostname IP          : ----
Dest IP                   : 232.10.10.0
Src Hostname              : dsg-server-a
Src Hostname IP           : 40.0.0.30
Src IP                    : 40.0.0.30
Src Prefix Length         : 32
Dest Port Start           : 2000
Dest Port End             : 13821
Priority                  : 1
In DCD                    : yes
Forwarded                 : 0
Received                  : 0
Cfr Id                    : 1010
State                     : enable
Resolved                  : yes
Applied                   : yes
Conflict                  : no
Conflict Cfr Id           : --
Error Code                : 0(DSG_CFR_ERR_NONE)
Tunnel Id                 : 1010
Dest Hostname             : ----
Dest Hostname IP          : ----
Dest IP                   : 232.10.10.10
Src Hostname              : dsg-server-b
Src Hostname IP           : 40.0.0.40
Src IP                    : 40.0.0.40
Src Prefix Length         : 32
Dest Port Start           : 2000
Dest Port End             : 13821
Priority                  : 1
In DCD                    : yes
Forwarded                 : 0
Received                  : 0
Cfr Id                    : 2000
State                     : enable
Resolved                  : yes
Applied                   : yes
Conflict                  : no
Conflict Cfr Id           : --
Error Code                : 0(DSG_CFR_ERR_NONE)
Tunnel Id                 : 2000
Dest Hostname             : ----
Dest Hostname IP          : ----
Dest IP                   : 232.10.11.0
Src Hostname              : dsg-server-c
Src Hostname IP           : 40.0.0.50
Src IP                    : 40.0.0.50
Src Prefix Length         : 32
Dest Port Start           : 13822
```

```
Dest Port End            : 13822
Priority                 : 1
In DCD                   : yes
Forwarded                : 0
Received                 : 0
Cfr Id                   : 2010
State                    : enable
Resolved                 : no
Applied                  : no
Conflict                 : no
Conflict Cfr Id          : --
Error Code               : 0(DSG_CFR_ERR_NONE)
Tunnel Id                : 2010
Dest Hostname            : ----
Dest Hostname IP         : ----
Dest IP                  : 232.10.11.10
Src Hostname             : non-exist-hostname
Src Hostname IP          : ----
Src IP                   : 0.0.0.0
Src Prefix Length        : 32
Dest Port Start          : 2000
Dest Port End            : 13821
Priority                 : 1
In DCD                   : yes
Forwarded                : 0
Received                 : 0
Cfr Id                   : 3000
State                    : enable
Resolved                 : yes
Applied                  : yes
Conflict                 : no
Conflict Cfr Id          : --
Error Code               : 0(DSG_CFR_ERR_NONE)
Tunnel Id                : 3000
Dest Hostname            : ----
Dest Hostname IP         : ----
Dest IP                  : 239.10.11.11
Src Hostname             : ----
Src Hostname IP          : ----
Src IP                   : 0.0.0.0
Src Prefix Length        : 32
Dest Port Start          : 2000
Dest Port End            : 13821
Priority                 : 1
In DCD                   : yes
Forwarded                : 0
Received                 : 0
```

To verify the detailed output for a single DSG classifier, use the **show cable dsg cfr** command as shown in the following example:

```
Router# show cable dsg cfr 1010 verbose
Cfr Id                   : 1010
State                    : enable
Resolved                 : yes
Applied                  : yes
Conflict                 : no
Conflict Cfr Id          : --
Error Code               : 0(DSG_CFR_ERR_NONE)
Tunnel Id                : 1010
Dest Hostname            : ----
Dest Hostname IP         : ----
Dest IP                  : 232.10.10.10
Src Hostname             : dsg-server-b
Src Hostname IP          : 40.0.0.40
Src IP                   : 40.0.0.40
Src Prefix Length        : 32
Dest Port Start          : 2000
Dest Port End            : 13821
Priority                 : 1
In DCD                   : yes
```

```
Forwarded                : 0
Received                 : 0
```

show cable dsg host

To verify the mapping of the DSG hostnames and IP addresses on a Cisco CMTS router, use the **show cable dsg host** command as shown in the following example:

```
Router# show cable dsg host
Host              IP Address      Reference  Last Update Time
dsgserver1        232.1.1.10      2          21:41 08/01/2011
dsgserver2        234.3.2.1       1          21:41 08/01/2011
dsgserver3        ----            1          never
dsgserver4        ----            1          never
dsgserver5        ----            1          never
dsgserver6        235.5.5.5       1          21:41 08/01/2011
dsgserver7        235.0.0.2       1          21:41 08/01/2011
```

To verify the verbose output of the mapping of the DSG hostnames and IP addresses on a Cisco CMTS router, use the **show cable dsg host** command as shown in the following example:

```
Router# show cable dsg host verbose
Host                    IP Address      Reference  Last Update Time
dsgserver1       232.1.1.10      2          21:41 08/01/2011
  Cfrs:
  cable dsg cfr 2 dest-ip 232.1.1.125 tunnel 1 priority 0 src-ip a.b.c.d d...
  cable dsg cfr 3 dest-ip 232.1.1.125 tunnel 1 priority 10 src-ip a.b.c.d ...
dsgserver2       234.3.2.1       1          21:41 08/01/2011
  Cfrs:
  cable dsg cfr 4 dest-ip aaabbccc priority 0 src-ip cccdddeee disable
dsgserver3       ----     1          never
  Cfrs:
  cable dsg cfr 4 dest-ip aaabbccc priority 0 src-ip cccdddeee disable
dsgserver4       235.0.0.2       1          21:41 08/01/2011
  Cfrs:
  cable dsg cfr 24 dest-ip g2 priority 0 disable
dsgserver5        235.0.0.3       1          21:41 08/01/2011
  Cfrs:
  cable dsg cfr 30 dest-ip g3 tunnel 1 priority 0 disable
```

show cable dsg tunnel

To display tunnel MAC address, state, tunnel group id, classifiers associated to tunnel and its state, use the **show cable dsg tunnel** command in privileged EXEC mode. This command also displays the number of interfaces to which a tunnel is associated, the clients associated, and the QoS service class name for all the configured tunnels.

The following example illustrates this command:

```
Router# show cable dsg tunnel
     tunnel              TG      cfr     tunnel   rule   client service
id  state mac-addr       id    id  state I/F    id state listId class
1      en 0100.5e01.0001 1     1      en C5/0   1     en 1      DSG-Rate1
                               6      en
                               7      en
                               8      en
2      en 0100.5e01.0002 1     2      en C5/0   2     en 2
3      en 0100.5e01.0003 1     3      en C5/0   3     en 3
4      en 0002.0002.0001 2     4      en C5/0   4     en 1
                                  C5/1   1     en 1
5      en 0002.0002.0002 2     5      en C5/0   5     en 2      DSG-Rate2
                                  C5/1   2     en 2
6      en 0002.0002.0003 2     9      en C5/0   6     en 21
                                  C5/1   3     en 21
```

show cable dsg tunnel ID

To display information for a given DSG tunnel, use the **show cable dsg tunnel** command, specifying the tunnel for which to display information.

show cable dsg tunnel *tunnel-id* [**cfr** | **clients** | **interfaces** | **statistics** | **verbose**]

- **cfr—**Shows DSG tunnel classifiers.
- **clients—**Shows DSG tunnel clients.
- **interfaces—**Shows DSG tunnel interfaces.
- **statistics—**Shows DSG tunnel statistics.
- **verbose—**Shows DSG tunnel detail information.

The below example illustrates this command for DSG Tunnel 1:

```
Router# show cable dsg tunnel 1
     tunnel              TG      cfr     tunnel   rule   client service
id  state mac-addr       id    id  state I/F    id state listId class
1      en 0100.5e01.0001 1     1      en C5/0   1     en 1      DSG-Rate1
                               6      en
                               7      en
                               8      en
```

The below example shows detailed information of all the classifiers associated to the specified tunnel.

```
Router# show cable dsg tunnel 1 cfr
tunnel cfr   cfr   cfr destination ip   source ip        srcPre d_port d_port
id     id    state pri address          address          length start  end
1      1     en    0   230.1.0.1        0.0.0.0          32     0      65535
       6     en    0   231.1.1.6        0.0.0.0          32     0      65535
       7     en    0   231.1.1.7        0.0.0.0          32     0      65535
       8     en    0   231.1.1.8        0.0.0.0          32     0      65535
```

The below example illustrates detailed information about all the clients associated to the specified tunnel.

```
Router# show cable dsg tunnel 1 clients
tunnel client client client          client          vendor
id     listId id     id type         address         group
1      1      1      MAC Addr        0100.5e00.0001
              2      Application ID  0x0951
              3      Broadcast       Unspecified
              4      Broadcast       4
```

The below example illustrates all DSG interfaces and rules associated to the specified tunnel.

```
Router# show cable dsg tunnel 1 interfaces
tunnel downstream   rule
id     interface    id
4      Cable5/0     4
       Cable5/1     1
```

show cable dsg tunnel ID statistics

The below example illustrates packet statistics information about the specified tunnel.

```
Router# show cable dsg tunnel 1 statistics
tunnel cfr   cfr   destination ip  source ip       total          total
id     id    state address         address         forwarded      received
1      1     en    230.1.0.1       0.0.0.0         0              0
       6     en    231.1.1.6       0.0.0.0         0              0
```

```
       7     en    231.1.1.7       0.0.0.0         0               0
       8     en    231.1.1.8       0.0.0.0         0               0
```

The below example illustrates all detailed information about the specified tunnel.

```
Router# show cable dsg tunnel 1 verbose
Tunnel ID                                       : 1
State                                           : enable
MAC Addr                                        : 0100.5e01.0001
TG Id                                           : 1
Cfr Id                                          : 1
State                                           : enable
Priority                                        : 0
Dest IP                                         : 230.1.0.1
Src IP                                          : 0.0.0.0
Src Prefix Length                               : 32
Dest Port Start                                 : 0
Dest Port End                                   : 65535
Forwarded                                       : 0
Received                                        : 0
Cfr Id                                          : 6
State                                           : enable
Priority                                        : 0
Dest IP                                         : 231.1.1.6
Src IP                                          : 0.0.0.0
Src Prefix Length                               : 32
Dest Port Start                                 : 0
Dest Port End                                   : 65535
Forwarded                                       : 0
Received                                        : 0
Cfr Id                                          : 7
State                                           : enable
Priority                                        : 0
Dest IP                                         : 231.1.1.7
Src IP                                          : 0.0.0.0
Src Prefix Length                               : 32
Dest Port Start                                 : 0
Dest Port End                                   : 65535
Forwarded                                       : 0
Received                                        : 0
Cfr Id                                          : 8
State                                           : enable
Priority                                        : 0
Dest IP                                         : 231.1.1.8
Src IP                                          : 0.0.0.0
Src Prefix Length                               : 32
Dest Port Start                                 : 0
Dest Port End                                   : 65535
Forwarded                                       : 0
Received                                        : 0
Client List Id                                  : 1
Client Id                                       : 1
Client Id Type                                  : MAC Addr        0100.5e00.0001
Client Id                                       : 2
Client Id Type                                  : Application ID  0x0951
Client Id                                       : 3
Client Id Type                                  : Broadcast       Unspecified
Client Id                                       : 4
Client Id Type                                  : Broadcast       4
Interface                                       : Cable5/0
Rule Id                                         : 1
```

show cable dsg tg

The below example illustrates configured parameters for all DSG tunnel groups.

```
Router# show cable dsg tg
TG    Chan  Chan         Rule Vendor UCID
id    id    state I/F    pri  Param  list
1     1     en    C5/0   16   1      1 2 3 4
```

```
1     2     en           0
2     1     en    C5/0   11   2
                  C5/1
2     2     en           0
```

Note Beginning with Cisco IOS Release 12.2(33)SCG, the "TG state" field in the **show cable dsg tg command output was replaced by "Chan state" to indicate that a channel belonging to a tunnel group is either enabled or diabled. It is possible that a tunnel group is enabled but a particular channel in that tunnel group is disabled.**

The below example displays the same information as above for the specified tunnel group.

```
Router# show cable dsg tg 1 channel 1
TG    Chan  Chan         Rule Vendor UCID
id    id    state I/F    pri  Param  list
1     1     en    C5/0   16   1      1 2 3 4
```

The below example illustrates detailed information for the specified tunnel group.

```
Router# show cable dsg tg 1 channel 1 verbose
TG: 1     Chan: 1     state: en pri: 16 Vendor: 1     UCID: 1 2 3 4
          rule        tunnel                    cfr                       clients
 I/F    id state id state mac-addr       id  state dest-ip         In-DCD listId
 C5/0   1     en 1     en 0101.5e01.0001 1      en 230.1.0.1       yes    1
                                         6      en 231.1.1.6       no
                                         7      en 231.1.1.7       no
                                         8      en 231.1.1.8       no
        2     en 2     en 0101.5e01.0002 2      en 230.1.0.2       yes    2
        3     en 3     en 0101.5e01.0003 3      en 230.1.0.3       yes    3
```

The following is a sample output for the **show cable dsg tg** command that displays the ignore option, introduced in Cisco IOS Release 12.2(33)SCD5, under the 'In DCD' column.

```
Router# show cable dsg tg 1 channel 1 verbose
TG: 1     Chan: 1     state: en pri: 16 Vendor: 1     UCID: 1 2 3 4
          rule        tunnel                    cfr                       clients
 I/F    id state id state mac-addr       id  state dest-ip         In-DCD listId
------ -------- ----------------------- ------------------------- --- -------
 C7/0/0 1     en 1     en 0101.5e01.0001 1      en 230.1.0.1       ign    1
                                         6      en 231.1.1.6       no
                                         7      en 231.1.1.7       no
                                         8      en 231.1.1.8       no
        2     en 2     en 0101.5e01.0002 2      en 230.1.0.2       yes    2
        3     en 3     en 0101.5e01.0003 3      en 230.1.0.3       yes    3
```

show running-config interface

To display a tunnel group attached to a subinterface, use the **show running-config interface** command in privileged EXEC mode, as shown in the example below:

```
Router# show running-config interface bundle 11.2
!
interface Bundle11.2
 ip address 4.4.2.1 255.255.255.0
 no ip unreachables
 ip pim sparse-mode
 ip igmp static-group 230.1.1.30
 no cable ip-multicast-echo
 cable dsg tg 61
end
```

Note The IGMP static group IP address created automatically at the time of DSG configuration is not displayed in the **show running-config interface command output i**n Cisco IOS Release 12.2(33)SCG and later.

show cable dsg static-group bundle

To verify all DSG static groups configured under a bundle interface, use the **show cable dsg static-group bundle** command in privileged EXEC mode as shown in the following example:

```
Router# show cable dsg static-group bundle 2
Bundle Interface     Group           Source
Bundle2              228.0.0.1       0.0.0.0
Bundle2              228.0.0.1       1.2.3.4
Bundle2              232.1.1.1       2.3.4.5
```

Displaying Interface-level Configurations for Advanced-Mode DSG 1.2

The following **show** commands display interface-level configurations for A-DSG 1.2.

show cable dsg tunnel interfaces

To display all interfaces and DSG rules for the associated tunnel, use the **show cable dsg tunnel interfaces** command in privileged EXEC mode.

show cable dsg tunnel (*tunnel-id*) **interfaces**

The following example illustrates this command:

```
Router# show cable dsg tunnel 1 interfaces
tunnel downstream   rule
id     interface    id
4      Cable5/0     4
       Cable5/1     1
```

show interfaces cable dsg downstream

To display DSG downstream interface configuration information, to include the number of DSG tunnels, classifiers, clients, and vendor-specific parameters, use the **show interfaces cable dsg downstream** command in privileged EXEC mode.

show interfaces cable {slot/port | slot/subslot/port} **dsg downstream**

Keywords for this command include the following:

- **dcd—**Displays the DSG downstream DCD message.
- **tg—**Displays the DSG downstream tunnel group.
- **tunnel—**Displays the DSG downstream tunnel.

The following example illustrates this command supporting DSG 1.2:

```
Router# show interfaces c5/0 dsg downstream
```

```
chan chFreq chan timer init    oper    twoWay oneWay num  num    num  num    num
list index  freq index timeout timeout timer  timer  rule tunnel cfr  client vsp
1    1      471  1     4       600     300    1800   6    6      3    4      2
     2      477
     3      483
     4      583
```

show interfaces cable dsg downstream dcd

To display DCD statistics for the given downstream, use the **show interfaces cable dsg downstream dcd** command in privileged EXEC mode. This command only displays DCD Type/Length/Value information if the **debug cable dsg** command is previously enabled.

show interfaces cable {slot/port | slot/subslot/port} **dsg downstream dcd**

The following example illustrates DCD statistics information supporting DSG 1.2:

```
Router# show interfaces c5/0 dsg downstream dcd
dcd   dcd   num of dcd           num of dcd           num of dcd  num of
state Tx    sent                fail                 change cnt  fragment
en    on    6502                0                    28          1
Router# debug cable dsg
CMTS DSG debugging is on
Router#
Router# show interfaces c5/0 dsg downstream dcd
dcd   dcd   num of dcd           num of dcd           num of dcd  num of
state Tx    sent                fail                 change cnt  fragment
en    on    6512                0                    28          1
Router#
02:08:42: DCD TLV last sent:
32360101 01020110 03040102 03040412 02060100 5E000001 04020951 01000102
00040506 01005E01 00010602 00012B08 08030000 01010101 170F0202 00010501
00090605 04E60100 01322801 01020201 10030401 02030404 0403020A BC050601
005E0100 02060200 022B0808 03000001 01010117 0F020200 02050100 09060504
E6010002 32280101 03020110 03040102 03040404 04020123 05060100 5E010003
06020003 2B080803 00000101 0101170F 02020003 05010009 060504E6 01000332
38010104 02010B04 12020601 005E0000 01040209 51010001 02000405 06000200
0200012B 09080300 00010102 01022B09 08030000 02010201 02322A01 01050201
0B040403 020ABC05 06000200 0200022B 09080300 00010102 01022B09 08030000
02010201 02324601 01060201 0B042002 06002100 21000102 06002100 21000202
06002100 21000302 06002100 21000405 06000200 0200032B 09080300 00010102
01022B09 08030000 02010201 02332801 041C12E3 C001041C 6E714001 041CC9FE
C0010422 BFDFC002 02000403 02025804 02012C05 020708
```

show interfaces cable dsg downstream tg

To display DSG tunnel group parameters, and rule information applying to the tunnel group, to include tunnels and tunnel states, classifiers, and client information, use the **show interfaces cable dsg downstream tg** command in privileged EXEC mode. You can display information for a specific tunnel, if specified.

show interfaces cable {slot/port | slot/subslot/port} **dsg downstream tg [channel** *channel-id***]**

The following example illustrates typical information displayed with this command in DSG 1.2:

```
Router# show interfaces c5/0 dsg downstream tg
TG: 1     Chan: 1     state: en pri: 16 Vendor: 1     UCID: 1 2 3 4
          rule        tunnel                    cfr                        client
 I/F    id state id state mac-addr       id  state dest-ip         In-DCD listId
 C5/0   1     en 1     en 0101.5e01.0001 1      en 230.1.0.1       yes    1
                                         6      en 231.1.1.6       no
                                         7      en 231.1.1.7       no
                                         8      en 231.1.1.8       no
        2     en 2     en 0101.5e01.0002 2      en 230.1.0.2       yes    2
        3     en 3     en 0101.5e01.0003 3      en 230.1.0.3       yes    3
TG: 2     Chan: 1     state: en pri: 11 Vendor: 2     UCID:
```

```
          rule        tunnel                    cfr                       client
 I/F    id state id state mac-addr       id  state dest-ip         In-DCD listId
 C5/0   4     en 4     en 0002.0002.0001 4      en 230.2.2.1       no     1
        5     en 5     en 0002.0002.0002 5      en 230.2.2.2       no     2
        6     en 6     en 0002.0002.0003 9      en 231.1.1.9       no     21
```

The following examples displays the same type of information as above for the given tunnel group.

```
Router# show interfaces c5/0 dsg downstream tg 1 channel 1
TG: 1     Chan: 1     state: en pri: 16 Vendor: 1     UCID: 1 2 3 4
          rule        tunnel                    cfr                       client
 I/F    id state id state mac-addr       id  state dest-ip         In-DCD listId
 C5/0   1     en 1     en 0101.5e01.0001 1      en 230.1.0.1       yes    1
                                         6      en 231.1.1.6       no
                                         7      en 231.1.1.7       no
                                         8      en 231.1.1.8       no
        2     en 2     en 0101.5e01.0002 2      en 230.1.0.2       yes    2
        3     en 3     en 0101.5e01.0003 3      en 230.1.0.3       yes    3
```

The following is a sample output for the **show interfaces cable dsg downstream tg** command that displays the ignore option, introduced in Cisco IOS Release 12.2(33)SCD5, under the 'In DCD' column.

```
Router# show interfaces cable 7/0/0 dsg downstream tg
TG: 1     Chan: 1     State: en  Pri: 0   Vendor:       UCID:
   rule        tunnel                    cfr              In  clients
 id state id  state mac-addr       id  state dest-ip         DCD listId
 -------- ----------------------- ------------------------- --- -------
 1     en 1      en 0100.5e01.0101 1      en 230.1.1.1       ign  1
```

show interfaces cable dsg downstream tunnel

To display DSG tunnel information associated with the downstream, use the **show interfaces cable dsg downstream tunnel** command in privileged EXEC mode.

show interfaces cable {*slot*/*port* | *slot*/*subslot*/*port*} **dsg downstream tunnel***tunnel-id*

The following is a sample output for the **show interfaces cable dsg downstream tunnel** command that displays the interface information for the DSG downstream tunnel in DSG 1.2:

```
Router# show interfaces c5/0 dsg downstream tunnel
     tunnel              TG      cfr       rule   client service
id  state mac-addr       id    id  state id state listId class
1      en 0100.5e01.0001 1     1      en 1     en 1      DSG-Rate1
                               6      en
                               7      en
                               8      en
2      en 0100.5e01.0002 1     2      en 2     en 2
3      en 0100.5e01.0003 1     3      en 3     en 3
4      en 0002.0002.0001 2     4      en 4     en 1
5      en 0002.0002.0002 2     5      en 5     en 2      DSG-Rate2
6      en 0002.0002.0003 2     9      en 6     en 21
```

The following is a sample output for the **show interfaces cable dsg downstream tunnel** command that displays information for the specified interface and tunnel:

```
Router# show interfaces c5/0 dsg downstream tunnel 1
     tunnel              TG      cfr       rule   client service
id  state mac-addr       id    id  state id state listId class
1      en 0100.5e01.0001 1     1      en 1     en 1      DSG-Rate1
                               6      en
                               7      en
                               8      en
```

Debugging Advanced-Mode DSG

To enable debugging for A-DSG on a Cisco CMTS router, use the debug cable dsg command in privileged EXEC mode.

Configuration Examples for Advanced-Mode DSG

This configuration example illustrates a sample DSG network featuring these components:

- Two Cisco universal broadband routers
- IP Multicast for each DSG implementation
- Two DSG Clients for each Cisco CMTS
- Two DSG Servers (one for each Cisco CMTS)

Each Cisco CMTS is configured as follows, and the remainder of this topic describes example configurations that apply to this architecture.

CMTS Headend 1

- DSG Server #1—Connected to Cisco CMTS via IP Multicast, with DSG Server having IP Address 12.8.8.1
- Destination IP Address for the Cisco CMTS—228.9.9.1
- DSG Tunnel Address—0105.0005.0005
- Downstream #1 Supporting two DSG Clients:
  - DSG Client #1—ID 101.1.1
  - DSG Client #2—ID 102.2.2

CMTS Headend 2

- DSG Server #2—Connected to Cisco CMTS via IP Multicast, with DSG Server having IP Address 12.8.8.2
- Destination IP Address for the Cisco CMTS—228.9.9.2
- DSG Tunnel Address—0106.0006.0006
- Downstream #2 Supporting two DSG Clients:
  - DSG Client #1—ID 101.1.1
  - DSG Client #2—ID 102.2.2

Example of Two DSG Tunnels with MAC DA Substitution

In this configuration, and given the two Cisco CMTS Headends cited above, below are the two sets of DSG rules, with each set applying to each Cisco CMTS, in respective fashion.

These settings apply to DSG #1 and two downstreams:

- DSG Rule ID 1
- DSG Client ID 101.1.1
- DSG Tunnel Address 105.5.5

These settings apply to DSG Rule #2 and two downstreams:

- DSG Rule ID 1
- DSG Client ID 102.2.2
- DSG Tunnel Address 106.6.6

DSG Example with Regionalization Per Downstream

In this configuration, and given the two Cisco CMTS Headends cited earlier in this topic, below are two downstream rules that can be configured in this architecture, for example:

- Downstream Rule #1
  - DSG Rule ID #1
  - DSG Client ID—101.1.1
  - DSG Tunnel Address—105.5.5
- Downstream Rule #2
  - DSG Rule ID #2
  - DSG Client ID—102.2.2
  - DSG Tunnel Address—106.6.6

DSG Example with Regionalization Per Upstream

In this configuration, and given the two Cisco CMTS Headends cited earlier in this topic, below are two upstream rules that can be configured in this architecture, for example:

- Upstream Rule #1
  - DSG Rule ID #1
  - DSG Client ID—101.1.1
  - DSG UCID Range—0 to 2
  - DSG Tunnel Address—105.5.5
- Upstream Rule #2
  - DSG Rule ID #2

- DSG Client ID—102.2.2
- DSG UCID Range—3 to 5
- DSG Tunnel Address—106.6.6

Example of Two DSG Tunnels with Full Classifiers and MAC DA Substitution

In this configuration, and given the two Cisco CMTS Headends cited above, below are the two sets of DSG rules, with each set applying to each Cisco CMTS, in respective fashion.

These settings apply to DSG #1:

- DSG Rule ID 1
- Downstreams 1 and 2
- DSG Client ID 101.1.1
- DSG Tunnel Address 105.5.5
- DSG Classifier ID—10
- IP SA—12.8.8.1
- IP DA—228.9.9.1
- UDP DP—8000

These settings apply to DSG Rule #2:

- DSG Rule ID 2
- Downstreams 1 and 2
- DSG Client ID 102.2.2
- DSG Tunnel Address 106.6.6
- DSG Classifier ID—20
- IP SA—12.8.8.2
- IP DA—228.9.9.2
- UDP DP—8000

Example of One DSG Tunnel Supporting IP Multicast from Multiple DSG Servers

In this configuration, and given the two Cisco CMTS Headends cited earlier in this topic, below is an example of one DSG Tunnel with multiple DSG servers supporting IP Multicast:

- DSG Rule ID 1
- Downstreams 1 and 2
- DSG Client ID 101.1.1 and 102.2.2
- DSG Tunnel Address 105.5.5
- DSG Classifier ID—10

- IP SA—12.8.8.1
- IP DA—228.9.9.1
- UDP DP—8000

- DSG Classifier ID—20
  - IP SA—12.8.8.2
  - IP DA—228.9.9.2
  - UDP DP—8000

Example: Enabling DNS Query

The following example shows how to enable a DNS query on the Cisco CMTS router:

```
Router# configure terminal
Router(config)# ip domain-lookup
Router(config)# ip domain-name cisco.com
Router(config)# ip name-server 131.108.1.111
Router(config)# cable dsg name-update-interval 10
Router(config)# end
```

Example: Disabling A-DSG Forwarding on the Primary Channel

The following example shows how to disable A-DSG forwarding on a primary capable modular interface on the Cisco CMTS router:

```
Router# configure terminal
Router(config)# interface modular-cable 1/0/0:0
Router(config-if)# cable downstream dsg disable
Router(config-if)# end
```

Additional References

The following sections provide references related to A-DSG 1.2.

Related Documents

Related Topic	Document Title
Cisco CMTS Commands	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
DOCSIS 3.0 Multicast Support on the CMTS Routers	DOCSIS 3.0 Multicast Support on the CMTS Routers http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ubr_d30_mcast_support.html

Standards

Standard	Title
CM-SP-DSG-I18-110623	DOCSIS Set-top Gateway (DSG) Interface Specification

MIBs

MIB	MIBs Link
DOCS-DSG-IF-MIB	*To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:* http://www.cisco.com/go/mibs

RFCs

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

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 Advanced-Mode DSG 1.2 for the Cisco 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.

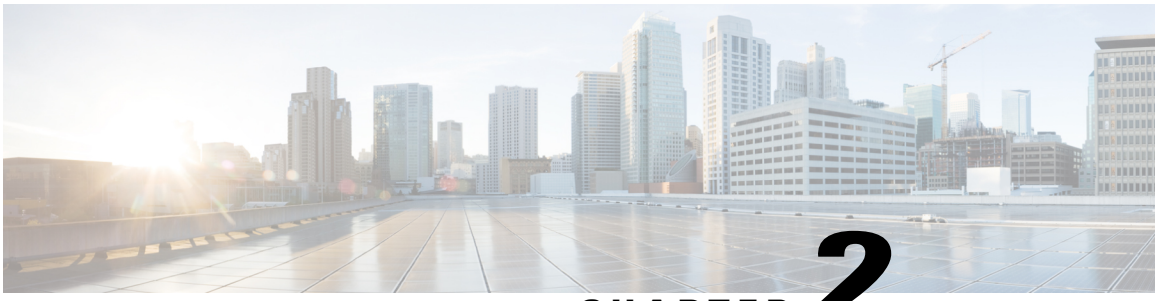
Table 2: Feature Information for DOCSIS Set-Top Gateway and A-DSG for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
DOCSIS Set-Top Gateway for the Cisco CMTS Routers	12.2(15)BC2	This feature was introduced for the Cisco uBR7100 series and Cisco uBR7246VXR universal broadband routers.
DOCSIS Set-Top Gateway for the Cisco CMTS Routers	12.3(9a)BC	Support for the Cisco uBR10012 universal broadband router was added.
Advanced-mode DOCSIS Set-Top Gateway 1.1 for the Cisco CMTS Routers	Release 12.3(13)BC	This feature was introduced to support DOCSIS 1.1 on the Cisco uBR7200 Series and Cisco uBR10012 universal broadband routers.
Advanced-mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS Routers	12.3(17a)BC2	This feature was introduced on the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.
Advanced-mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS Routers	12.2(33)SCA	This feature was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR universal broadband router was added.
Advanced-mode DOCSIS Set-Top Gateway 1.2 on a Subinterface for the Cisco CMTS Routers	12.2(33)SCB4	This feature was introduced on the Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.

Feature Name	Releases	Feature Information
Default Multicast QoS	12.2(33)SCC1	This feature was modified to configure the service class name of the default multicast quality of service (MQoS) for the QoS profile. The following command was introduced or modified: • cable multicast group-qos default
Advanced-mode DOCSIS Set-Top Gateway 1.2 on a Subinterface for the Cisco CMTS Routers	12.2(33)SCC1	This feature was integrated into Cisco IOS Release 12.2(33)SCC1.
Advanced-mode DOCSIS Set-Top Gateway 1.2 on a Subinterface for the Cisco CMTS Routers	12.2(33)SCD	Support was added for the Cisco uBR-MC88V line card.
Advanced-mode DOCSIS Set-Top Gateway 1.2 on a Subinterface for the Cisco CMTS Routers	12.2(33)SCD5	This feature was modified to add the **ignore** option to the **in-dcd** keyword of the **cable dsg cfr** command to exclude DSG classifiers from the DCD message and enable the DSG rules regardless of the DSG tunnel MAC address. The following commands were introduced or modified: • **cable dsg cfr** • **show cable dsg tg** • **show interfaces cable dsg downstream tg**

Feature Name	Releases	Feature Information
FQDN Support	12.2(33)SCG	You can specify either an FQDN or IP address while configuring an A-DSG classifier on a Cisco CMTS router. The following commands were introduced or modified: • **cable dsg cfr** • cable dsg tg default-priority • cable dsg tg priority • debug cable dsg • show cable dsg cfr • show cable dsg host
DNS Query and DSG Name Process	12.2(33)SCG	One or more DNS servers must be configured to enable a Cisco CMTS router to perform a DNS query. The **cable dsg name-update-interval command** was introduced to support this feature. The following sections provide information about this feature:
DOCSIS 3.0 DSG MDF Support	12.2(33)SCG	DOCSIS 3.0 DSG MDF support is introduced using DSG DA-to-DSID Association Entry TLV in the MDD message. For details about this feature, see Information About Advanced-Mode DSG Issue 1.2, on page 4.

Feature Name	Releases	Feature Information
A-DSG Forwarding on the Primary Channel	12.2(33)SCG	This feature allows you to exclude a primary capable interface from A-DSG forwarding. The following sections provide information about this feature: The following commands were introduced or modified: • **cable downstream dsg disable** • **cable downstream dsg tg** • show cable dsg static-group bundle • show interface cable dsg downstream



CHAPTER 2

Call Home Feature for the Cisco CMTS Routers

First Published: November 29, 2010

Note Use this document in conjunction with the Configuring Call Home for Cisco 7200 Series Routers feature guide.

For Cisco IOS Release 12.2(33)SCE, the Call Home feature provides a mechanism to automatically create cases and update Cisco, customer, or a partner about events and changes on a Cisco device in a customer network. This feature provides e-mail and web-based notification of critical system events. Multiple message formats are available for optimum compatibility with pager services, e-mail, or XML-based automated parsing applications. Common uses of this feature include paging a network support engineer, sending an e-mail notification to a Network Operations Center, XML-based message delivery to a support website, and generating a direct case with the Cisco Systems Technical Assistance Center (TAC).

For more information, see the Configuring Call Home for Cisco 7200 Series Routers feature guide.

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 Call Home Feature for the Cisco CMTS Routers

Table below shows the hardware compatibility matrix for this feature.

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

Table 3: Call Home Feature for the Cisco CMTS Routers - Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards	SIP/SPA
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCE and later releases • PRE2 • PRE4	Cisco IOS Release 12.2(33)SCE and later releases • Cisco uBR10-MC5X20U/H • Cisco UBR-MC20X20V • Cisco uBR-MC3GX60V [4]	Cisco Wideband SPA

4 The Cisco uBR-MC3GX60V cable interface line card is not compatible with PRE2. You must use PRE4 with the Cisco uBR3GX60V cable interface line card.

Note For support of this feature on the Cisco uBR 7200 series universal broadband routers, see the Configuring Call Home for Cisco 7200 Series Routers feature guide.

Information About the Call Home Feature for the Cisco CMTS Routers

The Call Home feature provides a reactive support mode of operation triggered by various system events on a Cisco uBR10012 universal broadband router. This feature also supports a proactive support mode where configuration and inventory change messages are automatically reported to a destination target specified in the system profile.

You can specify a Call Home Server on the Cisco network as a destination target.

The Call Home functionality in a Cisco device is provided by one or more network devices or through an appliance, such as the Smart Call Home server. Each system event provides a set of call home triggers required for reactive mode situations, for example, hardware failures.

The Call Home function can leverage Cisco, customer, or a partner support. Flexible message delivery and format options allow for easy integration of specific support requirements into the Call Home and Call Home Server.

For more information on setting up and configuring this feature, see the Configuring Call Home for Cisco 7200 Series Routers feature guide.

Subscribing to Alert Groups

An alert group is a predefined subset of Call Home alerts supported in all Cisco universal broadband routers. Different Call Home alerts are classified into different groups depending on their type. For Cisco IOS Release 12.2(33)SCE, the alert groups are:

- Configuration
- Inventory
- Syslog

Sample Configuration Alert Notification in XML Format

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>MC2:SPE100202ZH:D060082A</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/configuration</aml-block:Type>
<aml-block:CreationDate>2010-10-13 10:27:54 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>uBR10000</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>GC3:SPE100202ZH:D060082A</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>1</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2010-10-13 10:27:39 GMT+00:00</ch:EventTime>
<ch:MessageDescription>Configuration Change</ch:MessageDescription>
<ch:Event>
<ch:Type>configuration</ch:Type>
<ch:SubType>delta</ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>Cisco uBR10K Series Routers</ch:Series>
```

```
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>uname@cisco.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>UBR10012@C@SPE100202ZH</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>uname@cisco.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>GC3:SPE100202ZH:D060082A</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>1</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2010-10-13 10:27:39 GMT+00:00</ch:EventTime>
<ch:MessageDescription>Configuration Change</ch:MessageDescription>
<ch:Event>
<ch:Type>configuration</ch:Type>
<ch:SubType>delta</ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>Cisco uBR10K Series Routers</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>uname@cisco.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>UBR10012@C@SPE100202ZH</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>uname@cisco.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>UBR10012</rme:Model>
<rme:HardwareVersion>257</rme:HardwareVersion>
<rme:SerialNumber>SPE100202ZH</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="800-09026-03" />
<rme:AD name="SoftwareVersion" value="12.2(20100929:171810)" />
<rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.317" />
<rme:AD name="SystemDescription" value="Cisco IOS Software, 10000 Software (UBR10K4-K9P6U2-M),
 Experimental Version 12.2(20100929:171810) [username-card 111]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 29-Sep-10 10:18 by username" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
```

```
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show diag</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Slot A:
 Active PRE card
RP EEPROM contents:
 Controller Type          : 1443
 Hardware Revision        : 1.0
 PCB Part Number          : 73-10867-03
 Board Revision           : B0
 Deviation Number         : 0-0
 Fab Version              : 05
 PCB Serial Number        : CAT1336F051
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
 Top Assy. Part Number    : 800-28163-03
 CLEI Code                : IPUCAM3BAC
 Product Identifier (PID) : ESR-PRE4
 Version Identifier (VID) : V03
FP EEPROM contents:
 Controller Type          : 1442
 Hardware Revision        : 1.0
 PCB Part Number          : 73-10866-03
 Board Revision           : B0
 Deviation Number         : 0-0
 Fab Version              : 04
 PCB Serial Number        : CAT1403F1JT
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
Operational Image Version, Slot A
 Cisco IOS Software, 10000 Software (UBR10K4-K9P6U2-M), Experimental Version
12.2(20100929:171810) [uname-card 111]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 29-Sep-10 10:18 by uname
Reset reason 0x00000002 (software reset)
Slot B:
 Standby PRE card
RP EEPROM Contents:
Slot 1:
 2jacket-1 card, 0 ports
 Card is full slot size
 Card is analyzed
 Card detected 2d06h ago
 Card uptime 2 days, 6 hours, 43 minutes, 51 seconds
 Card idle time 1 days, 11 hours, 59 minutes, 24 seconds
 Voltage status: 3.3V Nominal 2.5V Nominal 1.5V Nominal 12V Nominal
EEPROM contents, slot 1/0:
 Controller Type          : 1045
 Hardware Revision        : 1.0
 Top Assy. Part Number    : 800-22843-04
 Board Revision           : A0
 Product Identifier (PID) : UBR10-2XDS-SIP
 Version Identifier (VID) : V01
 Deviation Number         : 89768
 Fab Version              : 03
 PCB Serial Number        : CAT112358KV
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
 CLEI Code                : IPUIA1HRAA
LCMON version, slot 1/0
 LCDOS (C10000 PowerQUICC-II Line Card MONitor Image Version 2 : Release
branch:c10k_lc_conn_isp 20040915:175538)
 Built by leccese at Thu Sep 16 12:28:56 2004.
 Reset reason 0x00000003/0x2 (PRE hard reset).
Operational Image version, slot 1/0
 LCDOS (C10000 2 Bay SPA Jacket (JACKET2) Image : DEVELOPMENT BUILD
```

```
Wideband Information:
Slot/Subslot 1/1:
 24rfchannel-spa-1 card, 1 port + 1 redundant port
 Card is half slot size
 Card is analyzed
 Card detected 2d06h ago
 Card uptime: Not Supported
 Card idle time: Not Supported
 Voltage status: 3.3V (+3.291) NOMINAL  2.5V (+2.490) NOMINAL
                 1.2V (+1.196) NOMINAL  1.8V (+1.806) FIXED
EEPROM contents, slot 1/1:
 Controller Type          : 1198
 Hardware Revision        : 1.0
 Boot Timeout             : 500 msecs
 PCB Serial Number        : CAT1228E21D
 PCB Part Number          : 73-9597-03
 PCB Revision             : B0
 Fab Version              : 03
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
 Deviation Number         : 0
 Product Identifier (PID) : SPA-24XDS-SFP
 Version Identifier (VID) : V01
 Top Assy. Part Number    : 68-2562-03
 Top Assy. Revision       : C0
 IDPROM Format Revision   : 36
 System Clock Frequency   : 00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00
 CLEI Code                : IPUIA1JRAA
 Base MAC Address         : 00 1E BE BE 8B C7
 MAC Address block size   : 1
 Manufacturing Test Data  : 00 00 00 00 00 00 00 00
 Field Diagnostics Data   : 00 00 00 00 00 00 00 00
 Calibration Data         : Minimum: 0 dBmV, Maximum: 0 dBmV
       Calibration values :
 Power Consumption        : 14000 mWatts (Maximum)
 Environment Monitor Data : 03 30 0C E4 46 32 09 C4
                            46 32 00 00 00 00 04 B0
                            46 32 00 00 00 00 07 08
                            46 32 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 FE 02 FA 6D
 Processor Label          : 00 00 00 00 00 00 00
 Platform features        : 00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
                            00 00 00 00 00 00 00 00
 Asset ID                 :
 Asset Alias              :
Slot/Subslot 2/1:
 2cable-dtcc card, 0 ports
 Card is half slot size
 Card is analyzed
 Card detected 2d06h ago
 Card uptime 2 days, 6 hours, 52 minutes, 34 seconds
 Card idle time 1 days, 5 hours, 1 minutes, 14 seconds
 Voltage status: 3.3V Nominal 2.5V Nominal 1.8V Nominal 1.2V Nominal
EEPROM contents, slot 2/1:
 Controller Type          : 1456
 Hardware Revision        : 2.0
 Top Assy. Part Number    : 800-29390-01
 Top Assy. Revision       : A0
 Product Identifier (PID) : UBR10-DTCC
 Version Identifier (VID) : V01
 CLEI Code                : IPUCAL1BAA
 Deviation Number         : 0
 Fab Version              : 02
 PCB Serial Number        : CAT1213E19M
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
```

```
 RMA History              : 00
<snip>...</snip>
Slot/Subslot 4/0:
 1gigethernet-hh-1 card, 1 port
 Card is half slot size
 Card is analyzed
 Card detected 2d06h ago
 Card uptime 2 days, 6 hours, 44 minutes, 31 seconds
 Card idle time 1 days, 16 hours, 12 minutes, 52 seconds
 Voltage status: 3.3V Nominal 2.5V Nominal
EEPROM contents, slot 4/0:
 Controller Type          : 912
 Hardware Revision        : 1.0
 Top Assy. Part Number    : 800-20373-03
 Board Revision           : A0
 Deviation Number         : 0-0
 Fab Version              : 03
 PCB Serial Number        : CAT09190TTY
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
 CLEI Code                : IP3IZ0VDAB
LCMON version, slot 8/0
 Cisco IOS Software, 10000 Software (UBR10KG4CLC-EBOOT-M), Version 12.2(32.7.22)SCE  Compiled
 Thu 17-Jun-10 02:39
 Reset due to: reload
Operational Image version, slot 8/0
 Cisco IOS Software, 10000 Software (UBR10KG4CLC-LCK8-M), Experimental Version
12.2(20101012:185925) [yiliu-cable-1012 120]
 Compiled Wed 13-Oct-10 14:54
 SW Version 1.0
 Code MD5 B0DCEC92BF050F9D0A22131AB8AB4E14
 FPGA MD5 00000000000000000000000000000000
 Expected Switchover Action: NO INFORMATION
Slot/Subslot 8/1:
 ubr10k-clc-3g60 card, 15 ports
 Card is half slot size
 Card is analyzed
 Card detected 2d06h ago
 Card uptime 0 days, 1 hours, 37 minutes, 46 seconds
 Card idle time N/A
 Voltage status: 3.3V Nominal 2.5V Nominal 1.8V Nominal 1.5V Nominal 1.2V Nominal 1.0V
Nominal 1.0V Nominal 1.1V Core Nominal 1.1V Cpu Plat Nominal
Router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show version</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[Cisco IOS Software, 10000 Software (UBR10K4-K9P6U2-M), Experimental Version
12.2(20100929:171810) [uname-card 111]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 29-Sep-10 10:18 by username
ROM: System Bootstrap, Version 12.2(20071113:194412) [uname-rom-1_2 101], DEVELOPMENT
SOFTWARE
BOOTLDR: Cisco IOS Software, 10000 Software (C10K4-EBOOT-M), Version 12.2(33)SB7, RELEASE
SOFTWARE (fc3)
 router uptime is 2 days, 6 hours, 45 minutes
Uptime for this control processor is 2 days, 6 hours, 45 minutes
System returned to ROM by reload at 06:03:47 UTC Wed Oct 6 2010
System image file is "tftp://223.255.254.254/uname/ubr10k4-k9p6u2-mz.card"
Last reload type: Normal Reload
Last reload reason: Reload command
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and
local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco uBR10000 (PRE4-RP) processor with 2588671K/163839K bytes of memory.
```

Sample Inventory Alert Notification in Long-Text Format

```
Processor board ID SPE100202ZH
SB-1 CPU at 800Mhz, Implementation 0x410, Rev 5.0, 512KB L2 Cache
Backplane version 1.1, 8 slot
Last reset from software reset
PXF processor tmc0 is running.
PXF processor tmc1 is running.
PXF processor tmc2 is running.
PXF processor tmc3 is running.
1 Jacket card(s): 1 SPA card(s)
1 FastEthernet interface
1 Gigabit Ethernet interface
40 Cable Modem interfaces
7039K bytes of non-volatile configuration memory.
126000K bytes of ATA compact flash in bootflash (Sector size 512 bytes).
1000944K bytes of ATA compact flash in disk0 (Sector size 512 bytes).
Configuration register is 0x0
Router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show running-config all</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Building configuration...
Current configuration with default configurations exposed : 876387 bytes
!
...<-- Running config information here -->
...
...
Router#]]></aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

Sample Inventory Alert Notification in Long-Text Format

```
TimeStamp : 2010-04-01 20:45 GMT+00:00
Message Name : inventory
Message Type : Call Home
Message Group : reactive
Severity Level : 1
Source ID : uBR7200 Family
Device ID : Cisco-uBR7246VXR@C@SAB044900Q0
Customer ID :
Contract ID :
Site ID :
Server ID : Cisco-uBR7246VXR@C@SAB044900Q0
Event Description : Module 35: UBR-MC28U is removed
System Name : router
Contact Email : sboochir@cisco.com
Contact Phone :
Street Address :
Affected Chassis : Cisco-uBR7246VXR
Affected Chassis Serial Number : SAB044900Q0
Affected Chassis Part No :  00-0000-00
Affected Chassis Hardware Version : 2.0
Supervisor Software Version : 12.2(20100331:225906)
Command Output Name : show diag
Attachment Type : command output
MIME Type : text/plain
```

Sample Inventory Alert Notification in XML Format

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<soap-env:Envelope
xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session
xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-
session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M4::CF1DC8D1</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block
xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/inventory</aml-blo
ck:Type>
<aml-block:CreationDate>2010-02-11 00:07:45
GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>C7200 Family</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G5::CF1DC8D1</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>1</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch-inv:CallHome
xmlns:ch-inv="http://www.cisco.com/2005/05/callhome/inventory"
version="1.0">
<ch-inv:EventTime>2010-02-11 00:07:41 GMT+00:00</ch-inv:EventTime>
<ch-inv:MessageDescription>Full Inventory</ch-inv:MessageDescription>
<ch-inv:Event>
<ch-inv:Type>inventory</ch-inv:Type>
<ch-inv:SubType>full</ch-inv:SubType>
<ch-inv:Brand>Cisco Systems</ch-inv:Brand>
<ch-inv:Series>Cisco 7200 Series Routers</ch-inv:Series>
</ch-inv:Event>
<ch-inv:CustomerData>
<ch-inv:UserData>
<ch-inv:Email>sboochir@cisco.com</ch-inv:Email>
</ch-inv:UserData>
<ch-inv:ContractData>
<ch-inv:CustomerId></ch-inv:CustomerId>
<ch-inv:SiteId></ch-inv:SiteId>
<ch-inv:ContractId></ch-inv:ContractId>
<ch-inv:DeviceId>@C@</ch-inv:DeviceId>
</ch-inv:ContractData>
<ch-inv:SystemInfo>
<ch-inv:Name>router</ch-inv:Name>
<ch-inv:Contact></ch-inv:Contact>
<ch-inv:ContactEmail>sboochir@cisco.com</ch-inv:ContactEmail>
<ch-inv:ContactPhoneNumber></ch-inv:ContactPhoneNumber>
<ch-inv:StreetAddress></ch-inv:StreetAddress>
</ch-inv:SystemInfo>
<ch-inv:CCOID></ch-inv:CCOID>
</ch-inv:CustomerData>
<ch-inv:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model></rme:Model>
<rme:HardwareVersion>2.0</rme:HardwareVersion>
<rme:SerialNumber></rme:SerialNumber>
```

Sample Inventory Alert Notification in XML Format

```
<rme:Card>
<rme:Model>PA-4E=</rme:Model>
<rme:SerialNumber>24508052</rme:SerialNumber>
<rme:LocationWithinContainer>1</rme:LocationWithinContainer>
<rme:PartNumber>73-1556-08</rme:PartNumber>
<rme:HardwareVersion>1.14</rme:HardwareVersion>
<rme:SoftwareIdentity>
<rme:VersionString></rme:VersionString>
</rme:SoftwareIdentity>
</rme:Card>
<rme:Card>
<rme:Model>PA-1GE=</rme:Model>
<rme:SerialNumber>18587776</rme:SerialNumber>
<rme:LocationWithinContainer>2</rme:LocationWithinContainer>
<rme:PartNumber>73-3144-03</rme:PartNumber>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SoftwareIdentity>
<rme:VersionString></rme:VersionString>
</rme:SoftwareIdentity>
</rme:Card>
<rme:Card>
<rme:Model>UBR-MC28U</rme:Model>
<rme:SerialNumber>CAT0841006F</rme:SerialNumber>
<rme:LocationWithinContainer>3</rme:LocationWithinContainer>
<rme:PartNumber></rme:PartNumber>
<rme:HardwareVersion>6.5</rme:HardwareVersion>
<rme:SoftwareIdentity>
<rme:VersionString></rme:VersionString>
</rme:SoftwareIdentity>
</rme:Card>
<rme:Card>
<rme:Model>UBR-MC28U</rme:Model>
<rme:SerialNumber>CAT08340U6N</rme:SerialNumber>
<rme:LocationWithinContainer>4</rme:LocationWithinContainer>
<rme:PartNumber></rme:PartNumber>
<rme:HardwareVersion>6.5</rme:HardwareVersion>
<rme:SoftwareIdentity>
<rme:VersionString></rme:VersionString>
</rme:SoftwareIdentity>
</rme:Card>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value=" 00-0000-00" />
<rme:AD name="SoftwareVersion" value="12.2(20091219:015541) " />
<rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.271" />
<rme:AD name="SystemDescription" value="Cisco IOS Software, 7200
Software (UBR7200-JK9SU2-M), Experimental Version 12.2(20091219:015541)
[sboochir-ubr-latest 269]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Fri 15-Jan-10 15:57 by sboochir" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch-inv:Device>
</ch-inv:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show diag</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Slot 1:
 Ethernet Port adapter, 4 ports
 Port adapter is disabled unsuitable deactivated powered off
 Port adapter insertion time unknown
 EEPROM contents at hardware discovery:
Slot 2:
 Gigabit Ethernet Port adapter, 1 port
 Port adapter is analyzed
 Port adapter insertion time 00:01:04 ago
 EEPROM contents at hardware discovery:
 Hardware revision 1.0          Board revision A1
 Serial number     18587776   Part number    73-3144-03
 FRU Part Number:  PA-1GE=
 Test history      0x0          RMA number     00-00-00
```

```
 EEPROM format version 1
 EEPROM contents (hex):
   0x20: 01 98 01 00 01 1B A0 80 49 0C 48 03 00 00 00 00
   0x30: 51 02 73 00 00 00 00 00 00 01 FF FF FF FF FF FF
Slot 3:
 DOCSIS Modem Card (Universal) 2 Down/8 Up (F-connector) with
Integrated Up-converter Port adapter, 2 ports
 Port adapter is analyzed
 Port adapter insertion time 00:01:04 ago
 EEPROM contents at hardware discovery:
 Controller Type          : 1053
 Hardware Revision        : 6.5
 Version Identifier (VID) : V01
 Top Assy. Part Number    : 800-17733-04
 Board Revision           : A0
 Product Identifier (PID) : UBR-MC28U
 CLEI Code                : IPUIAF2RAB
 Deviation Number         : 0-0
 Fab Version              : 06
 PCB Serial Number        : CAT0841006F
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
 EEPROM format version 4
 EEPROM contents (hex):
   0x00: 04 FF 40 04 1D 41 06 05 89 56 30 31 20 C0 46 03
   0x10: 20 00 45 45 04 42 41 30 CB 89 55 42 52 2D 4D 43
   0x20: 32 38 55 C6 8A 49 50 55 49 41 46 32 52 41 42 80
   0x30: 00 00 00 00 02 06 C1 8B 43 41 54 30 38 34 31 30
   0x40: 30 36 46 03 00 81 00 00 00 00 04 00 FF FF FF FF
   0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x80: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x90: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xA0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xB0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xC0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xD0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xE0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xF0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF B9 1D
 Calibration Data
       US calibration ID  : 0x5553
       calibration date   : 20041007
       H/W version        : 6.5
       Number of US points: 8
       Number of freqs    : 3

       ------ NA data ------
                          measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0     5000     28.3000    26.4440    24.0820    19.7360
10.3904
        1     5000     28.3000    26.4440    24.0820    19.7360
10.4262
        2     5000     28.3000    26.4440    24.0820    19.4748
10.3700
        3     5000     28.3000    26.4440    24.0820    19.7377
10.4714
        4     5000     28.3000    26.0539    24.0820    19.4693
10.3700
        5     5000     28.3000    26.4440    24.0820    19.7360
10.3956
        6     5000     28.3000    26.4440    24.0820    19.7360
10.3904
        7     5000     28.3000    26.4440    24.0820    19.7360
10.4817
                          measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0    24000     28.9440    27.1336    25.1060    20.0496
11.3960
```

```
        1    24000     28.9440    27.2340    25.1060    20.1656
11.3916
        2    24000     28.9440    26.8480    25.1060    20.0000
11.3640
        3    24000     28.9440    27.2340    25.1060    20.8280
12.2560
        4    24000     28.9440    26.8480    25.1060    20.0165
11.3686
        5    24000     28.9440    27.2340    25.1060    20.8280
11.6802
        6    24000     28.9440    26.8634    25.1060    20.0165
11.3824
        7    24000     28.9440    27.2340    25.1060    20.8280
11.5947
                         measured gain
       US  freq(kHz)       0db        2db        4db        8db
16db
        0    42000     28.6017    26.4440    24.6080    20.0000
11.3640
        1    42000     28.6280    26.8480    24.6080    20.0000
11.3640
        2    42000     28.3000    26.4440    24.0820    19.7817
11.3640
        3    42000     28.6280    26.8480    24.6080    20.0000
11.3640
        4    42000     28.3000    26.4440    24.0925    20.0000
11.3640
        5    42000     28.6280    26.8480    24.6080    20.0000
11.3640
        6    42000     28.6214    26.4520    24.6080    20.0000
11.3640
        7    42000     28.6280    26.8480    24.6080    20.0000
11.3640

       ------ EU data ------
                         measured gain
       US  freq(kHz)       0db        2db        4db        8db
16db
        0     5000     28.6280    26.4440    24.0820    19.7377
11.3640
        1     5000     28.6280    26.4440    24.0925    20.0000
11.3640
        2     5000     28.6280    26.4440    24.0820    19.7360
10.4210
        3     5000     28.6280    26.4440    24.0820    20.0000
11.3640
        4     5000     28.3000    26.4440    24.0820    19.7360
10.4108
        5     5000     28.6280    26.4440    24.0820    19.7377
11.3640
        6     5000     28.6280    26.4440    24.0820    19.7377
11.3640
        7     5000     28.6280    26.4440    24.1030    20.0000
11.3640
                         measured gain
       US  freq(kHz)       0db        2db        4db        8db
16db
        0    30000     29.2480    27.2340    25.1060    20.8280
12.2560
        1    30000     29.2480    27.6040    25.1060    20.8280
12.2560
        2    30000     28.9440    27.2340    25.1060    20.8280
12.2560
        3    30000     29.2480    27.6040    25.1060    20.8280
12.2560
        4    30000     29.2480    27.2340    25.1060    20.8280
12.2560
        5    30000     29.2480    27.6040    25.1060    20.8280
12.2560
        6    30000     29.2480    27.6040    25.1060    20.8280
12.2560
        7    30000     29.2480    27.6040    25.1530    20.8280
12.2560
```

```
                        measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0    65000     28.9440    26.8480    24.6080    20.0000
11.3640
        1    65000     28.9440    26.8480    24.6080    20.0000
11.3640
        2    65000     28.6280    26.4440    24.0820    19.7360
10.3854
        3    65000     28.9440    26.8480    24.6080    20.0000
11.3640
        4    65000     28.9440    26.8480    24.6080    20.0000
11.3640
        5    65000     28.9440    26.8480    24.6080    20.0000
11.3640
        6    65000     28.9440    26.8480    24.1977    19.7483
11.3640
        7    65000     29.2480    26.9406    24.6080    20.0000
11.3640
Slot 4:
 DOCSIS Modem Card (Universal) 2 Down/8 Up (F-connector) with
Integrated Up-converter Port adapter, 2 ports
 Port adapter is analyzed
 Port adapter insertion time 00:01:05 ago
 EEPROM contents at hardware discovery:
 Controller Type          : 1053
 Hardware Revision        : 6.5
 Version Identifier (VID) : V01
 Top Assy. Part Number    : 800-17733-04
 Board Revision           : A0
 Product Identifier (PID) : UBR-MC28U
 CLEI Code                : IPUIAF2RAB
 Deviation Number         : 0-0
 Fab Version              : 06
 PCB Serial Number        : CAT08340U6N
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
 EEPROM format version 4
 EEPROM contents (hex):
   0x00: 04 FF 40 04 1D 41 06 05 89 56 30 31 20 C0 46 03
   0x10: 20 00 45 45 04 42 41 30 CB 89 55 42 52 2D 4D 43
   0x20: 32 38 55 C6 8A 49 50 55 49 41 46 32 52 41 42 80
   0x30: 00 00 00 00 02 06 C1 8B 43 41 54 30 38 33 34 30
   0x40: 55 36 4E 03 00 81 00 00 00 00 04 00 FF FF FF FF
   0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x80: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x90: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xA0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xB0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xC0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xD0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xE0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0xF0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF E9 1C
 Calibration Data
       US calibration ID  : 0x5553
       calibration date   : 20040824
       H/W version        : 6.5
       Number of US points: 8
       Number of freqs    : 3

       ------ NA data ------
                        measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0     5000     27.9580    26.0200    23.5220    19.3700
10.3700
        1     5000     27.9580    26.0200    24.0820    19.4362
10.3854
        2     5000     27.9580    26.0200    24.0820    19.4178
10.3700
```

Sample Inventory Alert Notification in XML Format

```
        3     5000     27.9580    26.0200    23.5220    19.3865
10.3700
        4     5000     27.9580    26.0200    23.5220    19.3920
10.3700
        5     5000     27.9580    26.0200    23.5220    19.3718
10.3700
        6     5000     27.9580    26.0200    23.5220    19.3057
10.3700
        7     5000     28.3000    26.4440    24.0820    19.4436
10.3700
                       measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0    24000     28.9440    27.2340    25.1060    20.1656
11.3778
        1    24000     29.2480    27.2340    25.1060    20.8280
12.2560
        2    24000     29.2419    27.2340    25.1060    20.8280
12.2560
        3    24000     28.9440    27.2340    25.1060    20.7783
11.3916
        4    24000     28.9440    27.2340    25.1060    20.0496
11.3732
        5    24000     28.9440    27.2340    25.1060    20.0331
11.3686
        6    24000     28.9440    26.8480    24.6080    20.0000
11.3640
        7    24000     29.2480    27.6040    25.1060    20.8280
12.2560
                       measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0    42000     28.9440    27.2340    25.1060    20.8280
12.2560
        1    42000     29.2480    27.6040    25.1060    20.8280
12.2560
        2    42000     29.2480    27.6040    25.1530    20.8280
12.2560
        3    42000     29.2480    27.6040    25.1060    20.8280
12.2560
        4    42000     28.9440    27.2340    25.1060    20.8280
12.0096
        5    42000     28.9440    27.2340    25.1060    20.8280
11.4640
        6    42000     28.9440    27.2340    25.1060    20.1324
11.3732
        7    42000     29.5126    27.6040    25.5760    20.8280
12.2560

       ------ EU data ------
                       measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0     5000     28.9440    26.8480    24.6080    20.0000
11.3640
        1     5000     28.9440    27.2340    25.1060    20.0165
11.4326
        2     5000     28.9440    26.8634    25.1060    20.0000
11.3686
        3     5000     28.9440    26.8480    24.6080    20.0000
11.3640
        4     5000     28.9440    26.8480    24.6080    20.0000
11.3640
        5     5000     28.9440    26.8480    24.6080    20.0000
11.3640
        6     5000     28.9440    26.8480    24.6080    20.0000
11.3640
        7     5000     29.2480    27.2340    25.1060    20.0331
11.3686
                       measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0    30000     28.9440    27.2340    25.1060    20.8280
```

```
11.4233
        1    30000     29.2480    27.2340    25.1060    20.8280
12.2560
        2    30000     29.2480    27.2340    25.1060    20.8280
12.2560
        3    30000     28.9440    27.2340    25.1060    20.8280
11.4188
        4    30000     28.9440    27.2340    25.1060    20.3808
11.4006
        5    30000     28.9440    27.2340    25.1060    20.3974
11.3778
        6    30000     28.9440    26.8480    25.1060    20.0000
11.3686
        7    30000     29.2480    27.6040    25.1060    20.8280
12.2560
                       measured gain
       US  freq(kHz)      0db        2db        4db        8db
16db
        0    65000     29.2480    27.2340    25.1060    20.2318
11.3732
        1    65000     29.5420    27.6040    25.1060    20.8280
12.2560
        2    65000     29.2480    27.2340    25.1060    20.0496
11.3732
        3    65000     29.2480    27.2340    25.1060    20.0331
11.3686
        4    65000     29.2419    27.2340    24.6378    20.0000
11.3640
        5    65000     29.2480    26.9406    24.6080    20.0000
11.3640
        6    65000     28.9440    26.8480    24.6080    20.0000
11.3640
        7    65000     29.5420    27.6040    25.1060    20.8280
12.2560
router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show version</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[Cisco IOS Software, 7200 Software (UBR7200-JK9SU2-M),
Experimental Version 12.2(20091219:015541) [sboochir-ubr-latest 269]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Fri 15-Jan-10 15:57 by uname
ROM: System Bootstrap, Version 12.3(4r)T1, RELEASE SOFTWARE (fc1)
 router uptime is 1 minute
System returned to ROM by reload at 23:55:23 UTC Wed Feb 10 2010
System image file is "disk2:ubr7200-jk9su2-mz"
Last reload type: Normal Reload
Last reload reason: Reload command
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and
local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
cisco uBR7246VXR (UBR7200-NPE-G1) processor (revision A) with 229376K/32768K bytes of memory.
Processor board ID SAB044900Q0
SB-1 CPU at 700Mhz, Implementation 0x401, Rev 0.2, 512KB L2 Cache
6 slot VXR midplane, Version 2.0
Last reset from power-on
PCI bus mb1 has 74 bandwidth points
PCI bus mb2 has 474 bandwidth points
4 Gigabit Ethernet interfaces
4 Cable Modem interfaces
509K bytes of non-volatile configuration memory.
1992816K bytes of ATA PCMCIA card at slot 2 (Sector size 512 bytes).
16384K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0
router#]]></aml-block:Data>
```

Sample Inventory Alert Notification in XML Format

```
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show inventory oid</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[NAME: "Chassis", DESCR: "uBR7246VXR Universal Broadband Router"
PID: UBR7246VXR        , VID: N/A, SN: SAB044900Q0
OID: 1.3.6.1.4.1.9.12.3.1.3.134
NAME: "UBR7200-NPE-G1 0", DESCR: "Cisco 7200 Series Network Processing
Engine NPE-G1"
PID: UBR7200-NPE-G1    , VID:    , SN: 31689947
OID: 1.3.6.1.4.1.9.12.3.1.9.5.56
NAME: "disk2", DESCR: "Compact Flash Disk for NPE-G1"
PID: Unknown Compact Flash, VID:    , SN:
OID: 1.3.6.1.4.1.9.12.3.1.9.2.120
NAME: "module 2", DESCR: "GigabitEthernet"
PID: PA-1GE=           , VID: N/A, SN: 18587776
OID: 1.3.6.1.4.1.9.12.3.1.9.4.59
NAME: "module 3", DESCR: "MC28U_F_connector"
PID: UBR-MC28U         , VID: V01 , SN: CAT0841006F
OID: 1.3.6.1.4.1.9.12.3.1.9.27.34
NAME: "module 4", DESCR: "MC28U_F_connector"
PID: UBR-MC28U         , VID: V01 , SN: CAT08340U6N
OID: 1.3.6.1.4.1.9.12.3.1.9.27.34
router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show environment all</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Power Supplies:
 Power Supply 1 is unmeasured.
 Power Supply 2 is unmeasured.
Temperature readings:
 NPE Inlet        measured at 34C/93F
 NPE Outlet       measured at 39C/102F
 chassis outlet 3 measured at 29C/84F
 chassis outlet 4 measured at 32C/89F
Voltage readings:
 +3.5 V           measured at +3.43 V
 +5.2 V           is unmeasured
 +12.2 V          is unmeasured
 -12.2 V          is unmeasured
 +16 V            is unmeasured
 -16 V            is unmeasured
Fans:
 Still warming up. Fan deltas not available.
Envm stats saved 0 time(s) since reload
router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show c7200</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[Network IO Interrupt Throttling:
 throttle count=0, timer count=0
 active=0, configured=1
 netint usec=4000, netint mask usec=400
uBR7200 Midplane EEPROM:
 Controller Type          : 374
 Number of Slots          : 6
 Hardware Revision        : 1.5
 Top Assy. Part Number    : 800-05443-03
 Board Revision           : A0
 Deviation Number         : 0-0
 Fab Version              : 03
 PCB Serial Number        : SDA05020652
 Chassis Serial Number    : SAB044900Q0
 Chassis MAC Address      : 0004.9bef.3400
 MAC Address block size   : 1024
 RMA Test History         : 00
 RMA Number               : 0-0-0-0
 RMA History              : 00
 EEPROM format version 4
 EEPROM contents (hex):
```

```
   0x00: 04 FF 40 01 76 01 06 41 01 05 C0 46 03 20 00 15
   0x10: 43 03 42 41 30 80 00 00 00 00 02 03 C1 8B 53 44
   0x20: 41 30 35 30 32 30 36 35 32 C2 8B 53 41 42 30 34
   0x30: 34 39 30 30 51 30 C3 06 00 04 9B EF 34 00 43 04
   0x40: 00 03 00 81 00 00 00 00 04 00 C7 20 45 53 00 45
   0x50: 00 50 00 40 00 44 00 3A 00 40 00 7F 00 7E 00 7F
   0x60: 00 84 00 88 00 BC A8 21 00 00 B8 9A FF FF FF FF
   0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
uBRuBR7246VXR CPU EEPROM:
 Controller Type          : 859
 Hardware Revision        : 1.4
 Top Assy. Part Number    : 800-22164-05
 CLEI Code                : CNSP30ZAAB
 PCB Part Number          : 73-6988-10
 Board Revision           : A0
 PCB Serial Number        : 31689947
 RMA History              : 00
 Fab Version              : 05
 Fab Part Number          : 28-5082-05
 Product Identifier (PID) : UBR7200-NPE-G1
 Deviation Number         : 0-0
 EEPROM format version 4
 EEPROM contents (hex):
   0x00: 04 FF 40 03 5B 41 01 04 C0 46 03 20 00 56 94 05
   0x10: C6 8A 43 4E 53 50 33 30 5A 41 41 42 82 49 1B 4C
   0x20: 0A 42 41 30 C1 8B 33 31 36 38 39 39 34 37 00 00
   0x30: 00 04 00 02 05 85 1C 13 DA 05 CB 8E 55 42 52 37
   0x40: 32 30 30 2D 4E 50 45 2D 47 31 80 00 00 00 00 FF
   0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
   0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
TLB entries (43/64 used):
Virt Address range      Phy Address range         Attributes
0x4B000000:0x4B1FFFFF   0x14B000000:0x14B1FFFFF   CacheMode=2, RW,
Invalid
0x4B200000:0x4B3FFFFF   0x14B200000:0x14B3FFFFF   CacheMode=2, RW,
Invalid
0x10000000:0x10001FFF   0x0FC010000:0x0FC011FFF   CacheMode=2, RW, Valid
0x42000000:0x43FFFFFF   0x062000000:0x063FFFFFF   CacheMode=2, RW, Valid
0x46000000:0x47FFFFFF   0x066000000:0x067FFFFFF   CacheMode=2, RW, Valid
0x3C000000:0x3C7FFFFF   0x068000000:0x0687FFFFF   CacheMode=2, RW,
Invalid
0x04000000:0x05FFFFFF   0x01F000000:0x020FFFFFF   CacheMode=2, RW,
Invalid
0x08000000:0x09FFFFFF   0x076000000:0x077FFFFFF   CacheMode=2, RW, Valid
0x30000000:0x31FFFFFF   0x06C000000:0x06DFFFFFF   CacheMode=2, RW, Valid
0x38000000:0x39FFFFFF   0x078000000:0x079FFFFFF   CacheMode=2, RW, Valid
0x34000000:0x35FFFFFF   0x070000000:0x071FFFFFF   CacheMode=2, RW,
Invalid
0x4C000000:0x4DFFFFFF   0x07C000000:0x07DFFFFFF   CacheMode=2, RW,
Invalid
0x1FC00000:0x1FC7FFFF   0x01FC00000:0x01FC7FFFF   CacheMode=2, RO, Valid
0x1E000000:0x1E7FFFFF   0x01E000000:0x01E7FFFFF   CacheMode=2, RW, Valid
0x1E800000:0x1E9FFFFF   0x01E800000:0x01E9FFFFF   CacheMode=2, RW, Valid
0x32000000:0x33FFFFFF   0x01F000000:0x020FFFFFF   CacheMode=2, RW,
Invalid
0x3A000000:0x3BFFFFFF   0x01F000000:0x020FFFFFF   CacheMode=2, RW,
Invalid
0x36000000:0x37FFFFFF   0x052000000:0x053FFFFFF   CacheMode=2, RW,
Invalid
0x4E000000:0x4FFFFFFF   0x05E000000:0x05FFFFFFF   CacheMode=2, RW,
Invalid
0x60000000:0x61FFFFFF   0x000000000:0x001FFFFFF   CacheMode=5, RO, Valid
0x62000000:0x627FFFFF   0x002000000:0x0027FFFFF   CacheMode=5, RO, Valid
0x62800000:0x62FFFFFF   0x002800000:0x002FFFFFF   CacheMode=5, RO, Valid
0x63000000:0x631FFFFF   0x003000000:0x0031FFFFF   CacheMode=5, RO, Valid
0x63200000:0x6321FFFF   0x003200000:0x00321FFFF   CacheMode=5, RO, Valid
0x63220000:0x63227FFF   0x003220000:0x003227FFF   CacheMode=5, RO, Valid
0x63228000:0x6322FFFF   0x003228000:0x00322FFFF   CacheMode=5, RO, Valid
0x63230000:0x63231FFF   0x003230000:0x003231FFF   CacheMode=5, RO, Valid
0x63232000:0x63233FFF   0x003232000:0x003233FFF   CacheMode=5, RO, Valid
0x63234000:0x63235FFF   0x003234000:0x003235FFF   CacheMode=5, RO, Valid
0x63236000:0x63237FFF   0x003236000:0x003237FFF   CacheMode=5, RW, Valid
```

Sample Inventory Alert Notification in XML Format

```
0x63238000:0x6323FFFF   0x003238000:0x00323FFFF   CacheMode=5, RW, Valid
0x63240000:0x6325FFFF   0x003240000:0x00325FFFF   CacheMode=5, RW, Valid
0x63260000:0x6327FFFF   0x003260000:0x00327FFFF   CacheMode=5, RW, Valid
0x63280000:0x632FFFFF   0x003280000:0x0032FFFFF   CacheMode=5, RW, Valid
0x63300000:0x6337FFFF   0x003300000:0x00337FFFF   CacheMode=5, RW, Valid
0x63380000:0x633FFFFF   0x003380000:0x0033FFFFF   CacheMode=5, RW, Valid
0x63400000:0x635FFFFF   0x003400000:0x0035FFFFF   CacheMode=5, RW, Valid
0x63600000:0x637FFFFF   0x003600000:0x0037FFFFF   CacheMode=5, RW, Valid
0x63800000:0x63FFFFFF   0x003800000:0x003FFFFFF   CacheMode=5, RW, Valid
0x64000000:0x65FFFFFF   0x004000000:0x005FFFFFF   CacheMode=5, RW, Valid
0x66000000:0x67FFFFFF   0x006000000:0x007FFFFFF   CacheMode=5, RW, Valid
0x68000000:0x6FFFFFFF   0x008000000:0x00FFFFFFF   CacheMode=5, RW, Valid
0x0E000000:0x0FFFFFFF   0x00E000000:0x00FFFFFFF   CacheMode=5, RW, Valid
System was restarted by reload at 23:55:23 UTC Wed Feb 10 2010
7200 Software (UBR7200-JK9SU2-M), Experimental Version
12.2(20091219:015541) [sboochir-ubr-latest 269]
Compiled Fri 15-Jan-10 15:57 by sboochir
Image text-base: 0x600092A4, data-base: 0x63243750
Current trace buffer contents:
FP: 0x68213ED0, RA: 0x60D29754
FP: 0x68213ED0, RA: 0x60D0F6EC
FP: 0x68213EE8, RA: 0x60D2F5D8
FP: 0x68213F00, RA: 0x60D33308
FP: 0x68213F48, RA: 0x60B750D0
FP: 0x68214078, RA: 0x60B475EC
FP: 0x68214100, RA: 0x60B731D0
FP: 0x68214198, RA: 0x60CBB68C
0 spurious cache errors detected.
System Controller Network Interrupts
 Wrapper is INSTALLED at address 0x60DF299C
 Interrupt Register is at 0xB0020040 (0x0000000000000000)
Registered Interrupts:
 Level Mask               Count      Data       Interrupt Handler
 0     0x0000000000200000 20         0x69486110 0x6017123C
(GigabitEthernet0/3)
 0     0x0000000000100000 0          0x69470C08 0x6017123C
(GigabitEthernet0/2)
 0     0x0000000000080000 82         0x6945AAC4 0x6017123C
(GigabitEthernet0/1)
 1     0x0000000800000000 2          0x00000000 0x60171888 (SBETH media
interrupt)
 1     0x0000000000001000 6          0x00000000 0x60DF2514 (BCM-1250
PCMCIA)
 2     0x0000000000000020 0          0x6831E720 0x60DF2DD0 (SB1250 Timer
3)
 2     0x0000000000000010 0          0x6831E658 0x60DF2DD0 (SB1250 Timer
2)
 2     0x0000000000000008 0          0x6831E590 0x60DF2DD0 (SB1250 Timer
1)
 2     0x0000000000000004 0          0x6831E4C8 0x60DF2DD0 (SB1250 Timer
0)
 4     0x007C00000000E0C3 0          0x00000000 0x60DFD240 (Spurious
Intr ERROR Handler)
 4     0x0000000000020000 0          0x00000000 0x60DFCD50 (Corrected
ECC Error Handler)
 4     0x0000000000010000 0          0x00000000 0x60DFC98C (Bad ECC
Error Handler)
 4     0x0000003000000000 0          0x00000000 0x60DF2530 (Sturgeon
Error Handler)
 4     0x0003000000000000 0          0x66A227C8 0x60DFCDD8 (BCM1250 Host
LDT Bridge Error Handler)
 4     0x0000000000040000 0          0x00000000 0x60DFD094 (BCM1250
IO-Bus Error Handler)
 4     0x0080000000000000 0          0x00000000 0x60DFCE60 (BCM1250 Host
PCI Bridge Error Handler)
router#]]></aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

Sample Syslog Alert Notification in XML Format

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>MDA:SPE100202ZH:D0600862</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2010-10-13 10:28:50 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>uBR10000</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>GDB:SPE100202ZH:D0600862</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>1</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2010-10-13 10:28:37 GMT+00:00</ch:EventTime>
<ch:MessageDescription>SLOT 8/1: Oct 13 10:28:36.658: %LICENSE-6-INSTALL: Feature US_License
 1.0 was installed in this device. UDI=UBR-MC3GX60V:CSJ13302903; StoreIndex=0:Primary License
 Storage</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>Cisco uBR10K Series Routers</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>uname@cisco.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>UBR10012@C@SPE100202ZH</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>uname@cisco.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>UBR10012</rme:Model>
<rme:HardwareVersion>257</rme:HardwareVersion>
```

```
<rme:SerialNumber>SPE100202ZH</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="800-09026-03" />
<rme:AD name="SoftwareVersion" value="12.2(20100929:171810)" />
<rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.317" />
<rme:AD name="SystemDescription" value="Cisco IOS Software, 10000 Software (UBR10K4-K9P6U2-M),
 Experimental Version 12.2(20100929:171810) [pauhuang-card 111]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 29-Sep-10 10:18 by pauhuang" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited, 15 flushes, 0 overruns,
 xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
    Console logging: level debugging, 4756 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 6755 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
    Trap logging: level informational, 6388 message lines logged
Log Buffer (12800000 bytes):
*Oct 11 03:42:07.367: CM file (ivfs:/ubr10k4-k9p6u2-m_matrix.cm) is not readable, using
internal matrix table
*Oct 11 03:42:08.799: %C10K_TOASTER-6-STARTLOAD: Downloading Microcode:
file=system:pxf/c10k-cr4-ucode.101.0.0.0, version=101.0.0.0, description=Nightly Build
Software created Mon 27-Sep-10 16:12
*Oct 11 03:42:10.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0/0, changed
 state to up
*Oct 11 03:42:10.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
 changed state to up
*Oct 11 03:42:10.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface LI-Null0, changed
state to up
*Oct 11 03:42:10.447: %LINK-3-UPDOWN: Interface FastEthernet0/0/0, changed state to up
*Oct 11 03:42:10.691: %RED-5-REDCHANGE: PRE B now Non-participant(0x0 => 0x1421)
*Oct 11 03:42:11.575: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0/0,
changed state to down
*Oct 11 03:42:11.639: %IPCOIR-5-IVFS_FILE_LOADING: Extracting 5cable-mc520u-d from
ivfs:/ubr10kclc-lck8-mz.card.
*Oct 11 03:42:12.403: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1/0,
 changed state to down
...
...
...
Modular-Cable1/1/0:0, changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Modular-Cable1/1/0:1,
 changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Modular-Cable1/1/0:2,
 changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Modular-Cable1/1/0:3,
 changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Modular-Cable1/1/0:4,
 changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface
...
...
...
GigabitEthernet3/1/0, changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet4/0/0,
 changed state to down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cable5/0/0, changed
```

```
state to down
*Oct 11 03:42:12.935: %SNMP-5-LINK_DOWN: LinkDown:Interface Cable5/0/0 changed state to
down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cable5/0/1, changed
state to down
*Oct 11 03:42:12.935: %SNMP-5-LINK_DOWN: LinkDown:Interface Cable5/0/1 changed state to
down
*Oct 11 03:42:12.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cable5/0/2, changed
state to down
*Oct 11 03:42:12.935: %SNMP-5-LINK_DOWN: LinkDown:Interface Cable5/0/2 changed state to
down
tate to up
*Oct 11 03:42:22.491: %UBR10000-5-UPDOWN: Interface Cable5/1/3 U0, changed state to down
*Oct 11 03:42:22.495: %UBR10000-5-USFREQCHG: Interface Cable5/1/3 U0, changed to Freq 25.000
 MHz
*Oct 11 03:42:22.503: %UBR10000-5-UPDOWN: Interface Cable5/1/3 U1, changed state to down
*Oct 11 03:42:22.507: %UBR10000-5-USFREQCHG: Interface Cable5/1/3 U1, changed to Freq 26.600
 MHz
*Oct 11 03:42:23.911: %UBR10000-5-USFREQCHG: Interface Cable7/1/2 U0.1, changed to Freq
10.000 MHz
*Oct 11 03:42:23.911: %UBR10000-5-USFREQCHG: Interface Cable7/1/2 U0.1, changed to Freq
10.000 MHz
*Oct 11 03:42:23.911: %UBR10000-5-UPDOWN: Interface Cable7/1/2 U0.1, changed state to down
*Oct 11 03:42:23.923: %UBR10000-5-UPDOWN: Interface Cable7/1/2 U1, changed state to down
*Oct 11 03:42:23.935: %UBR10000-5-UPDOWN: Interface Cable7/1/2 U2, changed state to down
*Oct 11 03:42:23.947: %UBR10000-5-UPDOWN: Interface Cable7/1/2 U3, changed state to down
*Oct 11 03:42:23.951: %UBR10000-5-UPDOWN: Interface Cable7/1/2 U3.1, changed state to down
...
...
...
*Oct 11 03:42:25.795: %LINK-3-UPDOWN: Interface Cable6/1/3, changed state to down
*Oct 11 03:42:25.795: %LINK-3-UPDOWN: Interface Cable6/1/4, changed state to down
*Oct 11 03:42:25.795: %UBR10000-5-UPDOWN: Interface Cable8/0/8 U0, changed state to down
*Oct 11 03:42:25.807: %UBR10000-5-UPDOWN: Interface Cable8/0/8 U1, changed state to down
*Oct 11 03:42:25.819: %UBR10000-5-UPDOWN: Interface Cable8/0/8 U2, changed state to down
*Oct 11 03:42:25.831: %UBR10000-5-UPDOWN: Interface Cable8/0/8 U3, changed state to down
...
...
...
*Oct 11 03:42:30.175: %IPCOIR-3-CARD_UNSUPPORTED: Unsupported card type (0x415) in slot
1/0.
*Oct 11 03:42:30.175: %IPCOIR-5-CARD_DETECTED: Card type 2jacket-1 (0x415) in slot 1/0
*Oct 11 03:42:30.175: %IPCOIR-5-CARD_LOADING: Loading card in slot 4/0 sw version 4.0 code
 MD5 FFE6204BD2DED9385026C375D457564A fpga MD5 E5099933C1DDD6B76260A6085BD1CDDF
*Oct 11 03:42:30.175: %IPCOIR-5-CARD_LOADING: Loading card in slot 1/0 sw version 1.1 code
 MD5 3716BEAEB613954FB02A236E6636B299 fpga MD5 00000000000000000000000000000000
*Oct 11 03:42:30.179: %IPCOIR-5-CARD_DETECTED: Card type 2cable-dtcc (0x5B0) in slot 2/1
*Oct 11 03:42:30.183: %IPCOIR-5-CARD_LOADING: Loading card in slot 2/1 sw version 1.0 code
 MD5 08BB3163BD9E82D61F2A78200397187D fpga MD5 00000000000000000000000000000000
*Oct 11 03:42:30.775: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 10000 Software (UBR10K4-K9P6U2-M), Experimental Version
12.2(20100929:171810) [pauhuang-card 111]
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 29-Sep-10 10:18 by pauhuang
*Oct 11 03:42:30.791: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-mc2020v (0x641) in slot
 6/0
*Oct 11 03:42:30.795: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/0 sw version 1.0 code
 MD5 3913D37E4C8CD8878EAE1E75669CFA1F fpga MD5 00000000000000000000000000000000
*Oct 11 03:42:31.115: %LINEPROTO-5-UPDOWN: Line protocol on Interface Bundle1, changed state
 to up
*Oct 11 03:42:31.119: %SNMP-5-LINK_UP: LinkUp:Interface Bundle1 changed state to up
*Oct 11 03:42:31.119: %LINEPROTO-5-UPDOWN: Line protocol on Interface Bundle2, changed state
 to up
*Oct 11 03:42:31.123: %SNMP-5-LINK_UP: LinkUp:Interface Bundle2 changed state to up
*Oct 11 03:42:31.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface Bundle3, changed state
 to up
*Oct 11 03:42:31.127: %SNMP-5-LINK_UP: LinkUp:Interface Bundle3 changed state to up
*Oct 11 03:42:31.131: %LINEPROTO-5-UPDOWN: Line protocol on Interface Bundle4, changed state
 to up
*Oct 11 03:42:31.131: %SNMP-5-LINK_UP: LinkUp:Interface Bundle4 changed state to up
*Oct 11 03:42:31.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0/0,
changed state to up
*Oct 11 03:42:31.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface Bundle60, changed
```

```
state to up
*Oct 11 03:42:31.135: %SNMP-5-LINK_UP: LinkUp:Interface Bundle60 changed state to up
*Oct 11 03:42:31.503: %SYS-6-BOOTTIME: Time taken to reboot after reload = 423551 seconds
*Oct 11 03:42:32.523: %LINK-3-UPDOWN: Interface HTDP0/0/1, changed state to up
*Oct 11 03:42:32.783: %C10K-5-LC_NOTICE: Slot[4/0] Line-card Image Downloaded...Booting...
*Oct 11 03:42:33.523: %LINEPROTO-5-UPDOWN: Line protocol on Interface HTDP0/0/1, changed
state to up
*Oct 11 03:42:35.555: %C10K_TOASTER-6-STARTPXF:
!!pxf clients started, forwarding code operational!!
*Oct 11 03:42:35.951: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-5x20s (0x348) in slot
6/1
*Oct 11 03:42:36.007: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/1 sw version 1.0 code
 MD5 33AD44802F7069858C7A18315833494D fpga MD5 00000000000000000000000000000000
*Oct 11 03:42:36.359: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-5x20s (0x348) in slot
5/0
...
...
...
*Oct 11 03:44:09.923: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/1/4 changed state to up
*Oct 11 03:45:40.751: cr10k_clnt_issu_start_nego_session at slot 8/0 clnt 0:rp-lc:rp-lc ses
 131081 nego Yes ISSU/my compat Yes/Yes
*Oct 11 03:45:41.823: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-3g60 (0x65D) in slot
8/0
*Oct 11 03:45:41.823: CR10K DOCSIS C8/0 is up for apps
*Oct 11 03:45:41.823: CR10K HCCP C8/0 is up for apps
*Oct 11 03:45:41.823: CR10K PKTCBL C8/0 is up for apps
*Oct 11 03:45:41.823: CR10K PLFM C8/0 is up for apps
*Oct 11 03:45:41.823: CR10K SNMP C8/0 is up for apps
*Oct 11 03:45:41.831: CR10K GUARDIAN C8/0 is up for apps
*Oct 11 03:45:41.835: %CMTS_LIC-6-CHANNEL_SHUTDOWN: Cable8/0/3 channel 0 has been shutdown
 due to insufficient licenses
*Oct 11 03:45:41.835: %UBR10000-5-UPDOWN: Interface Cable8/0/3 U0, changed state to down
*Oct 11 03:45:41.835: %CMTS_LIC-6-CHANNEL_SHUTDOWN: Cable8/0/3 channel 1 has been shutdown
 due to insufficient licenses
*Oct 11 03:45:41.835: %UBR10000-5-UPDOWN: Interface Cable8/0/3 U1, changed state to down
*Oct 11 03:45:41.835: %CMTS_LIC-6-CHANNEL_SHUTDOWN: Cable8/0/3 channel 2 has been shutdown
 due to insufficient licenses
*Oct 11 03:45:41.835: %UBR10000-5-UPDOWN: Interface Cable8/0/3 U2, changed state to down
*Oct 11 03:45:41.835: %CMTS_LIC-6-CHANNEL_SHUTDOWN: Cable8/0/3 channel 3 has been shutdown
 due to insufficient licenses
...
...
...
*Oct 11 04:08:41.287: %CMTS_LIC-6-CHANNEL_NO_SHUTDOWN: Cable8/0/3 channel 0 has been restored
 to no shut
*Oct 11 04:08:41.287: %CMTS_LIC-6-OUT_OF_RANGE: LC 8/0, Forced Shut US License Count is
already 0
-Traceback= 40ACB68C 401C7694 401C77E4 401C71F8 401AC3CC 40258AA8 401C7A94 401C7FCC 401C8140
 401C9288 401C94D0 401AE5BC 40CEFD3C 40CFD49C 40A50BAC 40150EC8
*Oct 11 04:08:41.291: %UBR10000-5-UPDOWN: Interface Cable8/0/3 U0, changed state to down
*Oct 11 04:08:41.291: %CMTS_LIC-6-CHANNEL_NO_SHUTDOWN: Cable8/0/3 channel 1 has been restored
 to no shut
*Oct 11 04:08:41.291: %CMTS_LIC-6-OUT_OF_RANGE: LC 8/0, Forced Shut US License Count is
already 0
...
...
...
*Oct 11 04:16:14.851: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/0 sw version 1.0 code
 MD5 3913D37E4C8CD8878EAE1E75669CFA1F fpga MD5 00000000000000000000000000000000
*Oct 11 04:18:48.847: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-mc2020v (0x641) in slot
 6/0
*Oct 11 04:18:48.851: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/0 sw version 1.0 code
 MD5 3913D37E4C8CD8878EAE1E75669CFA1F fpga MD5 00000000000000000000000000000000
*Oct 11 04:21:18.859: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-mc2020v (0x641) in slot
 6/0
*Oct 11 04:21:18.859: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/0 sw version 1.0 code
 MD5 3913D37E4C8CD8878EAE1E75669CFA1F fpga MD5 00000000000000000000000000000000
*Oct 11 04:29:09.763: %UBR10K-1-POWCYCLE: Power cycle slot 6/0
*Oct 11 04:29:17.931: %LCINFO-4-LCHUNG: Slot [6/0] down on last 11 checks.  HW RESET # 3
...
...
...
*Oct 11 09:05:26.702: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet8/0/0,
```

```
 changed state to down
*Oct 11 09:05:39.382: cr10k_crane_delete_cdb Modular-Cable
*Oct 11 09:05:39.382: in cr10k_crane_delete_cdb Modular-Cable
*Oct 11 09:05:39.382: wbchannel_delete_context Modular-Cable
*Oct 11 09:05:39.582: cr10k_crane_delete_cdb Modular-Cable
*Oct 11 09:05:39.582: in cr10k_crane_delete_cdb Modular-Cable
*Oct 11 09:05:39.582: wbchannel_delete_context Modular-Cable
*Oct 11 09:05:39.782: cr10k_crane_delete_cdb Modular-Cable
*Oct 11 09:05:39.782: in cr10k_crane_delete_cdb Modular-Cable
*Oct 11 09:05:39.782: wbchannel_delete_context Modular-Cable
*Oct 11 09:05:39.986: %C10K-3-DEACTIVATED: card in slot [8/0] disabled.
*Oct 11 09:05:47.670: %UBR10000-5-USFREQCHG: Interface Cable8/0/0 U0, changed to Freq 10.000
 MHz
...
...
...
*Oct 11 16:48:26.188: CR10K DOCSIS C8/1 is up for apps
*Oct 11 16:48:26.188: CR10K HCCP C8/1 is up for apps
*Oct 11 16:48:26.188: CR10K PKTCBL C8/1 is up for apps
*Oct 11 16:48:26.188: CR10K PLFM C8/1 is up for apps
*Oct 11 16:48:26.188: CR10K SNMP C8/1 is up for apps
*Oct 11 16:48:26.704: CR10K GUARDIAN C8/1 is up for apps
*Oct 11 16:48:28.068: cr10k_clnt_issu_start_nego_session at slot 8/0 clnt 0:rp-lc:rp-lc ses
 458761 nego Yes ISSU/my compat Yes/Yes
*Oct 11 16:48:28.084: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-3g60 (0x65D) in slot
8/0
*Oct 11 16:48:28.084: CR10K DOCSIS C8/0 is up for apps
*Oct 11 16:48:28.084: CR10K HCCP C8/0 is up for apps
*Oct 11 16:48:28.084: CR10K PKTCBL C8/0 is up for apps
*Oct 11 16:48:28.084: CR10K PLFM C8/0 is up for apps
*Oct 11 16:48:28.084: CR10K SNMP C8/0 is up for apps
*Oct 11 16:48:28.092: CR10K GUARDIAN C8/0 is up for apps
*Oct 11 16:48:50.456: CR10K DOCSIS C8/0 is down for apps
*Oct 11 16:48:50.456: CR10K HCCP C8/0 is down for apps
*Oct 11 16:48:50.456: CR10K PKTCBL C8/0 is down for apps
*Oct 11 16:48:50.456: CR10K PLFM C8/0 is down for apps
*Oct 11 16:48:50.456: CR10K SNMP C8/0 is down for apps
*Oct 11 16:48:50.456: CR10K GUARDIAN C8/0 is down for apps
*Oct 11 16:48:50.460: %IPCOIR-3-TIMEOUT: Timeout waiting for a response from slot 8/0.
*Oct 11 16:48:50.460: %IPCOIR-2-CARD_UP_DOWN: Card in slot 8/0 is down.  Notifying
ubr10k-clc-3g60 driver.
*Oct 11 16:48:51.456: %C10K-5-SUBSLOT_RESET: Card in slot 8/0 has been reset
*Oct 11 16:49:23.744: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-3g60 (0x65D) in slot
8/0
*Oct 11 16:49:23.744: %IPCOIR-5-CARD_LOADING: Loading card in slot 8/0 sw version 1.0 code
 MD5 15247BBB545BF3FAE97D7E7D34C1177C fpga MD5 00000000000000000000000000000000
*Oct 11 16:49:26.708: %CR10K_CLNT-3-TIMEOUT: Timeout waiting for RP-LIC: card license ready,
 slot 8/1
-Traceback= 40ACB68C 40DCA7FC 401AE8E0 40CEDF00 40CF37CC 40BC79DC 40BC79C8
*Oct 11 16:49:28.092: %CR10K_CLNT-3-TIMEOUT: Timeout waiting for RP-LIC: card license ready,
 slot 8/0
...
...
...
*Oct 13 04:12:04.931: cr10k_clnt_issu_receive_nego_message at slot 8/1 clnt 0:rp-lc:rp-lc
ses 1179700 nego Yes ISSU/my compat Yes/Yes
*Oct 13 04:12:05.143: CR10K HCCP C8/1 is up for apps
*Oct 13 04:12:05.203: CR10K GUARDIAN C8/1 is up for apps
*Oct 13 04:12:05.259: CR10K PLFM C8/1 is up for apps
*Oct 13 04:12:05.271: CR10K PKTCBL C8/1 is up for apps
*Oct 13 04:12:05.299: CR10K SNMP C8/1 is up for apps
*Oct 13 04:12:05.795: CR10K DOCSIS C8/1 is up for apps
*Oct 13 04:12:07.739: %IPCOIR-3-TIMEOUT: Timeout waiting for a response from slot 8/0.
*Oct 13 04:12:07.739: %IPCOIR-2-CARD_UP_DOWN: Card in slot 8/0 is down.  Notifying
ubr10k-clc-3g60 driver.
*Oct 13 04:12:07.739: %C10K-3-EEPROM_ERROR: c10k_load_slot_eeprom_copy failed on subslot
8/0
-Traceback= 40ACB68C 40CDD418 40CCE018 40CCE2F4 40A50BAC 40150EC8 40A7D068 40BC79DC 40BC79C8
*Oct 13 04:12:07.743: %C10K-3-EEPROM_ERROR: c10k_load_slot_eeprom_copy failed on subslot
8/0
-Traceback= 40ACB68C 40CDD274 40CCE05C 40CCE2F4 40A50BAC 40150EC8 40A7D068 40BC79DC 40BC79C8
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/0, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/1, changed state to down
```

```
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/2, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/3, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/4, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/5, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/6, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/7, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/8, changed state to down
*Oct 13 04:12:09.919: %LINK-3-UPDOWN: Interface Cable8/0/9, changed state to down
...
...
...
*Oct 13 05:38:38.083: %LINK-3-UPDOWN: Interface GigabitEthernet8/1/0, changed state to down
*Oct 13 05:38:38.083: %LINK-3-UPDOWN: Interface GigabitEthernet8/1/2, changed state to down
*Oct 13 05:38:38.083: %LINK-3-UPDOWN: Interface GigabitEthernet8/1/4, changed state to down
*Oct 13 05:38:46.815: %IPCOIR-5-CARD_DETECTED: Card type ubr10k-clc-3g60 (0x65D) in slot
8/0
*Oct 13 05:38:46.839: cr10k_clnt_issu_receive_nego_message at slot 8/0 clnt 0:rp-lc:rp-lc
ses 589887 nego Yes ISSU/my compat Yes/Yes
*Oct 13 05:38:48.095: CR10K HCCP C8/0 is up for apps
*Oct 13 05:38:48.159: CR10K GUARDIAN C8/0 is up for apps
*Oct 13 05:38:48.271: CR10K PLFM C8/0 is up for apps
*Oct 13 05:38:48.283: CR10K PKTCBL C8/0 is up for apps
*Oct 13 05:38:48.311: CR10K SNMP C8/0 is up for apps
*Oct 13 05:38:48.679: CR10K DOCSIS C8/0 is up for apps
*Oct 13 05:38:50.735: %IPCOIR-2-CARD_UP_DOWN: Card in slot 8/0 is up.  Notifying
ubr10k-clc-3g60 driver.
*Oct 13 05:38:50.847: %LINK-3-UPDOWN: Interface Cable8/0/0, changed state to up
*Oct 13 05:38:50.851: %LINK-3-UPDOWN: Interface Cable8/0/1, changed state to up
*Oct 13 05:38:50.851: %LINK-3-UPDOWN: Interface Cable8/0/2, changed state to up
...
...
...
*Oct 13 09:39:14.606: %SYS-5-CONFIG_I: Configured from console by console
*Oct 13 09:42:05.710: %SYS-5-CONFIG_I: Configured from console by console
*Oct 13 09:43:31.778: %SYS-5-CONFIG_I: Configured from console by console
*Oct 13 09:46:28.726: %LINK-3-UPDOWN: Interface GigabitEthernet8/0/0, changed state to down
*Oct 13 09:46:29.726: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet8/0/0,
 changed state to down
*Oct 13 09:46:32.730: %LINK-3-UPDOWN: Interface GigabitEthernet8/0/0, changed state to up
*Oct 13 09:46:33.730: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet8/0/0,
 changed state to up
*Oct 13 10:14:39.302: %SYS-5-CONFIG_I: Configured from console by console
*Oct 13 10:27:39.126: %SYS-5-CONFIG_I: Configured from console by console
Oct 13 10:28:35.938: CLC-LIC: cmts_clc_cisl_event_notify_feature_us, 1383: received event
1 notification
Oct 13 10:28:35.938: CLC-LIC: cmts_clc_cisl_event_notify_feature_us, 1404: feature US_License
 license_type 0 notifycount 20 usage_count 0 oldcount 0 newcount 0
Oct 13 10:28:35.938: CLC-LIC:cr10k_clc_cisl_handle_count_change_us: slot 8/1 oldcount 0,
newcount 0
...
...
...
SLOT 8/1: Oct 13 10:28:36.658: %LICENSE-6-INSTALL: Feature US_License 1.0 was installed in
 this device. UDI=UBR-MC3GX60V:CSJ13302903; StoreIndex=0:Primary License Storage
SLOT 8/1: Oct 13 10:28:36.662: %LICENSE-6-INSTALL: Feature DS_License 1.0 was installed in
 this device. UDI=UBR-MC3GX60V:CSJ13302903; StoreIndex=2:Primary License Storage
router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show inventory</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[NAME: "Chassis" DESCR: "uBR10000 chassis"
PID: UBR10012          , VID:    , SN: SPE100202ZH
NAME: "RP A" DESCR: "Performance Routing Engine"
PID: ESR-PRE4          , VID: V03 , SN: CAT1336F051
NAME: "RP A flash card 0" DESCR: "Flash Card"
PID: ESR-PRE-MEM-FD128 , VID:    , SN:
NAME: "RP A flash card 1" DESCR: "Flash Card"
PID: ESR-PRE-CF-1GB    , VID:    , SN:
NAME: "RP B" DESCR: "Performance Routing Engine"
PID: ESR-PRE4          , VID:    , SN:
NAME: "Jacket-Card-Slot 1/0" DESCR: "2 bays I/O slot SPA Interface Processor"
PID: UBR10-2XDS-SIP    , VID: 1.0, SN: CAT112358KV
```

```
NAME: "SPA bay 1/1" DESCR: "WIDEBAND DOCSIS SPA"
PID: SPA-24XDS-SFP     , VID: V01, SN: CAT1228E21D
NAME: "SFP 1/1/0" DESCR: "Copper GigE SFP"
PID: SP7041-E          , VID: E   , SN: MTC133100GM
NAME: "module 1/1" DESCR: "2 port utility Clock Card"
PID: UBR10-TCC+-T1     , VID:    , SN:
NAME: "module 2/1" DESCR: "2 port DTI UC"
PID: UBR10-DTCC        , VID: 2.0, SN: CAT1213E19M
NAME: "module 3/1" DESCR: "Half-height Gigabit Ethernet MAC Controller"
PID: ESR-HH-1GE        , VID:    , SN:
NAME: "module 4/0" DESCR: "Half-height Gigabit Ethernet MAC Controller"
PID: ESR-HH-1GE        , VID: 1.0, SN: CAT09190TTY
NAME: "module 5/0" DESCR: "MC520U_D_connector"
PID: UBR10-MC5X20U-D   , VID:    , SN: CAT10110AG6
NAME: "module 5/1" DESCR: "MC520U_D_connector"
PID: UBR10-MC5X20S     , VID:    , SN:
NAME: "module 6/0" DESCR: "MC2020H_D_connector"
PID: UBR10-MC20X20H    , VID:    , SN:
NAME: "module 6/1" DESCR: "MC520U_D_connector"
PID: UBR10-MC5X20U-D   , VID:    , SN: CAT100614L7
NAME: "module 7/1" DESCR: "MC3GX60V"
PID: UBR10-MC3GX60V    , VID:    , SN:
NAME: "module 8/0" DESCR: "MC3GX60V"
PID: UBR-MC3GX60V      , VID: V01 , SN: CSJ13422931
NAME: "SFP 8/0/0/0" DESCR: "SFP"
PID: SP7041-E          , VID: E  , SN: MTC1331009J
NAME: "module 8/1" DESCR: "MC3GX60V"
PID: UBR-MC3GX60V      , VID: V01 , SN: CSJ13302903
NAME: "power-supply 0" DESCR: "DC Power Entry Module for UBR10012"
PID: UBR10-PWR-DC      , VID:    , SN:
NAME: "power-supply 1" DESCR: "DC Power Entry Module for UBR10012"
PID: UBR10-PWR-DC      , VID:    , SN:
NAME: "fan-tray" DESCR: "BLOWER ASSEMBLY FOR UBR10012"
PID: UBR10-FAN-ASSY    , VID:    , SN:
router#]]></aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

Additional References

Related Documents

Related Topic	Document Title
CMTS Command Reference	Cisco Broadband Cable Command Reference Guide, at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Configuring Call Home for Cisco 7200 Series Routers	http://www.cisco.com/en/US/docs/routers/7200/configuration/feature_guides/callhome_7200.html
Cisco License Call Home	http://www.cisco.com/en/US/docs/ios/csa/configuration/guide/csa_callhome.html

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	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

RFCs

RFC	Title
None	—

Technical Assistance

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

Feature Information for the Call Home Feature for the Cisco CMTS Routers

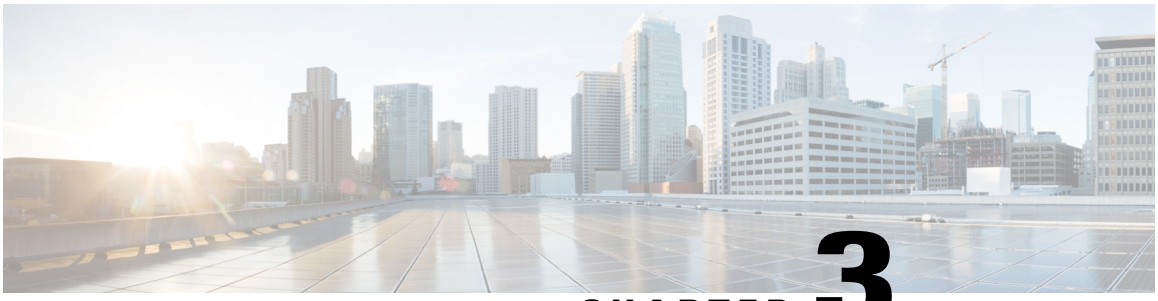
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release,

feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

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

Table 4: Feature Information for Call Home Feature for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Call Home Feature for the Cisco CMTS Routers	12.2(33)SCE	This feature was introduced on the Cisco universal broadband routers



CHAPTER 3

Cisco Network Registrar for the Cisco CMTS Routers

First Published: February 14, 2008

Last Updated: February 9, 2009

This chapter supplements the Cisco Network Registrar (CNR) documentation by providing additional cable-specific instructions to provision a hybrid fiber-coaxial (HFC) network using Cisco universal broadband routers as CMTSs at the headend of the network.

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.

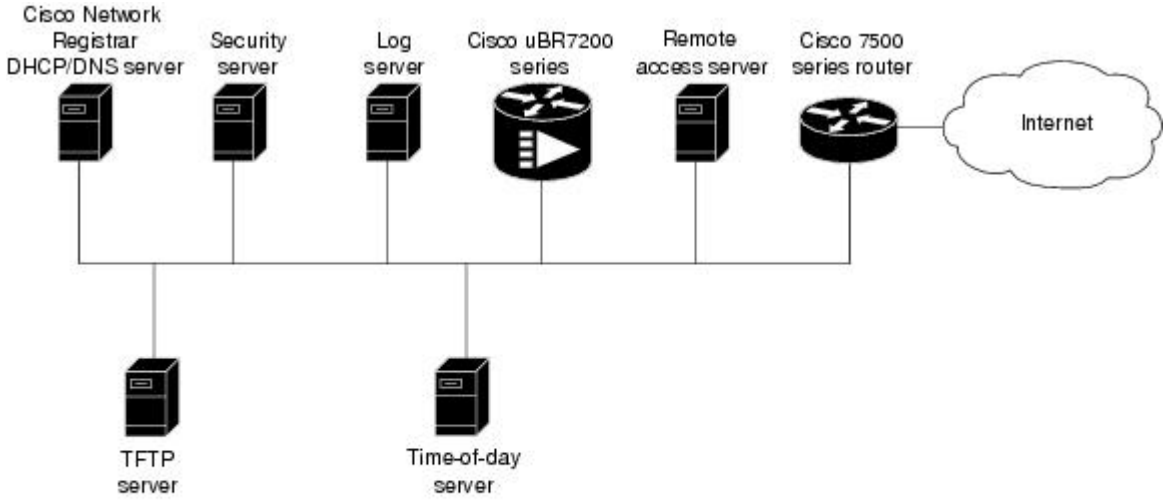
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Servers Required on the HFC Network

A TFTP server, DHCP server, and time-of-day (TOD) server are required to support two-way data cable modems on an HFC network. A cable modem will not boot if these servers are not available. The log server and security servers are not required to configure and operate a cable modem. If the log server or security servers are not present, a cable modem will generate warning messages, but it will continue to boot and function properly.

Figure 1: Servers Required on a Two-Way HFC Network



In this provisioning model, TOD and TFTP servers are standard Internet implementations of the RFC 868 and RFC 1350 specifications. Most computers running a UNIX-based operating system supply TOD and TFTP servers as a standard software feature. Typically, the TOD server is embedded in the UNIX *inetd* and it requires no additional configuration. The TFTP server is usually disabled in the standard software but can be enabled by the user. Microsoft NT server software includes a TFTP server that can be enabled with the services control panel. Microsoft NT does not include a TOD server. A public domain version of the TOD server for Microsoft NT can be downloaded from several sites.

The DHCP and Domain Name System (DNS) server shown in Figure above must be the DHCP/DNS server available in Cisco Network Registrar version 2.0 or later. CNR is the only DHCP server that implements

policy-based assignment of IP addresses. The headend must be a Cisco uBR7200 series universal broadband router or Cisco uBR10012 universal broadband router. The remote access server is only required on HFC networks that are limited to one-way (downstream only) communication. In a one-way HFC network, upstream data from a PC through the headend to the Internet is carried over a dialup connection. This dialup connection for upstream data is referred to as telco return. For simplification, the model will not include a log or security server. Cable modems can be set up to use the logging and security servers by including the appropriate DHCP options in the cable modem policy as described in the *Cisco Network Registrar User Manual*.

Cisco Network Registrar Description

CNR is a dynamic IP address management system, running on Windows or Solaris, that uses the Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to cable interfaces, PCs, and other devices on the broadband network. The CNR tool includes script extensions that allow a cable system administrator to define and view individual DHCP options, define the identity or type of device on the network, and assign the device to a predefined class or group.

Using the CNR tool, a cable system administrator can specify policies to provide:

- Integrated DHCP and Domain Name Server (DNS) services
- Time of Day (ToD) and Trivial File Transfer Protocol (TFTP) server based on the size of the network
- DHCP safe failover and dynamic DNS updates

Note This is available only in CNR 3.0 or higher.

Using the CNR tool and the extension scripts identified in the Overview of Scripts, on page 78 section, a cable system administrator can specify scopes, policies, and options for the network and each cable interface based on the services and configuration to support at each subscriber site.

Note Scopes refer to the administrative grouping of TCP/IP addresses; all IP addresses within a scope should be on the same subnet.

The cable system administrator defines system default policies for all standard options and uses scope-specific policies for options related to particular subnets, such as cable interfaces. This allows DHCP to send the information with the IP address.

Seven entry points exist for scripts:

- post-packet-decode
- pre-client-lookup
- post-client-lookup—Examines and takes action on results of the client-class process, places data items in the environment dictionary to use at the pre-packet-encode extension point, includes DHCP relay option
- check-lease-acceptable
- pre-packet-encode
- post-sent-packet

- pre-dns-add-forward

Overview of DHCP Using CNR

Cisco Network Registrar (CNR) is a dynamic IP address management system that uses the Dynamic Host Configuration Protocol (DHCP) and assigns IP addresses to PCs and other devices on a network based on a predefined set of policies, such as class of service. CNR assigns available IP addresses from address pools based on the identity or type of the requesting device and the policies in effect. For example, CNR can distinguish between registered devices, unregistered devices, and registered devices that have been assigned to a particular class of service.

CNR also provides extensions that can be customized (via programming or a script) so that you can view individual DHCP options, determine the identity or type of a device based on the content of the options, and assign a device to a predefined class or group. Using these extensions, you can determine the difference between PCs and cable modems and assign them IP addresses from different address pools.

In typical data-over-cable environments, service providers are interested in simplifying provisioning to limit the amount of information that must be collected about subscribers' customer premise equipment (CPEs). To support current provisioning models, a field technician must be sent to a subscriber's home or business to install and setup a cable modem. During this site visit, the technician might register the serial number and MAC address of the cable modem in the customer account database. Because a field technician must go to a subscriber's site to replace a cable modem, you can easily track modem information.

Manually registering and tracking information about a cable subscriber's PC is more difficult. A subscriber might purchase a new PC or exchange the network interface card (NIC) without notifying you of the change. Automatic provisioning with CNR reduces the amount of customer service involvement needed to track customer equipment. To use the provisioning model described in this document, you must still track serial numbers and MAC addresses for cable modems, but you do not need to track information about the PC or NIC cards installed at a subscriber site.

The remainder of this document describes how to configure CNR to support this model. The following sections describe the equipment and servers required for the cable headend, provide an overview of the interaction between DOCSIS-compatible cable modems and the Cisco universal broadband routers, and provide a guide on how to configure CNR to support this provisioning model.

How Cisco Universal Broadband Routers and Cable Modems Work

Cisco universal broadband routers and cable modems are based on the Data Over Cable Service Interface Specification (DOCSIS) standards. These standards were created by a consortium of cable service providers called Multimedia Cable Network Systems, Ltd. (MCNS) to that cable headend and cable modem equipment produced by different vendors will interoperate. The key DOCSIS standards provide the basis for a cable modem to communicate with any headend equipment and headend equipment to communicate with any cable modem.

Cable modems are assigned to operate on specific cable channels so activity can be balanced across several channels. Each Cisco uBR7200 series router installed at the headend serves a specific channel. Part of network planning is to decide which channel each cable modem can use.

A cable modem cannot connect to the network until the following events occur:

- The cable modem initializes and ranges through available frequencies until it finds the first frequency that it can use to communicate to the headend. The cable modem might be another vendor's DOCSIS-compatible device and the headend might have a Cisco uBR7200 series router installed. At this point on the initial connection, the cable modem cannot determine if it is communicating on the correct channel.
- The cable modem goes through the DHCP server process and receives a configuration file from the server.
- One of the parameters in the configuration file tells the cable modem which channel it can use.
- If the assigned channel is not available on the Cisco uBR7200 series router to which the cable modem is currently connected, it resets itself and comes up on the assigned channel.
- During this second DHCP process, the modem will be connected to the correct CMTS. This time, the configuration file will be loaded. For a DOCSIS-compatible cable modem to access the network, it might go through the DHCP server two times on two different networks; therefore, one-lease-per-client IP addressing is critical.

DHCP Fields and Options for Cable Modems

DHCP options and packet fields are required to enable cable modems to boot and operate properly. Table below lists the required DHCP options and fields.

Table 5: Required DHCP Fields and Options

Required Field/Option	Field/Option In Cisco Network Registrar	Value/Description
Fields		
giaddr	-	IP address. As a DHCP packet passes through the relay agent to the DHCP server, the relay agent supplies a unique IP address to the packet and stores it in this field. The relay agent is a uBR7200 series router with the iphelper attribute defined.
subnet-mask	-	Subnet mask for the IP address stored in the giaddr field. This value is also stored in the DHCP packet by the relay agent.
file	Packet-file-name	Name of the cable modem configuration file that will be read from a TFTP server.
siaddr	Packet-siaddr	IP address of the TFTP server where configuration files are stored.

Required Field/Option	Field/Option In Cisco Network Registrar	Value/Description
Options		
Time-servers	-	List of hosts running the time server specified in the RFC 868 standard.
Time-offset	-	Time offset of a cable modem internal clock from Universal Time Coordinated (UTC). This value is used by cable modems to calculate the local time that is stored in time-stamping error logs.
MCNS-security-server	-	IP address of the security server. This should be set if security is required. See RFC 1533 for details.

Cisco Network Registrar Sample Configuration

You can use the following information to set up Cisco Network Registrar in a trial configuration. The configuration describes DHCP-related setup only; it does not cover setting up DNS or configuring dynamic DNS (DDNS). You should be familiar with important CNR concepts including scopes, primary and secondary scopes, scope selection tags, client classes, and CNR policies. See the Using Network Registrar publication for detailed information on these concepts.

In the trial configuration, you can configure CNR to perform the following operations:

- Receive DHCP requests from a cable modem and a PC on an HFC network via a port supporting multiple network numbers. The Cisco uBR7200 series router at the headend must be configured as a forwarder (iphelper is configured).
- Serve IP addresses on two networks; a net-10 network (non-Internet routable) and a net-24 network (Internet routable).
- Tell the difference between a cable modem and a PC based on the MAC address of the device and provide net-24 addresses to the PC and net-10 addresses to the cable modem.
- Refuse to serve IP addresses to MAC addresses that it does not recognize.

To perform these options, you must implement the following CNR configuration items:

- Create two scope selection tags; one for PCs, one for cable modems.
- Create two client-classes; one for PCs , one for cable modems.
- Create a lease policy appropriate for the cable modem devices.
- Create a lease policy appropriate for the PC devices.
- Create a scope containing Class A net-24 (routable) addresses.

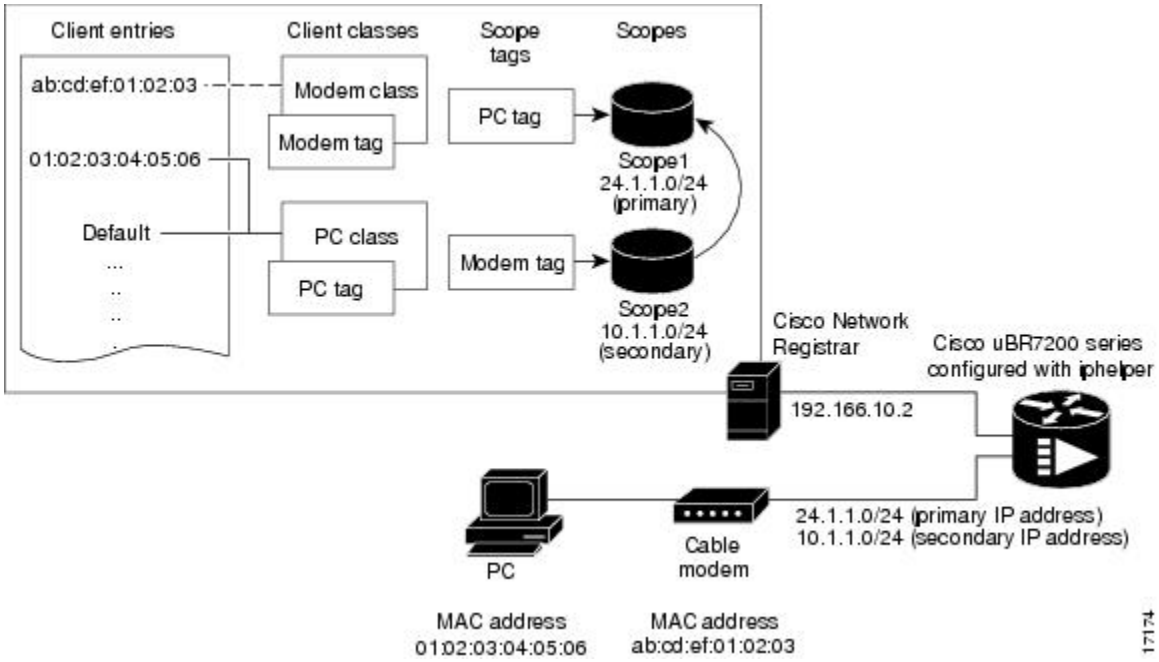
- Create a scope containing Class A net-10 (nonroutable) addresses.
- Identify the scope containing the net-24 addresses as the primary scope and configure the other scope containing the net-10 addresses as secondary to the net-24 scope.

Note The Cisco uBR7200 series router upstream ports must be configured with the primary network address on the net-24 network; such as 24.1.1.1.

- Assign the policies to the appropriate scope.
- Add the MAC address of the cable modem and the PC to the client-entry list.
- Associate the PC tag with the scope containing routable addresses.
- Associate the cable modem tag with the scope containing nonroutable addresses.
- Associate the cable modem tag with the cable modem client-class.
- Associate the PC tag with the PC client-class.
- Assign the PC MAC to the PC class.
- Assign the cable modem MAC to the cable modem class.
- Enable client-class processing.

Figure below shows the trial CNR configuration in an HFC network.

Figure 2: Trial Configuration in an HFC Network



These configuration items and their associations can be created using either the CNR management graphical user interface (GUI) or command-line interface (CLI). The following sample script configures DHCP for a sample server:

```
File: cabledemo.rc
Command line: nrcmd -C <cluster> -N <user name> -P <password> -b < cabledemo.rc
-------------------------------------------------------------------------------
scope-selection-tag tag-CM create
scope-selection-tag tag-PC create
client-class create class-CM
client-class class-CM set selection-criteria=tag-CM
client-class create class-PC
client-class class-PC set selection-criteria=tag-PC
policy cmts-cisco create
policy cmts-cisco setleasetime 1800
policy cmts-cisco setoption domain-name-servers 192.168.10.2
policy cmts-cisco setoption routers 10.1.1.1
policy cmts-cisco setoption time-offset  604800
policy cmts-cisco setoption time-servers 192.168.10.20
policy cmts-cisco set packet-siaddr=192.168.10.2
policy cmts-cisco setoption log-servers 192.168.10.2
policy cmts-cisco setoption mcns-security-server 192.168.10.2
policy cmts-cisco set packet-file-name=golden.cfg
policy cmts-cisco set dhcp-reply-options=packet-file-name,packet-siaddr,mcns-security-server
policy pPC create
policy pPC set server-lease-time 1800
policy pPC setleasetime 1800
policy pPC setoption domain-name-servers 192.168.10.2
policy pPC setoption routers 24.1.1.1
scope S24.1.1.0 create 24.1.1.0 255.255.255.0
scope S24.1.1.0 addrange 24.1.1.5 24.1.1.254
scope S24.1.1.0 set policy=pPC
scope S24.1.1.0 set selection-tags=tag-PC
scope S10.1.1.0 create 10.1.1.0 255.255.255.0
scope S10.1.1.0 addrange 10.1.1.5 10.1.1.254
scope S10.1.1.0 set policy=cmts-cisco
scope S10.1.1.0 set selection-tags=tag-CM
scope S10.1.1.0 set primary-scope=S24.1.1.0
client 01:02:03:04:05:06 create client-class-name=class-PC
client ab:cd:ef:01:02:03 create client-class-name=class-CM
client default create action=exclude
dhcp enable client-class
dhcp enable one-lease-per-client
save
dhcp reload
```

In addition to the DHCP server setup, you might want to enable packet-tracing. When packet-tracing is enabled, the server parses both requests and replies, and then adds them to the logs. If you do enable tracing, performance will be adversely affected, and the logs will roll over quickly.

Use the following nrcmd command to set packet tracing.

DHCP set log-settings=incoming-packet-detail,outgoing-packet-detail

Cable Modem DHCP Response Fields

Each cable interface on the broadband network requires the following fields in the DHCP response:

- CM's IP address
- CM's subnet mask

Note For cable operators with less experience in networking, you can fill in a guess based on the network number and indicate how your IP network is divided.

- Name of the DOCSIS configuration file on the TFTP server intended for the cable interface
- Time offset of the cable interface from the Universal Coordinated Time (UTC), which the cable interface uses to calculate the local time when time-stamping error logs
- Time server address from which the cable interface obtains the current time

DOCSIS DHCP Fields

DOCSIS DHCP option requirements include:

- IP address of the next server to use in the TFTP bootstrap process; this is returned in the siaddr field
- DOCSIS configuration file that the cable interface downloads from the TFTP server

Note If the DHCP server is on a different network that uses a relay agent, then the relay agent must set the gateway address field of the DHCP response.

- IP address of the security server should be set if security is required

DHCP Relay Option (DOCSIS Option 82)

DOCSIS Option82 modifies DHCPDISCOVER packets to distinguish cable interfaces from the CPE devices or “clients” behind them. The DOCSIS Option82 is comprised of the following two suboptions:

- Suboption 1, Circuit ID:

```
Type 1 (1 byte)
Len 4 (1 byte)
Value (8 bytes)
<bit 31,30,.....................0)
<xYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY>
```

where the MSB indicates if the attached device is a cable interface.

x=1 Cable Modem REQ

x=0 CPE device (Behind the cable interface with the cable interface MAC address shown in suboption 2.)

The rest of the bits make up the SNMP index to the CMTS interface.

Y=0xYYYYYYY is the SNMP index to the CMTS interface.

- Suboption 2, MAC address of the cable interface:

```
Type 2 (1 byte)
Len 6 (1 byte)
Value xxxx.xxxx.xxxx (6 bytes)
```

Overview of Scripts

This section lists the scripts applicable to cable interface configuration.

Two-way Cable Modem Scripts

To support two-way configurations at a subscriber site, use these scripts:

- **Relay.tcl**
- **SetRouter.tcl**

Telco Return Cable Modem Scripts

To support telco return and two-way cable interface configurations on the same cable interface card or chassis, use these scripts:

- **PostClientLookup.tcl**
- **PrePacketEncode.tcl**

Placement of Scripts

Windows NT

For CNR running on Windows NT, place the appropriate scripts in the following directory:

```
\program files\network registrar\extensions\dhcp\scripts\tcl
```

Solaris

For CNR running on Solaris, place the appropriate scripts in the following directory:

```
/opt/nwreg2/extensions/dhcp/scripts/tcl
```

Activating Scripts in Cisco Network Registrar

To activate the scripts after you have placed them in the appropriate directory:

Step 1 Open up a text editor.

Step 2 Open one of the scripts at the nrcmd> command prompt.

Step 3 Create the extension points and attach them to the system.

Note The easiest way to do this is to simply cut and paste the command lines from the scripts to the nrcmd> command line.

Step 4 After you have created and attached the extension points, do a dhcp reload.

The scripts are active.

Configuring the Cisco CMTS Routers to Use Scripts

Each cable interface must be set up as a BOOTP forwarder and have the relay option enabled. The primary and secondary IP addresses for each cable interface must be in sync with the CNR tool.

To properly communicate with scripts in the system, use the following commands on the Cisco CMTS router:

- To enable option 82, use the **ip dhcp relay info option** command.
- To disable the validation of DHPC relay agent information in forwarded BOOTREPLY messages, use the **no ip dhcp relay information option check** command.

Note You can also use the cable dhcp-giaddr command in cable interface configuration mode to modify the GIADDR field of DHCPDISCOVER and DHCPREQUEST packets to provide a relay IP address before packets are forwarded to the DHCP server. Use this command to set a “policy” option such that primary addresses are used for CMs and secondary addresses are used for hosts behind the CMs.

Configuring the System Default Policy

Add these options to the system default policy for:

- Cable modems to support on your network
- PCs to support behind each cable interface on your network

Cable Modems

Define these settings following the CNR tool documentation:

- TFTP server (IP address) for those cable interfaces using BOOTP
- Time-server (IP address)
- Time-offset (Hex value, 1440 for Eastern Standard Time)
- Packet-siaddr (IP address of CNR)
- Router (set to 0.0.0.0)
- Boot-file (name of .cm file for those cable interfaces using BOOTP)
- Packet-file-name (.cm file name)

PCs

Define these settings following the CNR tool documentation:

- Domain name
- Name servers (IP address of DNS servers)

Creating Selection Tag Scopes

General

When you create your scope selection tags:

Step 1 Cut and paste the scope selection tag create commands from the scripts into the nrcmd> command line.
Note These names have to be exactly as they appear in the scripts.

Step 2 Then attach the selection tags to the appropriate scripts:
Example:

CM_Scope tagCablemodem

PC_Scope tagComputer

Telco Return for the Cisco uBR7200 Series Router

Before You Begin

Note If you are using the prepacketencode and postclientlookup .tcl scripts for telco return, the telco return scope does not have a selection tag associated to the scope.

SUMMARY STEPS

1. Put the tag Telcocablemodem on the primary cable interface scope to pull addresses from that pool instead.
2. Follow the same procedure as above, but use a telco return policy which has a different .cm file with telco-specific commands in it.

DETAILED STEPS

Step 1 Put the tag Telcocablemodem on the primary cable interface scope to pull addresses from that pool instead.

Step 2 Follow the same procedure as above, but use a telco return policy which has a different .cm file with telco-specific commands in it.

Creating Network Scopes

Following is an example for creating scopes for your network. This example assumes two Cisco uBR7200 series universal broadband routers in two locations, with one cable interface card on one Cisco uBR7200 series configured for telco return.

```
cm-toledo1_2-0 10.2.0.0 255.255.0.0 assignable 10.2.0.10-10.2.254.254 tagCablemodem
tagTelcomodem Default GW=10.2.0.1 (assigned by scripts)
cm-toledo1_3-0 10.3.0.0 255.255.0.0 assignable 10.3.0.10-10.3.254.254 tagCablemodem
tagTelcomodem Default GW=10.3.0.1 (assigned by scripts)
pc-toledo1_2-0 208.16.182.0 255.255.255.248 assignable 208.16.182.2-208.16.182.6 tagComputer
 Default GW=208.16.182.1 (assigned by scripts)
pc-toledo1_3-0 208.16.182.8 255.255.255.248 assignable 208.16.182.10-208.16.182.14 tagComputer
 Default GW=208.16.182.9 (assigned by scripts)
telco_return_2-0 192.168.1.0 255.255.255.0 (No assignable addresses, tag was put on cable
modem primary scope to force telco-return cable modem to pull address from primary scope)
cm-arlington1_2-0 10.4.0.0 255.255.0.0 assignable 10.4.0.10-10.4.254.254 tagCablemodem
Default GW=10.4.0.1 (assigned by scripts)
cm-arlington1_3-0 10.5.0.0 255.255.0.0 assignable 10.5.0.10-10.5.254.254 tagCablemodem
Default GW=10.5.0.1 (assigned by scripts)
pc-arlington1_2-0 208.16.182.16 255.255.255.248 assignable 208.16.182.17-208.16.182.22
tagComputer Default GW=208.16.182.17 (assigned by scripts)
pc-toledo1_3-0 208.16.182.24 255.255.255.248 assignable 208.16.182.2-208.16.182.30 tagComputer
 Default GW=208.16.182.25 (assigned by scripts)
```

Note Remember the last valid address in the .248 subnet range is the broadcast address; do not use this.

Creating Policies for Class of Service or for Upgrading Cable Modem Cisco IOS Images

To support Class of Service (CoS), define:

- Scope selection tags—Identifiers that describe types of scope configurations

Note This is needed for Option82.

- Client classes—Class with which a group of clients is associated

Note Scope selection tags are excluded from or included in client-classes.

- Client—Specific DHCP clients and the defined class to which they belong

To assign the CoS or use Option82, make a client entry with a MAC address and point to the appropriate policy. To use client-based MAC provisioning, add a client entry "default - exclude," then put in MAC addresses for all devices (for example, cable interfaces and PCs) in the client tab and select the policy to use, including the appropriate tag.

CNR Steps to Support Subinterfaces

The CNR configuration is done differently if subinterfaces are configured. Here is an example. If you have configured two ISP subinterfaces and one management subinterface on a Cisco uBR7200 series, make sure that the management subinterface is the first subinterface that is configured. If cable interface three—c3/0—is being used, create c3/0.1, c3/0.2 and c3/0.3 as three subinterfaces and c3/0.1 as the first subinterface configured as the management subinterface.

Note The Cisco uBR7200 series requires management subinterfaces to route DHCP packets from CMs when they first initialize because the Cisco uBR7200 series does not know the subinterfaces they belong to until it has seen the IP addresses assigned to them by gleaning DHCP reply message from CNR.

In CNR, complete the following steps for such a configuration:

SUMMARY STEPS

1. Create two scope selection tags such as: isp1-cm-tag and isp2-cm-tag
2. Configure three scopes; for example, mgmt-scope, isp1-cm-scope, and isp2-cm-scope such that isp1-cm-scope and isp2-cm-scope each define mgmt-scope to be the primary scope
3. Also configure two scopes for PCs for each of the ISPs; isp1-pc-scope and isp2-pc-scope. For scope isp1-cm-scope, configure isp1-cm-tag to be the scope selection tag. For scope isp2-cm-scope, configure isp2-cm-tag to be the scope selection tag
4. Configure two client classes; for example, isp1-client-class and isp2-client-class
5. Create client entries with their MAC addresses for CMs that belong to ISP1 and assign them to isp1-client-class. Also assign the scope selection tag isp1-cm-tag
6. Create client entries for CMs that belong to ISP2 and assign them to isp2-client-class. Also assign the scope selection tag isp2-cm-tag
7. Enable client class processing from the scope-selection-tag window

DETAILED STEPS

Step 1 Create two scope selection tags such as: isp1-cm-tag and isp2-cm-tag

Step 2 Configure three scopes; for example, mgmt-scope, isp1-cm-scope, and isp2-cm-scope such that isp1-cm-scope and isp2-cm-scope each define mgmt-scope to be the primary scope

Step 3 Also configure two scopes for PCs for each of the ISPs; isp1-pc-scope and isp2-pc-scope. For scope isp1-cm-scope, configure isp1-cm-tag to be the scope selection tag. For scope isp2-cm-scope, configure isp2-cm-tag to be the scope selection tag

Step 4 Configure two client classes; for example, isp1-client-class and isp2-client-class

Step 5 Create client entries with their MAC addresses for CMs that belong to ISP1 and assign them to isp1-client-class. Also assign the scope selection tag isp1-cm-tag

Step 6 Create client entries for CMs that belong to ISP2 and assign them to isp2-client-class. Also assign the scope selection tag isp2-cm-tag

Step 7 Enable client class processing from the scope-selection-tag window
Overlapping address ranges cannot be configured on these subinterfaces because software gleans the DHCP reply to figure out the subinterface it really belongs to. Although CNR can be configured with overlapping address range scopes, it cannot be used to allocate addresses from these scopes.

Additional References

The following sections provide references related to Cisco Network Registrar for use with the Cisco CMTS routers.

Related Documents

Related Topic	Document Title
Cisco Network Registrar documentation	• Go to: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/tsd_products_support_series_home.html
Frequently Asked Questions	• *CNR and DHCP FAQs for Cable Environment* http://www.cisco.com/en/US/tech/tk86/tk808/technologies_q_and_a_item09186a008009434c.shtml
CNR configuration recommendations for performance and troubleshooting tips.	• *Recommended CNR Settings and Management* http://www.cisco.com/warp/public/477/CNR/cnr_best_settings.html

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

Standards

Standards	Title
SP-CMCI-I02-980317	Cable Modem to Customer PremiseEquipment Interface Specification http://www.cablemodem.com)
SP-RFI-I04-980724	*Radio Frequency Interface Specification* http://www.cablemodem.com)
SP-CMTRI-I01-970804	*Cable Modem Telephony Return Interface Specification* (http://www.cablemodem.com)

MIBs

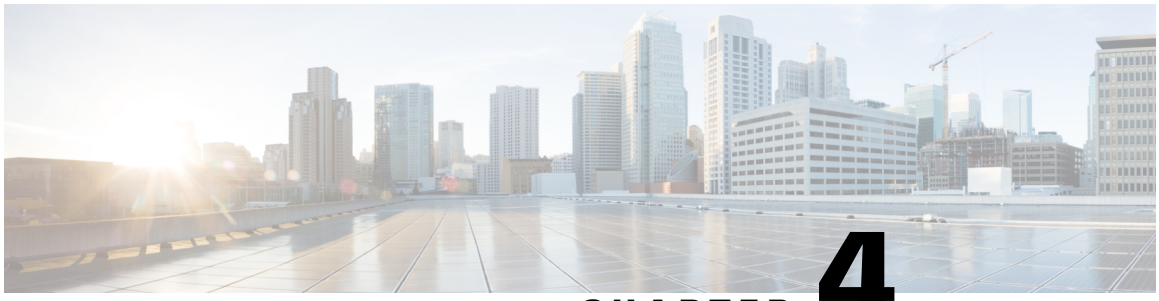
MIBs	MIBs Link
Cisco IOS MIBs Tools	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2131	*Dynamic Host Configuration Protocol*
RFC 2132	*DHCP Options and BOOTP Vendor Extensions*

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 4

DHCP, ToD, and TFTP Services for the CMTS Routers

First Published: February 14, 2008

Last Updated: February 9, 2009

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

This document describes how to configure Cisco Cable Modem Termination System (CMTS) platforms so that they support onboard servers that provide Dynamic Host Configuration Protocol (DHCP), Time-of-Day (ToD), and Trivial File Transfer Protocol (TFTP) services for use in Data-over-Cable Service Interface Specifications (DOCSIS) networks. In addition, this document provides information about optional configurations that can be used with external DHCP servers.

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 DHCP, ToD, and TFTP Services

- Cisco recommends the most current Cisco IOS Release 12.1 EC software release for DOCSIS 1.0 operations. For DOCSIS 1.1 operations, Cisco recommends the most current Cisco IOS Release 12.2 BC software release.
- A separate DOCSIS configuration file editor is required to build DOCSIS 1.1 configuration files, because the internal DOCSIS configuration file editor that is onboard the Cisco CMTS router supports only DOCSIS 1.0 configuration files.
- To be able to use the Cisco CMTS as the ToD server, either alone or along with other, external ToD servers, you must configure the DHCP server to provide the IP address Cisco CMTS as one of the valid ToD servers (DHCP option 4) for cable modems.

Restrictions for DHCP, ToD, and TFTP Services

- The “all-in-one” configuration should not be used as the only set of servers except for small cable plants (approximately 2,500 cable modems, lab environments, initial testing, small deployments, and troubleshooting. The “all-in-one” configuration can be used in larger networks, however, to supplement other redundant and backup servers.

Note The CMTS does not support the configuration of both Local DHCP Pools and DHCP Relay at the same time.

- The ToD server must use the UDP protocol to conform to DOCSIS specifications.
- For proper operation of the DOCSIS network, especially a DOCSIS 1.1 network using BPI+ encryption and authentication, the system clock on the Cisco CMTS must be set accurately. You can achieve this by manually using the **set clock** command, or by configuring the CMTS to use either the Network Time Protocol (NTP) or the Simple Network Time Protocol (SNTP).
- The internal DHCP server that is onboard the Cisco CMTS router does not support the **cable source-verify** command.
- Cisco cBR series routers do not support internal DHCP servers.

Information About DHCP, ToD, and TFTP Services

This section provides the following information about the DHCP, ToD, and TFTP Services feature, and its individual components:

Feature Overview

All Cisco CMTS platforms support onboard servers that provide DHCP, ToD, and TFTP proxy-services for use in DOCSIS cable networks. These servers provide the registration services needed by DOCSIS 1.0- and 1.1-compliant cable modems:

- Internal DHCP Servers—Provides the cable modem with an IP address, a subnet mask, default gateway, and other IP related parameters. The cable modem connects with the DHCP server when it initially powers on and logs on to the cable network.
- External DHCP Servers—Provides DHCP services. External DHCP servers are usually part of an integrated provisioning system that is more suitable when managing large cable networks.
- Time-of-DayServer_—Provides an RFC 868 -compliant ToD service so that cable modems can obtain the current date and time during the registration process. The cable modem connects with the ToD server after it has obtained its IP address and other DHCP-provided IP parameters.

Although cable modems do not need to successfully complete the ToD request before coming online, this allows them to add accurate timestamps to their event logs so that these logs are coordinated to the clock used on the CMTS. In addition, having the accurate date and time is essential if the cable modem is trying to register with Baseline Privacy Interface Plus (BPI+) encryption and authentication.

- External TFTP_Server—Downloads the DOCSIS configuration file to the cable modem. The DOCSIS configuration file contains the operational parameters for the cable modem. The cable modem downloads its DOCSIS configuration file after connecting with the ToD server.

You can configure and use each server separately, or you can configure an “all-in-one” configuration so that the CMTS acts as a DHCP, ToD, and TFTP server. With this configuration, you do not need any additional servers, although additional servers provide redundancy, load-balancing, and scalability.

Note You can add additional servers in a number of ways. For example, most cable operators use Cisco Network Registrar (CNR) to provide the DHCP and TFTP servers. ToD servers are freely available for most workstations and PCs. You can install the additional servers on one workstation or PC or on different workstations and PCs.

Internal DHCP Server

At power-up, DOCSIS cable modems send a broadcast message through the cable interface to find a DHCP server that can provide the information needed for IP connectivity across the network. After the cable modem comes online, the CPE devices connected to the cable modem can also make their own DHCP requests. You can configure all Cisco CMTS platforms to act as DHCP servers that provide the IP addressing and other networking information that is needed by DOCSIS cable modems and their CPE devices.

DHCP Field Options

In its DHCP request message, the cable modem identifies itself by its MAC hardware address. In reply, a DOCSIS-compatible DHCP server should provide, at minimum, the following fields when replying to cable modems that are authorized to access the cable network:

- yiaddr—IP address for the cable modem.
- Subnet Mask (option 1)—IP subnet mask for the cable modem.
- siaddr—IP address for the TFTP server that will provide the DOCSIS configuration file.
- file—Filename for the DOCSIS configuration file that the cable modem must download.
- Router Option (option 3)—IP addresses for one or more gateways that will forward the cable modem traffic.
- Time Server Option (option 4)—One or more ToD servers from which the cable modem can obtain its current date and time.
- Time Offset (option 2)—Universal Coordinated Time (UTC) that the cable modem should use in calculating local time.
- giaddr—IP address for a DHCP relay agent, if the DHCP server is on a different network from the cable modem.
- Log Server Option (option 7)—IP address for one or more SYSLOG servers that the cable modem should send error messages and other logging information (optional).
- IP Address Lease Time (option 51)—Number of seconds for which the IP address is valid, at which point the cable modem must make another DHCP request.

If you decide to also provide IP addresses to the CPE devices connected to the cable modems, the DHCP server must also provide the following information for CPE devices:

- yiaddr—IP address for the CPE device.
- Subnet Mask (option 1)—IP subnet mask for the CPE device.
- Router Option, option 3—IP addresses for one or more gateways that will forward the CPE traffic.
- Domain Name Server Option (option 6)—IP addresses for the domain name system (DNS) servers that will resolve hostnames to IP addresses for the CPE devices.
- Domain Name (option 15)—Fully-qualified domain name that the CPE devices should add to their hostnames.
- IP Address Lease Time (option 51)—Number of seconds for which the IP address is valid, at which point the CPE device must make another DHCP request.

The DHCP server on the Cisco CMTS can also provide a number of options beyond the minimum that are required for network operation. A basic configuration is suitable for small installations as well as lab and experimental networks.

You can also configure the CMTS in a more complex configuration that uses the functionality of DHCP pools. DHCP pools are configured in a hierarchical fashion, according to their network numbers. A DHCP pool with a network number that is a subset of another pool's network number inherits all of the characteristics of the larger pool.

DHCP Security Options

Because the DOCSIS specification requires cable modems to obtain their IP addresses from a DHCP server, cable networks are susceptible to certain types of configuration errors and theft-of-service attacks, including:

- Duplicate IP addresses being assigned to two or more cable modems or CPE devices
- Duplicate MAC addresses being reported by two or more cable modems or CPE devices
- Unauthorized use of a DHCP-assigned IP address as a permanent static address
- One user hijacking a valid IP address from another user and using it on a different network device
- Configuring IP addresses with network addresses that are not authorized for a cable segment
- Unauthorized ARP requests on behalf of a cable segment, typically as part of a theft-of-service attack

To help combat these attacks, the Cisco CMTS dynamically maintains a database that links the MAC and IP addresses of known CPE devices with the cable modems that are providing network access for those CPE devices. The CMTS builds this database using information from both internal and external DHCP servers:

- When using the internal DHCP server, the CMTS automatically populates the database from the DHCP requests and replies that are processed by the server.
- When using an external server, the CMTS populates the database by inspecting all broadcast DCHP transactions that are sent over a cable interface between the cable modems and CPE devices on that interface and the DHCP servers.

Note The Cisco CMTS also monitors IP traffic coming from CPE devices to associate their IP and MAC addresses with the cable modem that is providing their Internet connection.

The CMTS can also use the DHCP Relay Agent Information option (DHCP option 82) to send particular information about a cable modem, such as its MAC address and the cable interface to which it is connected to the DHCP server. If the DHCP server cannot match the information with that belonging to a cable modem in its database, the Cisco CMTS identifies that the device is a CPE device. This allows the Cisco CMTS and DHCP server to retain accurate information about which CPE devices are using which cable modems and whether the devices should be allowed network access.

The DHCP Relay Agent Information option can also be used to identify cloned modems or gather geographical information for E911 and other applications. Using the **cable dhcp-insert** command, users configure the Cisco CMTS to insert downstream, upstream, service class, or hostname descriptors into DHCP packets. Multiple types of strings can be configured as long as the maximum relay information option size is not exceeded.

Multiple DHCP Pools

You can also configure any number of DHCP pools for the DHCP server to use in assigning IP addresses. A single pool can be used for a basic configuration, or you can optionally create separate pools for cable modems and CPE devices. You can also use DHCP address pools to provide special services, such as static IP addresses, to customers who are paying for those service.

When creating multiple DHCP pools, you can configure them independently, or you can optionally create a hierarchical structure of pools that are organized according to their network numbers. A DHCP pool that has a network number that is a subset of another pool's network number inherits all of the characteristics of the larger pool. In addition to the inherited characteristics, you can further customize each pool with any number of options.

The advantage of DHCP pools is that you can create a number of different DHCP configurations for particular customers or applications, without having to repeat CLI commands for the parameters that the pools have in common. You can also change the configuration of one pool without affecting customers in other pools.

External DHCP Servers

The Cisco CMTS router provides the following optional configurations that can enhance the operation and security of external DHCP servers that you are using on the DOCSIS cable network:

Cable Source Verify Feature

To combat theft-of-service attacks, you can enable the **cable source-verify** command on the cable interfaces on the Cisco CMTS router. This feature uses the router's internal database to verify the validity of the IP packets that the CMTS receives on the cable interfaces, and provides three levels of protection:

- Internal DHCP Server—Provides the cable modem with an IP address, a subnet mask, default gateway, and other IP related parameters. The cable modem connects with the DHCP server when it initially powers on and logs on to the cable network.
- At the most basic level of protection, the Cable Source Verify feature examines every IP upstream packet to prevent duplicate IP addresses from appearing on the cable network. If a conflict occurs, the Cisco CMTS recognizes only packets coming from the device that was assigned the IP address by the DHCP server. The devices with the duplicate addresses are not allowed network address. The CMTS also refuses to recognize traffic from devices with IP addresses that have network addresses that are unauthorized for that particular cable segment.
- Adding the **dhcp** option to the **cable source-verify** command provides a more comprehensive level of protection by preventing users from statically assigning currently-unused IP addresses to their devices. When the Cisco CMTS receives a packet with an unknown IP address on a cable interface, the CMTS drops the packet but also issues a DHCP LEASEQUERY message that queries the DHCP servers for any information about the IP and MAC addresses of that device. If the DHCP servers do not return any information about the device, the CMTS continues to block the network access for that device.
- When you use the **dhcp** option, you can also enable the **leasetimer** option, which instructs the Cisco CMTS to periodically check its internal CPE database for IP addresses whose lease times have expired. The CPE devices that are using expired IP addresses are denied further access to the network until they renew their IP addresses from a valid DHCP server. This can prevent users from taking DHCP-assigned IP addresses and assigning them as static addresses to their CPE devices.
- In addition to the dhcp option, you can also configure prefix-based source address verification (SAV) on the Cisco CMTS using the cable source-verify group command. A CM may have a static IPv4 or IPv6 prefix configured, which belongs to an SAV group. When the SAV prefix processing is enabled on the Cisco CMTS, the source IP address of the packets coming from the CM is matched against the configured prefix and SAV group (for that CM) for verification. If the verification fails, the packets are dropped, else the packets are forwarded for further processing. For more information on SAV prefix processing and SAV prefix configuration, see Prefix-based Source Address Verification , on page 93 and Configuring Prefix-based Source Address Verification, on page 111

Prefix-based Source Address Verification

The Source Address Verification (SAV) feature verifies the source IP address of an upstream packet to ensure that the SID/MAC and IP are consistent. The DOCSIS 3.0 Security Specification introduces prefix-based SAV where every CM may have static IPv4 or IPv6 prefixes configured. These prefixes are either preconfigured on the CMTS, or are communicated to the CMTS during CM registration. The Cisco CMTS uses these configured prefixes to verify the source IP address of all the incoming packets from that CM.

An SAV group is a collection of prefixes. A prefix is an IPv4 or IPv6 subnet address. You can use the cable source-verify group command in global configuration mode to configure SAV groups. A total of 255 SAV groups are supported on a CMTS, with each SAV group having a maximum of four prefixes. Prefixes can be configured using the prefix command.

During registration, CMs communicate their configured static prefixes to the CMTS using two TLVs, 43.7.1 and 43.7.2. The TLV 43.7.1 specifies the SAV prefix group name that the CM belongs to, and TLV 43.7.2 specifies the actual IPv4 or IPv6 prefix. Each CM can have a maximum of four prefixes configured. When the Cisco CMTS receives these TLVs, it first identifies if the specified SAV group and the prefixes are already configured on the Cisco CMTS. If they are configured, the Cisco CMTS associates them to the registering CM. However if they are not configured, the Cisco CMTS automatically creates the specified SAV group and prefixes before associating them to the registering CM.

The SAV group name and the prefixes that are provided by these TLVs are considered valid by the Cisco CMTS. The packets received (from the CM) with the source IP address belonging to the prefix specified by the TLV are considered authorized. For example, if a given CM has been configured with an SAV prefix of 10.10.10.0/24, then any packet received from this CM (or CPE behind the CM) that is sourced with this address in the subnet 10.10.10.0/24 is considered to be authorized.

For more information on how to configure SAV groups and prefixes see Configuring Prefix-based Source Address Verification, on page 111.

Smart Relay Feature

The Cisco CMTS supports a Smart Relay feature (the **ip dhcp smart-relay** command), which automatically switches a cable modem or CPE device to secondary DHCP servers or address pools if the primary server runs out of IP addresses or otherwise fails to respond with an IP address. The relay agent attempts to forward DHCP requests to the primary server three times. After three attempts with no successful response from the primary, the relay agent automatically switches to the secondary server.

When you are using the **cable dhcp-giaddr policy** command to specify that the CPE devices should use the secondary DHCP pools corresponding to the secondary addresses on a cable interface, the smart relay agent automatically rotates through the available secondary in a round robin fashion until an available pool of addresses is found. This ensures that clients are not locked out of the network because a particular pool has been exhausted.

GIADDR Field

When using separate IP address pools for cable modems and CPE devices, you can use the **cable dhcp-giaddr policy** command to specify that cable modems should use an address from the primary pool and that CPE devices should use addresses from the secondary pool. The default is for the CMTS to send all DHCP requests to the primary DHCP server, while the secondary servers are used only if the primary server does not respond. The different DHCP servers are specified using the **cable helper** commands.

Beginning with Cisco IOS Release 12.2(33)SCD5, the GIADDR option simply changes the source IP address of the DHCP request so that the DHCP server can use different subnets to assign the right IP address depending on the types of CPE devices (namely cable modems, media terminal adapters [MTA], portal servers [PS], and set-top boxes [STB]). This enables faster processing of IP addresses; and in case the IP address does not belong to the subnets on the DHCP server, there is minimal usage of CPU resources.

DHCP Relay Agent Sub-option

The Cisco IOS Release 12.2(33)SCF2 introduces support for the DHCP Relay Agent Information sub-option (DHCP Option 82, Suboption 9) enhancement to simplify provisioning of the CPE devices. Using this sub-option, the cable operators can relay the service class or QoS information of the CPE to the DHCP server to get an appropriate IP address.

To provision a CPE, the DHCP server should be made aware of the service class or QoS information of the CPE. The DHCP server obtains this information using the DHCP DISCOVER message, which includes the service class or QoS information of the CM behind which the CPE resides.

During the provisioning process, the Cisco CMTS uses the DHCPv4 Relay Agent Information sub-option to advertise information about the service class or QoS profile of the CMs to the DHCP server. Using the same technique, the CPE information is relayed to the DHCP server to get an appropriate IP address.

To enable the service classes option, the service class name specified in the CM configuration file must be configured on the Cisco CMTS. This is done by using the **cable dhcp-insert service-class** command.

To configure service-class or QoS-profile on the Cisco CMTS, see Configuring DHCP Service, on page 97.

Note To insert service class relay agent information option into the DHCP DISCOVER messages, the **ip dhcp relay information option-insert** command must be configured on the bundle interface.

Time-of-Day Server

The Cisco CMTS can function as a ToD server that provides the current date and time to the cable modems and other customer premises equipment (CPE) devices connected to its cable interfaces. This allows the cable modems and CPE devices to accurately timestamp their Simple Network Management Protocol (SNMP) messages and error log entries, as well as ensure that all of the system clocks on the cable network are synchronized to the same system time.

Tip The initial ToD server on the Cisco CMTS did not work with some cable modems that used an incompatible packet format. This problem was resolved in Cisco IOS Release 12.1(8)EC1 and later 12.1 EC releases, and in Cisco IOS Release 12.2(4)BC1 and later 12.2 BC releases.

The DOCSIS 1.0 and 1.1 specifications require that all DOCSIS cable modems request the following time-related fields in the DHCP request they send during their initial power-on provisioning:

- Time Offset (option 2)—Specifies the time zone for the cable modem or CPE device, in the form of the number of seconds that the device's timestamp is offset from Greenwich Mean Time (GMT).
- Time Server Option (option 4)—Specifies one or more IP addresses for a ToD server.

After a cable modem successfully acquires a DHCP lease time, it then attempts to contact one of the ToD servers provided in the list provided by the DHCP server. If successful, the cable modem updates its system clock with the time offset and timestamp received from the ToD server.

If a ToD server cannot be reached or if it does not respond, the cable modem eventually times out, logs the failure with the CMTS, and continues on with the initialization process. The cable modem can come online without receiving a reply from a ToD server, but it must periodically continue to reach the ToD server at least once in every five-minute period until it successfully receives a ToD reply. Until it reaches a ToD server, the cable modem must initialize its system clock to midnight on January 1, 1970 GMT.

Note Initial versions of the DOCSIS 1.0 specification specified that the cable device must obtain a valid response from a ToD server before continuing with the initialization process. This requirement was removed in the released DOCSIS 1.0 specification and in the DOCSIS 1.1 specifications. Cable devices running older firmware that is compliant with the initial DOCSIS 1.0 specification, however, might require receiving a reply from a ToD server before being able to come online.

Because cable modems will repeatedly retry connecting with a ToD server until they receive a successful reply, you should consider activating the ToD server on the Cisco CMTS, even if you have one or more other ToD servers at the headend. This ensures that an online cable modem will always be able to connect with the ToD server on the Cisco CMTS, even if the other servers go down or are unreachable because of network congestion, and therefore will not send repeated ToD requests.

Tip To be able to use the Cisco CMTS as the ToD server, either alone or with other, external servers, you must configure the DHCP server to provide the IP address Cisco CMTS as one of the valid ToD servers (DHCP option 4) for cable modems. See Creating and Configuring a DHCP Address Pool for Cable Modems, on page 98 for details on this configuration.

In addition, although the DOCSIS specifications do not require that a cable modem successfully obtain a response from a ToD server before coming online, not obtaining a timestamp could prevent the cable modem from coming online in the following situations:

- If DOCSIS configuration files are being timestamped, to prevent cable modems from caching the files and replaying them, the clocks on the cable modem and CMTS must be synchronized. Otherwise, the cable modem cannot determine whether a DOCSIS configuration file has the proper timestamp.
- If cable modems register using Baseline Privacy Interface Plus (BPI+) authentication and encryption, the clocks on the cable modem and CMTS must be synchronized. This is because BPI+ authorization requires that the CMTS and cable modem verify the timestamps on the digital certificates being used for authentication. If the timestamps on the CMTS and cable modem are not synchronized, the cable modem cannot come online using BPI+ encryption.

Note DOCSIS cable modems must use RFC 868 -compliant ToD server to obtain the current system time. They cannot use the Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) service for this purpose. However, the Cisco CMTS can use an NTP or SNTP server to set its own system clock, which can then be used by the ToD server. Otherwise, you must manually set the clock on the CMTS using the **clock set** command each time that the CMTS boots up.

Tip Additional servers can be provided by workstations or PCs installed at the cable headend. UNIX and Solaris systems typically include a ToD server as part of the operating system, which can be enabled by putting the appropriate line in the inetd.conf file. Windows systems can use shareware servers such as Greyware and Tardis. The DOCSIS specifications require that the ToD servers use the User Datagram Protocol (UDP) protocol instead of the TCP protocol for its packets.

TFTP Server

All Cisco CMTS platforms can be configured to provide a TFTP server that can provide the following types of files to DOCSIS cable modems:

- DOCSIS Configuration File—After a DOCSIS cable modem has acquired a DHCP lease and attempted to contact a ToD server, the cable modem uses TFTP to download a DOCSIS configuration file from an authorized TFTP server. The DHCP server is responsible for providing the name of the DOCSIS configuration file and IP address of the TFTP server to the cable modem.
- Software Upgrade File—If the DOCSIS configuration file specifies that the cable modem must be running a specific version of software, and the cable modem is not already running that software, the cable modem must download that software file. For security, the cable operator can use different TFTP servers for downloading DOCSIS configuration files and for downloading new software files.
- Cisco IOS Configuration File—The DOCSIS configuration file for Cisco cable devices can also specify that the cable modem should download a Cisco IOS configuration file that contains command-line interface (CLI) configuration commands. Typically this is done to configure platform-specific features such as voice ports or IPSec encryption.

Note Do not confuse the DOCSIS configuration file with the Cisco IOS configuration file. The DOCSIS configuration file is a binary file in the particular format that is specified by the DOCSIS specifications, and each DOCSIS cable modem must download a valid file before coming online. In contrast, the Cisco IOS configuration file is an ASCII text file that contains one or more Cisco IOS CLI configuration commands. Only Cisco cable devices can download a Cisco IOS file.

All Cisco CMTS platforms can be configured as TFTP servers that can upload these files to the cable modem. The files can reside on any valid device but typically should be copied to the Flash memory device inserted into the Flash disk slot on the Cisco CMTS.

In addition, the Cisco CMTS platform supports an internal DOCSIS configuration file editor in Cisco IOS Release 12.1(2)EC, Cisco IOS Release 12.2(4)BC1, and later releases. When you create a DOCSIS configuration file using the internal configuration file editor, the CMTS stores the configuration file in the form of CLI commands. When a cable modem requests the DOCSIS configuration file, the CMTS then dynamically creates the binary version of the file and uploads it to the cable modem.

Note The internal DOCSIS configuration file editor supports only DOCSIS 1.0 configuration files. To create DOCSIS 1.1 configuration files, you must use a separate configuration editor, such as the Cisco DOCSIS Configurator tool, which at the time of this document's publication is available on Cisco.com at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/cpe-conf

For enhanced security, current versions of Cisco IOS software for Cisco CMTS platforms include a "TFTP Enforce" feature (**cable tftp-enforce** command) that allows you to require that all cable modems must attempt a TFTP download through the cable interface before being allowed to come online. This prevents a common theft-of-service attack in which hackers reconfigure their local network so that a local TFTP server downloads an unauthorized DOCSIS configuration file to the cable modem. This ensures that cable modems download only a DOCSIS configuration file that provides the services they are authorized to use.

Benefits

- The "all-in-one" configuration allows you to set up a basic cable modem network without having to invest in additional servers and software. This configuration can also help troubleshoot plant and cable modem problems.
- The DHCP configuration can more effectively assigns and manages IP addresses from specified address pools within the CMTS to the cable modems and their CPE devices.
- The Cisco CMTS can act as a primary or backup ToD server to ensure that all cable modems are synchronized with the proper date and time before coming online. This also enables cable modems to come online more quickly because they will not have to wait for the ToD timeout period before coming online.
- The ToD server on the Cisco CMTS ensures that all devices connected to the cable network are using the same system clock, making it easier for you to troubleshoot system problems when you analyze the debugging output and error logs generated by many cable modems, CPE devices, the Cisco CMTS, and other services.
- The Cisco CMTS can act as a TFTP server for DOCSIS configuration files, software upgrade files, and Cisco IOS configuration files.
- Aa separate workstation or PC is not required to create and store DOCSIS configuration files.
- The "TFTP Enforce" feature ensures that users download only an authorized DOCSIS configuration file and prevents one of the most common theft-of-service attacks.

How to Configure DHCP, ToD, and TFTP Services

See the following configuration tasks required to configure DHCP service, time-of-day service, and TFTP service on a Cisco CMTS:

All procedures are required unless marked as optional (depending on the desired network configuration and applications).

Configuring DHCP Service

To configure the DHCP server on the Cisco CMTS, use the following procedures to create the required address pools for the server to use. You can create one pool for all DHCP requests (cable modems and CPE devices), or separate pools for cable modems and for CPE devices, as desired.

Creating and Configuring a DHCP Address Pool for Cable Modems

To use the DHCP server on the Cisco CMTS, you must create at least one address pool that defines the IP addresses and other network parameters that are given to cable modems that make DHCP requests. To create an address pool, use the following procedure, beginning in EXEC mode. Repeat this procedure as needed to create additional address pools.

DETAILED STEPS

	Command or Action	Purpose

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

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

Step 3	**ip dhcp pool** *name*
	
	Example:
	
	`Router(config)# ip dhcp pool local`
	`Router(dhcp-config)#`
		Creates a DHCP address pool and enters DHCP pool configuration file mode. The *name* can be either an arbitrary string, such as **service**, or a number, such as **1**.

Step 4	**network** *network-number* [*mask*]
	
	Example:
	
	`Router(dhcp-config)# network 10.10.10.0 255.255.0.0`
	`Router(dhcp-config)#`
		Configures the address pool with the specified *network-number* and subnet *mask* , which are the DHCP *yiaddr* field and Subnet Mask (DHCP option 1) field. If you do not specify the *mask* value, it s to 255.255.255.255.
		Note To create an address pool with a single IP address, use the **host** command instead of **network**.

Step 5	**bootfile** *filename*
	
	Example:
	
	`Router(dhcp-config)# bootfile platinum.cm`
	`Router(dhcp-config)#`
		Specifies the name of the default DOCSIS configuration file (the DHCP *file* field) for the cable modems that are assigned IP addresses from this pool. The *filename* should be the exact name (including path) that is used to request the file from the TFTP server.

Step 6	**next-server** *address* [*address2 ...address8*]
	
	Example:
	
	`Router(dhcp-config)# next-server 10.10.11.1`
	`Router(dhcp-config)#`
		Specifies the IP address (the DHCP *siaddr* field) for the next server in the boot process of a DHCP client. For DOCSIS cable modems, this is the IP address for the TFTP server that provides the DOCSIS configuration file. You must specify at least one IP address, and can optionally specify up to eight IP addresses, in order of preference.

	Command or Action	Purpose

Step 7	**default-router** *address* [*address2 ...address8*]
	
	Example:
	
	`Router(dhcp-config)# default-router 10.10.10.12`
	`Router(dhcp-config)#`
		Specifies the IP address for the Router Option (DHCP option 3) field, which is the default router for the cable modems in this address pool. You must specify at least one IP address, and can optionally specify up to eight IP addresses, where the default routers are listed in their order of preference (*address* is the most preferred server, *address2* is the next most preferred, and so on).
		
		Note The first IP address must be the IP address for the cable interface that is connected to cable modems using this DHCP pool.

Step 8	**option 2 hex** *gmt-offset*
	
	Example:
	
	`Router(dhcp-config)# option 2 hex FFFF.8F80`
	`Router(dhcp-config)#`
		Specifies the Time Offset field (DHCP option 2), which is the local time zone, specified as the number of seconds, in hexadecimal, offset from Greenwich Mean Time (GMT). The following are some sample values for *gmt-offset* :
		
		FFFF.8F80 = Offset of –8 hours (–28800 seconds, Pacific Time) FFFF.9D90 = Offset of –7 hours (Mountain Time) FFFF.ABA0 = Offset of –6 hours (Central Time) FFFF.B9B0 = Offset of –5 hours (Eastern Time)

Step 9	**option 4 ip** *address* [*address2 ...address8*]
	
	Example:
	
	`Router(dhcp-config)# option 4 ip 10.10.10.13 10.10.11.2`
	`Router(dhcp-config)#`
		Specifies the Time Server Option field (DHCP option 4), which is the IP address of the time-of-day (ToD) server from which the cable modem can obtain its current date and time.
		
		You must specify at least one IP address, and can optionally specify up to eight IP addresses, listed in their order of preference.
		
		Note If you want to use the Cisco CMTS as the ToD server, you must enter its IP address as part of this command.

Step 10	**option 7 ip** *address* [*address2 ...address8*]
	
	Example:
	
	`Router(dhcp-config)# option 7 ip 10.10.10.13`
	`Router(dhcp-config)#`
		(Optional) Specifies the Log Server Option field (DHCP option 7), which is the IP address for a System Log (SYSLOG) server that the cable modem should send error messages and other logging information.
		
		You can optionally specify up to eight IP addresses, listed in their order of preference.

Step 11	**lease**{*days* [*hours*][*minutes*]|**infinite**}
	
	Example:
	
	`Router(dhcp-config)# lease 0 12 30`
	`Router(dhcp-config)#`
		Specifies the IP Address Lease Time (option 51), which is the duration of the lease for the IP address that is assigned to the cable modem. Before the lease expires, the cable modem must make another DHCP request to remain online. The default is one day.
		
		You can specify the lease time as follows:
		
		• *days* —Duration of the lease in numbers of days (0 to 365).
		
		• *hours* — Number of hours in the lease (0 to 23, optional). A *days* value must be supplied before you can configure an *hours* value.
		
		• *minutes* — Number of minutes in the lease (0 to 59, optional). A *days* value and an *hours* value must be supplied before you can configure a *minutes* value.
		
		• **infinite**— Unlimited lease duration.
		
		Note In most cable networks, cable modems cannot come online if the lease time is less than 3 minutes. For stability in most cable networks, the minimum lease time should be 5 minutes.

	Command or Action	Purpose

Step 12	**client-identifier** *unique-identifier*
	
	Example:
	
	`Router(dhcp-config)# client-identifier 0100.0C01.0203.04`
	
	`Router(dhcp-config)#`
		(Optional) Specifies the MAC address that identifies the particular cable modem that should receive the parameters from this pool. The unique-identifier is created by combining the one-byte Ethernet identifier ("01") with the six-byte MAC address for the cable modem. For example, to specify a cable modem with the MAC address of 9988.7766.5544, specify a *unique-identifier* of 0199.8877.6655.44.
		
		Note This option should be used only for DHCP pools that assign a static address to a single cable modem.

Step 13	**cable dhcp-insert** {**downstream-description** | **hostname** | **service-class** | **upstream-description**}
	
	Example:
	
	`Router(dhcp-config)# cable dhcp-insert service-class`
	`Router(dhcp-config)#`
		(Optional) Specifies which descriptors to append to DHCP packets. The DHCP server can then use these descriptors to identify cable modem clones and extract geographical information:
		
		• **downstream-description—** Appends received DHCP packets with downstream port descriptors.
		• **hostname—** Appends received DHCP packets with router host names.
		• **service-class—** Appends received DHCP packets with router service class.
		• **upstream-description—** Appends received DHCP packets with upstream port descriptors.
		
		Note Multiple types of descriptor strings can be configured as long as the maximum relay information option size is not exceeded.

Step 14	**exit**
	
	Example:
	
	`Router(dhcp-config)# exit`
	`Router(config)#`
		Exits DHCP configuration mode.

Step 15	**exit**
	
	Example:
	
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Creating and Configuring a DHCP Address Pool for CPE Devices

In addition to providing IP addresses for cable modems, the DHCP server on the Cisco CMTS server can optionally provide IP addresses and other network parameters to the customer premises equipment (CPE) devices that are connected to the cable modems on the network. To do so, create a DHCP address pool for those CPE devices, using the following procedure, beginning in EXEC mode. Repeat this procedure as needed to create additional address pools.

Note You can use the same address pools for cable modems and CPE devices, but it simplifies network management to maintain separate pools.

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 dhcp pool** *name* **Example:** `Router(config)# ip dhcp pool local`	Creates a DHCP address pool and enters DHCP pool configuration file mode. The *name* can be either an arbitrary string, such as **service**, or a number, such as **1**.
Step 4	**network** *network-number* [*mask*] **Example:** `Router(dhcp-config)# network 10.10.10.0 255.255.0.0`	Configures the address pool with the specified *network-number* and subnet *mask* , which are the DHCP *yiaddr* field and Subnet Mask (DHCP option 1) field. If you do not specify the *mask* value, it defaults to 255.255.255.255. **Note** To create an address pool with a single IP address, use the **host** command instead of **network**.
Step 5	**default-router** *address* [*address2 ...address8*] **Example:** `Router(dhcp-config)# default-router 10.10.10.12`	Specifies the IP address for the Router Option (DHCP option 3) field, which is the default router for the cable modems and CPE devices in this address pool. You must specify at least one IP address, and can optionally specify up to eight IP addresses, where the default routers are listed in order of preference (*address* is the most preferred server, *address2* is the next most preferred, and so on).
Step 6	**dns-server** *address* [*address2 ...address8*] **Example:** `Router(dhcp-config)# dns-server 10.10.10.13`	Specifies one or more IP address for the Domain Name Server Option (DHCP option 6) field, which are the domain name system (DNS) servers that will resolve host names to IP addresses for the CPE devices. You must specify at least one IP address, and can optionally specify up to eight IP addresses, listed in order of preference.
Step 7	**domain-name***domain* **Example:** `Router(dhcp-config)# domain-name cisco.com`	Specifies the Domain Name (DHCP option 15) field, which is the fully-qualified domain name that the CPE devices should add to their hostnames. The *domain* parameter should be the domain name used by devices on the cable network.

	Command or Action	Purpose
Step 8	**lease** {*days* [*hours*][*minutes*]|**infinite**} **Example:** `Router(dhcp-config)# lease 0 12 30`	Specifies the IP Address Lease Time (option 51), which is the duration of the lease for the IP address that is assigned to the CPE device. Before the lease expires, the CPE device must make another DHCP request to remain online. The default is one day. You can specify the lease time as follows: • *days* **—**Duration of the lease in numbers of days (0 to 365). • *hours* **—** Number of hours in the lease (0 to 23, optional). A *days* value must be supplied before you can configure an *hours* value. • *minutes* **—** Number of minutes in the lease (0 to 59, optional). A *days* value and an *hours* value must be supplied before you can configure a *minutes* value. • **infinite —** Unlimited lease duration.
Step 9	**client-identifier** *unique-identifier* **Example:** `Router(dhcp-config)# client-identifier 0100.0C01.0203.04`	(Optional) Specifies the MAC address that identifies a particular CPE device that should receive the parameters from this pool. The unique-identifier is created by combining the one-byte Ethernet identifier ("01") with the six-byte MAC address for the device. For example, so specify a device with the MAC address of 9988.7766.5544, specify a unique-identifier of 0199.8877.6655.44. **Note** This option should be used only for DHCP pools that assign a static address to a single CPE device.
Step 10	**cable dhcp-insert** {**downstream-description** | **hostname** | **service-class** | **upstream-description**} **Example:** `Router(dhcp-config)# cable dhcp-insert service-class`	(Optional) Specifies which descriptors to append to DHCP packets. The DHCP server can then use these descriptors to identify CPEs and extract geographical information: • **downstream-description—** Appends received DHCP packets with downstream port descriptors. • **hostname—** Appends received DHCP packets with router host names. • **service-class—** Appends received DHCP packets with router service class. • **upstream-description—** Appends received DHCP packets with upstream port descriptors.
Step 11	**exit** **Example:** `Router(dhcp-config)# exit`	Exits DHCP configuration mode.
Step 12	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring Time-of-Day Service

This section provides procedures for enabling and disabling the time-of-day (ToD) server on the Cisco CMTS routers.

Prerequisites

To be able to use the Cisco CMTS as the ToD server, either alone or with other, external servers, you must configure the DHCP server to provide the IP address Cisco CMTS as one of the valid ToD servers (DHCP option 4) for cable modems. See Creating and Configuring a DHCP Address Pool for Cable Modems for details on this configuration when using the internal DHCP server.

Enabling Time-of-Day Service

To enable the ToD server on a Cisco CMTS, use the following procedure, beginning in EXEC mode.

DETAILED STEPS

	Command or Action	Purpose

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

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

Step 3	**service udp-small-servers max-servers no-limit**
	
	Example:
	
	`Router(config)# service udp-small-servers max-servers no-limit`
	`Router(config)#`
		Enables use of minor servers that use the UDP protocol (such as ToD, echo, chargen, and discard).
		
		The max-servers no-limit option allows a large number of cable modems to obtain the ToD server at one time, in the event that a cable or power failure forces many cable modems offline. When the problem has been resolved, the cable modems can quickly reconnect.

Step 4	**cable time-server**
	
	Example:
	
	`Router(config)# cable time-server`
	`Router(config)#`
		Enables the ToD server on the Cisco CMTS.

	Command or Action	Purpose

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

Disabling Time-of-Day Service

To disable the ToD server, use the following procedure, beginning in EXEC mode.

DETAILED STEPS

	Command or Action	Purpose

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

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

Step 3	**no cable time-server**
	
	Example:
	
	`Router(config)# cable time-server`
	`Router(config)#`
		Disables the ToD server on the Cisco CMTS.

Step 4	**no service udp-small-servers**
	
	Example:
	
	`Router(config)# no service udp-small-servers`
	`Router(config)#`
		(Optional) Disables the use of all minor UDP servers.
		
		Note Do not disable the minor UDP servers if you are also enabling the other DHCP or TFTP servers.

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

Configuring TFTP Service

To configure TFTP service on a Cisco CMTS where the CMTS can act as a TFTP server and download a DOCSIS configuration file to cable modems, perform the following steps:

- Create the DOCSIS configuration files using the DOCSIS configuration editor of your choice.
- You can also use the internal DOCSIS configuration file editor on the Cisco CMTS to create DOCSIS configuration files.
- Copy all desired files (DOCSIS configuration files, software upgrade files, and Cisco IOS configuration files) to the Flash memory device on the Cisco CMTS. Typically, this is done by placing the files first on an external TFTP server, and then using TFTP commands to transfer them to the router's Flash memory.

Note If you are using the internal DOCSIS configuration editor on the Cisco CMTS to create the DOCSIS configuration files, you do not need to copy the files to a Flash memory device because they are already part of the router's configuration.

- Enable the TFTP server on the Cisco CMTS with the **tftp-server** command.
- Optionally enable the TFTP enforce feature so that cable modems must attempt a TFTP download of the DOCSIS configuration file through the cable interface with the CMTS before being allowed to come online.

Each configuration task is required unless otherwise listed as optional.

Step 1 Use the **show file systems** command to display the Flash memory cards that are available on your CMTS, along with the free space on each card and the appropriate device names to use to access each card.
Most configurations of the Cisco CMTS platforms support both linear Flash and Flash disk memory cards. Linear Flash memory is accessed using the **slot0** (or **flash**) and **slot1** device names. Flash disk memory is accessed using the **disk0** and **disk1** device names.

For example, the following command shows a Cisco uBR7200 series router that has two linear Flash memory cards installed. The cards can be accessed by the **slot0** (or **flash**) and **slot1** device names.

Example:

```
Router# show file systems

File Systems:
     Size(b)     Free(b)      Type  Flags  Prefixes
    48755200    48747008     flash     rw   slot0: flash:
    16384000    14284000     flash     rw   slot1:
    32768000    31232884     flash     rw   bootflash:
*          -           -      disk     rw   disk0:
           -           -      disk     rw   disk1:
           -           -    opaque     rw   system:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
      522232      507263     nvram     rw   nvram:
           -           -   network     rw   rcp:
```

```
           -           -   network     rw   ftp:
           -           -   network     rw   scp:
Router#
```

The following example shows a Cisco uBR10012 router that has two Flash disk cards installed. These cards can be accessed by the **disk0** and **sec-disk0** device names.

Example:

```
Router# show file systems

File Systems:
     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -     flash     rw   slot0: flash:
           -           -     flash     rw   slot1:
    32768000    29630876     flash     rw   bootflash:
*  128094208    95346688      disk     rw   disk0:
           -           -      disk     rw   disk1:
           -           -    opaque     rw   system:
           -           -     flash     rw   sec-slot0:
           -           -     flash     rw   sec-slot1:
*  128094208    95346688      disk     rw   sec-disk0:
           -           -      disk     rw   sec-disk1:
    32768000    29630876     flash     rw   sec-bootflash:
           -           -     nvram     rw   sec-nvram:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
      522232      505523     nvram     rw   nvram:
           -           -   network     rw   rcp:
           -           -   network     rw   ftp:
           -           -   network     rw   scp:
Router#
```

Tip The Cisco uBR10012 router supports redundant processors, a primary and a secondary, and each processor contains its own Flash memory devices. You typically do not have to copy files to the secondary Flash memory devices (which have the **sec** prefix) because the Cisco uBR10012 router synchronizes the secondary processor to the primary one.

Step 2 Verify that the desired Flash memory card has sufficient free space for all of the files that you want to copy to the CMTS.

Step 3 Use the **ping** command to verify that the remote TFTP server that contains the desired files is reachable. For example, the following shows a **ping** command being given to an external TFTP server with the IP address of 10.10.10.1:

Example:

```
Router# ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/6 ms
```

Step 4 Use the **copy tftp** *devname* command to copy each file from the external TFTP server to the appropriate Flash memory card on the CMTS, where *devname* is the device name for the destination Flash memory card. You will then be prompted for the IP address for the external TFTP server and the filename for the file to be transferred.
The following example shows the file docsis.cm being transferred from the external TFTP server at IP address 10.10.10.1 to the first Flash memory disk (disk0):

Example:

```
Router# copy tftp disk0
Address or name of remote host []? 10.10.10.1

Source filename []? config-files/docsis.cm
```

```
Destination filename [docsis.cm]?
Accessing tftp://10.10.10.1/config-file/docsis.cm......
Loading docsis.cm from 10.10.10.1 (via Ethernet2/0): !!!
[OK - 276/4096 bytes]
276 bytes copied in 0.152 secs
Router#
```

Step 5 Repeat Step 4, on page 106 as needed to copy all of the files from the external TFTP server to the Flash memory card on the Cisco CMTS.

Step 6 Use the **dir** command to verify that the Flash memory card contains all of the transferred files.

Example:

```
Router# dir disk0:

Directory of disk0:/
    1  -rw-    10705784   May 30 2002 19:12:46  ubr10k-p6-mz.122-2.8.BC
    2  -rw-        4772   Jun 20 2002 18:12:56  running.cfg.save
    3  -rw-         241   Jul 31 2002 18:25:46  gold.cm
    4  -rw-         225   Jul 31 2002 18:25:46  silver.cm
    5  -rw-         231   Jul 31 2002 18:25:46  bronze.cm
    6  -rw-          74   Oct 11 2002 21:41:14  disable.cm
    7  -rw-     2934028   May 30 2002 11:22:12  ubr924-k8y5-mz.bin
    8  -rw-     3255196   Jun 28 2002 13:53:14  ubr925-k9v9y5-mz.bin
128094208 bytes total (114346688 bytes free)
Router#
```

Step 7 Use the **configure terminal** command to enter global configuration mode:

Example:

```
Router# configure terminal

Router(config)#
```

Step 8 Use the **tftp-server** command to specify which particular files can be transferred by the TFTP server that is onboard the Cisco CMTS. You can also use the **alias** option to specify a different filename that the DHCP server can use to refer to the file. For example, the following commands enable the TFTP transfer of the configuration files and software upgrade files:

Example:

```
Router(config)# tftp-server disk0:gold.cm alias gold.cm

Router(config)# tftp-server disk0:silver.cm alias silver.cm

Router(config)# tftp-server disk0:bronze.cm alias bronze.cm

Router(config)# tftp-server disk0:ubr924-k8y5-mz.bin alias ubr924-codefile

Router(config)# tftp-server disk0:ubr925-k9v9y5-mz.bin alias ubr925-codefile

Router(config)#
```

Note The **tftp-server** command also supports the option of specifying an access list that restricts access to the particular file to the IP addresses that match the access list.

Step 9 (Optional) Use the following command to enable the use of the UDP small servers, and to allow an unlimited number of connections at one time. This will allow a large number of cable modems that have gone offline due to cable or power failure to rapidly come back online.

Example:

```
Router(config)# service udp-small-servers max-servers no-limit
```

```
Router(config)#
```

Step 10 (Optional) Use the **cable tftp-enforce** command in interface configuration mode to require that each cable modem perform a TFTP download of its DOCSIS configuration file through its cable interface with the CMTS before being allowed to come online. This can prevent the most common types of theft-of-service attacks in which users configure their local networks so as to download an unauthorized configuration file to their cable modems.

Example:

```
Router(config)# interface cable
x/y

Router(config-if)# cable tftp-enforce

Router(config-if)#
```

You can also specify the **mark-only** option so that cable modems can come online without attempting a TFTP download, but the cable modems are marked in the **show cable modems** command so that network administrators can investigate the situation further before taking any action.

Example:

```
Router(config)# interface cable
x/y

Router(config-if)# cable tftp-enforce mark-only

Router(config-if)#
```

Configuring A Basic All-in-One Configuration

The basic all-in-one configuration requires configuring the DHCP, ToD, and TFTP servers, as described in the following sections in this document:

You must also have the necessary DOCSIS configuration files available for the TFTP server. You can do this in two ways:

- Create the DOCSIS configuration files using the Cisco DOCSIS Configurator tool, and then copy them to the Flash memory device. For instructions on copying the configuration files to Flash memory, see the Configuring TFTP Service, on page 105.
- Dynamically create the DOCSIS configuration files with the **cable config-file** command.

For an example of a basic all-in-one configuration, see the Basic All-in-One Configuration Example, on page 118.

Configuring an Advanced All-in-One Configuration

The advanced all-in-one configuration sample is identical to the basic configuration except that it uses a hierarchy of DHCP pools. Any DHCP pool with a network number that is a subset of another pool's network number inherits all the characteristics of that other pool. This saves having to repeat identical commands in the multiple DHCP pool configurations.

For information on the required tasks, see the following sections in this guide:

You must also have the necessary DOCSIS configuration files available for the TFTP server. You can do this in two ways:

- Create the DOCSIS configuration files using the Cisco DOCSIS Configurator tool, and then copy them to the Flash memory device. For instructions on copying the configuration files to Flash memory, see the Configuring TFTP Service, on page 105.
- Dynamically create the DOCSIS configuration files with the **cable config-file** command.

For an example of an advanced all-in-one configuration, see the Advanced All-in-One Configuration Example, on page 121.

Optimizing the Use of an External DHCP Server

The Cisco CMTS offers a number of options that can optimize the operation of external DHCP servers on a DOCSIS cable network. See the following sections for details. All procedures are optional, depending on the needs of your network and application servers.

Configuring Cable Source Verify Option

To enhance security when using external DHCP servers, you can optionally configure the Cable Source Verify feature with the following procedure.

Restriction

- The Cable Source Verify feature supports only external DHCP servers. It cannot be used with the internal DHCP server.

DETAILED STEPS

	Command or Action	Purpose

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

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

	Command or Action	Purpose

Step 3	**interface cable** *x/y*
	
	Example:
	
	`Router(config)# interface cable 4/0`
	`Router(config-if)#`
		Enters cable interface configuration mode for the specified cable interface.

Step 4	**cable source-verify** [**dhcp** | **leasetimer** *value*]
	
	Example:
	
	`Router(config-if)# cable source-verify dhcp`
	
	Example:
	
	`Router(config-if)# cable source-verify leasetimer 30`
	`Router(config-if)#`
		(Optional) Ensures that the CMTS allows network access only to those IP addresses that DCHP servers issued to devices on this cable interface. The CMTS examines DHCP packets that pass through the cable interfaces to build a database of which IP addresses are valid on which interface.
		• **dhcp** = (Optional) Drops traffic from all devices with unknown IP addresses, but the CMTS also sends a query to the DHCP servers for any information about the device. If a DHCP server informs the CMTS that the device has a valid IP address, the CMTS then allows the device on the network.
		• **leasetimer** *value* = (Optional) Specifies how often, in minutes, the router should check its internal CPE database for IP addresses whose lease times have expired. This can prevent users from taking DHCP-assigned IP addresses and assigning them as static addresses to their CPE devices. The valid range for value is 1 to 240 minutes, with no default.
		
		Note The **leasetimer** option takes effect only when the **dhcp** option is also used on an interface.

Step 5	**no cable arp**
	
	Example:
	
	`Router(config-if)# no cable arp`
	`Router(config-if)#`
		(Optional) Blocks Address Resolution Protocol (ARP) requests originating from devices on the cable network. Use this command, together with the **cable source-verify dhcp** command, to block certain types of theft-of-service attacks that attempt to hijack or spoof IP addresses.
		
		Note Repeat Step 3, on page 110 through Step 5, on page 110 for each desired cable interface.

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

Step 7	**ip dhcp relay information option**
	
	Example:
	
	`Router(config)# ip dhcp relay information option`
	`Router(config)#`
		(Optional) Enables the CMTS to insert DHCP relay information (DHCP option 82) in relayed DHCP packets. This allows the DHCP server to store accurate information about which CPE devices are using which cable modems. You should use this command if you are also using the **cable source-verify dhcp** command.

Step 8	**exit** **Example:**	Exits global configuration mode.

	Command or Action	Purpose

	Note Cisco IOS releases before Release 12.1(2)EC1 used the **cable relay-agent-option** command for this purpose, but current releases should use the **ip dhcp relay information option** command.
	`Router(config)# exit`
	`Router#`	

Configuring Prefix-based Source Address Verification

To enhance security when using external DHCP servers, you can configure a prefix-based SAV with the following procedure, beginning in global configuration (config) mode.

DETAILED STEPS

	Command or Action	Purpose

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

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

Step 3	cable source-verify enable-sav-static
	Example:
	`Router# cable source-verify enable-sav-static`
	`Router(config)#`
		Enables SAV prefix processing on the Cisco CMTS.

Step 4	**cable source-verify group** *groupname* **Example:** `Router(config)# cable source-verify group sav-1`	Configures the SAV group name. *groupname*— Name of the SAV group with a maximum length of 16 characters.
Step 5	**prefix** [**ipv4_prefix/ipv4_prefix_length** | **ipv6_prefix/ipv6_prefix_length**]	Configures the IPv4 or IPv6 prefix associated with the SAV group. • *ipv4_prefix*— IPv4 prefix associated with the SAV group, specified in the X.X.X.X/X format.

	Command or Action	Purpose

	Example:
	`Router(config-sav)# prefix 10.10.10.0/24`
	`Router(config-sav)#`
		• ipv4_prefix_length—Length of the IPv4 prefix. The valid range is from 0 to 32.
		• ipv6_prefix—IPv6 prefix associated with a particular SAV group, specified in the X:X:X:X::/X format.
		• ipv6_prefix_length—Length of the IPv6 prefix. The valid range is from 0 to 128.
		A maximum of four prefixes can be configured in a single SAV group. These prefixes can be either IPv4s, IPv6s, or a combination of both.

Step 6	**exit** **Example:** `Router(config-sav)# exit`	Exits SAV configuration mode.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring Optional DHCP Parameters

When using an external DHCP server, the Cisco CMTS supports a number of options that can enhance operation of the cable network in certain applications. To configure these options, use the following procedure, beginning in EXEC mode.

DETAILED STEPS

	Command or Action	Purpose

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

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

	Command or Action	Purpose

Step 3	**ip dhcp smart-relay**
	
	Example:
	
	`Router(config)# ip dhcp smart-relay`
	`Router(config)#`
		(Optional) Enables the DHCP relay agent on the CMTS to automatically switch a cable modem or CPE device to a secondary DHCP server or address pool if the primary DHCP server does not respond to three successive requests. If multiple secondary servers have been defined, the relay agent forwards DHCP requests to the secondary servers in a round robin fashion.

Step 4	**ip dhcp ping packet 0**
	
	Example:
	
	`Router(config)# ip dhcp ping packet 0`
	`Router(config)#`
		(Optional) Instructs the DHCP server to assign an IP address from its pool without first sending an ICMP ping to test whether a client is already currently using that IP address. Disabling the ping option can speed up address assignment when a large number of modems are trying to connect at the same time. However, disabling the ping option can also result in duplicate IP addresses being assigned if users assign unauthorized static IP addresses to their CPE devices.
		
		Note By default, the DHCP server pings a pool address twice before assigning a particular address to a requesting client. If the ping is unanswered, the DHCP server assumes that the address is not in use and assigns the address to the requesting client.

Step 5	**ip dhcp relay information check**
	
	Example:
	
	`Router(config)# ip dhcp relay information check`
	`Router(config)#`
		(Optional) Configures the DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages. Invalid messages are dropped.
		
		Note The **ip dhcp relay information** command contains several other options that might be useful for special handling of DHCP packets. See its command reference page in the Cisco IOS documentation for details.

Step 6	**interface cable** *x/y*
	
	Example:
	
	`Router(config)# interface cable 4/0`
	`Router(config-if)#`
		Enters cable interface configuration mode for the specified cable interface.

Step 7	**cable dhcp-giaddr policy** [**host** | **stb** | **mta** | **ps**] *giaddr*
	
	Example:
	
	`Router(config-if)# cable dhcp-giaddr policy mta 172.1.1.10`
	`Router(config-if)#`
		Sets the DHCP GIADDR field for DHCP request packets to the primary address for cable modems, and the secondary address for CPE devices. This enables the use of separate address pools for different clients.
		
		• **host—**Specifies the GIADDR for hosts.
		• **mta—**Specifies the GIADDR for MTAs.
		• **ps—**Specifies the GIADDR for PSs.
		• **stb—**Specifies the GIADDR for STBs.
		• *giaddr***—**IP addresses of the secondary interface of the bundle interface.
		
		Note The **cable dhcp-giaddr** command also supports the **primary** option. The **primary** option forces all device types to use only the primary interface IP address as GIADDR and not rotate through the secondary address if the primary address fails.

Step 8	**cable helper-address** *address* [**cable-modem** | **host** | **mta** | **stb**]	(Optional) Enables load-balancing of DHCP requests from cable modems and CPE devices by specifying different DHCP servers according to the cable interface or

	Command or Action	Purpose

	Example:
	`Router(config-if)# cable helper-address 10.10.10.13`
	`Router(config-if)#`
		subinterface. You can also specify separate servers for cable modems and CPE devices.
		• *address* = IP address of a DHCP server to which UDP broadcast packets will be sent via unicast packets.
		• **cable-modem** = Specifies this server should only accept cable modem packets (optional).
		• **host** = Specifies this server should only accept CPE device packets (optional).
		• **mta**= Specifies this server should only accept MTA packets (optional). You must also complete Step 9, on page 114.
		• **stb** = Specifies this server should only accept STB packets (optional). You must also complete Step 9, on page 114.
		Note If you do not specify an option, the helper-address will support all cable devices, and the associated DHCP server will accept DHCP packets from all cable device classes.
		Note If you specify only one option, the other types of devices (cable modem, host, mta, or stb) will not be able to connect with a DHCP server. You must specify each desired option in a separate command
		Tip Repeat this command to specify more than one helper address on each cable interface. You can specify more than 16 helper addresses, but the Cisco IOS software uses only the first 16 valid addresses.
		Tip If you configure different helper addresses on different sub-bundles within a bundle, the cable modem may not come online. We recommend that you use the same helper address on all sub-bundles within a bundle.
		Note The **ip helper-address** command performs a similar function to **cable helper-address**, but it should be used on non-cable interfaces. The **cable helper-address** command should be used on cable interfaces because it is optimized for the operation of DHCP requests on DOCSIS networks.

Step 9	**cable dhcp-parse option-***optnum*
	Example:
	`Router(config-if)# cable dhcp-parse option-43`
	`Router(config-if)#`
		(Optional) Enables the parsing of certain DHCP options.
		• *optnum* = Specifies which option should be enabled. Valid values are **43** or **60**.
		Note If you specified the **mta** or **stb** option in Step 8, on page 113, you must parse DHCP packets to allow for the extraction of cable device classes.
		Tip If you know in advance that certain options are not used by your CMTS, you can disable their parsing using the **no cable dhcp-parse option-optnum** command.
		Note Repeat Step 6, on page 113 through Step 8, on page 113 for each desired cable interface.

Step 10	**cable dhcp-giaddr policy** **Example:** `Router(config-if)# cable dhcp-giaddr policy`	Selects the control policy, so the primary address is used for cable modems and the secondary addresses are used for hosts and other customer premises equipment (CPE) devices. This setting is typically used when the CMs on the interface are configured for routing mode, so that the cabel modems and hosts can use IP addresses on different subnets.

	Command or Action	Purpose

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

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

Configuration Examples

This section provides examples for the following configurations:

DHCP Server Examples

The following sections gave sample configurations for configuring DHCP pools for cable modems and CPE devices:

DHCP Pools for Cable Modems

The following examples show three typical DHCP pools for cable modems. Each pool includes the following fields:

- The dhcp pool command defines a unique string for the pool's name, which in this case identifies the DOCSIS configuration file that is to be downloaded to the cable modem.
- The **network** command defines the range of IP addresses for each pool.
- The **bootfile** command specifies the DOCSIS configuration file to be downloaded to the cable modem. In these examples, three DOCSIS configuration files are specified (platinum.cm, gold.cm, and silver.cm).
- The **next-server** command specifies the IP address for the TFTP server.
- The **default-router** command specifies the default gateway.
- The three **option** commands specify the time offset, ToD server, and log server.
- The **lease** command specifies that the DHCP lease expires in is 7 days, 0 hours, and 10 minutes. (The cable modem will typically attempt to renew the lease at the halfway mark of approximately 3 days and 12 hours.)

```
!
ip dhcp pool cm-platinum
```

```
   network 10.128.4.0 255.255.255.0
   bootfile platinum.cm
   next-server 10.128.4.1
   default-router 10.128.4.1
   option 2 hex ffff.8f80
   option 4 ip 10.1.4.1
   option 7 ip 10.1.4.1
   lease 7 0 10
!
ip dhcp pool cm-gold
   network 10.129.4.0 255.255.255.0
   bootfile gold.cm
   next-server 10.129.4.1
   default-router 10.129.4.1
   option 2 hex ffff.8f80
   option 4 ip 10.1.4.1
   option 7 ip 10.1.4.1
   lease 7 0 10
!
ip dhcp pool cm-silver
   network 10.130.4.0 255.255.255.0
   bootfile silver.cm
   next-server 10.130.4.1
   default-router 10.130.4.1
   option 2 hex ffff.8f80
   option 4 ip 10.1.4.1
   option 7 ip 10.1.4.1
   lease 7 0 10
```

DHCP Pools for Disabling Cable Modems

The following examples shows typical DHCP pool configurations for cable modems that disable network access for their attached CPE devices. With this configuration, the cable modem can come online and is able to communicate with the CMTS, but the CPE devices cannot access the cable network. Each pool includes the following fields:

- The DHCP pool name is a unique string that indicates the MAC address for each cable modem that should be disabled.
- The **host** option specifies a single static IP address.
- The **client-identifier** option identifies a particular cable modem to be denied access. The cable modem is identified by the combination of the Ethernet media code (“01”) plus the cable modem’s MAC address.
- The **bootfile** option specifies a DOCSIS configuration file (“disable.cm”) that disables network access.

```
!
ip dhcp pool DisabledModem(0010.aaaa.0001)
    host 10.128.1.9 255.255.255.0
    client-identifier  0100.10aa.aa00.01
    bootfile disable.cm
!
ip dhcp pool DisabledModem(0020.bbbb.0002)
    host 10.128.1.10 255.255.255.0
    client-identifier  0100.20bb.bb00.02
    bootfile disable.cm
ip dhcp pool DisabledModem(1010.9581.7f66)
   host 10.128.1.11 255.255.255.0
   client-identifier 0100.1095.817f.66
   bootfile disable.cm
```

DHCP Pools for CPE Devices

The following examples show a typical DHCP pool for CPE devices. Each pool includes the following fields:

- The **network** command defines the range of IP addresses to be assigned to the CPE devices. Typically, this command specifies a subnet in the secondary address range for the cable interface.
- The **default-router** command specifies the default gateway.
- The **dns-server** command specifies one or more IP addresses for the DNS name-resolution servers that the CPE devices should use.
- The **domain-name** command specifies the fully-qualified domain name that the CPE devices should use.
- The **lease** command specifies that the DHCP lease expires in is 7 days, 0 hours, and 10 minutes. (The CPE device will typically attempt to renew the lease at the halfway mark of approximately 3 days and 12 hours.)

```
!
ip dhcp pool hosts
    network 10.254.1.0 255.255.255.0
    default-router 10.254.1.1
    dns-server 10.254.1.1 10.128.1.1
    domain-name ExamplesDomainName.com
    lease 7 0 10
!
```

The following example shows a DHCP pool that assigns a permanent, static IP address to a particular CPE device. This example is identical to the previous pool except for the following commands:

- The **host** command is used (instead of the **network** command) to specify a single static IP address that will be assigned to the CPE device.
- The **client-identifier** command identifies the particular CPE device. The CPE device is identified by the combination of the Ethernet media code (“01”) plus the device’s MAC address (0001.dddd.0001).

```
!
ip dhcp pool staticPC(0001.dddd.0001)
    host 10.254.1.12 255.255.255.0
    client-identifier 0100.01dd.dd00.01
    default-router 10.254.1.1
    dns-server 10.254.1.1 10.128.1.1
    domain-name ExamplesDomainName.com
    lease 7 0 10
```

ToD Server Example

The following example shows a typical ToD server configuration:

```
service udp-small-servers max-servers no-limit
cable time-server
```

These are the only commands required to enable the ToD server.

TFTP Server Example

The following lines are an excerpt from a configuration that includes a TFTP server. Change the files listed with the **tftp-server** command to match the specific files that are on your system.

```
! Enable the user of unlimited small servers
 service udp-small-servers max-servers no-limit
!
...
! Enable the TFTP server and specify the files that can be
!   downloaded along with their aliases
 tftp-server disk0:gold.cm alias gold.cm
 tftp-server disk0:silver.cm alias silver.cm
 tftp-server disk0:bronze.cm alias bronze.cm
 tftp-server disk0:ubr924-k8y5-mz.bin alias ubr924-codefile
 tftp-server disk0:ubr925-k9v9y5-mz.bin alias ubr925-codefile
```

Basic All-in-One Configuration Example

The basic "all-in-one configuration" sample below summarizes all the components described in examples in the Configuration Examples, on page 115. Five DOCSIS configuration files are available. The internal DOCSIS configuration file editor has been used to create four (platinum.cm, gold.cm, silver.cm, and disable.cm), and the fifth file, bronze.cm, has been loaded on to the slot0 Flash memory device. The disable.cm file disables network access for all CPE devices attached to a cable modem, and the other four files provide different levels of Quality-of-Service (QoS).

The configuration has two DHCP pools with two different address spaces. One pool provides IP addresses and platinum-level service for cable modems, and the other pool provides IP addresses for CPE devices.

```
!
version 12.1
no service pad
! provides nice timestamps on all log messages
service timestamps debug datetime msec localtime
service timestamps log uptime
! turn service password-encryption on to encrypt passwords
no service password-encryption
! provides additional space for longer configuration file
service compress-config
! supports a large number of modems / hosts attaching quickly
service udp-small-servers max-servers no-limit
!
hostname Router
!
boot system disk0:
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
! permits cable modems to obtain Time of Day (TOD) from uBR7100
cable time-server
!
! High performance DOCSIS config file, additional options may be added
!   10 Mbit/sec download, 128 Kbit/sec upload speed, 10 Kbit/sec guaranteed upstream
! NOTE: cable upstream 0 admission-control 150 will prevent modems from
!   connecting after 150% of guaranteed-bandwidth has been allocated to
!   registered modems. This can be used for peek load balancing.
! max-burst 1600 prevents a modem with concatenation turned on from consuming
!   too much wire time, and interfering with VoIP traffic.
! cpe max 8 limits the modem to 8 hosts connected before the CMTS refuses
!   additional host MAC addresses.
! Timestamp option makes the config file only valid for a short period of time.
```

```
!
cable config-file platinum.cm
  service-class 1 max-upstream 128
  service-class 1 guaranteed-upstream 10
  service-class 1 max-downstream 10000
  service-class 1 max-burst 1600
  cpe max 8
  timestamp
!
! Medium performance DOCSIS config file, additional options may be added
!   5 Mbit/sec download, 128 Kbit/sec upload speed
!
cable config-file gold.cm
  service-class 1 max-upstream 64
  service-class 1 max-downstream 5000
  service-class 1 max-burst 1600
  cpe max 3
  timestamp
!
! Low performance DOCSIS config file, additional options may be added
!   1 Mbit/sec download, 64 Kbit/sec upload speed
!
cable config-file silver.cm
  service-class 1 max-upstream 64
  service-class 1 max-downstream 1000
  service-class 1 max-burst 1600
  cpe max 1
  timestamp
!
! No Access DOCSIS config file, used to correctly shut down an unused cable modem
!   1 kbit/sec download, 1 Kbit/sec upload speed, with USB/ethernet port shut down.
!
cable config-file disable.cm
  access-denied
  service-class 1 max-upstream 1
  service-class 1 max-downstream 1
  service-class 1 max-burst 1600
  cpe max 1
  timestamp
!
ip subnet-zero
! Turn on cef switching / routing, anything but process switching (no ip route-cache)
ip cef
ip cef accounting per-prefix
! Disables the finger server
no ip finger
! Prevents CMTS from looking up domain names / attempting to connect to
!   machines when mistyping commands
no ip domain-lookup
! Prevents issuance of IP address that is already in use.
ip dhcp ping packets 1
!
! DHCP reply settings for DOCSIS cable modems.
!   All settings here are "default response settings" for this DHCP pool.
! DOCSIS bootfile (cable modem config-file) as defined above
! next-server = IP address of  server which sends bootfile
! default-router = default gateway for cable modems, necessary to get DOCSIS files
! option 4 = TOD server IP address
! option 2 = Time offset for TOD, in seconds, HEX, from GMT, -28,000 = PST = ffff.8f80
! option 7 = Optional SYSLOG server
! Lease length, in days, hours, minutes
!
ip dhcp pool CableModems-Platinum
    network 10.128.1.0 255.255.255.0
    bootfile platinum.cm
    next-server 10.128.1.1
    default-router 10.128.1.1
    option 2 hex ffff.8f80
    option 4 ip 10.128.1.1
    option 7 ip 10.128.1.1
    lease 7 0 10
!
! DHCP reply settings for IP hosts behind DOCSIS cable modems.
```

```
! All settings here are "default response settings" for this DHCP pool.
! default-router = default gateway for cable modems, necessary to get DOCSIS files
! dns-server = IP address for DNS server, place up to 8 addresses on the same
!   line as a list
! NOTE: changing the DNS-server on a Windows PC, Mac, or Unix box require
!   reloading the OS, but changing it in the DHCP response is quick and easy.
! domain-name = default domain name for the host
! Lease length, in days, hours, minutes
!
ip dhcp pool hosts
    network 10.254.1.0 255.255.255.0
    default-router 10.254.1.1
    dns-server 10.254.1.1 10.128.1.1
    domain-name ExamplesDomainName.com
    lease 1 0 10
!
!
!
interface FastEthernet0/0
  ip address 10.17.123.1 255.255.255.0
  no ip mroute-cache
  no shutdown
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  no ip mroute-cache
  shutdown
  duplex auto
  speed auto
!
! Primary address is for cable modems, use only one, so make it large enough!
! Secondary addresses are for hosts, use as many as necessary
! These addresses must match the remainder of the configuration file,
! or modems won't work.
! cable downstream frequency sets the upconverter frequency
! cable down rf-power 55, sets the upconverter output power in dBmV
! each upstream interface can have a description, use it!
! All four upstreams have been set to the same default frequency, don't
! connect wire them together while on the same frequency!
! cable upstream 0 admission-control 150: limits the number of modems
! which can connect with guaranteed-bandwidth.
! NOTE: will prevent some modems from connecting once this limit is hit.
!
! High security option:
! no cable arp: prevents the uBR7100 from ever arping towards the cable modems
! for any IP-mac address pairing. Forces EVERY host to use DHCP at least
! once every time the uBR7100 is reloaded, or the arp table is cleared out.
! Forces users to use DHCP release/renew cycle on their computers if
! ARP entry is ever lost.
! Makes it impossible for an end user to type in a static IP address,
! or steal somebody else's IP address.
!
! cable-source verify dhcp: -- Forces the CMTS to populate the arp table from
! the DHCP server
! If the DHCP server does not have a valid DHCP lease for that IP / MAC combination,
! the host is unreachable.
! cable dhcp-giaddr policy:  use primary IP address for modems, secondary for
! hosts behind modems
!
!
interface Cable1/0
  description Cable Downstream Interface
  ip address 10.254.1.1 255.255.255.0 secondary
  ip address 10.128.1.1 255.255.255.0
  no keepalive
  cable downstream rate-limit token-bucket shaping
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
  cable downstream frequency 851000000
  cable down rf-power 55
```

```
  cable upstream 0 description Cable upstream interface, North
  cable upstream 0 frequency 37008000
  cable upstream 0 power-level 0
  cable upstream 0 admission-control 150
  no cable upstream 0 shutdown
  cable upstream 1 description Cable upstream interface, South
  cable upstream 1 frequency 37008000
  cable upstream 1 power-level 0
  cable upstream 1 admission-control 150
  no cable upstream 1 shutdown
  cable upstream 2 description Cable upstream interface, East
  cable upstream 2 frequency 37008000
  cable upstream 2 power-level 0
  cable upstream 2 admission-control 150
  no cable upstream 2 shutdown
  cable upstream 3 description Cable upstream interface, West
  cable upstream 3 frequency 37008000
  cable upstream 3 power-level 0
  cable upstream 3 admission-control 150
  no cable upstream 3 shutdown
  no cable arp
  cable source-verify dhcp
  cable dhcp-giaddr policy
!
!
! default route to Fast ethernet 0/0, probably best to set
! this as an IP address so interface flaps don't create route flaps.
! IP http server: enables internal http server
!
ip classless
no ip forward-protocol udp netbios-ns
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
ip http server
!
!
! Enable TFTP downloads of the silver.cm file on the Flash device
!   this DOCSIS config file is built using DOCSIS CPE Configurator.
tftp-server slot0:bronze.cm alias bronze.cm
!
! Aliases for frequently used commands
!
alias exec scm show cable modem
alias exec scf show cable flap
alias exec scp show cable qos profile
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
  speed 19200
line vty 0 4
  session-timeout 60
  login
!
ntp clock-period 17179977
ntp server 192.168.35.51
end
```

Advanced All-in-One Configuration Example

The advanced all-in-one configuration is identical to the basic configuration, except that it uses a hierarchical structure of DHCP pools to provide unique DHCP options, such as static IP addresses, to individual cable modems and CPE devices. The DHCP pools are given unique and relevant names to simplify administration, and the cable modems and CPE devices that use these pools are specified by the **client-identifier** commands.

The DHCP pools for the individual cable modems and CPE devices inherit the options from the parent pools, so you do not need to specify all of the required options for those particular pools. Instead, the new pools need to specify only those commands, such as **client-identifier**, that should be different from the parent pools.

Because the static IP addresses that are given to the cable modems and CPE devices are in the range of 10.1.4.60 and 10.1.4.70, the **ip dhcp exclude** command is used to instruct the DHCP server that it should not hand out addresses in this range to other cable modems or CPE devices.

```
!
version 12.1
no service pad
! provides nice timestamps on all log messages
service timestamps debug datetime msec localtime
service timestamps log uptime
! turn service password-encryption on to encrypt passwords
no service password-encryption
! provides additional space for longer configuration file
service compress-config
! supports a large number of modems / hosts attaching quickly
service udp-small-servers max-servers no-limit
!
hostname Router
!
boot system disk0:
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
! permits cable modems to obtain Time of Day (TOD) from uBR7100
cable time-server
!
! High performance DOCSIS config file, additional options may be added
!   10 Mbit/sec download, 128 Kbit/sec upload speed, 10 Kbit/sec guaranteed upstream
! NOTE: cable upstream 0 admission-control 150 will prevent modems from
!   connecting after 150% of guaranteed-bandwidth has been allocated to
!   registered modems. This can be used for peek load balancing.
! max-burst 1600 prevents a modem with concatenation turned on from consuming
!   too much wire time, and interfering with VoIP traffic.
! cpe max 8 limits the modem to 8 hosts connected before the CMTS refuses
!   additional host MAC addresses.
! Timestamp option makes the config file only valid for a short period of time.
!
cable config-file platinum.cm
  service-class 1 max-upstream 128
  service-class 1 guaranteed-upstream 10
  service-class 1 max-downstream 10000
  service-class 1 max-burst 1600
  cpe max 8
  timestamp
!
! Medium performance DOCSIS config file, additional options may be added
!   5 Mbit/sec download, 128 Kbit/sec upload speed
!
cable config-file gold.cm
  service-class 1 max-upstream 64
  service-class 1 max-downstream 5000
  service-class 1 max-burst 1600
  cpe max 3
  timestamp
!
! Low performance DOCSIS config file, additional options may be added
!   1 Mbit/sec download, 64 Kbit/sec upload speed
!
cable config-file silver.cm
  service-class 1 max-upstream 64
  service-class 1 max-downstream 1000
  service-class 1 max-burst 1600
  cpe max 1
  timestamp
!
! No Access DOCSIS config file, used to correctly shut down an unused cable modem
!   1 kbit/sec download, 1 Kbit/sec upload speed, with USB/ethernet port shut down.
!
cable config-file disable.cm
  access-denied
```

```
  service-class 1 max-upstream 1
  service-class 1 max-downstream 1
  service-class 1 max-burst 1600
  cpe max 1
  timestamp
!
ip subnet-zero
! Turn on cef switching / routing, anything but process switching (no ip route-cache)
ip cef
ip cef accounting per-prefix
! Disables the finger server
no ip finger
! Prevents CMTS from looking up domain names / attempting to connect to
!   machines when mistyping commands
no ip domain-lookup
! Prevents the issuance of IP addresses in this range, allows for use in
!   static configurations.
ip dhcp excluded-address 10.128.1.60 10.128.1.70
! Prevents issuance of IP address that is already in use.
ip dhcp ping packets 1
!
! DHCP reply settings for DOCSIS cable modems.
!   All settings here are "default response settings" for this DHCP pool.
! DOCSIS bootfile (cable modem config-file) as defined above
! next-server = IP address of  server which sends bootfile
! default-router = default gateway for cable modems, necessary to get DOCSIS files
! option 4 = TOD server IP address
! option 2 = Time offset for TOD, in seconds, HEX, from GMT, -28,000 = PST = ffff.8f80
! option 7 = Optional SYSLOG server
! Lease length, in days, hours, minutes
!
ip dhcp pool CableModems-Platinum
    network 10.128.1.0 255.255.255.0
    bootfile platinum.cm
    next-server 10.128.1.1
    default-router 10.128.1.1
    option 2 hex ffff.8f80
    option 4 ip 10.128.1.1
    option 7 ip 10.128.1.1
    lease 7 0 10
!
! DHCP reply settings for IP hosts behind DOCSIS cable modems.
! All settings here are "default response settings" for this DHCP pool.
! default-router = default gateway for cable modems, necessary to get DOCSIS files
! dns-server = IP address for DNS server, place up to 8 addresses on the same
!   line as a list
! NOTE: changing the DNS-server on a Windows PC, Mac, or Unix box require
!   reloading the OS, but changing it in the DHCP response is quick and easy.
! domain-name = default domain name for the host
! Lease length, in days, hours, minutes
!
ip dhcp pool hosts
    network 10.254.1.0 255.255.255.0
    default-router 10.254.1.1
    dns-server 10.254.1.1 10.128.1.1
    domain-name ExamplesDomainName.com
    lease 1 0 10
!
! DHCP reply settings for a static IP address for a PC and cable modems
! All settings here will override "default response settings" for this DHCP pool.
! client-identifier is the ethernet MAC address of the device, preceded by 01
!   Thus, the Host with an mac address of 08.00.09.af.34.e2 will ALWAYS get the
!   same IP address
! Lease length, in days, hours, minutes, set to infinite.
! Use a relevant name here, as there will be lots of these entries.
!
ip dhcp pool staticPC(0800.09af.34e2)
    host 10.254.1.12 255.255.255.0
    client-identifier 0108.0009.af34.e2
    client-name staticPC(0800.09af.34e2)
    lease infinite
ip dhcp pool cm-0050.04f9.efa0cm-
   host 10.128.1.65 255.255.255.0
```

```
   client-identifier 0100.107b.ed9b.45
   bootfile disable.cm
!
ip dhcp pool cm-0030.d002.41f5
   host 10.128.1.66 255.255.255.0
   client-identifier 0100.107b.ed9b.23
   bootfile silver.cm
!
! DHCP reply settings for a cable modem, to change from default provisioning
! All settings here will override "default response settings" for this DHCP pool.
!   client-identifier is the ethernet MAC address of the device, preceded by 01
!   Thus, the modem with a mac address of 00.10.95.81.7f.66 will ALWAYS get the
!   same IP address
! This cable modem will get the gold.cm config file, and a consistent IP address
!   some IP address within the DHCP pool for the cable downstream interface is
!   required, or the reference correct config file will NOT be issued.
! Use a relevant name here, as there will be lots of these entries.
!
! WARNING: When changing config files for a modem, it is necessary to clear the
!  address with “clear ip dhcp binding <ip-address>” and then reset the modem using
!  "clear cable modem <mac-address> | <ip-address> reset"
!
ip dhcp pool goldmodem
    host 10.128.1.67 255.255.255.0
    client-identifier 0100.1095.817f.66
    bootfile gold.cm
!
! DHCP reply settings for a disabled cable modem.
! This will prevent this cable modem user from accessing the network.
!   client-identifier is the ethernet MAC address of the device, preceded by 01
! This cable modem will get the disable.cm config file, and a consistent IP address
!   some IP address within the DHCP pool for the cable downstream interface is
!   required, or the reference correct config file will NOT be issued.
! Use a relevant name here, as there will be lots of these entries.
!
! WARNING: When changing config files for a modem, it is necessary to clear the
!  address with “clear ip dhcp binding <ip-address>” and then reset the modem using
!  "clear cable modem <mac-address> | <ip-address> reset"
!
ip dhcp pool DisabledModem(0010.aaaa.0001)
    host 10.128.1.68 255.255.255.0
    client-identifier 0100.1095.817f.66
    bootfile disable.cm
!
ip dhcp pool DisabledModem(0000.bbbb.0000)
    client-identifier 0100.00bb.bb00.00
    host 10.128.1.69 255.255.255.0
    bootfile disable.cm
!
!
!
interface FastEthernet0/0
  ip address 10.17.123.1 255.255.255.0
  no ip mroute-cache
  no shutdown
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  no ip mroute-cache
  shutdown
  duplex auto
  speed auto
!
! Primary address is for cable modems, use only one, so make it large enough!
! Secondary addresses are for hosts, use as many as necessary
! These addresses must match the remainder of the configuration file,
! or modems won't work.
! cable downstream frequency sets the upconverter frequency
! cable down rf-power 55, sets the upconverter output power in dBmV
! each upstream interface can have a description, use it!
! All four upstreams have been set to the same default frequency, don't
```

```
! connect wire them together while on the same frequency!
! cable upstream 0 admission-control 150: limits the number of modems
! which can connect with guaranteed-bandwidth.
! NOTE: will prevent some modems from connecting once this limit is hit.
!
! High security option:
! no cable arp: prevents the uBR7100 from ever arping towards the cable modems
! for any IP-mac address pairing. Forces EVERY host to use DHCP at least
! once every time the uBR7100 is reloaded, or the arp table is cleared out.
! Forces users to use DHCP release/renew cycle on their computers if
! ARP entry is ever lost.
! Makes it impossible for an end user to type in a static IP address,
! or steal somebody else's IP address.
!
! cable-source verify dhcp: -- Forces the CMTS to populate the arp table from
! the DHCP server
! If the DHCP server does not have a valid DHCP lease for that IP / MAC combination,
! the host is unreachable.
! cable dhcp-giaddr policy:  use primary IP address for modems, secondary for
! hosts behind modems
!
!
interface Cable1/0
  description Cable Downstream Interface
  ip address 10.254.1.1 255.255.255.0 secondary
  ip address 10.128.1.1 255.255.255.0
  no keepalive
  cable downstream rate-limit token-bucket shaping
  cable downstream annex B
  cable downstream modulation 64qam
  cable downstream interleave-depth 32
  cable downstream frequency 851000000
  cable down rf-power 55
  cable upstream 0 description Cable upstream interface, North
  cable upstream 0 frequency 37008000
  cable upstream 0 power-level 0
  cable upstream 0 admission-control 150
  no cable upstream 0 shutdown
  cable upstream 1 description Cable upstream interface, South
  cable upstream 1 frequency 37008000
  cable upstream 1 power-level 0
  cable upstream 1 admission-control 150
  no cable upstream 1 shutdown
  cable upstream 2 description Cable upstream interface, East
  cable upstream 2 frequency 37008000
  cable upstream 2 power-level 0
  cable upstream 2 admission-control 150
  no cable upstream 2 shutdown
  cable upstream 3 description Cable upstream interface, West
  cable upstream 3 frequency 37008000
  cable upstream 3 power-level 0
  cable upstream 3 admission-control 150
  no cable upstream 3 shutdown
  no cable arp
  cable source-verify dhcp
  cable dhcp-giaddr policy
!
!
! default route to Fast ethernet 0/0, probably best to set
! this as an IP address so interface flaps don't create route flaps.
! IP http server: enables internal http server on uBR7100
!
ip classless
no ip forward-protocol udp netbios-ns
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
ip http server
!
!
! Enable TFTP downloads of the silver.cm file on the Flash device
!   this DOCSIS config file is built using DOCSIS CPE Configurator.
tftp-server slot0:bronze.cm alias bronze.cm
!
! Aliases for frequently used commands
```

```
!
alias exec scm show cable modem
alias exec scf show cable flap
alias exec scp show cable qos profile
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
  speed 19200
line vty 0 4
  session-timeout 60
  login
!
ntp clock-period 17179977
ntp server 192.168.35.51
```

Additional References

For additional information related to DHCP, ToD, and TFTP Services for the CMTS Routers, refer to the following references:

Related Documents

Related Topic	Document Title
All-In-One Configuration	For information on how to configure a Cisco CMTS that acts as a Dynamic Host Configuration Protocol (DHCP), Time-of-Day (ToD), and TFTP server in an "all-in-one configuration," see the following URL: http://www.cisco.com/en/US/tech/tk86/tk804/technologies_configuration_example09186a0080134b34.shtml
DHCP Configuration	To configure the DHCP server beyond the minimum options given in this chapter, see the "Configuring DHCP" chapter in the "IP Addressing and Services" section of the *Cisco IOS IP and IP Routing Configuration Guide* , Release 12.2 at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/fipr_c.html For information on all DHCP commands, see the "DHCP Commands" chapter in the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2 at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/ipaddr/command/reference/fipras_r.html
TFTP Server Command	For more information about the **tftp-server** command, see the "Configuring Basic File-Transfer Services" section of the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf011.html

Related Topic	Document Title
NTP or SNTP Configuration	For information on configuring the Cisco CMTS to use NTP or SNTP to set its system clock, see the "Performing Basic System Management" chapter in the "System Management" section of the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* , at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf012.html
Cable Source Verify Feature	For a more detailed description of the cable source-verify command and how it can be used to prevent certain types of denial of service attacks, see the following Tech Note on Cisco.com: http://www.cisco.com/en/US/customer/tech/tk86/tk803/technologies_tech_note09186a00800a7828.shtml
Calculating the Hexadecimal Value for DHCP Option 2	For information on how to calculate the hexadecimal time value that is used to set the DHCP Time Offset option (DHCP option 2), see the following URL: http://www.cisco.com/en/US/customer/tech/tk86/tk804/technologies_tech_note09186a0080093d76.shtml
Cisco DOCSIS Configurator Tool	For information on creating DOCSIS 1.1 configuration files, you can use the Cisco DOCSIS Configurator tool, which at the time of this document's publication is available at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/cpe-conf
CMTS Command Reference	*Cisco IOS CMTS Cable Command Reference Guide,* at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html

Related Topic	Document Title
Cisco uBR7100 Series Universal Broadband Router Documentation	*Cisco uBR7100 Series Universal Broadband Router Hardware Installation Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr7100/installation/guide/hig7100.html *Cisco uBR7100 Series Universal Broadband Router Software Configuration Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr7100/configuration/guide/scg7100.html
Cisco uBR7200 Series Universal Broadband Router Documentation	*Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/installation/guide/ub72khig.html *Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/configuration/guide/cr72scg.html
Cisco uBR10012 Universal Broadband Router Documentation	*Cisco uBR10012 Universal Broadband Router Hardware Installation Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/installation/guide/hig.html *Cisco uBR10012 Universal Broadband Router Software Configuration Guide* , at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/configuration/guide/scg.html

Standards

Standards[5]	Title
ANSI/SCTE 22-1 2002 (formerly SP-RFI-C01-011119)	Data-Over-Cable Service Interface Specification DOCSIS 1.0 Radio Frequency Interface (RFI) (http://www.cablemodem.com)
SP-RFIv1.1-I08-020301	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification DOCSIS 1.1 (http://www.cablemodem.com)
SP-BPI+-I08-020301	DOCSIS Baseline Privacy Interface Plus Specification (http://www.cablemodem.com)

5 Not all supported standards are listed.

MIBs

MIBs[6]	MIBs Link
• DOCS-CABLE-DEVICE-MIB (RFC 2669)	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

6 Not all supported MIBs are listed.

RFCs

RFCs[7]	Title
RFC 868	Time Protocol
RFC 1350	The TFTP Protocol (Revision 2)
RFC 2131	Dynamic Host Configuration Protocol
RFC 2132	DCHP Options and BOOTP Vendor Extensions
RFC 2349	TFTP Timeout Interval and Transfer Size Options
RFC 3046	DHCP Relay Agent Information Option
RFC4243	DHCP Relay Agent Information Sub-Option

7 Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for the DHCP, ToD, and TFTP Services for the CMTS Routers

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

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

Table 6: Feature Information for the DHCP, ToD, and TFTP Services for the CMTS Routers

Feature Name	Releases	Feature Information
DHCP, ToD, and TFTP Services	11.3 NA	The **cable source-verify** and **ip dhcp** commands are now supported on the Cisco uBR7200 series routers.
DHCP, ToD, and TFTP Services	12.1(5)T	The **cable tftp-enforce** command is now supported.

Feature Name	Releases	Feature Information
DHCP, ToD, and TFTP Services	12.1(13)EC	The following commands are now supported on the Cisco IOS Release 12.1 EC train: **clear cable dhcp-giaddr-policy** **clear cable dhcp-lease-timer** **clear cable dhcp-server-timer** The **cable source-verify** command has been expanded to include the **dhcp** keyword.
DHCP, ToD, and TFTP Services	12.1(13)EC	The Cisco uBR10012 series routers are now supported.

Feature Name	Releases	Feature Information
DHCP, ToD, and TFTP Services	12.1(13)EC	The Cisco uBR10012 series, Cisco uBR7200 series, and Cisco uBR7100 routers now support the above commands.
DHCP, ToD, and TFTP Services	12.1(13)EC 12.2(4)BC1	The **cable tftp-enforce** command is now supported.
DHCP, ToD, and TFTP Services	12.1(13)EC 12.2(4)BC1	The **cable source-verify** command has been expanded to include the **leasetimer** keyword.

Feature Name	Releases	Feature Information
DHCP, ToD, and TFTP Services	12.2(33)SCC	The cable dhcp-giaddr policy command has been expanded to allow selection of MAC address

Feature Name	Releases	Feature Information
DHCP, ToD, and TFTP Services	12.2(33)SCC	

Feature Name	Releases	Feature Information
		The **cable dhcp-giaddr** command has been expanded to further specify where to forward DHCP packets based on origin from a cable modem, MTA, SIP, or other cable device. The **cable dhcp-insert** command allows users to configure the CMTS to insert circuit ID options into DHCP packets using option 82. DHCP

Feature Name	Releases	Feature Information
		servers can then detect cable modems and extract geographical information The **show cable modem** **docsis** **docsis** command is now supported
DHCP, ToD, and TFTP Services	12.1(5)T	The **cable dhcp-giaddr** command was modified to support the **host**, **mta**, **ps**, and **stb** keywords

Feature Name	Releases	Feature Information
DHCP Relay Agent Source Address Validation	Cisco IOS XE Release 3.7.0S	The support for the DHCP Relay Agent Source Address Validation (SAV) feature was added. The following new commands were introduced: cable dhcp-giaddr policy cable dhcp-giaddr policy cable dhcp-giaddr p

Feature Name	Releases	Feature Information
DHCP Relay Agent Sub-option 82	12.2(15)BC2	Support was added for the DHCP Relay Agent Information Sub-option 82 feature. The following command was modified: cable dhcp-giaddr

Supported Platforms

Cisco uBR7100 series, Cisco uBR7200 series, Cisco uBR10012 universal broadband routers.