



Cisco TFTP

The Cisco TFTP service builds and serves files that are consistent with the trivial file transfer protocol, which is a simplified version of the File Transfer Protocol (FTP). 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 CallManagers for a device (telephones and gateways), the TCP port on which the device connects to those Cisco CallManagers, and an executable load identifier. Configuration files for selected devices, including Cisco IP Phone 7960, 7940, and 7935 models, also contain 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 format or a .cnf.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 8-1](#):

Table 8-1 *Devices with Build Selective BuildCNFType*

Device Type	Device Name
MODEL_30SPP	Cisco 30 SP+
MODEL_12SPP	Cisco 12 SP+

Table 8-1 *Devices with Build Selective BuildCNFType (continued)*

Device Type	Device Name
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 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, page 8-2](#)
- [Understanding How Devices Use DHCP and Cisco TFTP, page 8-3](#)
- [Understanding How Devices Access the TFTP Server, page 8-5](#)
- [Understanding How Devices Identify the TFTP Server, page 8-6](#)
- [Alternate TFTP Paths, page 8-8](#)
- [Configuring a Backup or Fallback TFTP Server, page 8-8](#)
- [TFTP Configuration Checklist, page 8-9](#)
- [Where to Find More Information, page 8-9](#)

TFTP Process Overview

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 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 CallManager name, it resolves the name by using DNS and opens a Cisco 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 processing the maximum number of requests (60, which is the maximum serving count) receive an error message from the TFTP server, which causes the device to request the configuration file later.

For a more detailed description of how devices boot, see the [“Understanding How Devices Use DHCP and Cisco TFTP”](#) section on page 8-3.

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 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 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 IOS 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 CallManager database, the device accesses a configuration file that corresponds to its device name. If auto-registration is enabled in Cisco CallManager, the phones access a default configuration file from the TFTP server.



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 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 8-1](#) provides a list of these devices.

Contacting Cisco CallManager

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

Cisco 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, see the [“Device Support” section on page 9-1](#).

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 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 a database publisher or subscriber, but usually you should configure it on a publisher. For small systems, the TFTP server can coexist with a Cisco CallManager on the same server.

Understanding How Devices Identify the TFTP Server

Phones and gateways have an order of precedence that they use 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 given by the 066 option if they are sent together. However, 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.

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 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 `AlternateFileLocation` parameters. For more information on TFTP service parameters, refer to the [“Service Parameters Configuration”](#) in the *Cisco CallManager Administration Guide*.

The primary TFTP server should have the alternate path values set for external CallManager clusters. The primary TFTP server serves configuration files from the alternate path for phones and devices in the external clusters. The TFTP servers on the external clusters should point to this shared file path by setting it as their primary path (that is, by setting it as the File Location service parameter). Note that TFTP servers in the external clusters build and write the configuration files on the shared "alternate path" location, so the path should be a shared accessible directory across all clusters. The main TFTP server can have caching on, but other TFTP servers must have it off.

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.

TFTP Configuration Checklist

Table 8-2 lists the steps that are needed to configure the Cisco TFTP service.

Table 8-2 TFTP Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Activate and start the TFTP service on the appropriate server.	<i>Cisco CallManager Serviceability Administration Guide</i>
Step 2	Configure the appropriate service parameters, including the Alternate File Location parameters, if appropriate.	Service Parameters Configuration , <i>Cisco CallManager Administration Guide</i>
Step 3	If you change a non-configuration file such as a load file or RingList.xml, start and stop the TFTP service or disable and re-enable the “Enable Caching of Constant and Bin Files at Startup” TFTP service parameter.	<i>Cisco CallManager Serviceability Administration Guide</i> Service Parameters Configuration , <i>Cisco CallManager Administration Guide</i>

Where to Find More Information

Related Topic

- [Service Parameters Configuration](#), *Cisco CallManager Administration Guide*

