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 CallManagers for a device (SCCP and SIP phones and gateways), the TCP ports on which the device connects to those Cisco Unified CallManagers, 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.

Configuration files may be 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 BuildCNFType 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 CallManager, TFTP, and Dynamic Configuration Protocol (DHCP) as well as the relationship between devices and the TFTP server. This section contains the following topics:

- TFTP Process Overview for SCCP Devices, page 10-2
- TFTP Process Overview for Cisco SIP IP Phones, page 10-3

TFTP Process Overview for SCCP Devices

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 model, 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 an internal cache, then primary and alternate paths (if specified) for the configuration file. If the TFTP server finds the configuration file, it sends it to the device. If the device receives the Cisco Unified CallManager name, it resolves the name by using DNS and opens a Cisco Unified CallManager connection. If the device does not receive an IP address or name, it uses the default server name.

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

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 10-4.

TFTP Process Overview for Cisco SIP IP Phones

Unlike SCCP phones, SIP phones get all of their configurations from the TFTP server. From initial startup, the SIP phone 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 CallManager.

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

The TFTP support for SIP phones builds and serves different formats of SIP configuration files from the Cisco Unified CallManager database for the following Cisco SIP 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 phone models
- Softkey templates on the preceding phone models

The TFTP server generates the following files from the Cisco Unified CallManager database for SIP phone configuration:

- 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.

The following configuration files get generated based on the SIP phone type.

Table 10-2 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 CallManager Administration and the devicename field in the Cisco Unified CallManager database. The MAC address uniquely identifies the phone.

SIP Phone Configuration Sequence

The SIP phone configuration sequence performs the following steps:

1. The administrator makes a change to the SIP phone (for example, by using either Phone Configuration, SIP Profile Configuration, or SIP Security Configuration in Cisco Unified CallManager Administration) and initiates a restart or reset of the phone.

2. The Cisco Unified CallManager database sends a change notification to the TFTP server and to Cisco Unified CallManager.
3. Upon notification (either automatically or by the administrator or user resetting or restarting the phone), Cisco Unified CallManager notifies the phone to get the configuration files again. 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 10-2).
4. The SIP phone requests the configuration files from the TFTP server.
5. After getting the necessary configuration files, the phone registers its configured lines with Cisco Unified CallManager.

SIP Phone Dial Plan Configuration Sequence

The SIP phone dial plan configuration sequence performs the following steps:

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

SIP Phone Softkey Template Configuration Sequence

The SIP phone softkey template configuration sequence performs the following steps:

1. The administrator configures the SIP softkey template and associates the softkey template with the SIP phone.
2. The Cisco Unified CallManager database sends a change notification to the TFTP server, which triggers the TFTP server to build a new set of files for the SIP phone.
3. The TFTP server rebuilds the softkey template configuration file and/or the configuration file for the SIP phone.
4. When all the updates to the softkeys have been made to the Cisco Unified CallManager 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 CallManager 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 CallManager Serviceability for troubleshooting purposes. See the *Cisco Unified CallManager Serviceability System Guide* and the *Cisco Unified CallManager Serviceability 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 (through DHCP or manual assignment), it requests a configuration file from the TFTP server.

If a device has been manually added into the Cisco Unified CallManager 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 CallManager.

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 CallManager 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 BuildCNFType 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 CallManager

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

Cisco Unified CallManager 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.

After a telephone is ready to make a call, it will request an available ringer list from the TFTP server. If the telephone user changes the ring type, the TFTP server sends the new ring type.

Understanding How Devices Access the TFTP Server

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 CallManager on the same server.

Understanding How Devices Identify the TFTP Server

Phones and gateways use an order of precedence for selecting the address of the TFTP server if they receive conflicting or confusing information from the DHCP 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. The phone or Catalyst 6000 gateway uses a locally configured TFTP server address.

   This address overrides any TFTP address that the DHCP server sends.

2. The phone or gateway queries the DNS name CiscoCM1, and it is resolved.

   The phone or 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. Cisco does not recommend this option because it does not scale.

3. The phone or 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 phone or gateway uses the site-specific option 150.

   This option resolves the issue that 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 phone or 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 phone or gateway 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.

Configuring a Backup or Fallback TFTP Server

You should configure only one TFTP server in a cluster unless you want to have a backup or a fallback TFTP server. If a device (phone or gateway) gets no response from the first TFTP server and if a fallback TFTP server is configured, the device will try to connect to the second TFTP server. The fallback TFTP server gets configured by option 150 in DHCP to a list of two TFTP servers in the same cluster.

Centralized TFTP in a Multiple Cluster Environment

A Centralized TFTP server supports multiple clusters within one large campus environment. The Centralized TFTP server design allows phones to be moved from one building to another within a campus. It also supports a mixed OS multicluster environment.

Devices that are registered and configured in any clusters can home into a single TFTP server (Centralized TFTP server) that will then serve files to those devices. The following sections describe how the Centralized TFTP server works in a Cisco Unified CallManager multicluster environment:

- Master Centralized TFTP Server, page 10-8
- Sending Files to the Master Centralized TFTP Server, page 10-8

Master Centralized TFTP Server

You can configure a single TFTP server to build the configuration files for devices in its cluster, to serve all security, firmware, and configuration files to those devices. This single server, a Master Centralized Server, serves files from all the other Cisco Unified CallManager clusters. The centralized TFTP server in the other clusters will build files only for devices that are configured for that particular cluster. All endpoint requests get sent to the master centralized TFTP server, either by hard coding or by DHCP configuration at the endpoint.

The master centralized TFTP queries files from other centralized TFTP servers if the requested file(s) is not found in the local cache of the master centralized TFTP server. When the master centralized TFTP server receives a file request, it looks first in the local cache for the requested file. If the file does not exist there, then the master centralized TFTP server will request the file from the other configured centralized TFTP servers. The request will eventually time out, if the response is not received within a set amount of time.

Sending Files to the Master Centralized TFTP Server

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

The off-cluster server indicates to the master centralized TFTP server, by using an HTTP Error 503 that it is busy and that the master centralized TFTP server should try the request again later. This message will also get sent to the endpoint device that made the original request.

Alternate TFTP Paths

You can specify alternate TFTP paths if you have multiple clusters. You only want to configure one server for many DHCP scopes or want to have one DHCP scope. The directory must be on the same node where the TFTP service is running. The TFTP server stores files for the cluster that contains the TFTP server in the primary path and stores the files for the other clusters in alternate paths. You can specify up to 10 alternate paths by entering a value for the Alternate File Location fields of the Cisco TFTP service parameter. For more information on service parameters, refer to the “Service Parameters Configuration” chapter in the *Cisco Unified CallManager Administration Guide*.

The alternate path can be a remote server. You can use either of the following syntax examples:

- host://<IP of the off-cluster TFTP server> (e.g., host://10.89.134.24)
- HOST://IP of the off-cluster TFTP server> (e.g., HOST://10.89.134.24)

No other syntax is allowed.

The primary TFTP server should have the alternate path values set for external Cisco Unified CallManager clusters. The primary TFTP server serves configuration files from the alternate path for phones and devices in the external clusters. You ensure that the TFTP servers on the external clusters point to this shared file path by setting it as their primary path (that is, by setting it as the File Location service parameter).

Configuration Tips for Centralized TFTP

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

- You should configure only the master centralized TFTP server with alternate file locations specified in its list. Off-cluster TFTP servers should have no alternate file locations. See the "Alternate TFTP Paths" section on page 10-8. Refer to "Service Parameters Configuration" in the *Cisco Unified CallManager Administration Guide* for information on how to configure the TFTP service.
- When phones are configured in a Cisco Unified CallManager other than the cluster where the master centralized TFTP server is configured and auto-registration is enabled, and the off-cluster Cisco Unified CallManager 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 CallManager. Therefore, you should disable auto-registration if it is not already disabled.

Customizing and Modifying Configuration Files

You can modify configuration files (for example, edit the xml files) and add customized files (for example, custom ring tones, call back tones, phone backgrounds) to the TFTP directory. You can modify files and/or add customized files to the TFTP directory in Cisco Unified Communications Platform Administration, from the TFTP Server File Upload page. Refer to the *Cisco Unified Communications Operating System Administration Guide* for information on how to upload files to the TFTP folder on a Cisco Unified CallManager server.

TFTP Configuration Checklist

Table 10-3 lists the steps that are needed to configure the Cisco TFTP service.

Table 10-3 TFTP Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Activate and start the Cisco TFTP service on the appropriate server.	*Cisco Unified CallManager Serviceability Administration Guide*

Table 10-3 TFTP Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 2	Configure the appropriate service parameters, including the Alternate File Location parameters, if appropriate.	Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*
Step 3	If you change a non-configuration file such as a load file or RingList.xml, start and stop the Cisco TFTP service or set the service parameter, Enable Caching of Constant and Bin Files at Startup TFTP, to True (if it is already set to True, set to False, click **Update**, set to True again, and click **Update**). **Note** You must upload files to the TFTP directory from Cisco Unified Communications Platform Administration. Refer to the *Cisco Unified Communications Operating System Administration Guide* for more information.	*Cisco Unified CallManager Serviceability Administration Guide* Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*

Where to Find More Information

Related Topic

- SIP Dial Rules, page 19-4
- Service Parameters Configuration, *Cisco Unified CallManager Administration Guide*
- DHCP Subnet Configuration, *Cisco Unified CallManager Administration Guide*
- DHCP Server Configuration, *Cisco Unified CallManager Administration Guide*
- SIP Dial Rules Configuration, *Cisco Unified CallManager Administration Guide*
- SIP Profile Configuration, *Cisco Unified CallManager Administration Guide*
- *Cisco Unified Communications Operating System Administration Guide*