



CHAPTER 10

Cisco TFTP

The Cisco TFTP service builds and serves files that are consistent with the Trivial File Transfer Protocol (TFTP). Cisco TFTP builds configuration files and serves embedded component executables, ringer files, and device configuration files.

A configuration file contains a prioritized list of Cisco Unified Communications Managers for a device (phones that are running SCCP and phones that are running SIP and gateways), the TCP ports on which the device connects to those Cisco Unified Communications Managers, and an executable load identifier. Configuration files for selected devices contain locale information and URLs for the phone buttons: messages, directories, services, and information. Configuration files for gateways contain all their configuration information.

You can find configuration files in a .cnf, a .cnf.xml, or an .xml format, depending on the device type and your TFTP service parameter settings. When you set the Build CNF Files service parameter to Build All, the TFTP server builds both .cnf.xml and .cnf format configuration files for all devices. When you set this service parameter to Build None, the TFTP server builds only .cnf.xml files for all devices. When this parameter is set to Build Selective, which is the default value, the TFTP server builds .cnf.xml files for all devices and, in addition, builds .cnf files only for a select list of device types that are provided in [Table 10-1](#):

Table 10-1 *Devices with Build Selective BuildCNFType*

Device Type	Device Name
MODEL_30SPP	Cisco 30 SP+
MODEL_12SPP	Cisco 12 SP+
MODEL_12SP	Cisco 12 SP
MODEL_12S	Cisco 12 S
MODEL_30VIP	Cisco 30 VIP or DPA
MODEL_IP_CONFERENCE_PHONE	Cisco 7935
MODEL_SCCP_PHONE	SCCP Phone
MODEL_VEGA	Analog Access
MODEL_UONE	Voice Mail Port

This section describes the relationship among Cisco Unified Communications Manager, TFTP, and Dynamic Configuration Protocol (DHCP) as well as the relationship between devices and the TFTP server. This section contains the following topics:

- [TFTP Configuration Checklist, page 10-2](#)
- [TFTP Process Overview for Devices That Run SCCP, page 10-3](#)
- [TFTP Process Overview for Cisco Unified IP Phones That Run SIP, page 10-4](#)
- [Understanding How Devices Use DHCP and Cisco TFTP, page 10-6](#)
- [Understanding How Devices That Use IPv4 Access the TFTP Server, page 10-7](#)
- [Understanding How Phones That Use IPv6 Access the TFTP Server, page 10-8](#)
- [Understanding How Devices Identify the TFTP Server, page 10-9](#)
- [Configuring a Redundant TFTP Server, page 10-11](#)
- [Centralized TFTP in a Multiple Cluster Environment, page 10-11](#)
- [Alternate Cisco File Servers, page 10-11](#)
- [Configuration Tips for Centralized TFTP, page 10-13](#)
- [Customizing and Modifying Configuration Files, page 10-14](#)
- [Where to Find More Information, page 10-14](#)

TFTP Configuration Checklist

The Cisco TFTP service builds and serves files that are consistent with the Trivial File Transfer Protocol (TFTP). Cisco TFTP builds configuration files and serves embedded component executables, ringer files, and device configuration files.

A configuration file contains a prioritized list of Cisco Unified Communications Managers for a device (phones that are running SCCP and phones that are running SIP and gateways), the TCP ports on which the device connects to those Cisco Unified Communications Managers, and an executable load identifier. Configuration files for selected devices contain locale information and URLs for the phone buttons: messages, directories, services, and information. Configuration files for gateways contain all their configuration information.

[Table 10-2](#) lists the steps that are needed to configure the Cisco TFTP service. For more information, see the [“Where to Find More Information”](#) section on [page 10-14](#).

Table 10-2 TFTP Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Activate and start the Cisco TFTP service on the appropriate server.	<i>Cisco Unified Serviceability Administration Guide</i>

Table 10-2 TFTP Configuration Checklist (continued)

Configuration Steps		Procedures and Related Topics
Step 2	Configure the appropriate service parameters, including the Alternate File Location parameters, if appropriate.	Service Parameters Configuration , <i>Cisco Unified Communications Manager Administration Guide</i>
Step 3	If you change a non-configuration file such as a load file or RingList.xml, start and stop the Cisco TFTP service. Note You must upload files to the TFTP directory from Cisco Unified Communications Operating System Administration. Refer to the <i>Cisco Unified Communications Operating System Administration Guide</i> for more information.	<i>Cisco Unified Serviceability Administration Guide</i> Service Parameters Configuration , <i>Cisco Unified Communications Manager Administration Guide</i>

TFTP Process Overview for Devices That Run SCCP

The TFTP server can handle simultaneous requests for configuration files. This section describes the request process.

When a device boots, it queries a DHCP server for its network configuration information. The DHCP server responds with an IP address for the device, a subnet mask, a default gateway, a Domain Name System (DNS) server address, and a TFTP server name or address. (Some devices, such as the Cisco Unified IP Phone 7960, support up to two TFTP servers. If the primary TFTP server is not reached, such devices attempt to reach the fallback TFTP server.)



Note

If DHCP is not enabled on a device, you must assign it an IP address and configure the TFTP server locally on the device.

The device requests a configuration file from the TFTP server. The TFTP server searches three internal caches, the disk, and then alternate Cisco file servers (if specified) for the configuration file. If the TFTP server finds the configuration file, it sends it to the device. If the configuration file provides Cisco Unified Communications Manager names, the device resolves the name by using DNS and opens a connection to the Cisco Unified Communications Manager. If the device does not receive an IP address or name, it uses the TFTP server name or IP address for setting up its registration connection.

If the TFTP server cannot find the configuration file, it sends a “file not found” message to the device.



Note

If the TFTP server returns a “file not found” message to the device, a “request not found” TFTP counter increments. In nonsecure clusters, this behavior does not represent an error because the CTL file does not exist on a Cisco Unified Communications Manager in nonsecure mode.

Devices that are requesting a configuration file while the TFTP server is rebuilding configuration files or while processing the maximum number of requests receive a message from the TFTP server, which causes the device to request the configuration file later. The Maximum Serving Count service parameter, which can be configured, specifies 200 as the maximum number of requests.

For a more detailed description of how devices boot, see the [“Understanding How Devices Use DHCP and Cisco TFTP”](#) section on page 10-6.

TFTP Process Overview for Cisco Unified IP Phones That Run SIP

Unlike phones that are running SCCP, phones that are running SIP get all their configurations from the TFTP server. From initial startup, the phone that is running SIP contacts the configured TFTP server (either manually configured or configured through the DHCP server) to get the configuration files; it then registers itself to its configured Cisco Unified Communications Manager.

When the configuration of the phone that is running SIP gets changed, the Cisco Unified Communications Manager database notifies the TFTP server to rebuild all the configuration files or to rebuild selectively. The TFTP server retrieves information from the Cisco Unified Communications Manager database and converts it into the proper output format, according to the device type, and saves the output in TFTP cache. When the TFTP server gets a request, it searches either the cache or Alternate File Server locations disk to serve the requested configuration file or default files.

The TFTP support for phones that are running SIP builds and serves different formats of SIP configuration files from the Cisco Unified Communications Manager database for the following Cisco Unified IP Phones:

- Cisco Unified IP Phone 7970/71, 7961, 7941, 7911 (These phones share the same SIP configuration file format.)
- Cisco Unified IP Phone 7960, 7940 (These phones share the same SIP configuration file format.)
- Cisco Unified IP Phone 7905, 7912
- SIP dial plans on the preceding phones
- Softkey templates on the preceding phones

The TFTP server generates the following files from the Cisco Unified Communications Manager database for configuration of phones that are running SIP:

- Systemwide default configuration files and per-device configuration files.
- List of systemwide dial plans for Cisco Unified IP Phones 7970/71, 7960/61, 7940/41, and 7911.
- List of systemwide softkey template files.

Table 10-3 lists the configuration files that get generated based on the type of phone that is running SIP.

Table 10-3 SIP Configuration Files That the TFTP Server Generates

SIP Configuration File Type	Model 7970/71, 7961, 7941, 7911	Model 7960/40	Model 7905	Model 7912
SIP IP Phone	SEP<mac>.cnf.xml	SIP<mac>.cnf	ld<mac>	gk<mac>
Dial Plan	DR<dialplan>.xml	<dialplan>.xml	Parameter in ld<mac>	Parameter in gk<mac>
Softkey Template	SK<softkey_template>.xml	Not configurable	Not configurable	Not configurable

The system derives filenames from the MAC Address and Description fields in the Phone Configuration window of Cisco Unified Communications Manager Administration and the devicename field in the Cisco Unified Communications Manager database. The MAC address uniquely identifies the phone.

Configuration Sequence for a Phone That Is Running SIP

The configuration sequence for a phone that is running SIP performs the following steps:

1. The administrator makes a change to the phone that is running SIP (for example, by using Phone Configuration, SIP Profile Configuration, or SIP Security Configuration in Cisco Unified Communications Manager Administration) and clicks Save.
2. The Cisco Unified Communications Manager database sends a change notification to the TFTP server and to Cisco Unified Communications Manager. The TFTP server then rebuilds all the configuration files for the selected phone. The configuration file name and format depend on the device type and protocol (see [Table 10-3](#)).
3. The administrator presses the reset/restart button to reset/restart the phones that are affected by the changes.
4. Upon notification (automatically, by the administrator, or by the user), Cisco Unified Communications Manager notifies the phone to get the configuration files again.
5. The phone that is running SIP requests the configuration files from the TFTP server, and the server sends the requested files to the phone.
6. After getting the necessary configuration files, the phone registers its configured lines with Cisco Unified Communications Manager.

Dial Plan Configuration Sequence for a Phone That Is Running SIP

The dial plan configuration sequence for a phone that is running SIP performs the following steps:

1. The administrator configures the SIP dial plan and associates the dial plan with the phone that is running SIP.
2. The Cisco Unified Communications Manager database sends a change notification to the TFTP server, which triggers the TFTP server to build a new set of files for the phone that is running SIP.
3. The TFTP server rebuilds the Dial Plan configuration file and/or the configuration file for the phone that is running SIP.
4. When all the updates to the dial rules have been made to the Cisco Unified Communications Manager database, the administrator clicks the Reset or Restart button to apply the change to the phone.

Softkey Template Configuration Sequence for a Phone That Is Running SIP

The softkey template configuration sequence for a phone that is running SIP performs the following steps:

1. The administrator configures the SIP softkey template and associates the softkey template with the phone that is running SIP.
2. The Cisco Unified Communications Manager database sends a change notification to the TFTP server, which triggers the TFTP server to build a new set of files for the phone that is running SIP.
3. The TFTP server rebuilds the softkey template configuration file and/or the configuration file for the phone that is running SIP.
4. When all the updates to the softkeys have been made to the Cisco Unified Communications Manager database, the administrator presses the Reset or Restart button to apply the change to the phone.

Interaction with Cisco Extension Mobility

When a user logs in to a device by using Cisco Extension Mobility, the Cisco Unified Communications Manager database notifies the TFTP server to rebuild the SEP<mac>.cnf.xml file to include the new dial plan filenames that are defined for the lines on the device profile.

Serviceability Counters

The TFTP server provides counters in Cisco Unified Serviceability for troubleshooting purposes.



Tip

If the TFTP server returns a “file not found” message to the device, a “request not found” TFTP counter increments. In nonsecure clusters, this behavior does not represent an error because the CTL file does not exist on a Cisco Unified Communications Manager in nonsecure mode.

See the *Cisco Unified Communications Manager Real-Time Monitoring Tool Administration Guide* for more information.

Understanding How Devices Use DHCP and Cisco TFTP

Cisco telephony devices require IP addresses that are assigned manually or by using DHCP. Devices also require access to a TFTP server that contains device loads and device configuration files.

Obtaining an IP Address

If DHCP is enabled on a device, DHCP automatically assigns IP addresses to the device when you connect it to the network. The DHCP server directs the device to a TFTP server (or to a second TFTP server, if available for the device). For example, you can connect multiple Cisco Unified IP Phones anywhere on the IP network, and DHCP automatically assigns IP addresses to them and provides them with the path to the appropriate TFTP server.

If DHCP is not enabled on a device, you must assign it an IP address and configure the TFTP server locally on the device.

The default DHCP setting varies depending on the device:

- Cisco Unified IP Phones stay DHCP-enabled by default. If you are not using DHCP, you need to disable DHCP on the phone and manually assign it an IP address.
- DHCP remains always enabled for Cisco Access Analog and Cisco Access Digital Gateways.
- For Cisco Catalyst 6000 8 Port Voice T1/E1 and Services Modules, the Network Management Processor (NMP) on the Cisco Catalyst 6000 may or may not have DHCP enabled. If DHCP is not enabled, you will need to configure the IP address through the Cisco CATOS command-line interface on the Cisco Catalyst 6000.

Requesting the Configuration File

After a device obtains an IP address, it requests a configuration file from the TFTP server.

If a device has been manually added into the Cisco Unified Communications Manager database, the device accesses a configuration file that corresponds to its device name. If a phone is not manually configured and auto-registration is enabled, the phone requests a default configuration file from the TFTP server and starts the auto-registration procedure with Cisco Unified Communications Manager.



Note

Phones represent the only device type that can auto-register and that have default configuration files. You must manually add all other devices to the Cisco Unified Communications Manager database.

If a phone has an XML-compatible load, it requests a .cnf.xml format configuration file; otherwise, it requests a .cnf file.

**Note**

When you set the Build CNF Type service parameter to Build All, the TFTP server builds both .cnf.xml and .cnf format configuration files for all devices. When you set this service parameter to Build None, the TFTP server builds only .cnf.xml files for all devices. When this parameter is set to Build Selective, which is the default value, the TFTP server builds .cnf.xml files for all devices and, in addition, builds .cnf files only for a select list of devices that do not support .cnf.xml. [Table 10-1](#) provides a list of these devices.

Contacting Cisco Unified Communications Manager

After obtaining the configuration file from the TFTP server, a device attempts to make a TCP connection to the highest priority Cisco Unified Communications Manager in the list that is specified in the configuration file. If the device was manually added to the database, Cisco Unified Communications Manager identifies the device. If auto-registration is enabled in Cisco Unified Communications Manager, phones that were not manually added to the database attempt to auto-register in the Cisco Unified Communications Manager database.

Cisco Unified Communications Manager informs devices that are using .cnf format configuration files of their load ID. Devices that are using .xml format configuration files receive the load ID in the configuration file. If the device load ID differs from the load ID that is currently executing on the device, the device requests the load that is associated with the new load ID from the TFTP server and resets itself. For more information on device loads, refer to the [“Device Support” section on page 11-1](#).

A phone gets the Ring Tones list after it performs its booting process, when the user wants to modify the Default Phone Ring setting, and when the user loads new ring tones.

Understanding How Devices That Use IPv4 Access the TFTP Server

**Tip**

This section assumes that the gateway or phone uses IPv4. If you have some devices that use IPv4 and some devices that use IPv6 in your network, Cisco recommends that you use DHCP custom option 150 for IPv4 and the TFTP Server Addresses option, a Cisco vendor-specific information option, for IPv6.

You can enable the IP phones and gateways to discover the TFTP server IP address in one or more of the following ways, depending on the device type:

- Gateways and phones can use DHCP custom option 150.

Cisco recommends this method. With this method, you configure the TFTP server IP address as the option value.

- Gateways and phones can use DHCP option 066.

You may configure either the host name or IP address of the TFTP server as the option value.

- Gateways and phones can query CiscoCM1.

Ensure the Domain Name System (DNS) can resolve this name to the IP address of the TFTP server. Cisco does not recommend this option because it does not scale.

- You can configure phones with the IP address of the TFTP server. If DHCP is enabled on the phone, you can still configure an alternate TFTP server IP address locally on the phone that will override the TFTP address that was obtained through DHCP.

- Gateways and phones also accept the DHCP Optional Server Name (sname) parameter.
- The phone or gateway can use the value of Next-Server in the boot processes (siaddr).

Devices save the TFTP server address in nonvolatile memory. If one of the preceding methods was available at least once, but is not currently available, the device uses the address that is saved in memory.

You can configure the TFTP service on the first node or a subsequent node, but usually you should configure it on the first node. For small systems, the TFTP server can coexist with a Cisco Unified Communications Manager on the same server.

**Note**

If your Cisco Unified Communications Manager server supports IPv6, dual-stack devices can access a TFTP server by using IPv4 or IPv6 addresses.

Understanding How Phones That Use IPv6 Access the TFTP Server

**Tip**

This section assumes that the phone uses IPv6. If you have some phones that use IPv4 and some phones that use IPv6 in your network, Cisco recommends that you use DHCP custom option 150 for IPv4 and the TFTP Server Addresses sub-option type 1, a Cisco vendor-specific information option, for IPv6.

In an IPv6 network, the DHCPv6 server uses the Cisco vendor-specific DHCPv6 information options in the DHCPv6 response message to pass the TFTP IPv6 address to the device. If the device obtains an IPv6 address and sends a request to the TFTP server while the TFTP server is using IPv4 to process requests, the TFTP server does not receive the request because the TFTP server is not listening for the request on the IPv6 stack. In this case, the device cannot register with Cisco Unified Communications Manager.

You can enable the IP phones to discover the TFTP server IP address in one or more of the following ways, depending on the device type:

- Phones can use the TFTP Server Addresses sub-option type 1, which is a Cisco vendor-specific information option. Consider this option equivalent to Option 150.
Cisco recommends this method. With this method, you configure the TFTP server IP address as the option value.
- Phones can use the TFTP Service sub-option type 2, which is another Cisco vendor-specific information option. Be aware that this option is equivalent to Option 66.
- You can configure phones with the IP address of the TFTP server. If DHCP is enabled on the phone, you can still configure on the phone an alternate TFTP server IP address that overrides the TFTP address that was obtained through DHCP.

Devices save the TFTP server address in nonvolatile memory. If one of the preceding methods was available at least once, but is not currently available, the device uses the address that is saved in memory.

You can configure the TFTP service on the first node or a subsequent node, but usually you should configure it on the first node. For small systems, the TFTP server can coexist with a Cisco Unified Communications Manager on the same server.

**Note**

If your Cisco Unified Communications Manager server supports IPv6, dual-stack devices can access a TFTP server by using IPv4 or IPv6 addresses.

**Tip**

For more information on IPv6 and TFTP, refer to [Internet Protocol Version 6 \(IPv6\)](#) in the *Cisco Unified Communications Manager Features and Services Guide*. Additionally, refer to *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1(x)*.

Understanding How Devices Identify the TFTP Server

The following sections describe how gateways and Cisco Unified IP Phones identify the TFTP server.

Gateways

When gateways receive conflicting or confusing information from the DHCP server, they have an order of precedence that they use for selecting the address of the TFTP server. The basis for the order of precedence depends on the method that is used to specify the TFTP server (method 1 in the following list has the highest precedence).

1. Catalyst 6000 gateway uses a locally configured TFTP server address. This address overrides any TFTP address that the DHCP server sends.
2. The gateway queries the DNS name CiscoCM1, and it is resolved. The gateway always tries to resolve the DNS name CiscoCM1. If this name is resolved, it overrides all information that the DHCP server sends.

You do not need to name the TFTP server CiscoCM1, but you must enter a DNS CName record to associate CiscoCM1 with the address or name of the TFTP server.

3. The gateway uses the value of Next-Server in the boot processes. The address of the TFTP server traditionally uses this DHCP configuration parameter. When BOOTP servers are configured, this field typically serves as the address of the TFTP server.

This information gets returned in the siaddr (server IP address) field of the DHCP header. Use this option, if available, because some DHCP servers will place their own IP address in this field when it is not configured.

4. The gateway that uses IPv4 uses the site-specific option 150. This option resolves the issue in which some servers do not allow the Next-Server configuration parameter. Some servers allow access to the Next-Server parameter only when IP addresses are statically assigned.
5. The gateway uses the Optional Server Name parameter. This DHCP configuration parameter designates the host name of a TFTP server. Currently, you can configure only a host name in this parameter; do not use a dotted decimal IP address.
6. The gateway that uses IPv4 uses the 066 option, which is the name of the boot server. Option 066 normally replaces the sname (server name) field when option overloading occurs. This name field can contain a host name or a dotted decimal IP address. Do not use the 066 option with the 150 option. The device prefers the IP address over the name that is given by the 066 option if they are sent together. If both a dotted decimal IP address and a 150 option are sent, order of preference depends on the order in which they appear in the option list. The device chooses the last item in the option list because option 066 and option 150 remain mutually exclusive.

Cisco Unified IP Phones



Tip

Methods two and four apply to phones that use IPv6 only or both IPv4 and IPv6 in dual-stack mode. For phones that only use IPv4, disregard methods two and four.

Similar to gateways, Cisco Unified IP Phones 7971, 7970, 7961, 7941, 7931, 7911, 7906, 7960, and 7940 (that are using release 8.0(4) firmware and later) also have an order of precedence that they use for selecting the address of the TFTP server when they receive conflicting or confusing information from the DHCP server. The method that is used to specify the TFTP server (method 1 in the following list has the highest precedence) provides basis for the order of precedence.

1. Cisco Unified IP Phones use a manually configured alternate TFTP option (IPv4 or IPv6), which is under the Settings Menu on the phone. When the alternate TFTP option is set to Yes locally on IP phones, both TFTP Server 1 and TFTP Server 2 address values override any TFTP addresses that the DHCP server sent.
2. Cisco Unified IP Phones use the TFTP Server Addresses option, which is the IPv6 address of the TFTP server. A maximum of two IP addresses get used, and only the first two IP addresses that the DHCP server provides get accepted.
3. Cisco Unified IP Phones use the option 150 value as the TFTP server IP address when Alternate TFTP option is set to No. You can assign only IP addresses as Option 150 values. A maximum of two IP addresses get used, and only the first two IP addresses that the DHCP server provides get accepted.
4. Cisco Unified IP Phones use the TFTP Service, which is a DNS name of the TFTP server. You cannot use multiple entries as part of this option values.
5. Cisco Unified IP Phones that use 066 option, which could be either a name (option 66 = DNS name) or dotted-decimal IP address (option 66 = dotted-decimal IP address) of the TFTP server. Be aware that the name may resolve to more than one address. Option 066 normally replaces the sname (server name) field when option overloading occurs. This name field can contain a DNS name or a dotted decimal IP address. You cannot use multiple entries as part of this option values.
6. Cisco Unified IP Phones use the value of Next-Server IP Address in the boot-up processes as its TFTP server IP address. This DHCP configuration parameter traditionally gives the address of the TFTP server. Be aware that the name may resolve to more than one address. When you configure BOOTP servers, this field typically gets referred to as the address of the TFTP server. The siaddr (server IP address) field of the DHCP header returns this information.
7. Cisco Unified IP Phones use the Optional Server Name parameter name as the TFTP server name. This DHCP configuration parameter represents the DNS name of a TFTP server. Currently you can configure only a DNS name in this parameter; do not use a dotted decimal IP address.

Cisco recommends that you use DHCP custom option 150 for gateways and phones that use IPv4 or dual-stack devices. With this method, the TFTP server IP address gets configured as the option 150 value. Phones only support two IP addresses for Option 150 values as TFTP Server 1 and TFTP Server 2 entries.



Note

Be aware that option 66 is defined to be a string type, option 150 is defined as an array of 32-bit IP address(es), and both TFTP Server 1 and TFTP Server 2 are 32 bit IP addresses.

Configuring a Redundant TFTP Server

You must have one TFTP server that is configured in a cluster; however, you may want to configure a redundant TFTP server. If a device (phone or gateway) gets no response from the first TFTP server, it tries to connect to the second TFTP server. Configure the second TFTP server in option 150 for IPv4 or the TFTP Server Addresses sub-option type 1 for IPv6 in the DHCP scope.

If the TFTP servers that are in the middle of rebuilding all configuration files return a delay message to the requesting device, the device does not attempt to use the second TFTP server; instead, it waits and retries the first TFTP server from which it received the message.

Alternate Cisco File Servers

You can specify alternate Cisco file servers if you have multiple clusters, if you want to configure only one server for many DHCP scopes, or if you want to have one DHCP scope. You can specify up to 10 alternate servers by entering a value in any of the Alternate Cisco File Server fields of the Cisco TFTP service parameter. For more information on service parameters, refer to the [“Service Parameters Configuration”](#) chapter in the *Cisco Unified Communications Manager Administration Guide*.

You can use either of the following syntax examples:

- `host://<IP of the off-cluster TFTP server>` (for example, `host://10.10.134.24`)
- `HOST://<IP of the off-cluster TFTP server>` (for example, `HOST://10.10.134.24`)

If DNS is also supported, you can also use one of the following syntax examples:

- `host://<name of the off-cluster TFTP server>` (for example, `host://tftp-prim`)
- `HOST://<name of the off-cluster TFTP server>` (for example, `HOST://tftp-second`)

You cannot use any other syntax.



Note

Cisco Unified Communications Manager supports both IPv4 and IPv6 addresses and hostnames that resolve to IPv4 and IPv6 addresses for alternate TFTP servers. The Enable IPv6 enterprise parameter does not affect serving files to off-cluster TFTP servers. If the TFTP server supports a dual IPv4/IPv6 stack, you can configure both an IPv4 and an IPv6 entry for an Alternate server and the system accesses the servers in the order that is configured.

The primary TFTP server should have the Alternate Cisco File Server (1 to 10) values set for external Cisco Unified Communications Manager clusters. The primary TFTP server serves configuration files from these servers for phones and devices in the external clusters. To avoid creating a loop, ensure that the TFTP servers on the external clusters do not point to each other.

Centralized TFTP in a Multiple Cluster Environment

Centralized TFTP supports multiple Cisco Unified Communications Manager clusters within one regional, or site-specific environment, such as a large campus. Centralized TFTP allows devices (phones and gateways) to be moved, such as from one building to another, without requiring the administrator to reconfigure the device's IP settings (for example, DHCP, VLAN/DHCP).

Another example would be when several T1s terminate at the same demarcation point, but the T1s are to be distributed to several clusters, the administrator needs only to configure the T1s in the appropriate clusters and have the DHCP scope point the TFTP requests to the Master TFTP Server. The Centralized TFTP solution will provide the appropriate cluster-specific information to the individual T1s.

Centralized TFTP also supports multiple clusters that are running different operating systems. Devices that are registered and configured in any cluster can be directed to use a single TFTP server (the Master TFTP Server) that then serves cluster-specific files to those devices.

The following sections describe how Centralized TFTP works in a Cisco Unified Communications Manager multicluster environment:

- [Master TFTP Server, page 10-12](#)
- [Sending Files to the Master TFTP Server, page 10-12](#)
- [Centralized TFTP with Secure Clusters, page 10-13](#)
- [Configuration Tips for Centralized TFTP, page 10-13](#)

Master TFTP Server

Each cluster must have at least one TFTP server. The primary function of the TFTP server is to build endpoint configuration files and to serve all files (such as configuration, security, firmware) to the endpoints.

In the Centralized TFTP environment, the Master TFTP Server represents a name that is applied to a single TFTP server, which gets designated to serve all files including security, firmware, and configuration files from all of the Cisco Unified Communications Manager clusters. Make this designation by simply directing all requests at the Master TFTP Server, either by hard-coding or by DHCP configuration at the endpoints.

If the Master TFTP Server does not find the requested file in its local cache, it begins a sequential search of each of the configured Alternate Cisco File Server service parameters. If the file is found in one of these off-cluster locations, the file gets sent to the Master TFTP Server via HTTP. The Master TFTP Server then serves the file to the endpoint via TFTP. If the alternate file server does not respond, the request eventually times out if the response is not received within a set time. The Master TFTP Server will then inform the endpoint.

Cisco strongly recommends that the Master TFTP Server belong to the cluster that has the most devices configured. In general, the system assumes that this configuration will provide the greatest chance for files to be found in the TFTP server cache and, therefore, will reduce the number of off-cluster searches.

Sending Files to the Master TFTP Server

When an off-cluster TFTP server receives a request from the Master TFTP Server, it searches for the file and, if found, sends the requested file back to the Master TFTP Server by using HTTP. The Master TFTP Server then uses TFTP to send the requested file to the device that originally requested the file. Should the off-cluster TFTP server not have the requested file, it will respond to the Master TFTP Server with File Not Found (HTTP Error 404). The Master TFTP Server continues the process with the next off-cluster TFTP server until either the file is located or no remaining options exist.

When the off-cluster server is busy, it sends HTTP Error 503 to the Master TFTP Server, so it should try the request again later. This message will also get sent to the endpoint device that made the original request.

Centralized TFTP with Secure Clusters

All off-cluster servers that are operating in mixed mode must add the Master TFTP Server or Master TFTP Server IP address to the off-clusters CTL file. (Without this updated CTL file, phones that register to a cluster where security is enabled and that attempt to download their config files will fail.) After the CTL file is updated, reboot the servers, so they can participate in the secure multicluster centralized TFTP network.

To update the CTL file for the TFTP servers, download the CTL Client plug-in by using **Application > Install Plugins** from Cisco Unified Communications Manager Administration. For more information about the CTL client and how to configure TFTP for security, refer to the *Cisco Unified Communications Manager Security Guide*.

Configuration Tips for Centralized TFTP

The following list comprises tips to remember when you are configuring a centralized TFTP environment:

- Only the master TFTP server gets configured with the Alternate Cisco File Server values.
- Ensure all off-cluster TFTP servers do not have Alternate Cisco File Server values configured. Refer to “[Service Parameters Configuration](#)” in the *Cisco Unified Communications Manager Administration Guide* for information on how to configure the TFTP service.
- You can configure 1 to 10 Alternate Cisco File Servers in the Cisco TFTP Service Parameters Configuration window. If Alternate Cisco File Server 1 contains an empty parameter value, TFTP will stop searching for alternate servers. For example, if Alternate Cisco File Servers 2 through 10 are configured, and 1 is empty, and TFTP is searching for servers, it will not search Alternate Cisco File Servers 2 through 10.
- When phones are configured in a Cisco Unified Communications Manager other than the cluster where the master TFTP server is configured, and auto-registration is enabled, and the off-cluster Cisco Unified Communications Manager goes down, if the phones are configured to submit a request from the centralized TFTP server, they may inadvertently get auto-registered on the central Cisco Unified Communications Manager. Therefore, you should disable auto-registration if it is not already disabled or delete the inadvertently registered phone after making sure that the cluster to which it belongs is up and running.
- For centralized TFTP configurations, ensure that the master TFTP server exists in the cluster that runs the highest version of Cisco Unified Communications Manager; for example, if you are using a centralized TFTP server between a compatible Cisco Unified CallManager 4.X cluster and a Cisco Unified Communications Manager 7.1 cluster, ensure that your master TFTP server exists in the Cisco Unified Communications Manager 7.1 cluster. If the master TFTP server exists in the cluster that runs the lower version of Cisco Unified Communications Manager, phones use locale files from the lower version of Cisco Unified Communications Manager, which can cause issues with the phone; for example, the phone displays Undefined or ??? for the Do Not Disturb feature instead of displaying that DND is active. These errors display on the phone because the locale files that are served to the phones from the master cluster do not include the localized phrases.

Customizing and Modifying Configuration Files

You can add customized files (for example, ring tones, callback tones, phone backgrounds). Refer to the *Cisco Unified Communications Operating System Administration Guide* for information on how to implement custom files and how to modify their corresponding system configuration files. If two TFTP servers exist in the cluster, ensure that the customized files are placed on both TFTP servers.

Where to Find More Information

Related Topic

- [TFTP Configuration Checklist](#), page 10-2
- [TFTP Process Overview for Devices That Run SCCP](#), page 10-3
- [TFTP Process Overview for Cisco Unified IP Phones That Run SIP](#), page 10-4
- [Understanding How Devices Use DHCP and Cisco TFTP](#), page 10-6
- [Understanding How Devices That Use IPv4 Access the TFTP Server](#), page 10-7
- [Understanding How Phones That Use IPv6 Access the TFTP Server](#), page 10-8
- [Understanding How Devices Identify the TFTP Server](#), page 10-9
- [Configuring a Redundant TFTP Server](#), page 10-11
- [Centralized TFTP in a Multiple Cluster Environment](#), page 10-11
- [Alternate Cisco File Servers](#), page 10-11
- [Configuration Tips for Centralized TFTP](#), page 10-13
- [Customizing and Modifying Configuration Files](#), page 10-14
- [SIP Dial Rules](#), page 19-4
- [Service Parameters Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [DHCP Subnet Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [DHCP Server Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [SIP Dial Rules Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [SIP Profile Configuration](#), *Cisco Unified Communications Manager Administration Guide*
- [Internet Protocol Version 6 \(IPv6\)](#), *Cisco Unified Communications Manager Features and Services Guide*
- [Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1\(x\)](#)
- [Cisco Unified Communications Operating System Administration Guide](#)