DHCP, ToD, and TFTP Services for CMTS Routers

Note Cisco IOS-XE Release 16.5.1 integrates support for this feature on Cisco CMTS routers.

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 Specification (DOCSIS) networks. In addition, this document provides information about optional configurations that can be used with external DHCP servers.

Prerequisites for DHCP, ToD, and TFTP Services

To use the Cisco CMTS as the ToD server, either standalone or with other external ToD servers, you must configure the DHCP server to provide the IP address of the Cisco CMTS as one of the valid ToD servers (DHCP option 4) for cable modems.

Restrictions for DHCP, ToD, and TFTP Services

- 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).
- 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:

- 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.

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.

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:

- 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 3 and Configuring Prefix-based Source Address Verification, on page 14

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 14.

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.

DHCP Relay Agent Sub-option

The DHCP Relay Agent Information sub-option (DHCP Option 82, Suboption 9) enhancement simplifies 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.

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.

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, 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.

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-XE Configuration File—The DOCSIS configuration file for Cisco cable devices can also specify that the cable modem should download a Cisco IOS-XE 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-XE 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-XE configuration file is an ASCII text file that contains one or more Cisco IOS-XE CLI configuration commands. Only Cisco cable devices can download a Cisco IOS-XE 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.

Benefits

- 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.

How to Configure ToD, and TFTP Services

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

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 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.

Enabling Time-of-Day Service

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

Procedure

	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.

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.

Procedure

	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.
- 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.
- Enable the TFTP server on the Cisco CMTS with the **tftp-server** command.

Each configuration task is required unless otherwise listed as optional.

Procedure

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#
```

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 11 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)#
```

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.

Procedure

	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	**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.

	Command or Action	Purpose
		Note Repeat Step 3, on page 13 through Step 5, on page 13 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:
	
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

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.

Procedure

	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`	Enables SAV prefix processing on the Cisco CMTS.

	Command or Action	Purpose
	enable-sav-static Router(config)#	
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**] **Example:** Router(config-sav)# **prefix 10.10.10.0/24** Router(config-sav)#	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. • 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.

Procedure

	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 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-XE 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.

	Command or Action	Purpose

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**]
	
	Example:
	
	`Router(config-if)# cable helper-address 10.10.10.13`
	`Router(config-if)#`
		(Optional) Enables load-balancing of DHCP requests from cable modems and CPE devices by specifying different DHCP servers according to the cable interface or 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—**(Optional) Specifies this server should only accept MTA packets .
		• **stb —**(Optional) Specifies this server should only accept STB packets .
		
		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.

	Command or Action	Purpose
		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-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.

Step 10	**exit**
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode.

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

How to Configure ToD, and TFTP Services

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

Configuration Examples

This section provides examples for the following configurations:

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
```

Additional References

Technical Assistance

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

Feature Information for 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://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note The 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 1: Feature Information for Downstream Interface Configuration

Feature Name	Releases	Feature Information
DHCP, ToD, and TFTP services	Cisco IOS-XE Release 16.5.1	This feature was integrated into Cisco IOS-XE Release 16.5.1 on the Cisco cBR Series Converged Broadband Routers.