

Before You Begin

- Prerequisites for Configuring Cisco Unified CME, on page 1
- Restrictions for Configuring Cisco Unified CME, on page 2
- Information About Planning Your Configuration, on page 2
- Cisco Unified CME Workflow, on page 5
- Install Cisco Voice Services Hardware, on page 9
- Install Cisco IOS Software, on page 11
- Configure VLANs on a Cisco Switch, on page 12
- Using Cisco IOS Commands, on page 17
- Voice Bundles, on page 18

Prerequisites for Configuring Cisco Unified CME

- Base Cisco Unified CME feature license and phone user licenses that entitle you to use Cisco Unified CME are purchased.

Note To support H.323 call transfers and forwards to network devices that do not support the H.450 standard, such as Cisco Unified Communications Manager, a tandem gateway is required in the network. The tandem gateway must be running Cisco IOS release 12.3(7)T or a later release and requires the Integrated Voice and Video Services feature license (FL-GK-NEW-xxx), which includes H.323 gatekeeper, IP-to-IP gateway, and H.450 tandem functionality.

- Your IP network is operational and you can access Cisco web.
- You have a valid Cisco.com account.
- You have access to a TFTP server for downloading files.
- Cisco router with all recommended services hardware for Cisco Unified CME is installed. For installation information, see Install Cisco Voice Services Hardware, on page 9.
- Recommended Cisco IOS IP Voice or higher image is downloaded to flash memory in the router.
    - To determine which Cisco IOS software release supports the recommended Cisco Unified CME version, see Cisco Unified CME and Cisco IOS Software Compatibility Matrix.

  - For a list of features for each Cisco IOS Software release, see Feature Navigator.
  - For installation information, see Install Cisco IOS Software, on page 11.

- VoIP networking must be operational. For quality and security purposes, we recommend separate virtual LANs (VLANs) for data and voice. The IP network assigned to each VLAN should be large enough to support addresses for all nodes on that VLAN. Cisco Unified CME phones receive their IP addresses from the voice network, whereas all other nodes such as PCs, servers, and printers receive their IP addresses from the data network. For configuration information, see Configure VLANs on a Cisco Switch, on page 12.

Restrictions for Configuring Cisco Unified CME

- Cisco Unified CME cannot register as a member of a Cisco Unified Communications Manager cluster.
- For conferencing and music on hold (MOH) support with G.729, hardware digital signal processors (DSPs) are required for transcoding G.729 between G.711.
- After a three-way conference is established, a participant cannot use call transfer to join the remaining conference participants to a different number.
- Cisco Unified CME does not support the following:
  - CiscoWorks IP Telephony Environment Monitor (ITEM)
  - Element Management System (EMS) integration
  - Media Gateway Control Protocol (MGCP) on-net calls
  - Java Telephony Application Programming Interface (JTAPI) applications, such as the Cisco IP Softphone, Cisco Unified Communications Manager Auto Attendant, or Cisco Personal Assistant
  - Telephony Application Programming Interface (TAPI)

    Cisco Unified CME implements only a small subset of TAPI functionality. It supports operation of multiple independent clients (for example, one client per phone line), but not full support for multiple-user or multiple-call handling, which is required for complex features such as automatic call distribution (ACD) and Cisco Unified Contact Center (formerly Cisco IPCC). Also, this TAPI version does not have direct media and voice-handling capabilities.
  - Co-location of CME and CUBE or LGW on the same device.

Information About Planning Your Configuration

System Design

Traditional telephony systems are based on physical connections and are therefore limited in the types of phone services that they can offer. Because phone configurations and directory numbers in a Cisco Unified CME system are software entities and because the audio stream is packet-based, an almost limitless number of combinations of phone numbers, lines, and phones can be planned and implemented.

Cisco Unified CME systems can be designed in many ways. The key is to determine the total number of simultaneous calls you want to handle at your site and at each phone at your site, and how many different directory numbers and phones you want to have. Even a Cisco Unified CME system has its limits, however. Consider the following factors in your system design:

- Maximum number of phones—This number corresponds to the maximum number of devices that can be attached. The maximum is platform- and version-dependent. To find the maximum for your platform and version, see Cisco CME Supported Firmware, Platforms, Memory, and Voice Products.
- Maximum number of directory numbers—This number corresponds to the maximum number of simultaneous call connections that can occur. The maximum is platform- and version-dependent. To find the maximum for your platform and version, see Cisco CME Supported Firmware, Platforms, Memory, and Voice Products.
- Telephone number scheme—Your numbering plan may restrict the range of telephone numbers or extension numbers that you can use. For example, if you have DID, the PSTN may assign you a certain series of numbers.
- Maximum number of buttons per phone—You may be limited by the number of buttons and phones that your site can use. For example, you may have two people with six-button phones to answer 20 different telephone numbers.

The flexibility of a Cisco Unified CME system is due largely to the different types of directory numbers (DNs) that you can assign to phones in your system. By understanding types of DNs and considering how they can be combined, you can create the complete call coverage that your business requires. For more information about DNs, see Configuring Phones to Make Basic Calls.

After setting up the DNs and phones that you need, you can add optional Cisco Unified CME features to create a telephony environment that enhances your business objectives. Cisco Unified CME systems are able to integrate with the PSTN and with your business requirements to allow you to continue using your existing number plans, dialing schemes, and call coverage patterns.

When creating number plans, dialing schemes, and call coverage patterns in Cisco Unified CME, there are several factors that you must consider:

- Is there an existing PBX or Key System that you are replacing and want to emulate?
- Number of phones and phone users to be supported?
- Do you want to use single-line or dual-line DNs?
- What protocols does your voice network support?
- Which call transfer and forwarding methods must be supported?
- What existing or preferred billing method do you want to use for transferred and forwarded calls?
- Do you need to optimize network bandwidth or minimize voice delay?

Because these factors can limit your choices for some of the configuration decisions that you will make when you create of a dialing plan, see the Cisco Unified Communications Manager Express Solution Reference Network Design Guide to help you understand the effect these factors have on your Cisco Unified CME implementation.

Toll Fraud Prevention

When a Cisco router platform is installed with a voice-capable Cisco IOS software image, appropriate features must be enabled on the platform to prevent potential toll fraud exploitation by unauthorized users. Deploy these features on all Cisco router Unified Communications applications that process voice calls, such as Cisco Unified Communications Manager Express (Cisco Unified CME), Cisco Survivable Remote Site Telephony (Cisco Unified SRST), Cisco Unified Border Element, Cisco IOS-based router and standalone analog and digital PBX and public-switched telephone network (PSTN) gateways, and Cisco contact-center VoiceXML gateways. These features include, but are not limited to, the following:

- Disable secondary dial tone on voice ports—By default, secondary dial tone is presented on voice ports on Cisco router gateways. Use private line automatic ringdown (PLAR) for foreign exchange office (FXO) ports and direct-inward-dial (DID) for T1/E1 ports to prevent secondary dial tone from being presented to inbound callers.
- Cisco router access control lists (ACLs)—Define ACLs to allow only explicitly valid sources of calls to the router or gateway, and therefore to prevent unauthorized Session Initiation Protocol (SIP) or H.323 calls from unknown parties to be processed and connected by the router or gateway.
- Close unused SIP and H.323 ports—If either the SIP or H.323 protocol is not used in your deployment, close the associated protocol ports. If a Cisco voice gateway has dial peers configured to route calls outbound to the PSTN using either time division multiplex (TDM) trunks or IP, close the unused H.323 or SIP ports so that calls from unauthorized endpoints cannot connect calls. If the protocols are used and the ports must remain open, use ACLs to limit access to legitimate sources.
- Change SIP port 5060—If SIP is actively used, consider changing the port to something other than well-known port 5060.
- SIP registration—If SIP registration is available on SIP trunks, turn on this feature because it provides an extra level of authentication and validation that only legitimate sources can connect calls. If it is not available, ensure that the appropriate ACLs are in place.
- SIP Digest Authentication—If the SIP Digest Authentication feature is available for either registrations or invites, turn this feature on because it provides an extra level of authentication and validation that only legitimate sources can connect calls.
- Explicit incoming and outgoing dial peers—Use explicit dial peers to control the types and parameters of calls allowed by the router, especially in IP-to-IP connections used on Cisco Unified CME, Cisco Unified SRST, and Cisco Unified Border Element. Incoming dial peers offer additional control on the sources of calls, and outgoing dial peers on the destinations. Incoming dial peers are always used for calls. If a dial peer is not explicitly defined, the implicit dial peer 0 is used to allow all calls.
- Explicit destination patterns—Use dial peers with more granularity than .T for destination patterns to block disallowed off-net call destinations. Use class of restriction (COR) on dial peers with specific destination patterns to allow even more granular control of calls to different destinations on the PSTN.
- Translation rules—Use translation rules to manipulate dialed digits before calls connect to the PSTN to provide better control over who may dial PSTN destinations. Legitimate users dial an access code and an augmented number for PSTN for certain PSTN (for example, international) locations.
- Tcl and VoiceXML scripts—Attach a Tcl/VoiceXML script to dial peers to do database lookups or additional off-router authorization checks to allow or deny call flows based on origination or destination numbers. Tcl/VoiceXML scripts can also be used to add a prefix to inbound DID calls. If the prefix plus DID matches internal extensions, then the call is completed. Otherwise, a prompt can be played to the caller that an invalid number has been dialed.

- Host name validation—Use the "permit hostname" feature to validate initial SIP Invites that contain a fully qualified domain name (FQDN) host name in the Request Uniform Resource identifier (Request URI) against a configured list of legitimate source hostnames.
- Dynamic Domain Name Service (DNS)—If you are using DNS as the "session target" on dial peers, the actual IP address destination of call connections can vary from one call to the next. Use voice source groups and ACLs to restrict the valid address ranges expected in DNS responses (which are used subsequently for call setup destinations).

For more configuration guidance, see Cisco IOS Unified Communications Toll Fraud Prevention and Configure Toll Fraud Prevention.

Cisco Unified CME Workflow

Table 1: Workflow for Creating or Modifying Basic Telephony Configuration, on page 5 lists the tasks for installing and configuring Cisco Unified CME and for modifying the configuration, in the order in which the tasks are to be performed and including links to modules in this guide that support each task.

Note Not all tasks are required for all Cisco Unified CME systems, depending on software version and on whether it is a new Cisco Unified CME, an existing Cisco router that is being upgraded to support Cisco Unified CME, or an existing Cisco Unified CME that is being upgraded or modified for new features or to add or remove phones.

Table 1: Workflow for Creating or Modifying Basic Telephony Configuration

Task	Cisco Unified CME Configuration		
	New	Modify	Documentation
Install Cisco router and all recommended services hardware for Cisco Unified CME.	Required	Optional	Install Cisco Voice Services Hardware, on page 9
Download recommended Cisco IOS IP Voice or higher image to flash memory in the router.	Optional	Optional	Install Cisco IOS Software, on page 11
Download recommended Cisco Unified CME software including phone firmware.	Optional	Optional	Install and Upgrade Cisco Unified CME Software
Configure separate virtual LANs (VLANS) for data and voice on the port switch.	Required	—	Network Assistant, on page 12 or Cisco IOS Commands, on page 13 or Internal Cisco Ethernet Switching Module, on page 16

Task	Cisco Unified CME Configuration		
	New	Modify	Documentation
• Enable calls in your VoIP network. • Define DHCP. • Set Network Time Protocol (NTP). • Configure DTMF Relay for H.323 networks in multisite installations. • Configure SIP trunk support. • Change the TFTP address on a DHCP server • Enable OOD-R.	Required	Optional	Network Parameters
• Configure Bulk Registration. • Set up Cisco Unified CME. • Set date and time parameters. • Block Automatic Registration. • Define alternate location and type of configuration files. • Change defaults for Time Outs. • Configure a redundant router.	Required	Optional	System-Level Parameters

Task	Cisco Unified CME Configuration		
	New	Modify	Documentation
• Create directory numbers and assigning directory numbers to phones. • Create phone configurations using Extension Assigner. • Generate configuration files for phones. • Reset or restart phones.	Required	Optional	Configure Phones to Make Basic Call
Connect to PSTN.	Required	—	Dial Plans
Install system- and user-defined files for localization of phones.	Optional	Optional	Localization Support

Table 2: Workflow for Adding Features in Cisco Unified CME, on page 7 contains a list of tasks for adding commonly configured features in Cisco Unified CME and the module in which they appear in this guide. For a detailed list of features, with links to corresponding information in this guide, see Cisco Unified CME Features Roadmap.

Table 2: Workflow for Adding Features in Cisco Unified CME

Task	Documentation
Configure transcoding to support conferencing, call transferring and forwarding, MOH, and Cisco Unity Express.	Transcoding Resources
Configure support for voice mail.	Voice Mail Integration
Configure interoperability with Cisco Unified CCX.	Interoperability with Cisco Unified CCX
Configure authentication support.	Security

Task	Documentation

Add features.
• Call Blocking
• Call-Coverage Features, including:
  • Call Hunt
  • Call Pickup
  • Call Waiting
  • Callback Busy Subscriber
  • Hunt Groups
  • Night Service
  • Overlaid Ephone-dns
• Call Park
• Call Transfer and Forwarding
• Caller ID Blocking
• Conferencing
• Intercom Lines
• Music on Hold (MOH)
• Paging
	• Automatic Line Selection
	• Call Blocking
	• Call Coverage Features
	• Call Park
	• Call Transfer and Forward
	• Caller ID Blocking
	• Conferencing
	• Directory Services
	• Do Not Disturb
	• Extension Mobility
	• Feature Access Codes
	• Headset Auto Answer
	• Intercom Lines
	• Loopback Call Routing
	• Music on Hold
	• Paging
	• Presence Service
	• Ringtones
	• Customize Softkeys
	• Speed Dial

Configure phone options, including: • Customized Background Images for Cisco Unified IP Phone 7970 • Fixed Line/Feature Buttons for Cisco Unified IP Phone 7931G • Header Bar Display • PC Port Disable • Phone Labels • Programmable vendorConfig Parameters • System Message Display • URL Provisioning for Feature Buttons	Modify Cisco Unified IP Phone Options

Task	Documentation
Configure video support.	Video Support
Configure Cisco Unified CME as SRST Fallback.	SRST Fallback Mode

Install Cisco Voice Services Hardware



Note Cisco routers are normally shipped with Cisco voice services hardware and other optional equipment that you ordered already installed. In the event that the hardware is not installed or you are upgrading your existing Cisco router to support Cisco Unified CME or Cisco Unity Express, you will be required to install hardware components.

Voice bundles do not include all the necessary components for Cisco Unity Express. Contact the Cisco IP Communications Express partner in your area for more information about including Cisco Unity Express in your configuration.

Before you begin

- Cisco router and all recommended hardware for Cisco Unified CME, and if required, Cisco Unity Express, is ordered and delivered, or is already onsite.

Procedure

Step 1 Install the Cisco router on your network. To find installation instructions for the Cisco router, access documents located at **www.cisco.com>Technical Support & Documentation>Product Support>Routers>*router you are using*>Install and Upgrade Guides**.

Step 2 Install Cisco voice services hardware.

a) To find installation instructions for any Cisco interface card, access documents located at **www.cisco.com>Technical Support & Documentation>Product Support>Cisco Interfaces and Modules>*interface you are using*>Install and Upgrade Guides** or Documentation Roadmap.

b) To install and configure your Catalyst switch, see Cisco Network Assistant.

c) To find installation instructions for any Cisco EtherSwitch module, access documents located at **www.cisco.com>Technical Support & Documentation>Product Support>Cisco Switches>*switch you are using*>Install and Upgrade Guides**.

Step 3 Connect to the Cisco router using a terminal or PC with terminal emulation. Attach a terminal or PC running terminal emulation to the console port of the router.

Use the following terminal settings:

- 9600 baud rate
- No parity
- 8 data bits

- 1 stop bit
- No flow control

Note
Memory recommendations and maximum numbers of Cisco IP phones identified in the next step are for common Cisco Unified CME configurations only. Systems with large numbers of phones and complex configurations may not work on all platforms and can require additional memory or a higher performance platform.

Step 4 Log in to the router and use the **show version** EXEC command or the **show flash** privileged EXEC command to check the amount of memory installed in the router. Look for the following lines after issuing the **show version** command.

Example:

```
Router> show version...
Cisco 2691 (R7000) processor (revision 0.1) with 177152K/19456K bytes of memory
...
31360K bytes of ATA System Compactflash (Read/Write)
```

The first line indicates how much Dynamic RAM (DRAM) and Packet memory is installed in your router. Some platforms use a fraction of their DRAM as Packet memory. The memory requirements take this into account, so you have to add both numbers to find the amount of DRAM available on your router (from a memory requirement point of view).

The second line identifies the amount of flash memory installed in your router.

or

Look for the following line after issuing the **show flash** command. Add the number available to the number used to determine the total flash memory installed in the Cisco router.

```
Router# show flash
...
2252800 bytes available, (29679616 bytes used]
```

Step 5 Identify DRAM and flash memory requirements for the Cisco Unified CME version and Cisco router model you are using. To find Cisco Unified CME specifications, see the appropriate Cisco Unified CME Supported Firmware, Platforms, Memory, and Voice Products.

Step 6 Compare the amount of memory required to the amount of memory installed in the router. To install or upgrade the system memory in the router, access documents located at **www.cisco.com>Technical Support & Documentation>Product Support>Routers>*router you are using*>Install and Upgrade Guides**.

Step 7 Use the **memory-size iomem** *i/o memory-percentage* privileged EXEC command to disable Smartinit and allocate ten percent of the total memory to Input/Output (I/O) memory.

Example:

```
Router# memory-size iomem 10
```

Install Cisco IOS Software

Note The Cisco router in a voice bundle is preloaded with the recommended Cisco IOS software release and feature set plus the necessary Cisco Unified CME phone firmware files to support Cisco Unified CME and Cisco Unity Express. If the recommended software is not installed or if you are upgrading an existing Cisco router to support Cisco Unified CME and Cisco Unity Express, you will be required to download and extract the required image and files.

To verify that the recommended software is installed on the Cisco router and if required, download and install a Cisco IOS Voice or higher image, perform the following steps.

Before you begin

- The Cisco router is installed including sufficient memory, all Cisco voice services hardware, and other optional hardware.

Procedure

Step 1 Identify which Cisco IOS software release is installed on router. Log in to the router and use the **show version EXEC** command.

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.3 T Software (C2600-I-MZ), Version 12.3(11)T, RELEASE SOFTWARE
```

Step 2 Compare the Cisco IOS release installed on the Cisco router to the information in the Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix to determine whether the Cisco IOS release supports the recommended Cisco Unified CME.

Step 3 If required, download and extract the recommended Cisco IOS IP Voice or higher image to flash memory in the router.

To find software installation information, access information located at **www.cisco.com>Technical Support & Documentation>Product Support> Cisco IOS Software>*Cisco IOS Software Mainline release you are using*> Configuration Guides> Cisco IOS Configuration Fundamentals and Network Management Configuration Guide>Part 2: File Management>Locating and Maintaining System Images**.

Step 4 To reload the Cisco Unified CME router with the new software after replacing or upgrading the Cisco IOS release, use the **reload** privileged EXEC command.

Example:

```
Router# reload
System configuration has been modified. Save [yes/no]:
Y
Building configuration...
OK
Proceed with reload? Confirm.
11w2d: %Sys-5-RELOAD: Reload requested by console. Reload reason: reload command . System bootstrap,
 System Version 12.2(8r)T, RELEASE SOFTWARE (fc1)
```

```
...
Press RETURN to get started.
...
Router>
```

What to do next

- If you installed a new Cisco IOS software release on the Cisco router, download and extract the compatible Cisco Unified CME version. See Install and Upgrade Cisco Unified CME Software.
- If you are installing a new stand-alone Cisco Unified CME system, see Configure VLANs on a Cisco Switch, on page 12.

Configure VLANs on a Cisco Switch

To configure two Virtual Local Area Networks (VLANs), one for voice and one for data, on a Cisco Catalyst switch or an internal Cisco NM, HWIC, or Fast Ethernet switching module, perform only *one* of the following tasks.

- Network Assistant, on page 12
- Cisco IOS Commands, on page 13
- Internal Cisco Ethernet Switching Module, on page 16

Network Assistant

To configure two Virtual Local Area Networks (VLANs), one for voice and one for data, on an external Cisco Catalyst switch and to implement Cisco Quality-of-Service (QoS) policies on your network, perform the following steps.

Before you begin

- The Cisco router is installed including sufficient memory, all Cisco voice services hardware and other optional hardware.
- The recommended Cisco IOS release and feature set plus the necessary Cisco Unified CME phone firmware files are installed.
- Determine if you can use the Cisco Network Assistant to configure VLANs on the switch for your Cisco Unified CME router, see *Devices Supported* in the appropriate Release Notes for Cisco Network Assistant.

Note A PC connected to the Cisco Unified CME router over the LAN is required to download, install, and run Cisco Network Assistant.

- If you want to use Cisco Network Assistant to configure VLANs on the Cisco Catalyst switch, verify that the PC on which you want to install and run Cisco Network Assistant meets the minimum hardware

and operating system requirements. See *Installing, Launching, and Connecting Network Assistant* in Getting Started with Cisco Network Assistant.

- An RJ-45-to-RJ-45 rollover cable and the appropriate adapter (both supplied with the switch) connecting the RJ-45 console port of the switch to a management station or modem is required to manage a Cisco Catalyst switch through the management console.

Procedure

Step 1 Install, launch, and connect Cisco Network Assistant. For instructions, see *Installing, Launching, and Connecting Network Assistant* in Getting Started with Cisco Network Assistant.

Step 2 Use Cisco Network Assistant to perform the following tasks. See online Help for additional information and procedures.

- Enable two VLANs on the switch port.
- Configure a trunk between the Cisco Unified CME router and the switch.
- Configure Cisco IOS Quality-of-Service (QoS).

Cisco IOS Commands

To configure two Virtual Local Area Networks (VLANs), one for voice and one for data, a trunk between the Cisco Unified CME router and the switch, and Cisco IOS Quality-of-Service (QoS) on an external Cisco Catalyst switch, perform the following steps.

Before you begin

- The Cisco router is installed including sufficient memory, all Cisco voice services hardware and other optional hardware.
- The recommended Cisco IOS release and feature set plus the necessary Cisco Unified CME phone firmware files are installed.
- An RJ-45-to-RJ-45 rollover cable and the appropriate adapter (both supplied with the switch) connecting the RJ-45 console port of the switch to a management station or modem is required to manage a Cisco Catalyst switch through the management console.

SUMMARY STEPS

1. **enable**
2. **vlan database**
3. **vlan** *vlan-number* **name** *vlan-name*
4. **vlan** *vlan-number* **name** *vlan-name*
5. **exit**
6. **wr**
7. **configure terminal**
8. **macro global apply cisco-global**

9. **interface** *slot-number* / *port-number*
10. **macro apply cisco-phone $AVID** *number* **$VVID** *number*
11. **interface** *slot-number* / *port-number*
12. **macro apply cisco-router $NVID** *number*
13. **end**
14. **wr**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**vlan database** **Example:** `Switch# vlan database`	Enters VLAN configuration mode.

Step 3	**vlan** *vlan-number* **name** *vlan-name*
	Example:
	`Switch(vlan)# vlan 10 name data`
	`VLAN 10 modified`
	`Name: DATA`
		Specifies the number and name of the VLAN being configured.
		• *vlan-number*—Unique value that you assign to the dial-peer being configured. Range: 2 to 1004.
		• *name*—Name of the VLAN to associate to the vlan-number being configured.

Step 4	**vlan** *vlan-number* **name** *vlan-name*
	Example:
	`Switch(vlan)# vlan 100 name voice`
	`VLAN 100 modified`
	`Name: VOICE`
		Specifies the number and name of the VLAN being configured.

Step 5	**exit** **Example:** `Switch(vlan)# exit`	Exits this configuration mode.
Step 6	**wr** **Example:** `Switch# wr`	Writes the modifications to the configuration file.
Step 7	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 8	**macro global apply cisco-global** **Example:** `Switch (config)# macro global apply cisco-global`	Applies the Smartports global configuration macro for QoS.
Step 9	**interface** *slot-number* / *port-number* **Example:** `Switch (config)# interface fastEthernet 0/1`	Specifies interface to be configured while in the interface configuration mode. • *slot-number*/*port-number*—Slot and port of interface to which Cisco IP phones or PCs are connected**.** **Note** The slash must be entered between the slot and port numbers.
Step 10	**macro apply cisco-phone $AVID** *number* **$VVID** *number* **Example:** `Switch (config-if)# macro apply cisco-phone $AVID 10 $VVID 100`	Applies VLAN and QoS settings in Smartports macro to the port being configured. • **$AVID** *number*—Data VLAN configured in earlier step. • **$VVID** *number*—Voice VLAN configured in earlier step.
Step 11	**interface** *slot-number* / *port-number* **Example:** `Switch (config-if)# interface fastEthernet 0/24`	Specifies interface to be configured while in the interface configuration mode. • *slot-number*/*port-number*—Slot and port of interface to which the Cisco router is connected**.** **Note** The slash must be entered between the slot and port numbers.
Step 12	**macro apply cisco-router $NVID** *number* **Example:** `Switch (config-if)# macro apply cisco-router $NVID 10`	Applies the VLAN and QoS settings in Smartports macro to the port being configured. • **$NVID** *number*—Data VLAN configured in earlier step.
Step 13	**end** **Example:** `Switch(config-if)# end`	Exits to privileged EXEC configuration mode.
Step 14	**wr** **Example:** `Switch# wr`	Writes the modifications to the configuration file.

What to do next

See Using Cisco IOS Commands, on page 17.

Internal Cisco Ethernet Switching Module

To configure two Virtual Local Area Networks (VLANs), one for voice and one for data, on an internal Cisco Ethernet switching module, perform the following steps.

Before you begin

- The Cisco router is installed including sufficient memory, all Cisco voice services hardware and other optional hardware.
- The recommended Cisco IOS release and feature set plus the necessary Cisco Unified CME phone firmware files are installed.
- The switch is in privileged EXEC mode.

SUMMARY STEPS

1. **enable**
2. **vlan database**
3. **vlan** *vlan-number* **name** *vlan-name*
4. **vlan** *vlan-number* **name** *vlan-name*
5. **exit**
6. **wr**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**vlan database** **Example:** `Switch# vlan database`	Enters VLAN configuration mode.

Step 3	**vlan** *vlan-number* **name** *vlan-name*
	Example:
	`Switch(vlan)# vlan 10 name data`
	`  VLAN 10 modified Name: DATA`
		Specifies the number and name of the VLAN being configured.
		• *vlan-number*—Unique value that you assign to dial-peer being configured. Range: 2 to 1004.
		• *name*—Name of the VLAN to associate to the vlan-number being configured.

Step 4	**vlan** *vlan-number* **name** *vlan-name* **Example:**	Specifies the number and name of the VLAN being configured.

	Command or Action	Purpose

	`Switch(vlan)# vlan 100 name voice`
	`VLAN 100 modified`
	`Name: VOICE`	

Step 5	**exit** **Example:** `Switch(vlan)# exit`	Exits this configuration mode.
Step 6	**wr** **Example:** `Switch# wr`	Writes the modifications to the configuration file.

What to do next

See Using Cisco IOS Commands, on page 17.

Using Cisco IOS Commands

Prerequisites

- Hardware and software to establish a physical or virtual console connection to the Cisco router using a terminal or PC running terminal emulation is available and operational.
- Connect to the Cisco router using a terminal or PC with terminal emulation. Attach a terminal or PC running terminal emulation to the console port of the router.

  For connecting to the router to be configured, use the following terminal settings:

  - 9600 baud rate
  - No parity
  - 8 data bits
  - 1 stop bit
  - No flow control

Your choice of configuration method depends on whether you want to create an initial configuration for your IP telephony system or you want to perform ongoing maintenance, such as routinely making additions and changes associated with employee turnover. Table 3: Comparison of Configuration Methods for Cisco Unified CME, on page 18 compares the different methods for configuring Cisco Unified CME.

Table 3: Comparison of Configuration Methods for Cisco Unified CME

Configuration Method	Benefits	Restrictions
Cisco IOS command line interface	• Generates commands for running configuration which can be saved on Cisco router to be configured. • Use for setting up or modifying all parameters and features during initial configuration and ongoing maintenance.	Requires knowledge of Cisco IOS commands and Cisco Unified CME.

Voice Bundles

Voice bundles include a Cisco Integrated Services Router for secure data routing, Cisco Unified CME software and licenses to support IP telephony, Cisco IOS SP Services or Advanced IP Services software for voice gateway features, and the flexibility to add Cisco Unity Express for voice mail and auto attendant capabilities. Voice bundles are designed to meet the diverse needs of businesses worldwide. To complete the solution, add digital or analog trunk interfaces to interface to the PSTN or the host PBX, Cisco IP phones, and Cisco Catalyst data switches supporting Power-over Ethernet (PoE).

Table 4: Cisco Tools for Deploying Cisco IPC Express, on page 18 contains a list of the Cisco tools for deploying Cisco IPC Express.

Table 4: Cisco Tools for Deploying Cisco IPC Express

Tool Name	Description
Cisco Configuration Professional Express (Cisco CP Express) and Cisco Configuration Professional (Cisco CP)	Cisco CP Express is a basic router configuration tool that resides in router Flash memory. It is shipped with every device ordered with Cisco CP. Cisco CP Express allows the user to give the device a basic configuration, and allows the user to install Cisco CP for advanced configuration and monitoring capabilities. Cisco CP is the next generation advanced configuration and monitoring tool. It enables you to configure such things as router LAN and WAN interfaces, a firewall, IPSec VPN, dynamic routing, and wireless communication. Cisco CP is installed on a PC. It is available on a CD, and can also be downloaded from www.cisco.com.
Cisco Network Assistant	Cisco Network Assistant is a PC-based network management application optimized for networks of small and medium-sized businesses.
Initialization Wizard for Cisco Unity Express See *Configuring the System for the First Time*, in the appropriate Cisco Unity Express GUI Administrator Guide.	Initialization Wizard in the Cisco Unity Express GUI prompts the user for required information to configure users, voice mailboxes, and other features of voice mail and auto attendant. The wizard starts automatically the first time you log in to the Cisco Unity Express GUI.

Tool Name	Description
Router and Security Device Manager (SDM)	Cisco Router and Security Device Manager (Cisco SDM) is an intuitive, Web-based device-management tool for Cisco routers. Cisco SDM simplifies router and security configuration through smart wizards, which help customers and Cisco partners quickly and easily deploy, and configure a Cisco router without requiring knowledge of the command-line interface (CLI). Supported on Cisco 830 Series to Cisco 7301 routers, Cisco SDM is shipping on Cisco 1800 Series, Cisco 2800 Series, and Cisco 3800 Series routers pre-installed by the factory.