CHAPTER 6

DHCP, ToD, and TFTP Services for the Cisco Cable Modem Termination System

Revised: June 8, 2009, OL-1467-08

This chapter 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 chapter provides information about optional configurations that can be used with external DHCP servers.

Feature Specifications for DHCP, ToD, and TFTP Services

Feature History	
Release	**Modification**
Release 11.3 NA	The **cable source-verify** and **ip dhcp** commands are now supported on the Cisco uBR7200 series routers.
Release 12.0(4)XI	The **cable time-server** command is now supported.
Release 12.1(2)EC1	The following commands are now supported on the Cisco IOS Release 12.1 EC train: • **cable config-file** • **cable dhcp-giaddr** • **cable helper-address** The **cable source-verify** command has been expanded to include the **dhcp** keyword.
Release 12.1(5)EC1	The Cisco uBR7100 series routers are now supported
Release 12.2(4)BC1	The Cisco uBR7100 series, Cisco uBR7200 series, and Cisco uBR10012 routers now support the above commands.
Release 12.1(11b)EC1, Release 12.2(8)BC2	The **cable tftp-enforce** command is now supported.
Release 12.1(13)EC, Release 12.2(11)BC1	The **cable source-verify** command has been expanded to include the **leasetimer** keyword.
Release 12.3(13)BC	The **cable source-verify dhcp** command has been expanded to allow exclusion of MAC addresses.

Release 12.3(21)BC	The **cable helper-address** command has been expanded to further specify where to forward DHCP packets based on origin: from a cable modem, MTA, STB, or other cable devices. The **cable dhcp-insert** command allows users to configure the CMTS to insert descriptors into DHCP packets using option 82. DHCP servers can then detect cable modem clones and extract geographical information. The **show cable modem docsis device-class** command is now supported.
Supported Platforms	
Cisco uBR7100 series, Cisco uBR7200 series, Cisco uBR10012 universal broadband routers.	

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

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.

- 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.

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, page 6-3
- Internal DHCP Server, page 6-4
- External DHCP Servers, page 6-6
- Time-of-Day Server, page 6-7
- TFTP Server, page 6-9

Feature Overview

All Cisco CMTS platforms support onboard servers that provide DHCP, ToD, and TFTP 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 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.
- External DHCP Servers—Provides the same functionality as the onboard DHCP server, but external DHCP servers are usually part of an integrated provisioning system that is more suitable when managing large cable networks.
- Time-of-Day Server—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.
- 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. If the DHCP server cannot match the information with that belonging to a cable modem in its database, the CMTS knows that the device is a CPE device. This allows the 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 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 CMTS to insert downstream, upstream, or hostname descriptors into DHCP packets. A DHCP server can then utilize such information to detect cloned modems or extract geographical information. 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, page 6-6
- Smart Relay Feature, page 6-7
- Giaddr Field, page 6-7

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 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 asks the DHCP servers for any information about that device's IP and MAC addresses. If the DHCP servers do not return any information about the device, the CMTS continues to block network access for the device.

- When you use the **dhcp** option, you can also enable the **leasetimer** option, which instructs the CMTS to periodically check its internal CPE database for IP addresses whose lease times have expired. 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.

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 CPE devices should use 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 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, and the secondary servers are used only if the primary server does not respond.

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 current 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" section on page 6-11 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 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/cisco/pub/software/portal/select.html?config=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.
- You do not need a separate workstation or PC 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:

- Configuring DHCP Service, page 6-11
- Configuring Time-of-Day Service, page 6-17
- Configuring TFTP Service, page 6-20
- Configuring A Basic All-in-One Configuration (optional), page 6-23
- Configuring an Advanced All-in-One Configuration (optional), page 6-23
- Optimizing the Use of an External DHCP Server, page 6-24

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, page 6-11
- Creating and Configuring a DHCP Address Pool for CPE Devices (optional), page 6-15
- Configuring the DHCP MAC Address Exclusion List for the cable-source verify dhcp Command

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **network** *network-number* [*mask*]
5. **bootfile** *filename*
6. **next-server** *address* [*address2...address8*]
7. **default-router** *address* [*address2...address8*]
8. **option 2 hex** *gmt-offset*
9. **option 4 ip** *address* [*address2...address8*]
10. **option 7 ip** *address* [*address2...address8*]
11. **lease** {*days* [*hours*][*minutes*] | **infinite**}

12. **client-identifier** *unique-identifier*
13. **cable dhcp-insert** {**downstream-description** | **hostname** | **upstream-description**}
14. **exit**
15. **exit**

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.

	Command or Action	Purpose

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.

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`** | **`upstream-description`**}	(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** = Received DHCP packets are appended with downstream port descriptors. • **hostname** = Received DHCP packets are appended with the router host names. • **upstream-description** = Received DHCP packets are appended 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.

	Command or Action	Purpose

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 (optional)

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **network** *network-number* [*mask*]
5. **default-router** *address* [*address2...address8*]
6. **dns-server** *address* [*address2...address8*]
7. **domain-name** *domain*
8. **lease** {*days* [*hours*][*minutes*] | **infinite**}
9. **client-identifier** *unique-identifier*
10. **exit**
11. **exit**

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

Step 11	**exit**
	Example:
	`Router(config)# exit`
	`Router#`
		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" section on page 6-11 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service udp-small-servers max-servers no-limit**
4. **cable time-server**
5. **exit**

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no cable time-server**
4. **no service udp-small-servers**
5. **exit**

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.

	Command or Action	Purpose

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.

```
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.

```
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:

```
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):

```
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 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.

```
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:

```
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 shown in Step 6:

```
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.

```
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.

```
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.

```
Router(config)# interface cable x/y
Router(config-if)# cable tftp-enforce mark-only
Router(config-if)#
```

Configuring A Basic All-in-One Configuration (optional)

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

- Configuring DHCP Service, page 6-11
- Configuring Time-of-Day Service, page 6-17
- Configuring TFTP Service, page 6-20

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" section on page 6-20.
- 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" section on page 6-35.

Configuring an Advanced All-in-One Configuration (optional)

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:

- Configuring DHCP Service, page 6-11
- Configuring Time-of-Day Service, page 6-17
- Configuring TFTP Service, page 6-20

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" section on page 6-20.
- 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" section on page 6-39.

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 (optional), page 6-24
- Configuring Optional DHCP Parameters (optional), page 6-26
- Configuring the DHCP MAC Address Exclusion List for the cable-source verify dhcp Command

Configuring Cable Source Verify Option (optional)

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

Restrictions

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** *x/y*
4. **cable source-verify** [**dhcp** | **leasetimer** *value*]
5. **no cable arp**
6. **exit**

7. **ip dhcp relay information option**
8. **exit**

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	**`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`
	`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 through Step 5 for each desired cable interface.	

	Command or Action	Purpose

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.
		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.

Step 8	`exit`
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Configuring Optional DHCP Parameters (optional)

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp smart-relay**
4. **ip dhcp ping packet 0**
5. **ip dhcp relay information check**
6. **interface cable** *x/y*
7. `cable dhcp-giaddr policy`
8. **cable helper-address** *address* [**cable-modem** | **host** | **stb** | **mta**]
9. **cable dhcp-parse option-***optnum* (optional)
10. **cable dhcp-giaddr policy**
11. **exit**
12. **exit**

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 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.

	Command or Action	Purpose

Step 7	**`cable dhcp-giaddr policy`**
	Example:
	`Router(config-if)# cable dhcp-giaddr policy`
	`Router(config-if)#`
		Sets the DHCP *giaddr* field of DHCP request packets to the primary address for cable modems and the secondary address for CPE devices, allowing the use of separate address pools for the different clients.
		Note The **cable dhcp-giaddr** command also supports the **primary** option, but this typically is used only for EuroDOCSIS cable modems and set-top boxes.

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**= Specifies this server should only accept MTA packets (optional). You must also complete Step 9.
		• **stb** = Specifies this server should only accept STB packets (optional). You must also complete Step 9.
		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.

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.

	Command or Action	Purpose

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, 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 through Step 9 for each desired cable interface.	

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.

Configuring the DHCP MAC Address Exclusion List for the cable-source verify dhcp Command

Cisco IOS Release 12.3(13)BC introduces the ability to exclude trusted MAC addresses from standard DHCP source verification checks, as supported in previous Cisco IOS releases for the Cisco CMTS. This feature enables packets from trusted MAC addresses to pass when otherwise packets would be rejected with standard DHCP source verification. This feature overrides the **cable source-verify** command on the Cisco CMTS for the specified MAC address, yet maintains overall support for standard and enabled DHCP source verification processes. This feature is supported on Performance Routing Engine 1 (PRE1) and PRE2 modules on the Cisco uBR10012 router chassis.

To enable packets from trusted source MAC addresses in DHCP, use the **cable trust** command in global configuration mode. To remove a trusted MAC address from the MAC exclusion list, use the **no** form of this command. Removing a MAC address from the exclusion list subjects all packets from that source to standard DHCP source verification.

cable trust *mac-address*

no cable trust *mac-address*

Syntax Description

mac-address	The MAC address of a trusted DHCP source, and from which packets will not be subject to standard DHCP source verification.

Usage Guidelines

This command and capability are only supported in circumstances in which the Cable Source Verify feature is first enabled on the Cisco CMTS.

When this feature is enabled in addition to cable source verify, a packet's source must belong to the MAC Exclude list on the Cisco CMTS. If the packet succeeds this exclusionary check, then the source IP address is verified against Address Resolution Protocol (ARP) tables as per normal and previously supported source verification checks. The service ID (SID) and the source IP address of the packet must match those in the ARP host database on the Cisco CMTS. If the packet check succeeds, the packet is allowed to pass. Rejected packets are discarded in either of these two checks.

Any trusted source MAC address in the optional exclusion list may be removed at any time. Removal of a MAC address returns previously trusted packets to non-trusted status, and subjects all packets to standard source verification checks on the Cisco CMTS.

Note When the **cable source-verify dhcp** feature is enabled, and a statically-defined IP address has been added to the CMTS for a CM using the **cable trust** command to override the **cable source-verify dhcp** checks for this device, packets from this CM will continue to be dropped until an entry for this CM is added to the ARP database of the CMTS. To achieve this, disable the **cable source-verify dhcp** feature, ping the CMTS from the CM to add an entry to the ARP database, and re-enable the **cable source-verify dhcp** feature.

For additional information about the enhanced Cable Source Verify DHCP feature, and general guidelines for its use, refer to the following documents on Cisco.com:

- *IP Address Verification for the Cisco uBR7200 Series Cable Router*

  Note This document has reached End of Life. For more information, see the following End-of-Life Announcement at the following URL: http://www.cisco.com/en/US/docs/ios/redirect/eol.html

- *Filtering Cable DHCP Lease Queries*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/cblsrcvy.pdf
- *Cisco Broadband Cable Command Reference Guide*

  http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
- *Cable Security*, *Cable Source-Verify and IP Address Security*, White Paper

  http://www.cisco.com/en/US/tech/tk86/tk803/technologies_tech_note09186a00800a7828.shtml

Configuration Examples

This section provides examples for the following configurations:

- DHCP Server Examples, page 6-31
- ToD Server Example, page 6-34
- TFTP Server Example, page 6-34
- Basic All-in-One Configuration Example, page 6-35
- Advanced All-in-One Configuration Example, page 6-39

DHCP Server Examples

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

- DHCP Pools for Cable Modems, page 6-32
- DHCP Pools for Disabling Cable Modems, page 6-33
- DHCP Pools for CPE Devices, page 6-33

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. The **cable tftp-enforce** command is optional but recommended for each cable interface. 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 Enforce feature on all cable interfaces
 interface Cable3/0
  cable tftp-enforce
 interface Cable4/0
  cable tftp-enforce
 interface Cable5/0
  cable tftp-enforce
!
!
...
! 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" section on page 6-30. 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 <module feature>, 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

Related Topic	Document Title
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
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/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/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/cisco/pub/software/portal/select.html?config=cpe-conf
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
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[1]	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.cablelabs.com/cablemodem)
SP-RFIv1.1-I08-020301	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification DOCSIS 1.1 (http://www.cablelabs.com/cablemodem)
SP-BPI+-I08-020301	DOCSIS Baseline Privacy Interface Plus Specification (http://www.cablelabs.com/cablemodem)

[1] Not all supported standards are listed.

MIBs

MIBs[1]	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

[1] Not all supported MIBs are listed.

RFCs

RFCs[1]	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

[1] 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