



# Cisco IP Phone Installation

---

- [Verify the Network Setup, on page 1](#)
- [Install the Cisco IP Phone, on page 2](#)
- [Activation Code Onboarding, on page 3](#)
- [Configure the Network from the Phone, on page 4](#)
- [Verify Phone Startup, on page 11](#)
- [Configure the Voice Codecs, on page 11](#)
- [Set the Optional Network Servers, on page 12](#)
- [VLAN Settings, on page 12](#)
- [SIP and NAT Configuration, on page 20](#)
- [Dial Plan, on page 30](#)
- [Regional Parameters and Supplementary Services, on page 38](#)
- [Cisco IP Phone 7800 Series Documentation, on page 43](#)

## Verify the Network Setup

Upon deployment of a new IP telephony system, system administrators and network administrators must complete several initial configuration tasks to prepare the network for IP telephony service.

For the phone to operate successfully as an endpoint in your network, your network must meet specific requirements.



---

**Note** The phone displays the date and time from Third-Party Call Control. The time displayed on the phone can differ from the Third-Party Call Control time by up to 10 seconds.

---

### Procedure

---

**Step 1** Configure a VoIP Network to meet the following requirements:

- VoIP is configured on your Cisco routers and gateways.
- Third-Party Call Control is installed in your network and is configured to handle call processing.

- Step 2** Set up the network to support one of the following:
- DHCP support
  - Manual assignment of IP address, gateway, and subnet mask
- 

## Install the Cisco IP Phone

After the phone connects to the network, the phone startup process begins, and the phone registers with the third party server. To finish installing the phone, configure the network settings on the phone depending on whether you enable or disable DHCP service.

If you used autoregistration, you need to update the specific configuration information for the phone such as associating the phone with a user, changing the button table, or directory number.



---

**Note** Before using external devices, read [External Devices](#).

---

If you only have one LAN cable at your desk, you can plug your phone into the LAN with the SW port and then connect your computer into the PC port.

You can also daisy chain two phones together. Connect the PC port of the first phone to the SW port of the second phone.



---

**Caution** Do not connect the SW and PC ports into the LAN.

---

### Procedure

---

**Step 1** Choose the power source for the phone:

- Power over Ethernet (PoE)
- External power supply

For more information, see [Phone Power Requirements](#).

**Step 2** Connect the handset to the handset port.

The wideband-capable handset is designed especially for use with a Cisco IP Phone. The handset includes a light strip that indicates incoming calls and waiting voice messages.

**Step 3** Connect a headset to the headset port. You can add a headset later if you do not connect one now.

**Note** The Cisco IP Phone 7811 does not have a headset port.

**Step 4** Connect a wireless headset. You can add a wireless headset later if you do not want to connect one now. For more information, see your wireless headset documentation.

**Note** The Cisco IP Phone 7811 does not support a headset.

- Step 5** Connect a straight-through Ethernet cable from the switch to the network port labeled 10/100 SW on the Cisco IP Phone (10/100/1000 SW on Cisco IP Phone 7841). Each Cisco IP Phone ships with one Ethernet cable in the box.
- Use Category 3, 5, 5e, or 6 cabling for 10 Mbps connections; Category 5, 5e, or 6 for 100 Mbps connections; and Category 5e or 6 for 1000 Mbps connections. For more information, see [Network and Computer Port Pinouts](#).
- Step 6** Connect a straight-through Ethernet cable from another network device, such as a desktop computer, to the computer port on the Cisco IP Phone. You can connect another network device later if you do not connect one now.
- Use Category 3, 5, 5e, or 6 cabling for 10 Mbps connections; Category 5, 5e, or 6 for 100 Mbps connections; and Category 5e or 6 for 1000 Mbps connections. For more information, see [Network and Computer Port Pinouts](#) for guidelines.
- Step 7** If the phone is on a desk, adjust the footstand. With a wall-mounted phone, you might need to adjust the handset rest to ensure that the receiver cannot slip out of the cradle.
- Note** You cannot adjust the Cisco IP Phone 7811 footstand.
- Step 8** Monitor the phone startup process. This step verifies that the phone is configured properly.
- Step 9** If you are configuring the network settings on the phone, you can set up an IP address for the phone by either using DHCP or manually entering an IP address.
- See [Configure the Network from the Phone, on page 4](#)
- Step 10** Upgrade the phone to the current firmware image.
- Firmware upgrades over the WLAN interface may take longer than upgrading over the wired interface, depending on the quality and bandwidth of the wireless connection. Some upgrades may take more than one hour.
- Step 11** Make calls with the Cisco IP Phone to verify that the phone and features work correctly.
- See the *Cisco IP Phone 7800 Series User Guide*.
- Step 12** Provide information to end users about how to use their phones and how to configure their phone options. This step ensures that users have adequate information to successfully use their Cisco IP Phones.

---

#### Related Topics

[Verify Phone Startup](#), on page 11

[Verify the Network Setup](#), on page 1

## Activation Code Onboarding

If your network is configured for Activation Code Onboarding, you can set up new phones to register automatically in a secure way. You generate and provide each user with a unique 16-digit activation code. The user enters the activation code, and the phone automatically registers.

Activation codes can be used only once, and have an expiry date. If a user enters an expired code, the phone displays `Invalid activation code` on the screen. If this happens, provide the user with a new code.

This feature is available in firmware release 11-2-3MSR1, BroadWorks Application Server Release 22.0 (patch AP.as.22.0.1123.ap368163 and its dependencies). However, you can change phones with older firmware to use this feature. To do this, use the following procedure.

### Before you begin

Ensure that you allow the `activation.webex.com` service through your firewall to support onboarding via activation code.

Access the phone web page . See [Access the Phone Web Page](#)

### Procedure

- 
- Step 1** Reset the phone to the factory settings.
  - Step 2** Select **Voice > Provisioning > Configuration Profile**.
  - Step 3** Enter the profile rule in the **Profile Rule** field in this format: `gds://`
  - Step 4** Select **Firmware Upgrade**.
  - Step 5** Enter the upgrade rule in the **Upgrade Rule** field in this format: `http://<server ip address>/sip88xx.11-2-3MSR1-1.loads/`
  - Step 6** Submit All Changes.

See below a sample `cfg.xml` file showing the profile rule, and upgrade rule.

```
<?xml version="1.0" encoding="UTF-8"?>
<device>
<flat-profile>
<!-- System Configuration -->
<Profile_Rule ua="na">gds://</Profile_Rule>
<!-- Firmware Upgrade -->
<Upgrade_Enable ua="na">Yes</Upgrade_Enable>
<Upgrade_Error_Retry_Delay ua="na">3600</Upgrade_Error_Retry_Delay>
<Upgrade_Rule ua="na">http://<server ip address>/sip88xx.11-2-3MSR1-1.loads</Upgrade_Rule>
<!-- <BACKUP_ACS_Password ua="na"/> -->
</flat-profile>
</device>
```

---


## Configure the Network from the Phone

The phone includes many configurable network settings that you may need to modify before it is functional for your users. You can access these setting through the phone menus.

The Network configuration menu provides you with options to view and configure a variety of network settings.

You can configure settings that are display-only on the phone in your Third-Party Call Control system.

## Procedure

- 
- Step 1** Press **Applications** .
  - Step 2** Select **Network configuration**.
  - Step 3** Use the navigation arrows to select the desired menu and edit.
  - Step 4** To display a submenu, repeat step 3.
  - Step 5** To exit a menu, press **Back**.
- 

## Network Configuration Fields

*Table 1: Network Configurations Menu Options*

Field	Field Type or Choices	Default	Description
Ethernet configuration			See the following Ethernet configuration submenu table.
IP mode	Dual mode IPv4 only IPv6 only	Dual mode	Select the Internet Protocol mode for which the phone operates. In dual mode, the phone can have both IPv4 and IPv6 addresses.
IPv4 address settings	DHCP Static IP Release DHCP IP	DHCP	See the IPv4 address submenu table in the following tables.
IPv6 address settings	DHCP Static IP	DHCP	See the IPv6 address submenu table in the following tables.
DHCPv6 option to use		17, 160, 159	Indicates the order in which the phone uses the IPv6 addresses provided by DHCP server.
Web server	On Off	On	Indicates whether the phone has web server enabled or disabled.

Table 2: Ethernet Configuration Submenu

Field	Field Type or Choices	Default	Description
802.1x authentication	Device authentication	Off	Enables you to turn on or turn off the 802.1x authentication. Valid options are: <ul style="list-style-type: none"> <li>• On</li> <li>• Off</li> </ul>
	Transaction status	Disabled	<ul style="list-style-type: none"> <li>• Transaction status—Indicates different authentication status when you turn on 802.1x in the <b>Device authentication</b> field. <ul style="list-style-type: none"> <li>• Disabled—Default status.</li> <li>• Connecting—802.1x authentication started in the device.</li> <li>• Authenticated—802.1x authentication established in the device.</li> </ul> </li> <li>• Protocol—Specifies the protocol of the server.</li> </ul>
Switch port config	Auto 10MB half 10MB full 100MB half 100MB full 1000 full (except for 7811 and 7821)	Auto	Select speed and duplex of the network port.  If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to autonegotiate.  If you change the setting of this option, you must change the PC Port config option to the same setting.
PC port config	Auto 10MB half 10MB full 100 MB half 100MB full 100 half 1000 full (except for 7811 and 7821)	Auto	Select Speed and duplex of the Computer (access) port.  If the phone is connected to a switch, configure the port on the switch to the same speed/duplex as the phone, or configure both to autonegotiate.  If you change the setting of this option, you must change the Switch Port config option to the same setting.

Field	Field Type or Choices	Default	Description
CDP	On Off	On	Enable or disable Cisco Discovery Protocol (CDP).  CDP is a device-discovery protocol that runs on all Cisco manufactured equipment.  Using CDP, a device can advertise its existence to other devices and receive information about other devices in the network.
LLDP-MED	On Off	On	Enable or disable LLDP-MED.  LLDP-MED enables the phone to advertise itself to devices that use the discovery protocol.
Startup delay		3 seconds	Set a value that causes a delay for the switch to get to the forwarding state before the phone sends out the first LLDP-MED packet. For configuration of some switches, you might need to increase this value to a higher value for LLDP-MED to work. Configuring a delay can be important for networks that use the Spanning Tree Protocol.  Default delay is 3 seconds.
VLAN	On Off	Off	Enable or disable VLAN.  Permits you to enter a VLAN ID when you use VLAN without CDP or LLDP. When you use a VLAN with CDP or LLDP, that associated VLAN takes precedent over the VLAN ID you manually entered.
VLAN ID		1	Enter a VLAN ID for the IP phone when you use a VLAN without CDP (VLAN enabled and CDP disabled). Note that only voice packets are tagged with the VLAN ID. Do not use the 1 value for the VLAN ID. If VLAN ID is 1, you cannot tag voice packets with the VLAN ID.
PC port VLAN ID		1	Enter a value of the VLAN ID that is used to tag communications from the PC port on the phone.  The phone tags all the untagged frames coming from the PC (it does not tag any frames with an existing tag).  Valid values: 0 through 4095  Default: 0
PC port mirror	On Off	Off	Adds the ability to port mirror on the PC port. When enabled, you can see the packets on the phone. Select <b>On</b> to enable PC port mirroring and select <b>Off</b> to disable it.

Field	Field Type or Choices	Default	Description
DHCP VLAN option			<p>Enter a predefined DHCP VLAN option to learn the voice VLAN ID.</p> <p>When you use a VLAN ID with CDP, LLDP, or manually select a VLAN ID, that VLAN ID takes precedent over the selected DHCP VLAN option.</p> <p>Valid values are:</p> <ul style="list-style-type: none"><li>• Null</li><li>• 128 to 149</li><li>• 151 to 158</li><li>• 161 to 254</li></ul> <p>Default value is null.</p> <p>Cisco recommends that you use DHCP Option 132.</p>



Table 3: IPv4 Address Settings Submenu

Field	Field Type or Choices	Default	Description
Connection type	DHCP		<p>Indicates whether the phone has DHCP enabled.</p> <ul style="list-style-type: none"> <li>• DNS1—Identifies the primary Domain Name System (DNS) server that the phone uses.</li> <li>• DNS2—Identifies the secondary Domain Name System (DNS) server that the phone uses.</li> <li>• DHCP address released—Releases the IP address that DHCP assigned. You can edit this field if DHCP is enabled. To remove the phone from the VLAN and release the IP address for reassignment, set this field to Yes and press <b>Set</b>.</li> </ul>
	Static IP		<p>When DHCP is disabled, you must set the Internet Protocol (IP) address of the phone.</p> <ul style="list-style-type: none"> <li>• Static IP address—Identifies the IP that you assign to the phone. The phone uses this IP address instead of acquiring an IP from the DHCP server on the network.</li> <li>• Subnet Mask—Identifies the subnet mask used by the phone. When DHCP is disabled, you must set the subnet mask.</li> <li>• Gateway address—Identifies the default router used by the phone.</li> <li>• DNS1—Identifies the primary Domain Name System (DNS) server that the phone uses. When DHCP is disabled, you must set this field manually.</li> <li>• DNS2—Identifies the primary Domain Name System (DNS) server that the phone uses. When DHCP is disabled, you must set this field manually.</li> </ul> <p>When you assign an IP address using this field, you must also assign a subnet mask and a gateway address. See the Subnet Mask and Default Router fields in this table.</p>


Table 4: IPv6 Address Settings Submenu

Field	Field Type or Choices	Default	Description
Connection type	DHCP		<p>Indicates whether the phone has Dynamic Host Configuration Protocol (DHCP) enabled.</p> <ul style="list-style-type: none"> <li>• DNS1—Identifies the primary DNS server that the phone uses.</li> <li>• DNS2—Identifies the secondary DNS server that the phone uses.</li> <li>• Broadcast Echo—Identifies if the phone responds to multicast ICMPv6 message with destination address of ff02::1.</li> <li>• Auto config— Identifies if the phone uses automatic configuration for the address.</li> </ul>
	Static IP		<p>When DHCP is disabled, you must set the Internet Protocol (IP) address of the phone and must set the values of the fields:</p> <ul style="list-style-type: none"> <li>• Static IP—Identifies the IP that you assign to the phone. The phone uses this IP address instead of acquiring an IP from the DHCP server on the network.</li> <li>• Prefix length—Identifies how many bits of a Global Unicast IPv6 Address are there in the network part.</li> <li>• Gateway—Identifies the default router used by the phone.</li> <li>• Primary DNS—Identifies the primary DNS server that the phone uses. When DHCP is disabled, you must set this field manually.</li> <li>• Secondary DNS—Identifies the primary DNS server that the phone uses. When DHCP is disabled, you must set this field manually.</li> <li>• Broadcast Echo—Identifies if the phone responds to multicast ICMPv6 message with destination address of ff02::1.</li> </ul>

## Text and Menu Entry From the Phone

When you edit the value of an option setting, follow these guidelines:

- Use the arrows on the navigation pad to highlight the field that you wish to edit. Press **Select** in the navigation pad to activate the field. After the field is activated, you can enter values.
- Use the keys on the keypad to enter numbers and letters.

- To enter letters by using the keypad, use a corresponding number key. Press the key one or more times to display a particular letter. For example, press the **2** key once for “a,” twice quickly for “b,” and three times quickly for “c.” After you pause, the cursor automatically advances to allow you to enter the next letter.
- Press the softkey  if you make a mistake. This softkey deletes the character to the left of the cursor.
- Press **Back** before pressing **Set** to discard any changes that you made.
- To enter a period (for example, in an IP address), press \* on the keypad.



---

**Note** The Cisco IP Phone provides several methods to reset or restore option settings, if necessary.

---

## Verify Phone Startup

After the Cisco IP Phone has power connected to it, the phone automatically cycles through a startup diagnostic process.

### Procedure

- 
- Step 1** If you are using Power over Ethernet, plug the LAN cable into the Network port.
- Step 2** If you are using the power cube, connect the cube to the phone and plug the cube into an electrical outlet.
- The buttons flash amber and then green in sequence during the various stages of bootup as the phone checks the hardware.
- If the phone completes these stages successfully, it has started up properly.
- 

## Configure the Voice Codecs

A codec resource is considered allocated if it has been included in the SDP codec list of an active call, even though it eventually might not be chosen for the connection. Negotiation of the optimal voice codec sometimes depends on the ability of the Cisco IP Phone to match a codec name with the far-end device or gateway codec name. The phone allows the network administrator to individually name the various codecs that are supported such that the correct codec successfully negotiates with the far-end equipment.

The Cisco IP Phone supports voice codec priority. You can select up to three preferred codecs. The administrator can select the low-bit-rate codec that is used for each line. G.711a and G.711u are always enabled.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

### Procedure

---

- Step 1** Select **Voice > Ext(n)**, where n is an extension number.
- Step 2** In the **Audio Configuration** section, configure the parameters.
- Step 3** Click **Submit All Changes**.
- 

## Set the Optional Network Servers

Optional network servers provide resources such as DNS lookup, network time, logging, and device discovery. It also enables you to add PC port mirroring on the user phone. Your user can also enable or disable this service from the phone.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

### Procedure

---

- Step 1** Select **Voice > System**.
- Step 2** In the **Optional Network Configuration** section, set up the fields as described in [Optional Network Configuration](#).
- Step 3** Click **Submit All Changes**.
- 

## VLAN Settings

The software tags your phone voice packets with the VLAN ID when you use a virtual LAN (VLAN).

In the VLAN Settings section of the **Voice > System** window, you can configure the different settings:

- LLDP-MED
- Cisco Discovery Protocol (CDP)
- Network Startup Delay
- VLAN ID (manual)
- DHCP VLAN Option

The multiplatform phones support these four methods to obtain VLAN ID information. The phone attempts to obtain the VLAN ID information in this order:

1. LLDP-MED
2. Cisco Discovery Protocol (CDP)

3. VLAN ID (manual)
4. DHCP VLAN Option

## Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is negotiation-based and determines which virtual LAN (VLAN) the Cisco IP Phone resides in. If you are using a Cisco switch, Cisco Discovery Protocol (CDP) is available and is enabled by default. CDP has these attributes:

- Obtains the protocol addresses of neighboring devices and discovers the platform of those devices.
- Shows information about the interfaces your router uses.
- Is media and protocol-independent.

If you are using a VLAN without CDP, you must enter a VLAN ID for the Cisco IP Phone.

## LLDP-MED

The Cisco IP Phone supports Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) for deployment with Cisco or other Third-Party network connectivity devices that use a Layer 2 auto discovery mechanism. Implementation of LLDP-MED is done in accordance with IEEE 802.1AB (LLDP) Specification of May 2005, and ANSI TIA-1057 of April 2006.

The Cisco IP Phone operates as a LLDP-MED Media End Point Class III device with direct LLDP-MED links to Network Connectivity Devices, according to the Media Endpoint Discovery Reference Model and Definition (ANSI TIA-1057 Section 6).

The Cisco IP Phone supports only the following limited set of Type-Length-Values (TLV) as an LLDP-MED Media Endpoint device class III:

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- Port Description TLV
- System Name TLV
- System Capabilities TLV
- IEEE 802.3 MAC/PHY Configuration/Status TLV (for wired network only)
- LLDP-MED Capabilities TLV
- LLDP-MED Network Policy TLV (for application type=Voice only)
- LLDP-MED Extended Power-Via-MDI TLV (for wired network only)
- LLDP-MED Firmware Revision TLV
- End of LLDPDU TLV

The outgoing LLDPDU contains all the preceding TLVs if applicable. For the incoming LLDPDU, the LLDPDU is discarded if any of the following TLVs are missing. All other TLVs are not validated and ignored.

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- LLDP-MED Capabilities TLV
- LLDP-MED Network Policy TLV (for application type=Voice only)
- End of LLDPDU TLV

The Cisco IP Phone sends out the shutdown LLDPDU if applicable. The LLDPDU frame contains the following TLVs:

- Chassis ID TLV
- Port ID TLV
- Time to live TLV
- End of LLDPDU TLV

There are some restrictions in the implementation of LLDP-MED on the Cisco IP Phones:

- Storage and retrieval of neighbor information are not supported.
- SNMP and corresponding MIBs are not supported.
- Recording and retrieval of statistical counters are not supported.
- Full validation of all TLVs does not take place; TLVs that do not apply to the phones are ignored.
- Protocol state machines as stated in the standards are used only for reference.

## Chassis ID TLV

For the outgoing LLDPDU, the TLV supports subtype=5 (Network Address). When the IP address is known, the value of the Chassis ID is an octet of the INAN address family number followed by the octet string for the IPv4 address used for voice communication. If the IP address is unknown, the value for the Chassis ID is 0.0.0.0. The only INAN address family supported is IPv4. Currently, the IPv6 address for the Chassis ID is not supported.

For the incoming LLDPDU, the Chassis ID is treated as an opaque value to form the MSAP identifier. The value is not validated against its subtype.

The Chassis ID TLV is mandatory as the first TLV. Only one Chassis ID TLV is allowed for the outgoing and incoming LLDPDUs.

## Port ID TLV

For the outgoing LLDPDU, the TLV supports subtype=3 (MAC address). The 6 octet MAC address for the Ethernet port is used for the value of Port ID.

For the incoming LLDPDU, the Port ID TLV is treated as an opaque value to form the MSAP identifier. The value is not validated against its subtype.

The Port ID TLV is mandatory as the second TLV. Only one Port ID TLV is allowed for the outgoing and incoming LLDPDU.

## Time to Live TLV

For the outgoing LLDPDU, the Time to Live TTL value is 180 seconds. This differs from the 120-second value that the standard recommends. For the shutdown LLDPDU, the TTL value is always 0.

The Time to Live TLV is mandatory as the third TLV. Only one Time to Live TLV is allowed for the outgoing and incoming LLDPDU.

## End of LLDPDU TLV

The value is 2-octet, all zero. This TLV is mandatory and only one is allowed for the outgoing and incoming LLDPDU.

## Port Description TLV

For the outgoing LLDPDU, in the Port Description TLV, the value for the port description is the same as “Port ID TLV” for CDP. The incoming LLDPDU, the Port Description TLV, is ignored and not validated. Only one Port Description TLV is allowed for outgoing and incoming LLDPDU.

## System Name TLV

For the Cisco IP Phone, the value is SEP+MAC address.

**Example:** SEPAC44F211B1D0

The incoming LLDPDU, the System Name TLV, is ignored and not validated. Only one System Name TLV is allowed for the outgoing and incoming LLDPDU.

## System Capabilities TLV

For the outgoing LLDPDU, in the System Capabilities TLV, the bit values for the 2 octet system capabilities fields should be set for Bit 2 (Bridge) and Bit 5 (Phone) for a phone with a PC port. If the phone does not have a PC port, only Bit 5 should be set. The same system capability value should be set for the enabled capability field.

For the incoming LLDPDU, the System Capabilities TLV is ignored. The TLV is not validated semantically against the MED device type.

The System Capabilities TLV is mandatory for outgoing LLDPDU. Only one System Capabilities TLV is allowed.

## Management Address TLV

The TLV identifies an address associated with the local LLDP agent (that may be used to reach higher layer entities) to assist discovery by network management. The TLV allows the inclusion of both the system interface number and an object identifier (OID) that are associated with this management address, if either or both are known.

- TLV information string length—This field contains the length (in octets) of all the fields in the TLV information string.
- Management address string length—This field contains the length (in octets) of the management address subtype + management address fields.

## System Description TLV

The TLV allows the network management to advertise the system description.

- TLV information string length—This field indicates the exact length (in octets) of the system description.
- System description—This field contains an alphanumeric string that is the textual description of the network entity. The system description includes the full name and version identification of the system hardware type, software operating system, and networking software. If implementations support IETF RFC 3418, the sysDescr object should be used for this field.

## IEEE 802.3 MAC/PHY Configuration/Status TLV

The TLV is not for autonegotiation, but for troubleshooting purposes. For the incoming LLDPDU, the TLV is ignored and not validated. For the outgoing LLDPDU, for the TLV, the octet value autonegotiation support/status should be:

- Bit 0—Set to 1 to indicate that the autonegotiation support feature is supported.
- Bit 1—Set to 1 to indicate that autonegotiation status is enabled.
- Bit 2-7—Set to 0.

The bit values for the 2 octets PMD autonegotiation advertised capability field should be set to:

- Bit 13—10BASE-T half duplex mode
- Bit 14—10BASE-T full duplex mode
- Bit 11—100BASE-TX half duplex mode
- Bit 10—100BASE-TX full duplex mode
- Bit 15—Unknown

Bit 10, 11, 13 and 14 should be set.

The value for 2 octets operational MAU type should be set to reflect the real operational MAU type:

- 16—100BASE-TX full duplex
- 15—100BASE-TX half duplex
- 11—10BASE-T full duplex
- 10—10BASE-T half duplex

For example, usually, the phone is set to 100BASE-TX full duplex. The value 16 should then be set. The TLV is optional for a wired network and not applicable for a wireless network. The phone sends out this TLV only when in wired mode. When the phone is not set for autonegotiation but specific speed/duplexity, for the outgoing LLDPDU TLV, bit 1 for the octet value autonegotiation support/status should be clear (0) to indicate that autonegotiation is disabled. The 2 octets PMD autonegotiation advertised capability field should be set to 0x8000 to indicate unknown.

## LLDP-MED Capabilities TLV

For the outgoing LLDPDU, the TLV should have the device type 3 (End Point Class III) with the following bits set for 2-octet Capability field:



Bit Position	Capability
0	LLDP-MED Capabilities
1	Network Policy
4	Extended Power via MDI-PD
5	Inventory

For the incoming TLV, if the LLDP-MED TLV is not present, the LLDPDU is discarded. The LLDP-MED Capabilities TLV is mandatory and only one is allowed for the outgoing and incoming LLDPDUs. Any other LLDP-MED TLVs will be ignored if they present before the LLDP-MED Capabilities TLV.

## Network Policy TLV

In the TLV for the outgoing LLDPDU, before the VLAN or DSCP is determined, the Unknown Policy Flag (U) is set to 1. If the VLAN setting or DSCP is known, the value is set to 0. When the policy is unknown, all other values are set to 0. Before the VLAN is determined or used, the Tagged Flag (T) is set to 0. If the tagged VLAN (VLAN ID > 1) is used for the phone, the Tagged Flag (T) is set to 1. Reserved (X) is always set to 0. If the VLAN is used, the corresponding VLAN ID and L2 Priority will be set accordingly. VLAN ID valid value is range from 1-4094. However, VLAN ID=1 will never be used (limitation). If DSCP is used, the value range from 0-63 is set accordingly.

In the TLV for the incoming LLDPDU, Multiple Network Policy TLVs for different application types are allowed.

## LLDP-MED Extended Power-Via-MDI TLV

In the TLV for the outgoing LLDPDU, the binary value for Power Type is set to “0 1” to indicate the power type for phone is PD Device. The Power source for the phone is set to “PSE and local” with binary value “1 1”. The Power Priority is set to binary “0 0 0 0” to indicate unknown priority while the Power Value is set to maximum power value. The Power Value for the Cisco IP Phone is 12900mW.

For the incoming LLDPDU, the TLV is ignored and not validated. Only one TLV is allowed in the outgoing and incoming LLDPDUs. The phone will send out the TLV for the wired network only.

The LLDP-MED standard was originally drafted in the context of Ethernet. Discussion is ongoing for LLDP-MED for Wireless Networks. Refer to ANSI-TIA 1057, Annex C, C.3 Applicable TLV for VoWLAN, table 24. It is recommended that the TLV is not applicable in the context of the wireless network. This TLV is targeted for use in the context of PoE and Ethernet. The TLV, if added, will not provide any value for network management or power policy adjustment at the switch.

## LLDP-MED Inventory Management TLV

This TLV is optional for Device Class III. For the outgoing LLDPDU, we support only Firmware Revision TLV. The value for the Firmware Revision is the version of firmware on the phone. For the incoming LLDPDU, the TLVs are ignored and not validated. Only one Firmware Revision TLV is allowed for the outgoing and incoming LLDPDUs.

# Final Network Policy Resolution and QoS

## Special VLANs

VLAN=0, VLAN=1, and VLAN=4095 are treated the same way as an untagged VLAN. Because the VLAN is untagged, Class of Service (CoS) is not applicable.

## Default QoS for SIP Mode

If there is no network policy from CDP or LLDP-MED, the default network policy is used. CoS is based on configuration for the specific extension. It is applicable only if the manual VLAN is enabled and manual VLAN ID is not equal to 0, 1, or 4095. Type of Service (ToS) is based on configuration for the specific extension.

## QoS Resolution for CDP

If there is a valid network policy from CDP:

- If the VLAN=0, 1, or 4095, the VLAN will not be set, or the VLAN is untagged. CoS is not applicable, but DSCP is applicable. ToS is based on the default as previously described.
- If the VLAN > 1 and VLAN < 4095, the VLAN is set accordingly. CoS and ToS are based on the default as previously described. DSCP is applicable.
- The phone reboots and restarts the fast start sequence.

## QoS Resolution for LLDP-MED

If CoS is applicable and if CoS = 0, the default is used for the specific extension as previously described. But the value shown on L2 Priority for TLV for outgoing LLDPDU is based on the value used for extension 1. If CoS is applicable and if CoS != 0, CoS is used for all extensions.

If DSCP (mapped to ToS) is applicable and if DSCP = 0, the default is used for the specific extension as previously described. But the value shown on DSCP for TLV for outgoing LLDPDU is based on value used for the extension 1. If DSCP is applicable and if DSCP != 0, DSCP is used for all extensions.

If the VLAN > 1 and VLAN < 4095, the VLAN is set accordingly. CoS and ToS are based on the default as previously described. DSCP is applicable.

If there is a valid network policy for the voice application from LLDP-MED PDU and if the tagged flag is set, the VLAN, L2 Priority (CoS), and DSCP (mapped to ToS) are all applicable.

If there is a valid network policy for the voice application from LLDP-MED PDU and if the tagged flag is not set, only the DSCP (mapped to ToS) is applicable.

The Cisco IP Phone reboots and restarts the fast start sequence.

## Coexistence with CDP

If both CDP and LLDP-MED are enabled, the network policy for the VLAN determines the last policy set or changed with either one of the discovery modes. If both LLDP-MED and CDP are enabled, during startup the phone sends CDP and LLDP-MED PDUs.

Inconsistent configuration and behavior for network connectivity devices for CDP and LLDP-MED modes could result in an oscillating rebooting behavior for the phone due to switching to different VLANs.

If the VLAN is not set by CDP and LLDP-MED, the VLAN ID that is configured manually is used. If the VLAN ID is not configured manually, no VLAN is supported. DSCP is used and the network policy determines LLDP-MED if applicable.

## LLDP-MED and Multiple Network Devices

You can use the same application type for network policy. However, phones receive different Layer 2 or Layer 3 QoS Network policies from multiple network connectivity devices. In such a case, the last valid network policy is accepted.

## LLDP-MED and IEEE 802.X

The Cisco IP Phone does not support IEEE 802.X and does not work in a 802.1X wired environment. However, IEEE 802.1X or Spanning Tree Protocols on network devices could result in delay of fast start response from switches.

## Configure VLAN Settings

### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

### Procedure

---

- Step 1** Select **Voice > System**.
  - Step 2** In the **VLAN Settings** section, configure the fields.
  - Step 3** Click **Submit All Changes**.
- 

## Set Up DHCP VLAN Option from Phone Web Page

You can add a predefined DHCP option to configure the voice VLAN for your phone.

### Before you begin

- Access the phone administration web page. See [Access the Phone Web Page](#).
- Disable CDP/LLDP and manual VLAN.

### Procedure

---

- Step 1** Select **Voice > System**.
- Step 2** In the **VLAN Settings** section, enter a value in the **DHCP VLAN Option** field.  
The field is empty, by default.

Valid values are:

- Null
- 128 to 149
- 151 to 158
- 161 to 254

Set the **DHCP VLAN Option** value to **Null** to disable the voice VLAN configuration.

Cisco recommends that you use DHCP Option 132.

**Step 3** Click **Submit All Changes**.

---

### What to do next

In the **VLAN Settings** section of the **Voice > System** tab, you can configure these settings:

- Cisco Discovery Protocol (CDP)
- LLDP-MED
- Network Startup Delay
- VLAN ID
- DHCP VLAN Option

## SIP and NAT Configuration

### SIP and the Cisco IP Phone

The Cisco IP Phone uses Session Initiation Protocol (SIP), which allows interoperation with all IT service providers that support SIP. SIP is an IETF-defined signaling protocol that controls voice communication sessions in an IP network.

SIP handles signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* controls the attributes of an end-to-end call.

In typical commercial IP telephony deployments, all calls go through a SIP Proxy Server. The receiving phone is called the SIP user agent server (UAS), while the requesting phone is called the user agent client (UAC).

SIP message routing is dynamic. If a SIP proxy receives a request from a UAS for a connection but cannot locate the UAC, the proxy forwards the message to another SIP proxy in the network. When the UAC is located, the response routes back to the UAS, and the two UAs connect using a direct peer-to-peer session. Voice traffic transmits between UAs over dynamically assigned ports using Real-time Protocol (RTP).

RTP transmits real-time data such as audio and video; RTP does not guarantee real-time delivery of data. RTP provides mechanisms for the sending and receiving applications to support streaming data. Typically, RTP runs on top of UDP.

## SIP Over TCP

To guarantee state-oriented communications, the Cisco IP Phone can use TCP as the transport protocol for SIP. This protocol provides *guaranteed delivery* that assures that lost packets are retransmitted. TCP also guarantees that the SIP packages are received in the same order that they were sent.

TCP overcomes the problem of UDP port-blocking by corporate firewalls. With TCP, new ports do not need to be open or packets dropped, because TCP is already in use for basic activities, such as internet browsing or e-commerce.

## SIP Proxy Redundancy

An average SIP Proxy Server can handle tens of thousands of subscribers. A backup server allows an active server to be temporarily switched out for maintenance. Cisco phones support the use of backup SIP Proxy Servers to minimize or eliminate service disruption.

A static list of proxy servers is not always adequate. If your user agent serves different domains, for example, you do not want to configure a static list of proxy servers for each domain into every Cisco IP Phone.

A simple way to support proxy redundancy is to configure a SIP Proxy Server in the Cisco IP Phone configuration profile. The DNS SRV records instruct the phones to contact a SIP Proxy Server in a domain named in SIP messages. The phone consults the DNS server. If configured, the DNS server returns an SRV record that contains a list of SIP Proxy Servers for the domain, with their hostnames, priority, listening ports, and so forth. The Cisco IP Phone tries to contact the hosts in the order of their priority.

If the Cisco IP Phone currently uses a lower-priority proxy server, the phone periodically probes the higher-priority proxy and switches to the higher-priority proxy when available.

## Dual Registration

The phone always registers to both primary (or primary outbound) and alternate (or alternate outbound) proxies. After registration, the phone sends out Invite and Non-Invite SIP messages through primary proxy first. If there is no response for the new INVITE from the primary proxy, after timeout, the phone attempts to connect with the alternate proxy. If the phone fails to register to the primary proxy, it sends an INVITE to the alternate proxy without trying the primary proxy.

Dual registration is supported on a per-line basis. Three added parameters can be configured through web user interface and remote provisioning:

- Alternate Proxy—Default is empty.
- Alternate Outbound Proxy—Default is empty.
- Dual Registration—Default is NO (turned off).

After you configure the parameters, reboot the phone for the feature to take effect.



---

**Note** Specify a value for primary proxy (or primary outbound proxy) and alternate proxy (or alternate outbound proxy) for the feature to function properly.

---

### Dual Registration and DNS SRV Limitations

- When Dual Registration is enabled, DNS SRV Proxy Fallback or Recovery must be disabled.

- Do not use Dual Registration along with other Fallback or Recovery mechanisms. For example: Broadsoft mechanism.
- There is no recovery mechanism for feature request. However, the administrator can adjust the reregistration time for a prompt update of the registration state for primary and alternate proxy.

### Dual Registration and Alternate Proxy

When the Dual Register parameter is set to **No**, Alternate Proxy is ignored.

## Failover and Recovery Registration

- Failover—The phone performs a failover when transport timeout/failure or TCP connection failures; if Try Backup RSC and Retry Reg RSC values are datafilled.
- Recovery—The phone attempts to reregister with the primary proxy while registered or actively connected to the secondary proxy.

Auto register when failover parameter controls the failover behavior when there is an error. When this parameter is set to yes, the phone re-registers upon failover or recovery.

### Fallback Behavior

The fallback occurs when the current registration expires or Proxy Fallback Intvl fires.

If the Proxy Fallback Intvl is exceeded, all the new SIP messages go to primary proxy.

For example, when the value for Register Expires is 3600 seconds and Proxy Fallback Intvl is 600 seconds, the fallback triggers 600 seconds later.

When the value for Register Expires is 800 seconds and Proxy Fallback Intvl is 1000 seconds, the fallback triggers at 800 seconds.

After successful registration back to the primary server, all SIP messages go to the primary server.

## RFC3311

The Cisco IP Phone supports RFC-3311, the SIP UPDATE Method.

## SIP NOTIFY XML-Service

The Cisco IP Phone supports the SIP NOTIFY XML-Service event. On receipt of a SIP NOTIFY message with an XML-Service event, the phone challenges the NOTIFY with a 401 response if the message does not contain correct credentials. The client must furnish the correct credentials using MD5 digest with the SIP account password for the corresponding line of the IP phone.

The body of the message can contain the XML event Message. For example:

```
<CiscoIPPhoneExecute>
  <ExecuteItem Priority="0" URL="http://xmlserver.com/event.xml"/>
</CiscoIPPhoneExecute>
```

Authentication:

```
challenge = MD5( MD5(A1) ":" nonce ":" nc-value ":" cnonce ":" qop-value
":" MD5(A2) )
```

```
where A1 = username ":" realm ":" passwd  
and A2 = Method ":" digest-uri
```

## SIP Configuration

SIP settings for the Cisco IP Phone are configured for the phone in general and for the extensions.

### Configure the Basic SIP Parameters

#### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

#### Procedure

---

- Step 1** Select **Voice > SIP**.
  - Step 2** In the **SIP Parameters** section, set the SIP parameters as described in [SIP Parameters](#).
  - Step 3** Click **Submit All Changes**.
- 

### Configure the SIP Timer Values

#### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

#### Procedure

---

- Step 1** Select **Voice > SIP**.
  - Step 2** In the **SIP Timer Values** section, set the SIP timer values in seconds as described in [SIP Timer Values \(sec\)](#).
  - Step 3** Click **Submit All Changes**.
- 

### Configure the Response Status Code Handling

#### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

#### Procedure

---

- Step 1** Select **Voice > SIP**.
- Step 2** In the **Response Status Code Handling** section, set the values as specified:

- **Try Backup RSC**—SIP response code that retries a backup server for the current request. Defaults to blank. For example, you can enter numeric values 500 or a combination of numeric values plus wild cards if multiple values are possible. For the later, you can use 5?? to represent all SIP Response messages within the 500 range. If you want to use multiple ranges, you can add a comma "," to delimit values of 5?? and 6??.
- **Retry Reg RSC**—SIP response code that the phone retries registration after failing during the last registration. Defaults to blank. For example, you can enter numeric values 500 or a combination of numeric values plus wild cards if multiple values are possible. For the later, you can use 5?? to represent all SIP Response messages within the 500 range. If you want to use multiple ranges, you can add a comma "," to delimit values of 5?? and 6??.

**Step 3** Click **Submit All Changes**.

---

## Configure NTP Server

You can configure NTP servers with IPv4 and IPv6. You can also configure NTP server with DHCPv4 option 42 or DHCPv6 option 56. Configuring NTP with Primary NTP Server and Secondary NTP server parameters has higher priority over configuring NTP with DHCPv4 option 42 or DHCPv6 option 56.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

### Procedure

---

- Step 1** Select **Voice > Systems**.
- Step 2** In the **Optional Network Configuration** section, enter IPv4 or IPv6 address in the **Primary NTP Server** and **Secondary NTP Server**.
- Step 3** Click **Submit All Changes**.
- 

## Configure the RTP Parameters

### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

### Procedure

---

- Step 1** Select **Voice > SIP**.
- Step 2** In the **RTP Parameters** section, set the Real-Time Transport Protocol (RTP) parameter values as described in [RTP Parameters](#).
- Step 3** Click **Submit All Changes**.
-



## Control SIP and RTP Behaviour in Dual Mode

You can control SIP and RTP parameters with SIP IP Preference and SDP IP Preference fields when phone is in dual mode.

SIP IP Preference parameter defines which IP address phone tries first when it is in dual mode.

**Table 5: SIP IP Preference and IP Mode**

IP Mode	SIP IP Preference	Address List from DNS, Priority, Result P1 - First Priority Address P2 - Second Priority Address	Failover Sequence
Dual Mode	IPv4	P1- 1.1.1.1, 2009:1:1:1::1 P2 - 2.2.2.2, 2009:2:2:2::2 <b>Result:</b> Phone will send the SIP messages to 1.1.1.1 first.	1.1.1.1 ->2009:1:1:1 -> 2.2.2.2 -> 2009:2:2:2
Dual Mode	IPv6	P1- 1.1.1.1, 2009:1:1:1::1 P2 - 2.2.2.2, 2009:2:2:2::2 <b>Result:</b> Phone will send the SIP messages to 2009:1:1:1::1 first.	2009:1:1:1 -> 1.1.1.1 -> 2009:2:2:2 -> 2.2.2.2
Dual Mode	IPv4	P1- 2009:1:1:1::1 P2 - 2.2.2.2, 2009:2:2:2::2 <b>Result:</b> Phone will send the SIP messages to 2009:1:1:1::1 first.	2009:1:1:1 -> 2.2.2.2 -> 2009:2:2:2
Dual Mode	IPv6	P1- 2009:1:1:1::1 P2 - 2.2.2.2, 2009:2:2:2::2 <b>Result:</b> Phone will send the SIP messages to 1.1.1.1 first.	2009:1:1:1 -> 2009:2:2:2 ->2.2.2.2
IPv4 Only	IPv4 or IPv6	P1 - 1.1.1.1, 2009:1:1:1::1 P2 - 2.2.2.2, 2009:2:2:2::2 <b>Result:</b> Phone will send the SIP messages to 1.1.1.1 first.	1.1.1.1 -> 2.2.2.2
IPv6 Only	IPv4 or IPv6	P1 - 1.1.1.1, 2009:1:1:1::1 P2 - 2.2.2.2, 2009:2:2:2::2 <b>Result:</b> Phone will send the SIP messages to 2009:1:1:1::1 first.	2009:1:1:1 -> 2009:2:2:2

SDP IP Preference - ALTC helps peers in dual-mode negotiate RTP address family.

**Before you begin**

Access the phone administration web page. See [Access the Phone Web Page](#).

**Procedure**

---

- Step 1** Select **Voice > SIP**.
- Step 2** In the **SIP Parameters** section, select **IPv4** or **IPv6** in the **SIP IP Preference** field.
- Step 3** In the **RTP Parameters** section, select **IPv4** or **IPv6** in the **SDP IP Preference** field.
- For details, see **SDP IP Preference** in [RTP Parameters](#).
- 

## Configure the SDP Payload Types

Configured dynamic payloads are used for outbound calls only when the Cisco IP Phone presents a Session Description Protocol (SDP) offer. For inbound calls with an SDP offer, the phone follows the caller's assigned dynamic payload type.

The Cisco IP Phone uses the configured codec names in outbound SDP. For incoming SDP with standard payload types of 0-95, the phone ignores the codec names. For dynamic payload types, the phone identifies the codec by the configured codec names (comparison is case-sensitive).

**Before you begin**

Access the phone administration web page. See [Access the Phone Web Page](#).

**Procedure**

---

- Step 1** Select **Voice > SIP**.
- Step 2** In the **SDP Payload Types** section, set the value as specified in [SDP Payload Types](#).
- **AVT Dynamic Payload**—Any nonstandard data. Both sender and receiver must agree on a number. Ranges from 96 to 127. Default: 101.
- Step 3** Click **Submit All Changes**.
- 

## Configure the SIP Settings for Extensions

**Before you begin**

Access the phone administration web page. See [Access the Phone Web Page](#).

**Procedure**

---

- Step 1** Select **Voice > Ext(n)**, where n is an extension number.

- Step 2** In the **SIP Settings** section, set the parameter values as described in [SIP Settings](#).
- Step 3** Click **Submit All Changes**.
- 

## Configure the SIP Proxy Server

### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

### Procedure

---

- Step 1** Select **Voice > Ext(n)**, where n is an extension number.
- Step 2** In the **Proxy and Registration** section, set the parameter values as described in [Proxy and Registration](#).
- Step 3** Click **Submit All Changes**.
- 

## Configure the Subscriber Information Parameters

### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

### Procedure

---

- Step 1** Select **Voice > Ext(n)**, where n is an extension number.
- Step 2** In the **Subscriber Information** section, set the parameter values as described in [Subscriber Information](#).
- Step 3** Click **Submit All Changes**.
- 

## Managing NAT Transversal with Phones

Network Address Translation (NAT) allows multiple devices to share a single, public, routable, IP address to establish connections over the Internet. NAT is present in many broadband access devices to translate public and private IP addresses. For VoIP to coexist with NAT, NAT traversal is required.

Not all service providers provide NAT traversal. If your service provider does not provide NAT traversal, you have several options:

- NAT Mapping with Session Border Controller
- NAT Mapping with SIP-ALG Router
- NAT Mapping with a Static IP Address
- NAT Mapping with STUN

## Enable NAT Mapping

You must enable NAT mapping to set NAT parameters.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

### Procedure

---

- Step 1** Select **Voice > Ext(n)**.
  - Step 2** Set up the fields as described in [NAT Settings](#).
  - Step 3** Click **Submit All Changes**.
- 

## NAT Mapping with Session Border Controller

We recommend that you choose a service provider that supports NAT mapping through a Session Border Controller. With NAT mapping provided by the service provider, you have more choices in selecting a router.

## NAT Mapping with SIP-ALG Router

NAT mapping can be achieved by using a router that has a SIP Application Layer Gateway (ALG). By using a SIP-ALG router, you have more choices in selecting an service provider.

## NAT Mapping with the Static IP Address

You can configure NAT mapping on the phone to ensure interoperability with the service provider.

- You must have an external (public) IP address that is static.
- The NAT mechanism used in the router must be symmetric. For more information, see [Determining Symmetric or Asymmetric NAT, on page 30](#).

Use NAT mapping only if the service provider network does not provide a Session Border Controller functionality.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

### Procedure

---

- Step 1** Select **Voice > SIP**.
- Step 2** In the **NAT Support Parameters** section, set **Handle VIA received**, **Insert VIA received**, **Substitute VIA Addr**, **Handle VIA rport**, **Insert VIA rport**, and **Send Resp To Src Port** fields to **Yes**.
- Step 3** In the **NAT Support Parameters** section, set a value for the **NAT Keep Alive Intvl** field.
- Step 4** Enter the public IP address for your router in the **EXT IP** field.
- Step 5** Click the **Ext(n)** tab.

**Step 6** In the **NAT Settings** section, set **NAT Mapping Enable** to **Yes**.

**Step 7** (Optional) Set **NAT Keep Alive Enable** to **Yes**.

The service provider might require the phone to send NAT keep alive messages to keep the NAT ports open. Check with your service provider to determine the requirements.

**Step 8** Click **Submit All Changes**.

---

### What to do next

Configure the firewall settings on your router to allow SIP traffic.

## Configure NAT mapping with STUN

If the service provider network does not provide a Session Border Controller functionality and if the other requirements are met, it is possible to use Session Traversal Utilities for NAT (STUN) to discover the NAT mapping. The STUN protocol allows applications operating behind a network address translator (NAT) to discover the presence of the network address translator and to obtain the mapped (public) IP address (NAT addresses) and the port number that the NAT has allocated for the User Datagram Protocol (UDP) connections to remote hosts. The protocol requires assistance from a third-party network server (STUN server) located on the opposing (public) side of the NAT, usually the public Internet. This option is considered a last resort and should be used only if the other methods are not available. To use STUN:

- The router must use asymmetric NAT. See [Determining Symmetric or Asymmetric NAT, on page 30](#).
- A computer running STUN server software is available on the network. You can also use a public STUN server or set up your own STUN server.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

### Procedure

---

**Step 1** Select **Voice > SIP**.

**Step 2** In the **NAT Support Parameters** section, set **Handle VIA received**, **Insert VIA received**, **Substitute VIA Addr**, **Handle VIA rport**, **Insert VIA rport**, and **Send Resp To Src Port** fields to **Yes**.

**Step 3** In the **NAT Support Parameters** section, set **STUN Enable** field to **Yes**.

**Step 4** Enter the IP address for your STUN server in the **STUN Server** field.

**Step 5** Click the **Ext(n)** tab.

**Step 6** In the **NAT Settings** section, set **NAT Mapping Enable** to **Yes**.

**Step 7** (Optional) Set **NAT Keep Alive Enable** to **Yes**.

The service provider might require the phone to send NAT keep alive messages to keep the NAT ports open. Check with your service provider to determine the requirements.

**Step 8** Click **Submit All Changes**.

---

**What to do next**

Configure the firewall settings on your router to allow SIP traffic.

**Determining Symmetric or Asymmetric NAT**

STUN does not work on routers with symmetric NAT. With symmetric NAT, IP addresses are mapped from one internal IP address and port to one external, routable destination IP address and port. If another packet is sent from the same source IP address and port to a different destination, a different IP address and port number combination is used. This method is restrictive because an external host can send a packet to a particular port on the internal host only if the internal host first sent a packet from that port to the external host.

This procedure assumes that a syslog server is configured and is ready to receive syslog messages.

To Determine Whether the Router Uses Symmetric or Asymmetric NAT:

**Procedure**

- 
- Step 1** Verify that the firewall is not running on your PC. (It can block the syslog port.) By default, the syslog port is 514.
  - Step 2** Click **Voice > System** and navigate to **Optional Network Configuration**.
  - Step 3** Enter the IP address for the **Syslog Server**, if the port number is anything other than the default, 514. It is not necessary to include the port number if it is the default.  
  
The address and port number must be reachable from the Cisco IP phone. The port number appears on the output log file name. The default output file is `syslog.514.log` (if port number was not specified).
  - Step 4** Set the **Debug Level** to **Error**, **Notice**, or **Debug**.
  - Step 5** To capture SIP signaling messages, click the **Ext** tab and navigate to **SIP Settings**. Set the **SIP Debug Option** to **Full**.
  - Step 6** To collect information about what type of NAT your router uses click the **SIP** tab and navigate to **NAT Support Parameters**.
  - Step 7** Click **Voice > SIP** and navigate to **NAT Support Parameters**.
  - Step 8** Set **STUN Test Enable** to **Yes**.
  - Step 9** Determine the type of NAT by viewing the debug messages in the log file. If the messages indicate that the device is using symmetric NAT, you cannot use STUN.
  - Step 10** Click **Submit All Changes**.
- 

## Dial Plan

### Dial Plan Overview

Dial plans determine how digits are interpreted and transmitted. They also determine whether the dialed number is accepted or rejected. You can use a dial plan to facilitate dialing or to block certain types of calls such as long distance or international.

Use the phone web user interface to configure dial plans on the IP phone.

This section includes information that you must understand about dial plans, and procedures to configure your own dial plans.

The Cisco IP Phone has various levels of dial plans and processes the digits sequence.

When a user presses the speaker button on the phone, the following sequence of events begins:

1. The phone begins to collect the dialed digits. The interdigit timer starts to track the time that elapses between digits.
2. If the interdigit timer value is reached, or if another terminating event occurs, the phone compares the dialed digits with the IP phone dial plan. This dial plan is configured in the phone web user interface in **Voice > Ext(n)** under the **Dial Plan** section.

## Digit Sequences

A dial plan contains a series of digit sequences, separated by the | character. The entire collection of sequences is enclosed within parentheses. Each digit sequence within the dial plan consists of a series of elements that are individually matched to the keys that the user presses.

White space is ignored, but can be used for readability.

Digit Sequence	Function
0 1 2 3 4 5 6 7 8 9 0 * #	Characters that represent a key that the user must press on the phone keypad.
x	Any character on the phone keypad.
[sequence]	<p>Characters within square brackets create a list of accepted key presses. The user can press any one of the keys in the list.</p> <p>A numeric range, for example, [2-9] allows a user to press any one digit from 2 through 9.</p> <p>A numeric range can include other characters. For example, [35-8*] allows a user to press 3, 5, 6, 7, 8, or *.</p>
.(period)	A period indicates element repetition. The dial plan accepts 0 or more entries of the digit. For example, 01. allows users to enter 0, 01, 011, 0111, and so forth.

Digit Sequence	Function
<dialled:substituted>	<p>This format indicates that certain <i>dialed</i> digits are replaced by the <i>substituted</i> characters when the sequence is transmitted. The <i>dialed</i> digits can be zero to 9. For example:</p> <pre>&lt;8:1650&gt;xxxxxxxx</pre> <p>When the user presses 8 followed by a seven-digit number, the system automatically replaces the dialed 8 with the sequence 1650. If the user dials <b>85550112</b>, the system transmits <b>16505550112</b>.</p> <p>If the <i>dialed</i> parameter is empty and there is a value in the <i>substituted</i> field, no digits are replaced and the <i>substituted</i> value is always prepended to the transmitted string. For example:</p> <pre>&lt;:1&gt;xxxxxxxxxxx</pre> <p>When the user dials <b>9725550112</b>, the number 1 is added at the beginning of the sequence; the system transmits <b>19725550112</b>.</p>
, (comma)	<p>An intersequence tone played (and placed) between digits plays an outside line dial tone. For example:</p> <pre>9, 1xxxxxxxxxxx</pre> <p>An outside line dial tone plays after the user presses 9. The tone continues until the user presses 1.</p>
! (exclamation point)	<p>Prohibits a dial sequence pattern. For example:</p> <pre>1900xxxxxxxx!</pre> <p>Rejects any 11-digit sequence that begins with 1900.</p>
*xx	Allows a user to enter a 2-digit star code.
S0 or L0	For Interdigit Timer Master Override, enter S0 to reduce the short interdigit timer to 0 seconds, or enter L0 to reduce the long interdigit timer to 0 seconds.
P	<p>To pause, enter P, the number of seconds to pause, and a space. This feature is typically used for implementation of a hotline and warm line, with a 0 delay for the hot line, and a nonzero delay for a warm line. For example:</p> <pre>P5</pre> <p>A pause of 5 seconds is introduced.</p>

## Digit Sequence Examples

The following examples show digit sequences that you can enter in a dial plan.

In a complete dial plan entry, sequences are separated by a pipe character (|), and the entire set of sequences is enclosed within parentheses:



```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

- Extensions on your system:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

[1-8]xx Allows a user to dial any three-digit number that starts with the digits 1 to 8. If your system uses four-digit extensions, enter the following string: [1-8]xxx

- Local dialing with seven-digit number:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | 0 | [49]111 )
```

9, xxxxxxxx After a user presses 9, an external dial tone sounds. The user can enter any seven-digit number, as in a local call.

- Local dialing with 3-digit area code and a 7-digit local number:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

9, <:1>[2-9]xxxxxxxxxx This example is useful where a local area code is required. After a user presses 9, an external dial tone sounds. The user must enter a 10-digit number that begins with a digit 2 through 9. The system automatically inserts the 1 prefix before it transmits the number to the carrier.

- Local dialing with an automatically inserted 3-digit area code:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

8, <:1212>xxxxxxx This example is useful where a local area code is required by the carrier but most calls go to one area code. After the user presses 8, an external dial tone sounds. The user can enter any seven-digit number. The system automatically inserts the 1 prefix and the 212 area code before it transmits the number to the carrier.

- U.S. long-distance dialing:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

9, 1 [2-9] xxxxxxxxxx After the user presses 9, an external dial tone sounds. The user can enter any 11-digit number that starts with 1 and is followed by a digit 2 through 9.

- Blocked number:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

9, 1 900 xxxxxxxx ! This digit sequence is useful if you want to prevent users from dialing numbers that are associated with high tolls or inappropriate content, such as 1-900 numbers in the U.S. After the user presses 9, an external dial tone sounds. If the user enters an 11-digit number that starts with the digits 1900, the call is rejected.

- U.S. international dialing:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

9, 011xxxxxx After the user presses 9, an external dial tone sounds. The user can enter any number that starts with 011, as in an international call from the U.S.

- Informational numbers:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

0 | [49]11 This example includes two-digit sequences, separated by the pipe character. The first sequence allows a user to dial 0 for an operator. The second sequence allows the user to enter 411 for local information or 911 for emergency services.

## Acceptance and Transmission of the Dialed Digits

When a user dials a series of digits, each sequence in the dial plan is tested as a possible match. The matching sequences form a set of candidate digit sequences. As the user enters more digits, the set of candidates diminishes until only one or none is valid. When a terminating event occurs, the IP PBX either accepts the user-dialed sequence and initiates a call, or else rejects the sequence as invalid. The user hears the reorder (fast busy) tone if the dialed sequence is invalid.

The following table explains how terminating events are processed.

Terminating Event	Processing
Dialed digits have not matched any sequence in the dial plan.	The number is rejected.
Dialed digits exactly match one sequence in the dial plan.	If the dial plan allows the sequence, the number is accepted and is transmitted according to the dial plan. If the dial plan blocks the sequence, the number is rejected.
A timeout occurs.	The number is rejected if the dialed digits are not matched to a digit sequence in the dial plan within the time that the applicable interdigit timer specifies. The Interdigit Long Timer applies when the dialed digits do not match any digit sequence in the dial plan. Default: 10 seconds. The Interdigit Short Timer applies when the dialed digits match one or more candidate sequences in the dial plan. Default: 3 seconds.
A user presses the # key or the dial softkey on the IP phone screen.	If the sequence is complete and is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan. If the sequence is incomplete or is blocked by the dial plan, the number is rejected.

## Dial Plan Timer (Off-Hook Timer)

You can think of the Dial Plan Timer as the off-hook timer. This timer starts when the phone goes off hook. If no digits are dialed within the specified number of seconds, the timer expires and the null entry is evaluated. Unless you have a special dial plan string to allow a null entry, the call is rejected. The default length of the Dial Plan Timer is 5 seconds.

### Syntax for the Dial Plan Timer

**SYNTAX:** (Ps<n> | dial plan)

- **s:** The number of seconds; if no number is entered after P, the default timer of 5 seconds applies. With the timer set to 0 seconds, the call transmits automatically to the specified extension when the phone goes off hook.
- **n:** (optional): The number to transmit automatically when the timer expires; you can enter an extension number or a DID number. No wildcard characters are allowed because the number is transmitted as shown. If you omit the number substitution, <n>, the user hears a reorder (fast busy) tone after the specified number of seconds.

### Examples for the Dial Plan Timer

Allow more time for users to start dialing after taking a phone off hook:

```
(P9 | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

P9 means that after taking a phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the user hears a reorder (fast busy) tone. By setting a longer timer, you allow more time for users to enter digits.

To create a hotline for all sequences on the System Dial Plan:

```
(P9<:23> | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

P9<:23> means that after taking the phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the call is transmitted automatically to extension 23.

To create a hotline on a line button for an extension:

```
(P0 <:1000>)
```

With the timer set to 0 seconds, the call is transmitted automatically to the specified extension when the phone goes off hook. Enter this sequence in the Phone Dial Plan for Ext 2 or higher on a client phone.

## Interdigit Long Timer (Incomplete Entry Timer)

You can think of this timer as the incomplete entry timer. This timer measures the interval between dialed digits. It applies as long as the dialed digits do not match any digit sequences in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated as incomplete, and the call is rejected. The default value is 10 seconds.

This section explains how to edit a timer as part of a dial plan. Alternatively, you can modify the Control Timer that controls the default interdigit timers for all calls.

## Syntax for the Interdigit Long Timer

**SYNTAX:** L:s, (dial plan)

- **s:** The number of seconds; if no number is entered after L:, the default timer is 5 seconds. With the timer set to 0 seconds, the call is transmitted automatically to the specified extension when the phone goes off hook.
- Note that the timer sequence appears to the left of the initial parenthesis for the dial plan.

### Example for the Interdigit Long Timer

```
L:15, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 9,8,011xx. | 9,8,xx.[1-8]xx)
```

L:15 means that this dial plan allows the user to pause for up to 15 seconds between digits before the Interdigit Long Timer expires. This setting is especially helpful to users such as sales people, who are reading the numbers from business cards and other printed materials while dialing.

## Interdigit Short Timer (Complete Entry Timer)

You can think of this timer as the complete entry timer. This timer measures the interval between dialed digits. The timer applies when the dialed digits match at least one digit sequence in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated. If the entry is valid, the call proceeds. If the entry is invalid, the call is rejected.

Default: 3 seconds.

### Syntax for the Interdigit Short Timer

**SYNTAX 1:** S:s, (dial plan)

Use this syntax to apply the new setting to the entire dial plan within the parentheses.

**SYNTAX 2:** *sequence* Ss

Use this syntax to apply the new setting to a particular dialing sequence.

**s:** The number of seconds; if no number is entered after S, the default timer of 5 seconds applies.

### Examples for the Interdigit Short Timer

To set the timer for the entire dial plan:

```
S:6, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 9,8,011xx. | 9,8,xx.[1-8]xx)
```

S:6 means that while the user enters a number with the phone off hook, the user can pause for up to 15 seconds between digits before the Interdigit Short Timer expires. This setting is especially helpful to users such as sales people, who are reading the numbers from business cards and other printed materials while dialing.

Set an instant timer for a particular sequence within the dial plan:

```
(9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxxS0 | 9,8,011xx. | 9,8,xx.[1-8]xx)
```

9,8,1[2-9]xxxxxxxxxxS0 means that with the timer set to 0, the call is transmitted automatically when the user dials the final digit in the sequence.

## Edit the Dial Plan on the IP Phone



**Note** You can edit the dial plan in the XML configuration file. Locate the `Dial_Plan_n` parameter in the XML configuration file, where `n` denotes the extension number. Edit the value of this parameter. The value must be specified in the same format as in the **Dial Plan** field on the phone administration web page, described below.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

### Procedure

- Step 1** Select **Voice > Ext(n)**, where `n` is an extension number.
- Step 2** Scroll to the **Dial Plan** section.
- Step 3** Enter the digit sequences in the **Dial Plan** field.
- The default (US-based) systemwide dial plan appears automatically in the field.
- Step 4** You can delete digit sequences, add digit sequences, or replace the entire dial plan with a new dial plan.
- Separate each digit sequence with a pipe character, and enclose the entire set of digit sequences within parentheses. Example:
- ```
(9,8<:1408>[2-9]xxxxxxx | 9,8,1[2-9]xxxxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```
- Step 5** Click **Submit All Changes**.
- The phone reboots.
- Step 6** Verify that you can successfully complete a call with each digit sequence that you entered in the dial plan.
- Note** If you hear a reorder (fast busy) tone, review your entries and modify the dial plan appropriately.

## Reset the Control Timers

If you need to edit a timer setting only for a particular digit sequence or type of call, you can edit the dial plan.

### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

### Procedure

- Step 1** Select **Voice > Regional**.
- Step 2** Scroll to the **Control Timer Values (sec)** section.

**Step 3** Enter the desired values in the **Interdigit Long Timer** field and the **Interdigit Short Timer** field.

**Step 4** Click **Submit All Changes**.

---

## Regional Parameters and Supplementary Services

### Regional Parameters

In the phone web user interface, use the **Regional** tab to configure regional and local settings, such as control timer values, dictionary server script, language selection, and locale to change localization. The Regional tab includes these sections:

- Call Progress Tones—Displays values of all ringtones.
- Distinctive Ring Patterns—Ring cadence defines the ringing pattern that announces a telephone call.
- Control Timer Values—Displays all values in seconds.
- Vertical Service Activation Codes—Includes Call Back Act Code and Call Back Deact Code.
- Outbound Call Codec Selection Codes—Defines the voice quality.
- Time—Includes local date, local time, time zone, and Daylight Saving Time.
- Language—Includes Dictionary Server Script, Language Selection, and Locale.

### Set the Control Timer Values

#### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

#### Procedure

---

**Step 1** Select **Voice > Regional**.

**Step 2** Configure the values in the fields in the **Control Timer Values (sec)** section.

**Step 3** Click **Submit All Changes**.

---

### Localize Your Cisco IP Phone

#### Before you begin

Access the phone administration web page. See [Access the Phone Web Page](#).

## Procedure

---

- Step 1** Select **Voice > Regional**.
- Step 2** Configure the values in the fields in the **Time** and **Language** sections.
- Step 3** Click **Submit All Changes**.
- 

## Time and Date Settings

The Cisco IP Phone obtains the time settings in one of three ways:

- **NTP Server**—When the phone boots up, it tries to contact the first Network Time Protocol (NTP) server to get the time. The phone periodically synchronizes its time with the NTP server. The synchronization period is fixed at 1 hour. Between updates, the phone tracks time with its internal clock.



---

**Note** NTP time takes priority over the time you set using the menu options on the phone screen. When you manually enter a time, this setting takes effect. On the next NTP synchronization, the time is corrected so that the NTP time is displayed.

When you manually enter the phone time, a pop-up is available that alerts you of this behavior.

---

- **Manual Setup**—You can use the phone web user interface to enter the time and date manually. However, the NTP time or SIP Message Date overwrites this value when either is available to the phone. Manual setup requires that you enter the time in 24-hour format only.

The time that the NTP Server and the SIP Date Header serve is expressed in GMT time. The local time is obtained by offsetting the GMT according to the time zone of the region.

You can configure the Time Zone parameter with the phone web user interface or through provisioning. This time can be further offset by the Time Offset (HH/mm) parameter. This parameter must be entered in 24-hour format and can also be configured from the IP phone screen.

The Time Zone and Time Offset (HH/mm) offset values are not applied to manual time and date setup



---

**Note** The time of the log messages and status messages are in UTC time and are not affected by the time zone setting.

---

## Configure Daylight Saving Time

The phone supports automatic adjustment for daylight saving time.



---

**Note** The time of the log messages and status messages are in UTC time. The time zone setting does not affect them.

---

**Before you begin**

Access the phone administration web page. See [Access the Phone Web Page](#).

**Procedure**

- 
- Step 1** Select **Voice > Regional**.
  - Step 2** Set the **Daylight Saving Time Enable** drop-down list box to **Yes**.
  - Step 3** In the **Daylight Saving Time Rule** field, enter the DST rule. This value affects the time stamp on the CallerID.
  - Step 4** Click **Submit All Changes**.
- 

**Daylight Saving Time Examples**

The following example configures daylight saving time for the U.S, adding one hour starting at midnight on the first Sunday in April and ending at midnight on the last Sunday of October; add 1 hour (USA, North America):

```
start=4/1/7/0:0:0;end=10/31/7/0:0:0;save=1
start=4/1/7;end=10/-1/7;save=1
start=4/1/7/0;end=10/-1/7/0;save=1
```

The following example configures daylight saving time for Egypt, starting at midnight on the last Sunday in April and ending at midnight on the last Sunday of September:

```
start=4/-1/7;end=9/-1/7;save=1 (Egypt)
```

The following example configures daylight saving time for New Zealand (in version 7.5.1 and higher), starting at midnight on the first Sunday of October and ending at midnight on the third Sunday of March.

```
start=10/1/7;end=3/22/7;save=1 (New Zealand)
```

The following example reflects the new change starting in March. DST starts on the second Sunday in March and ends on the first Sunday in November:

```
start=3/8/7/02:0:0;end=11/1/7/02:0:0;save=1
```

The following example configures the daylight saving time starting on the last Monday (before April 8) and ending on the first Wednesday (after May 8.)

```
start=4/-8/1;end=5/8/3;save=1
```

**Phone Display Language**

The Cisco IP Phone supports multiple languages for the phone display.

By default, the phone is set up for English. To enable the use of another language, you must set up the dictionary for the language. For some languages, you must also set up the font for the language.

After the setup is complete, you or your users can specify the desired language for the phone display.



## Supported Languages for the Phone Display

On the phone administration web page, go to **Admin Login > Advanced > Voice > Regional**. In the **Language** section, click the **Locale** drop-down list box to see the supported languages for the phone display.

- bg-BG (Bulgarian)
- ca-ES (Catalan)
- cs-CZ (Czech)
- da-DK (Danish)
- de-DE (German)
- en-AU (English-Australia)
- en-CA (English-Canada)
- en-GB (English-Great Britain)
- en-NZ (English-New Zealand)
- en-US (English-United States)
- es-ES (Spanish-Spain)
- es-MX (Spanish-Mexico)
- fi-FI (Finnish)
- fr-CA (French-Canada)
- fr-FR (French-France)
- hr-HR (Hungarian)
- it-IT (Italian)
- ja-JP (Japanese)
- ko-KR (Korean)
- nl-NL (Dutch)
- nn-NO (Norwegian)
- pl-PL (Polish)
- pt-BZ (Portuguese-Brazil)
- pt-PT (Portuguese-Portugal)
- ru-RU (Russian)
- sk-SK (Slovak)
- sv-SE (Swedish)
- tr-TR (Turkish)
- zh-CN (Chinese-Simplified)
- zh-HK (Chinese-Hong Kong)

## Set Up Dictionaries and Fonts

Languages other than English require dictionaries. Some languages also require a font.

### Procedure

- 
- Step 1** Download the locale zip file for your firmware version, from [cisco.com](http://cisco.com). Place the file on your server, and unzip the file.
- Dictionaries and fonts for all the supported languages are included in the zip file. Dictionaries are XML scripts. Fonts are standard TTF files.
- Step 2** On the phone administration web page, go to **Admin Login > Advanced > Voice > Regional**. In the **Language** section, specify the necessary parameters and values in the **Dictionary Server Script** field as described below. Use a semicolon (;) to separate multiple parameter and value pairs.
- Specify the location of the dictionary and font files with the `serv` parameter.  
For example: `serv=http://10.74.128.101/Locales/`  
Make sure to include the IP address of the server, the path, and folder name.
  - For each language that you want to set up, specify a set of parameters as described below.

**Note** In these parameter specifications, *n* denotes a serial number. This number determines the sequential order in which the language options are displayed in the **Settings** menu of the phone. 0 is reserved for US-English, which has a default dictionary. You can use it optionally, to specify your own dictionary.

Use numbers starting with 1 for other languages.

- Specify the language name with the *d<sub>n</sub>* parameter.

For example: `d1=Chinese-Simplified`

This name is displayed as a language option in the **Settings** menu of the phone.

- Specify the name of the dictionary file with the *x<sub>n</sub>* parameter.

For example: `x1=zh-CN_78xx_68xx-11.2.1.1004.xml`

Make sure to specify the correct file for the language and phone model that you use.

- If a font is required for the language, specify the name of the font file with the *f<sub>n</sub>* parameter.

For example: `f1=zh-CN_78xx_68xx-11.2.1.1004.ttf`

Make sure to specify the correct file for the language and phone model that you use.

**Note** Font files with 'BMP' in the file name are for the Cisco IP Phone 7821.

See [Setup for Latin Languages, on page 42](#) for specific details on setting up Latin languages.

See [Setup for an Asian Language, on page 42](#) for specific details on setting up an Asian language.

### Step 3 Click **Submit All Changes**.

## Setup for Latin Languages

If you use Latin languages such as French or German, you can configure up to 9 language options for the phone. The options are displayed in the **Settings** menu of the phone. To enable the options, set up a dictionary for each language that you want to include. To do this, specify a pair of the *d<sub>n</sub>* and *x<sub>n</sub>* parameters and values in the **Dictionary Server Script** field, for each language that you want to include.

Example for including French and German:

```
serv=http://10.74.128.101/Locales/;d1=French;x1=fr-FR_78xx_68xx-11.2.1.1004.xml;
d2=German;x2=de-DE_78xx_68xx-11.2.1.1004.xml
```

## Setup for an Asian Language

If you use an Asian language such as Chinese, Japanese, or Korean, you can only set up one language option for the phone.

You must set up the dictionary and the font for the language. To do this, specify the *d<sub>1</sub>*, *x<sub>1</sub>* and *f<sub>1</sub>* parameters and values in the **Dictionary Server Script** field.

Example for setting up Chinese-Simplified:

```
serv=http://10.74.128.101/Locales/;d1=Chinese-Simplified;
x1=zh-CN_78xx_68xx-11.2.1.1004.xml;f1=zh-CN_78xx_68xx-11.2.1.1004.ttf
```

## Specify a Language for the Phone Display



---

**Note** Your users can select the language on the phone, from **Settings > Device Administration > Language**.

---

### Before you begin

The dictionaries and fonts required for the language are set up. See [Set Up Dictionaries and Fonts](#), on page 41 for details.

### Procedure

---

- Step 1** On the phone administration web page, go to **Admin Login > Advanced > Voice > Regional, Language** section. In the **Language Selection** field, specify the value of the appropriate `dn` parameter value from the **Dictionary Server Script** field, for the language of your choice.
- Step 2** Click **Submit All Changes**.
- 

## Cisco IP Phone 7800 Series Documentation

Refer to publications that are specific to your language and phone model, and phone firmware release. Navigate from the following documentation URL:

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-7800-series-multiplatform-firmware/tsd-products-support-series-home.html>

