Telephony Using Cisco UCM

TECHNOLOGY DESIGN GUIDE

August 2013

VALIDATED DESIGN

Table of Contents

Preface

Cisco Validated Designs (CVDs) provide the framework for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-
transmit 48 exceed-action transmit
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- **Centralized Unified Communications**—Organizations require high-quality voice and video communications that can scale to tens of thousands of users. They need a solution that is fast to deploy and easy to manage from a central location, without replicating costly features at their remote sites.

For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- Unified communications applications, such as IP telephony and voicemail
- Telephony call agent
- Voicemail server
- Virtualized servers
- Voice gateways and conference bridges
- IP telephones with remote-site survivability
- Session Initiation Protocol (SIP) and Skinny Client Control Protocol (SCCP) signaling
- Quality of service (QoS) and bandwidth control
- Lightweight Directory Access Protocol integration
- Integration of the above with LAN, WAN, and data-center switching infrastructure

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNP Voice**—3 to 5 years designing, installing, and troubleshooting voice and unified communications applications, devices, and networks
- **VCP VMware**—At least 6 months installing, deploying, scaling, and managing VMware vSphere environments

Related CVD Guides

Help Desk Using Cisco UCCX Technology Design Guide

On-Premises IM Using Cisco Jabber Technology Design Guide

VCS and UCM Video Integration Technology Design Guide

To view the related CVD guides, click the titles or visit the following site: http://www.cisco.com/go/cvd

Introduction

Communication is the lifeblood of an organization, and in today's global economy, the desire to stay in touch in many different ways has never been greater. The methods people have used to collaborate have changed over the years, but the ability to work seamlessly with others has always been very important to the success of a business.

To remain competitive, you need to provide reliable and consistent access to your communications resources. The importance of dependable collaboration channels inside and outside of your organization cannot be overstated. You also need to minimize the time required to select and absorb your collaboration technology investments and reduce your overall operational costs.

Technology Use Case

Collaboration has always been an essential component of a successful organization. New pressures, heightened by a challenging global economic environment, are making organizations realize collaboration is more important than ever. Specifically, they are trying to manage operational expenses and capital expenses, while increasing worker productivity and staying ahead of the competition. This "do more with less" approach can only be accomplished by finding the means to do the following:

- Empower your workforce—Users are empowered when they have communication tools at their disposal that allow them to access and use information when they need it most. Younger employees—especially those of the "Generation Y" demographic, who are now in their twenties—are bringing these networking tools into the workplace. Organizations need to develop a concerted strategy to proactively manage these technologies and, ideally, develop organizational capabilities to best take advantage of them.
- Provide real-time information—Collaborative applications make real-time information available to empowered users and provide for information sharing and privacy. Because information is shared across the entire user community, its accuracy is more easily verified and corrected.
- Accelerate through innovation—Organizations that successfully adopt new collaborative processes are able to move faster, make better decisions, draw from a deeper base of information, and more effectively operate across time and distance barriers. As is always the case in business, either you pull ahead, or the competition will leave you behind.

The challenges are addressed with collaboration services, such as web conferencing applications, unified communications, and video collaboration meetings. However, providing these types of capabilities to an entire organization requires a robust and scalable network infrastructure.

Use Case: Centralized Unified Communications

Organizations require high-quality voice and video communications that can scale to tens of thousands of users. They need a solution that is fast to deploy and easy to manage from a central location, without replicating costly features at their remote sites.

This design guide enables the following capabilities:

- **Single cluster centralized design**—Makes the solution simpler to deploy and easier to manage from a centralized site while saving on infrastructure components. In the single cluster centralized design, each remote site connects to the headquarters site through a WAN and each site receives call processing features from the headquarters location.
- **Phone auto-registration**—Automatically registers phones for quick and easy deployment.
- **Lightweight Directory Access Protocol integration**—Uses an LDAP directory integration option in Cisco Unified CM and Cisco Unity Connection for designs that require a single source of information for user management.
- **North American Numbering Plan**—Allows you to choose between two North American Numbering Plans as part of the path selection for public switched telephone network (PSTN) destinations. Dial plans from other countries can easily be imported using the configuration tool included with this guide.
- **Uniform On-net Dial Plan**—Uses endpoint addressing that consists of a uniform on-net dial plan containing 4-digit extensions. An optional access code and 2-digit or 3-digit site codes are available with local site 4-digit dialing.
- **Local route groups**—Uses local route groups in order to reduce the number of route patterns required to provision SIP gateways for all sites.
- **Class of service**—Provisions class of service (CoS) categories with the use of partitions and calling search spaces in order to allow emergency, local, long distance and international dialing capabilities.
- **Survivable Remote Site Telephony**—Provides failover at each remote site by standard SRST for SIP and Skinny Client Control Protocol (SCCP) phones.
- **Device Mobility**—Uses the Device Mobility feature, which allows Cisco Unified CM to determine the physical locations of devices.
- **Server load balancing**—Load balances phones across Cisco Unified CM redundancy groups on a phone-by-phone basis.
- **Extension Mobility**—Uses the Cisco Extension Mobility feature for all phones, which enables users to assign a Cisco Unified IP Phone as their own or they can move from phone to phone within the organization.
- **Media resources**—Provisions individual media resources, such as conference bridges for every site.
- **Voice messaging**—Provisions Cisco Unified CM for voice messaging integration and documents the Cisco Unity Connection configuration.
- **Call Admission Control**—Provides locations-based Call Admission Control (CAC) for a typical hub-and-spoke WAN environment.

Design Overview

This design guide eases the organization's cost of technology selection and implementation by recommending equipment that is appropriate for organizations, using methods and procedures that have been developed and tested by Cisco. Applying the guidance within this document reduces the time required for adoption of the technology and allows the components to be deployed quickly and accurately, so the organization can achieve a head start in realizing the return on its investment.

IP telephony as a technology is the migration of the old standalone phone switch to a software-based switch, where the data network becomes the physical transport for voice communications, rather than using separate cabling plants for data and voice communications. The market category that defines IP telephony and other forms of voice and video communications is known as *unified communications*.

Cisco Unified Computing System

Because Cisco Unified Communications applications, such as IP telephony and voicemail, have different processing and storage requirements based on the number of users and the features applied, it is important to select the appropriate server platform based on expected usage.

The information for the unified communications hardware scaling options is summarized in the following table. *Co-resident* means the virtual machine server instance is installed on the same Cisco Unified Computing System (UCS) hardware as other server instances.

For 500 users or fewer, Cisco Business Edition (BE) 6000 is recommended. A second Cisco UCS server is added to BE 6000 for organizations that need hardware redundancy.

Table 1 - Unified computing system hardware scaling options

	Unified CM	Unity Connection
500 Users (BE 6000)	C220 M3 Rack Servers (1)	Co-resident
1000 Users	C220 M3 Rack Servers (1)	Co-resident
2500 Users	C220 M3 Rack Servers (2)	Co-resident
5000 Users	C240 M3 Rack Servers (2)	Co-resident
10,000 Users	C240 M3 Rack Servers (3)	C240 M3 Rack Servers (1)

Cisco Voice Gateways

Voice gateways provide connectivity to networks outside of the organization, conferencing resources, and remote survivability. The combination of these voice services into a single platform offers savings over the individual components. The voice services can be integrated into an existing WAN router, or they can be deployed in a standalone router for additional capacity and redundancy.

The decision to integrate voice into an existing router depends on voice capacity and the overall performance of the router selected. If a router is consistently running above 40% CPU, the voice services are better suited for a standalone gateway in order to avoid processing delays for voice traffic. If the router has limited slots available for voice interface cards or digital signal processors, a standalone gateway is recommended to allow additional capacity when needed. Standalone gateways at the headquarters location are connected to the datacenter or server room switches. At a remote location, they are connected to the access or distribution switches.

Because Cisco Integrated Services Router Generation 2 (ISR G2) have different processing capabilities based on the number of phones and the features applied, it is important to select the appropriate platform based on expected usage. The sizing information in this guide supersedes the information from the various CVD WAN design guides because the number of Survivable Remote Site Telephony (SRST) users determines the proper router model, as listed in Table 2.

Table 2 - Standalone voice gateway scaling options

	Voice gateway	Voice T1/E1	Trunk ports	Conference bridge ports
4 users	Cisco 880	N/A	4	2
50 users	Cisco 2911	4	120	25
100 users	Cisco 2921	6	180	50
250 users	Cisco 2951	8	240	75
730 users	Cisco 3925	12	360	100
1200 users	Cisco 3945	18	540	150

Cisco Unified Communications

The products and priorities for this design were based on requirements from customers, partners, and Cisco field personnel. Your specific business requirements may be different from those in this guide, in which case, the product selection may not exactly match your needs. Please contact an authorized Cisco partner or representative to validate any design changes that you plan to deploy.

Cisco Unified Communications has the following software components:

- Cisco Unified CM provides the Internet Protocol private branch exchange (IP-PBX) functionality for all users within the headquarters site as well as the remote sites. The first Unified CM appliance is known as the *publisher* because it contains the master database to which all other Unified CM appliances within the same cluster subscribe. The rest of the appliances are known as either *subscribers* or *TFTP servers* based on their function in the cluster.
- Cisco Unity Connection provides services such as voicemail, voicemail integration with your email inbox, and many other productivity features. Voicemail is considered part of the unified communications foundation.

The following cluster design options are used in this guide:

- A dedicated TFTP server for clusters with more than 1250 phones or two dedicated TFTP servers for 5000 or more phones.
- A 1:1 subscriber redundancy in all configurations.
- Hardware redundancy for installations of more than 1000 phones.

Single Cluster Centralized Design

The following single cluster centralized design models provide a highly available and scalable call-control and voicemail system capable of email client integration:

- The Cisco Business Edition 6000 uses a single Cisco UCS server platform for up to 500 users. The virtualized server provides the following:
  - The publisher, subscriber and TFTP functions are combined with Cisco Unity Connection on a single hardware platform in order to help lower the capital and operational expenses.
  - The Cisco UCS C220 M3 hardware platform for the BE 6000 is a 1 RU form factor.
  - Even though they are not covered in this guide, the Business Edition 6000 also supports Cisco Unified Presence and Cisco Unified Contact Center Express on the same virtual server platform. A redundant server can also be added to this configuration if an organization requires it.
- For 500 to 2500 users, additional server instances on the Cisco UCS C220 M3 hardware platform provide a balance between future services and cost. The additional server instances provide the following:
  - With one Cisco Unified CM server instance acting as a publisher and TFTP server and another server acting as a subscriber and TFTP server, the cluster will scale up to 1000 users with capacity to spare.
  - For medium-sized organizations with 1000 to 2500 users, configure one Cisco Unified CM server instance as a publisher, two as subscribers, and one as a dedicated TFTP server. Two Unified CM groups are created, and phones are balanced between the groups on a phone-by-phone basis. When the Cisco IOS routers are configured in the "Configuring Conference Bridges, PSTN, Dial Peers, and SRST" process, the conference bridges and dial peers are configured with the two subscriber servers.
  - Cisco Unity Connection, with the properly defined virtual machine, supports up to 2500 users with voice mailboxes accessible through the phone or integrated into their email client.
  - For redundancy and resiliency purposes, the primary and backup subscribers are installed on different virtual server hardware for installations of more than 1000 users.

Figure 1 - 1:1 subscriber redundancy with Cisco Unified CM groups for 1000 and 2500 users

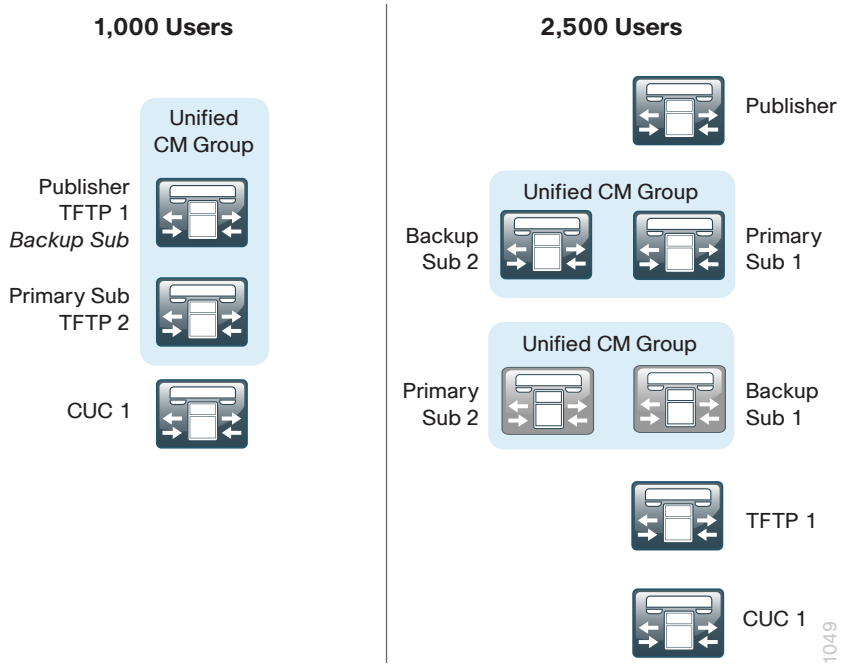
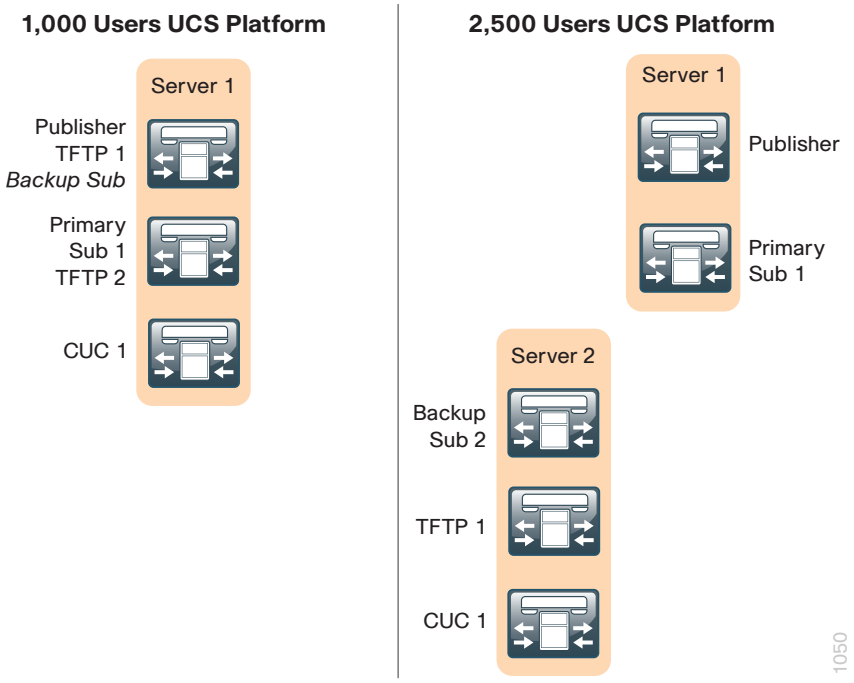


Figure 2 - Hardware platform redundancy for 2500 users



- For 2500 to 10,000 users, the computing power and advanced features of the Cisco UCS C240 M3 platform provides an organization the ability to add server instances for scaling capabilities. The larger servers and additional server instances provide the following:
    - Configure one Cisco Unified CM server instance as a publisher, two as subscribers, and two as dedicated TFTP servers to allow the cluster to scale up to 5000 users. Two Unified CM groups are created, and phones are balanced between the groups on a phone-by-phone basis. When the Cisco IOS routers are configured in the "Deploying Conference Bridges, Gateways and SRST" process, the conference bridges and dial-peers are configured with the two subscriber servers.
    - For 10,000 users, one server instance is the publisher, four are subscribers, and two are dedicated TFTP servers. Two Cisco Unified CM groups are created, and phones are balanced between the groups on a phone-by-phone basis. When the Cisco IOS routers are configured in the "Deploying Conference Bridges, Gateways and SRST" process, the conference bridges and dial-peers are configured with four subscriber servers.
    - Cisco Unity Connection, with the properly defined virtual machine, supports up to 10,000 users with voice mailboxes accessible through the phone or integrated into their email client.
    - The Cisco UCS C240 M3 hardware platform is a 2 RU form factor.
    - For redundancy and resiliency purposes, the primary and backup subscribers are installed on different server hardware. For 10,000 users, the publisher uses its own hardware platform so additional services, such as Cisco Unified Contact Center Express, can be installed in the future. Unity Connection also requires its own hardware because it needs six CPUs, plus one more for running the VMware process.

Figure 3 - 1:1 subscriber redundancy with Cisco Unified CM groups for 5000 and 10,000 users

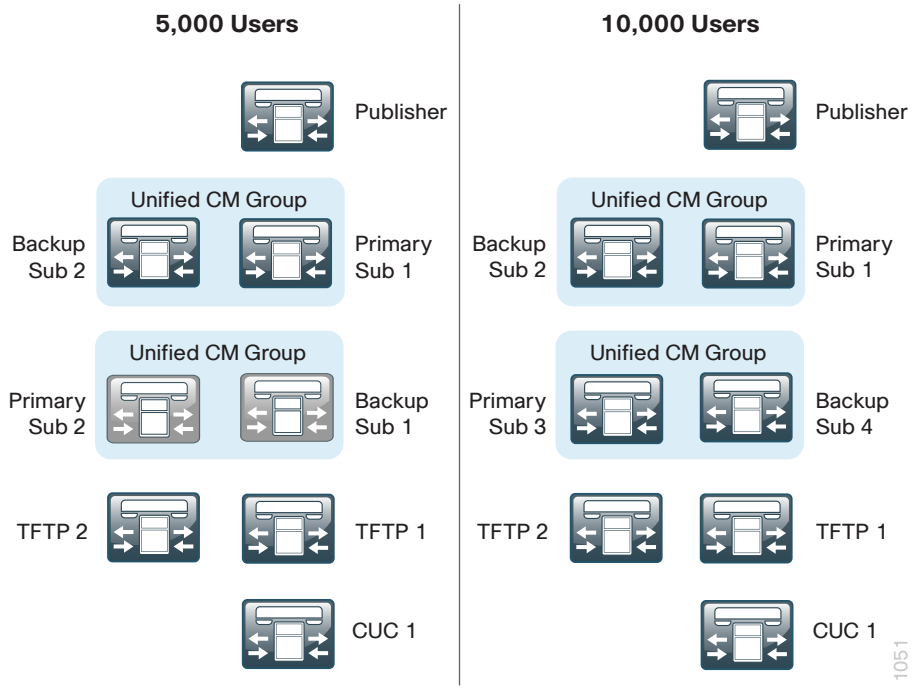
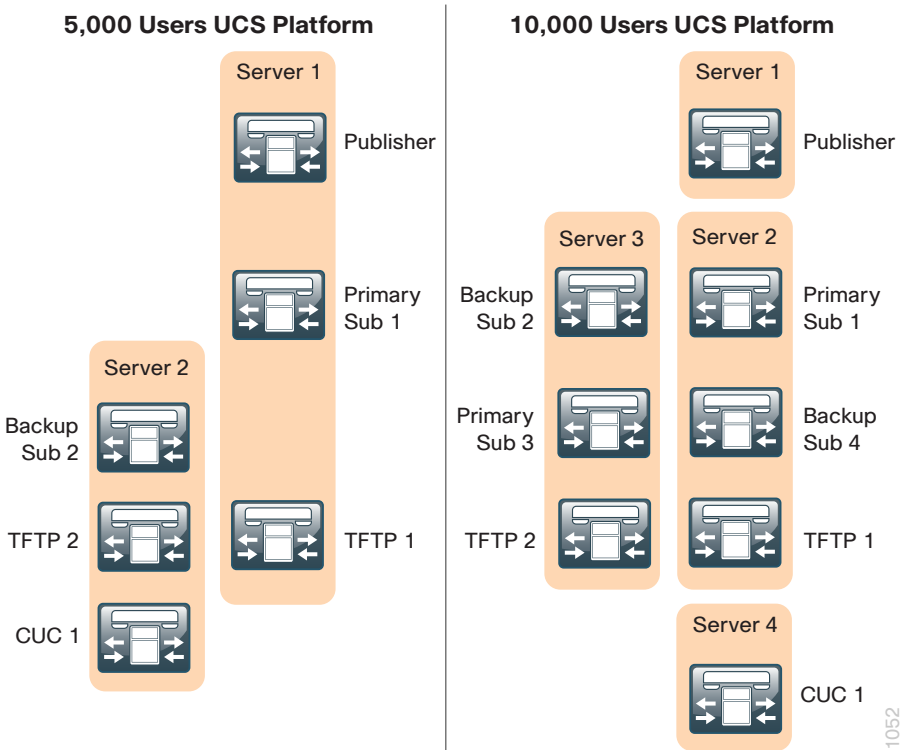


Figure 4 - Hardware platform redundancy for 5000 and 10,000 users



The centralized design models are summarized in the table below. *Shared* means the TFTP service shares the same server with Cisco Unified CM. *Dedicated* means the TFTP service runs on a server without Unified CM. *Common* means the two groups have the same two Unified CM servers in common, using a reverse order of preference.

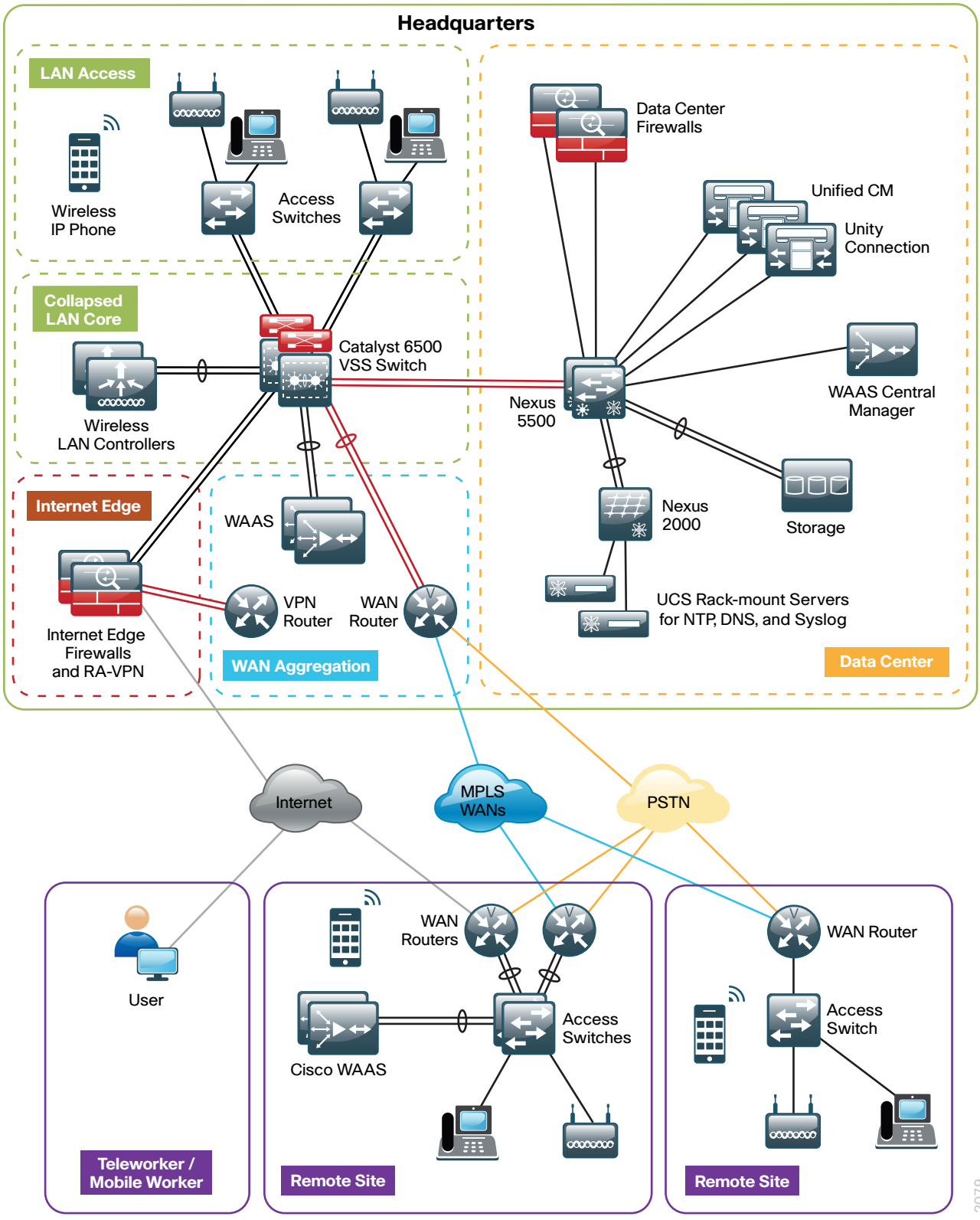
Table 3 - Cisco Unified Communications Manager centralized design models

	500 users	1000 users	2500 users	5000 users	10,000 users
Publisher	1	1	1	1	1
Subscribers	1	1	2	2	4
TFTP	1 (shared)	2 (shared)	1 (dedicated)	2 (dedicated)	2 (dedicated)
Groups	1	1	2 (common)	2 (common)	2
Remote sites	50	90	500	500	500
UCS servers	1	1	2	2	4

For all of the design models, the following features are provided:

- Connect each server to a different switch within the server room or data center in order to provide for high availability should a switch or link connection fail.
- There is sufficient capacity for multiple devices for each user. For example, you can enable a desk phone and a soft phone with enough computer telephony integration to allow a high percentage of users to have click-to-call or other applications that can remotely control their phones.
- There is additional capacity available for phones that are not assigned to a specific user, such as those in public areas, meeting rooms, storage areas, and break rooms.
- A Redundant Array of Independent Disks (RAID) and dual power supplies provide high server availability.
- Cisco Unity Connection is deployed as a simple voicemail system. However, with additional configuration, it will provide calendar-based call-handling integration with Microsoft Exchange, Cisco Unified MeetingPlace, and other networkable voicemail systems. Cisco Unity Connection is deployed in the architecture as non-redundant, although a second high-availability server can be added, if required.
- It is possible to support other services, including presence and instant messaging, advanced conferencing, contact center, and video conferencing. These advanced services require additional hardware and software, and they are not covered in this document.

Figure 5 - Cisco Unified CM and Unity Connection



The centralized design consists of a headquarters site and up to 500 remote sites. The Cisco Unified CM and the Cisco Unity Connection server instances are placed at the main site to handle the call processing for up to 10,000 telephony users with voice messaging. Each remote site takes advantage of the Cisco ISR G2 router that was deployed as part of the WAN deployment.

Auto-Registration

Auto-registration allows Cisco Unified CM to automatically assign a directory number to new phones as they are deployed in your network. With Cisco Unified Configurator for Collaboration (CUCC), auto-registration is enabled by default in order to allow for quick and easy deployment of phones. After the phones are registered and the guide has been followed completely, users configured in the system can utilize Cisco Extension Mobility to log into the auto-registered phones.

By default, auto-registered phones are able to dial on-net directory numbers as well as off-net emergency 911 calls. They are not, however, able to dial off-net numbers.

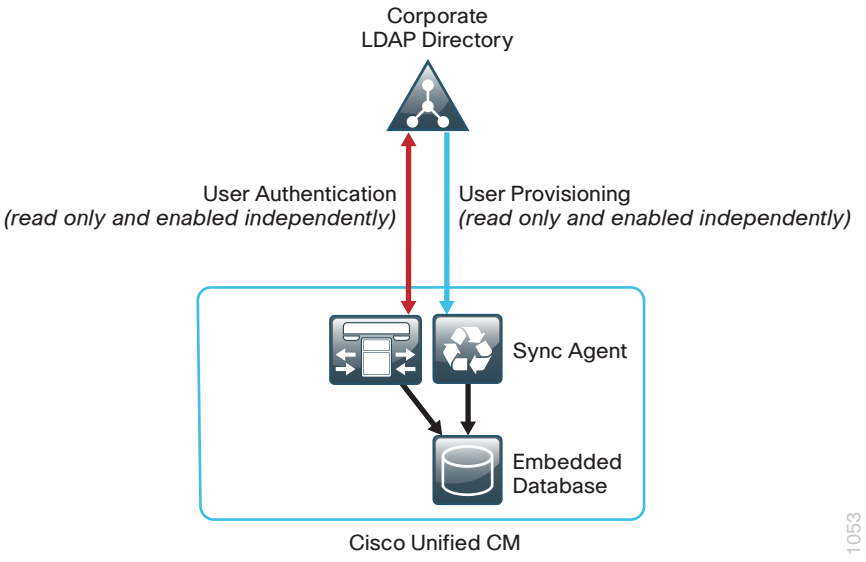
Tech Tip

Leaving auto-registration enabled carries a security risk in that "rogue" phones can automatically register with Cisco Unified CM. You should only allow auto-registration for brief periods when you want to perform bulk phone adds during phone deployment.

Active Directory Integration

Active Directory integration allows you to provision users automatically from the corporate directory into the Cisco Unified CM database, which makes it possible to maintain a single directory as opposed to separate directories. Therefore, you don't have to add, remove, or modify core user information manually in Unified CM each time a change occurs in the corporate directory. The other advantage is that end users are able to authenticate to Unified CM and Cisco Unity Connection by using the same credentials in Active Directory, which reduces the number of passwords across the network.

Figure 6 - Directory integration with Cisco Unified CM



Dial Plan

The dial plan is one of the key elements of an IP telephony system and an integral part of all call-processing agents. Generally, the dial plan is responsible for instructing the call-processing agent on how to route calls. CUCC configures a North American Numbering Plan (NANP) dial plan as part of the path selection for PSTN destinations. You can modify the dial plan to meet your specific needs, but CUCC has the options to configure the NANP with 7-digit or 10-digit local dialing. The following two sets of patterns can be selected.

Figure 7 - NANP with 7-digit local dialing

Route Pattern	Route Partition
9.911	PAR_Base
911	PAR_Base
9.[2-9]XXXXXX	PAR_PSTN_Local
9.1[2-9]XX[2-9]XXXXXX	PAR_PSTN_National
9.011!	PAR_PSTN_Intl
9.011!#	PAR_PSTN_Intl

Figure 8 - NANP with 10-digit local dialing

Route Pattern	Route Partition
9.911	PAR_Base
911	PAR_Base
9.[2-9]XX[2-9]XXXXXX	PAR_PSTN_Local
9.1[2-9]XX[2-9]XXXXXX	PAR_PSTN_National
9.011!	PAR_PSTN_Intl
9.011!#	PAR_PSTN_Intl

There are two configured international route patterns: one to route the variable-length dialed digits and one configured with a pound (octothorpe) in order to allow users to bypass the inter-digit timeout. The 911 and 9.911emergency route patterns are created with Urgent Priority to prevent inter-digit timeout delays when they are entered from a phone.

Site Codes

It is recommended that you use a uniform on-net dial plan containing an access code, a site code, and a 4-digit extension. The use of access and site codes enables the on-net dial plan to differentiate between extensions at remote sites that could otherwise overlap with each other.

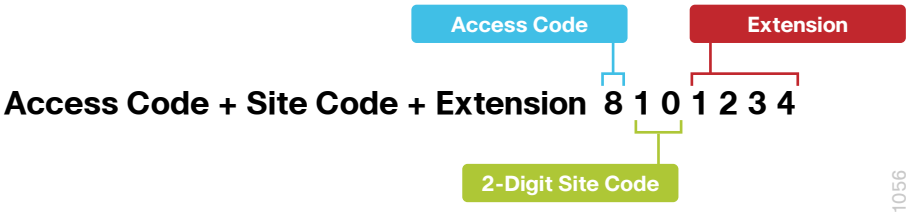
When you use this method, a phone in San Jose, CA can have the same 4-digit extension as one in Houston, TX without creating a numbering conflict. For example: 408-525-1234 in San Jose and 713-448-1234 in Houston.

For networks with 90 sites or less, the dial plan consists of the following:

- One digit as an inter-site access code
- Two digits for the site code to accommodate up to 90 sites
- Four digits for the site extension

CUCC requires a format of 8 + SS + XXXX, where 8 is the on-net access code, SS is a 2-digit site code of 10-99, and XXXX is a 4-digit extension number, giving a total of seven digits.

Figure 9 - Two-digit site code format

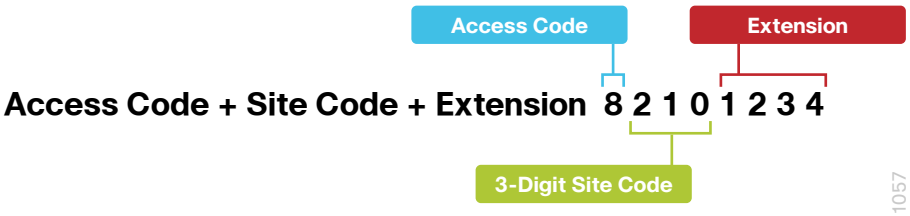


For networks with greater than 90 sites, the dial plan consists of the following:

- One digit as an inter-site access code
- Three digits for the site code to accommodate up to 900 sites
- Four digits for the site extension

CUCC requires a format of 8 + SSS + XXXX, where 8 is the on-net access code, SSS is a 3-digit site code of 100-999, and XXXX is a 4-digit extension number, giving a total of eight digits.

Figure 10 - Three-digit site code format



When site codes are used, CUCC creates a new partition, calling search space, and translation pattern per site to allow four-digit dialing between phones at the same site, which is what most users prefer. The same translation patterns are also used by the SIP trunks which route only the last four digits of the dialed number to the phones at each site.

Class of Service

Class of service is configured in Cisco Unified CM by utilizing calling search spaces and partitions. There are four classes of service, and they provide PSTN access for emergency, local, national, and international dialing.

Figure 11 - Calling search spaces and partitions

	Calling Search Space	Route Partition 1	Route Partition 2	Route Partition 3
1	CSS_Base	PAR_Base	—	—
2	CSS_LocalPSTN	PAR_PSTN_Local	—	—
3	CSS_NationalPSTN	PAR_PSTN_Local	PAR_PSTN_National	—
4	CSS_InternationalPSTN	PAR_PSTN_Local	PAR_PSTN_National	PAR_PSTN_Intl

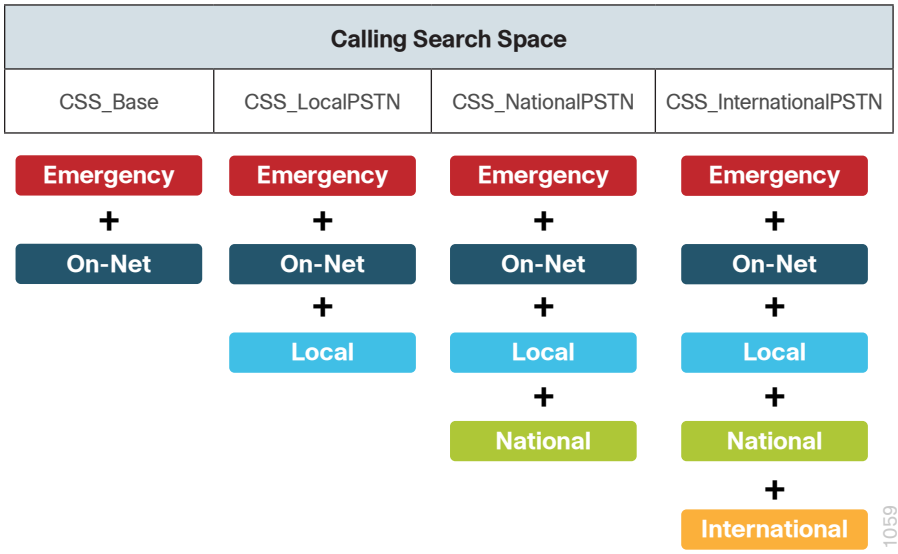
1 Emergency Dialing
2 Local Dialing
3 National Dialing
4 International Dialing

1058

With CUCC, devices are auto-registered with the CSS_Base calling search space. This allows all devices to dial both on-net and emergency off-net numbers.

The remaining calling search spaces are configured on the user device profile directory number and provide local 7-digit or local 10-digit, national, and international dialing capabilities.

Figure 12 - Calling capabilities for calling search spaces



1059

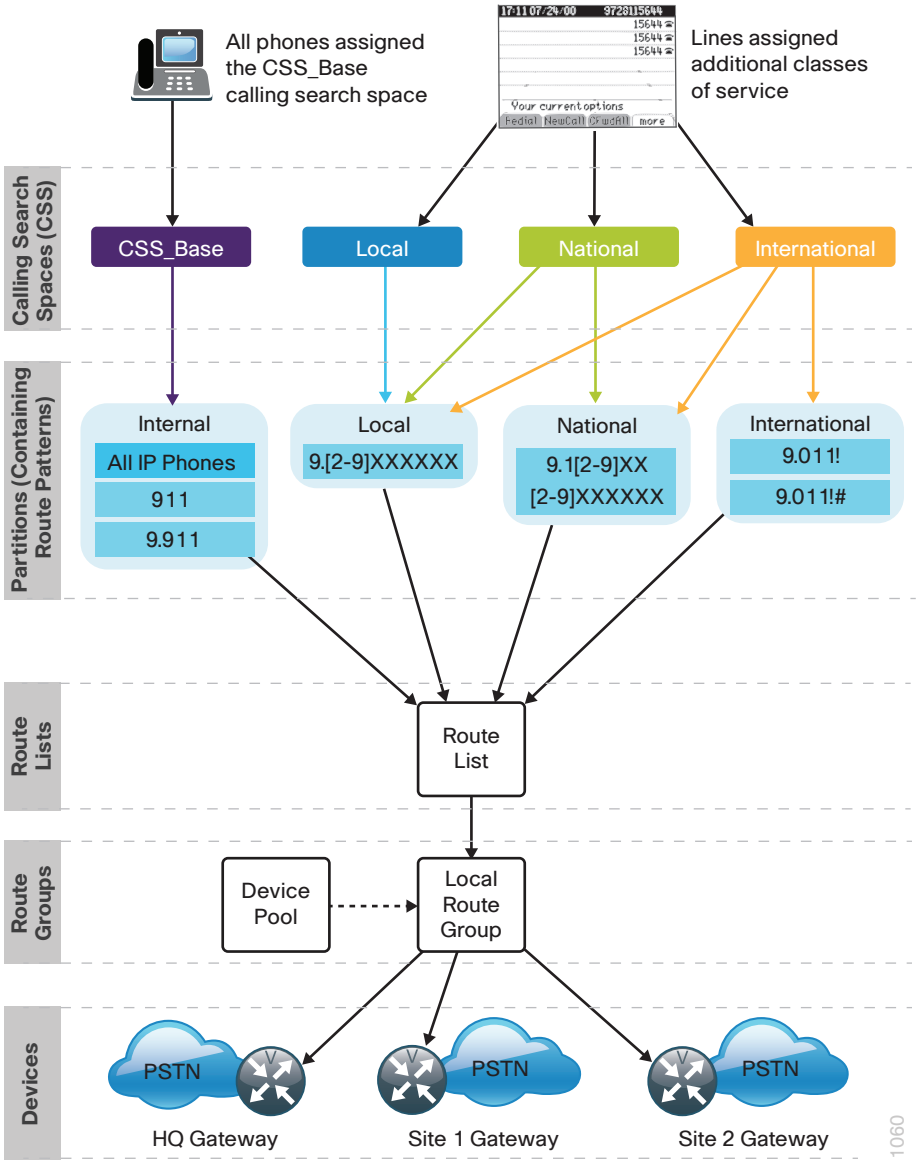
For example, if a user requires international dialing capability, their directory number would be assigned the CSS_InternationalPSTN calling search space, which includes dialing accessibility to all PSTN route patterns as well as national, local, emergency, and on-net numbers.

Local Route Groups

The Local Route Group feature in Cisco Unified CM decouples the PSTN gateway physical location from the route patterns and route lists that are used to access the gateway. The feature assigns a local route group to each route group, based on the device pool setting of the originating device. Therefore, phones and other devices from different locations can use a single set of route patterns, but Unified CM selects the correct gateway to route the call.

CUCC assigns a unique route group to a device pool so each site can choose the correct SIP gateway. The route group is associated with the device pool by using the local route group setting. This simplifies the process of provisioning by allowing the administrator to create a single set of route patterns for all sites. When a call is made from a device that matches the route pattern, Cisco Unified CM uses the Local Route Group device pool setting to determine the proper route group, which selects the SIP gateway assigned to the site.

Figure 13 - Cisco Unified CM call routing



Survivable Remote Site Telephony (SRST)

In a centralized design, when IP phones lose connectivity to Cisco Unified CM because the application is unreachable, IP phones in remote-site offices or teleworker homes lose call-processing capabilities. The SRST feature provides basic IP telephony backup services because IP phones fall back to the local router at the remote site when connectivity is lost. IP phones continue to make calls within the site and out the local gateway to the PSTN.

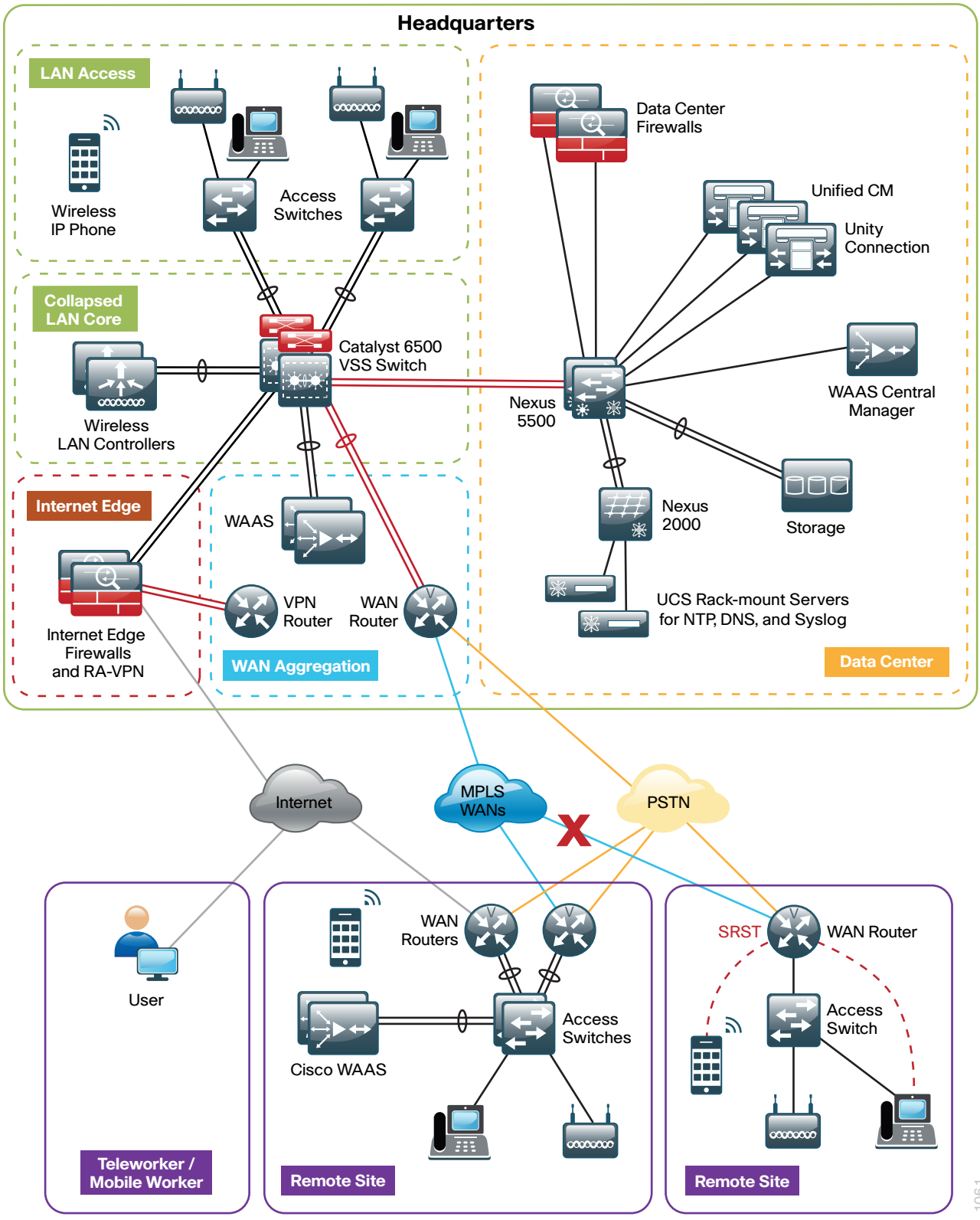
At a remote site with more than one PSTN gateway, configure SRST on the router with the most voice ports. If only one router has PSTN interfaces, SRST must be configured on the router to reduce complications.

Using the Cisco 3945 ISR router, a maximum of 1200 phones are supported at a remote site. If you have more phones than a single SRST router can manage, you should consider clustering over the WAN or using the Cisco Unified CM distributed design model for the larger sites. More information on these two options can be found in the Solution Reference Network Design for Cisco Unified Communications at the following URL: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_uc_mgr.html

Phones can use SCCP or SIP to register with the SRST process on the remote-site router. Different commands are needed for each type of phone, and the commands can be configured together or individually on each router within the organization.

The following diagram shows SRST providing service to phones at a remote site when the WAN is down.

Figure 14 - SRST at a remote site



When a remote site falls back to SRST and site codes are in use, voice translation commands are required in the router to maintain 4-digit local dialing. The commands are explained in more detail in the deployment section of this guide.

Device Mobility

CUCC uses a feature called *device mobility* that allows Cisco Unified CM to determine if the IP phone is at its home or a roaming location. Unified CM uses the device's IP subnet to determine the physical location of the IP phone. By enabling device mobility within a cluster, mobile users can roam from one site to another, thus acquiring the site-specific settings. Unified CM then uses these dynamically allocated settings for call routing, codec selection, media resource selection, and Unified CM groups.

This feature is used primarily to reduce the configuration on the devices themselves by allowing configuration of many parameters at the site level. These parameters are dynamically applied based on the subnet to which the device is attached. This allows for a fast and reliable deployment because the administrator does not have to configure each phone individually or ensure the phone is at the correct location.

Server Load-balancing

CUCC allows phones to be load-balanced between Cisco Unified CM redundancy groups by assigning them to two different device pools within each location. The site-specific device pools are identical except for the Unified CM group that changes the phone's subscriber preference. The tool looks at the phone's IP address and uses the information from the device mobility feature in order to alternate between the device pools at each site, creating an optimal balance.

Extension Mobility

CUCC uses the Extension Mobility feature, enabling end users to personalize a Cisco Unified IP Phone, either temporarily or permanently, based on business requirements. The Extension Mobility feature dynamically configures a phone according to the authenticated user's device profile. Users log into an IP phone with their username and PIN, and their device profile is uploaded to the IP phone. Extension Mobility alleviates the need for device-to-user association during provisioning. This saves deployment time while simultaneously allowing the user to log into any phone within the organization, allowing phone-sharing capabilities.

Extension Mobility can be enabled in such a way that it allows users to log into IP phones but does not allow them to log out. With this method, Extension Mobility is exclusively designed for IP phone deployment, but not as an ongoing feature in the organization. By default, the CUCC configuration allows users to log out of the IP phone, which enables Extension Mobility for both IP phone deployment and user feature functionality.

Tech Tip

The user-provisioning capabilities of this guide require an IP phone that supports services to allow the use of Extension Mobility. All users imported with CUCC will have a default PIN of '112233'.

Media Resources

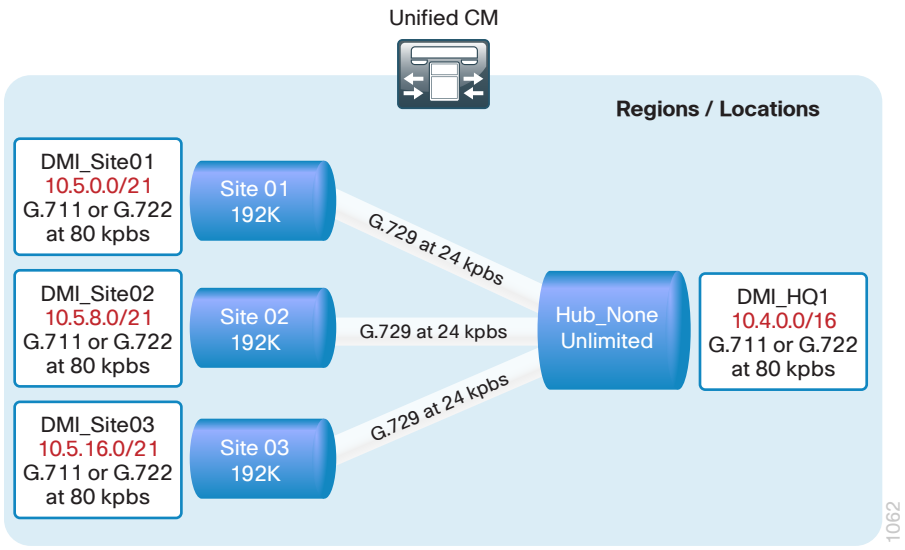
Media resources have been provisioned as part of the procedure for every site in order to ensure that remote sites use their local conference bridges and avoid unnecessary voice traffic over the WAN. The naming of the conference bridges needs to match those provisioned by CUCC. The names are always CFB1<*Site Name*> and CFB2<*Site name*>, if there are two. For example, if the headquarters site is HQ1, the conference bridge names are CFB1HQ1 and CFB2HQ1.

Call Admission Control

The default design is a hub-and-spoke topology in which each remote site is connected to the headquarters site over a bandwidth-constrained WAN. The CUCC design uses regions and locations to define locations-based Call Admission Control. For calls within a site, the regions are configured for the G.722 or G.711 codec running at 80 kbps, and there are no limits to the number of calls allowed within a site. For calls between the sites, the regions are configured for the G.729 codec running at 24 kbps. The size of the site determines the CUCC default voice bandwidth setting for inter-site calls. For sites with only 500 users, the default setting is two inter-site calls (48 kbps); for sites with 10,000 users, the default is eight inter-site calls (192 kbps). The amount of bandwidth in and out of each site can be modified within CUCC, if the defaults do not match the provisioned WAN bandwidth.

By default, Call Admission Control is not calculated for calls to and from the central site (headquarters). It's expected that as long as the spokes are provisioned for Call Admission Control, the hub will not be oversubscribed on a traditional WAN. This is the case for all hub-and-spoke topologies; however, for a Multiprotocol Label Switching (MPLS)-based network, which is considered a hub-less hub and spoke, you will need to modify the headquarters site default bandwidth within CUCC to provide the correct Call Admission Control based on the speed of the link.

Figure 15 - Hub-and-spoke topology for Call Admission Control



CUCC Directories and Filenames

The Cisco Unified Configurator for Collaboration (CUCC) tool is available in a Windows and Mac version. The different versions can be downloaded from the following URLs:

- Windows: http://cvddocs.com/fw/Rel2-430-a
- Mac: http://cvddocs.com/fw/Rel2-430-b

CUCC has several directories and key filenames that are referenced throughout this guide. The following table lists the directories and filenames.

Table 4 - CUCC directories and filenames

Type	Path or filename	Description
Default	.\	Default directory
	.\CUCC.exe or CUCC.app	CUCC application
	.\Sample User.csv	Sample csv file for New Users and Device Profiles
	.\Readme.txt	This table
Log	.\log	System log directory
	.\log\ccts.log	General log for all areas
	.\log\new_server.log	New Server and Site log
	.\log\export_gateway.log	Gateway Template log
	.\log\new_user.log	New Users and Device Profiles log
	.\log\modify_server.log	Modify Server and Site log
	.\log\modify_user.log	Modify Users and Device Profiles log
	.\log\phone.log	Phone Deployment log
Summary	.\Overview	Summary overview directory for data used in Server and Site
Output	.\packet	Output packet directory
	.\packet\gateway	Output text files for Gateway Templates formatted as follows: SIP_Site_Name_GWY.txt
	.\packet\saveAllData	Output tar file for Saved Entered Data
	.\packet\server	Output tar files for Server and Site formatted as follows: Server_YYYYMMDDhhmm.tar
	.\packet\user	Output tar files for Users and Device Profiles formatted as follows: User_ YYYYMMDDhhmm.tar
Input	.\template	Input template directory
	.\template\dialplan	Input csv files for Dial Plan
	.\template\user	Input csv and xml files for Users and Device Profiles
	.\template\gateway	Input xml file for Gateway Templates
	.\template\Server	Input tar file for base Unified CM configuration
	.\template\site	Input csv sample files for Site Information
	.\template\temp	Input csv files extracted from base Unified CM tar file
	.\template\udp	Input xml files for Device Profiles

Deployment Details

This guide uses the Cisco Unified Configurator for Collaboration (CUCC) to install, configure, and deploy basic telephony and simple voice messaging. This turnkey solution is easy and quick. It also provides a solid foundation for further configuration and deployment of advanced unified communications features, without the need to redesign or reengineer when a new element or service is added.

The first process presents detailed procedures for preparing your network for IP phones and provides a section on how to choose the correct Cisco Unified IP Phones for your organization.

PROCESS

Preparing the Network for IP Phones

1. Enable DHCP option 150

The campus design is voice-ready because it includes the QoS settings, VLANs, and IP subnets needed for voice endpoints. It also includes the Dynamic Host Configuration Protocol (DHCP) scopes for the voice VLANs. However, the DHCP option that automatically assigns the call-control agent to the voice endpoints is covered in this module because it is specific to the Cisco Unified Communications solution.

Procedure 1 Enable DHCP option 150

DHCP is used to obtain an IP address, subnet mask, default gateway, domain name, Domain Name System (DNS) addresses, and Trivial File Transfer Protocol (TFTP) server information. When configuring DHCP for use in a Cisco Unified CM deployment, this design recommends a localized server or Cisco IOS device to provide DHCP service at each site. This type of deployment ensures that DHCP services are available to remote-site telephony devices during WAN failures.

DHCP option 150 provides the IP addresses of the TFTP servers, which allows the phones to download their configuration files and firmware. This option is added to the voice scopes for wired and wireless networks. Option 150 allows up to two IP addresses to be returned to phones as part of the DHCP scope.

The phone always tries the first address in the list, and it only tries the subsequent address if it cannot establish communications with the first TFTP server. The second address provides a redundancy mechanism that enables phones to obtain TFTP services from another server if their primary TFTP server is unreachable. However, it does not provide dynamic load balancing between the two servers. This design recommends that you configure different ordered address lists of TFTP servers in the DHCP scopes to allow for manual load balancing.

For example:

- In subnet 10.5.2.0/24, option 150: CUCM-TFTP1 (primary), CUCM-TFTP2 (secondary)
- In subnet 10.5.13.0/24, option 150: CUCM-TFTP2 (secondary), CUCM-TFTP1 (primary)

Under normal operations, a phone in subnet 10.5.2.0/24 will request TFTP services from CUCM-TFTP1, while a phone in subnet 10.5.13.0/24 will use CUCM-TFTP2. If CUCM-TFTP1 fails, then phones from both subnets will request TFTP services from CUCM-TFTP2. The method for load sharing between the DHCP scopes is left up to the network administrator, because they will have the best knowledge of how many phones reside in each subnet.

If the remote site has a single WAN router without a distribution layer, the best place for DHCP is on the router. If the remote site has dual WAN routers or a distribution layer, the DHCP service should be located on a standalone server or on a distribution switch.

In all situations, phones need option 150 added to their DHCP scope configurations. If the headquarters site uses the primary TFTP server as the first choice, the remote sites should use the secondary TFTP as the first choice until the phone count is balanced between the two servers.

If you are using a Microsoft DHCP server, complete Option 1 of this procedure. If you are using the Cisco IOS DHCP server feature, complete Option 2.

Option 1: Enable option 150 on Microsoft DHCP server

Use the following commands in order to enable option 150 on a Microsoft DHCP server.

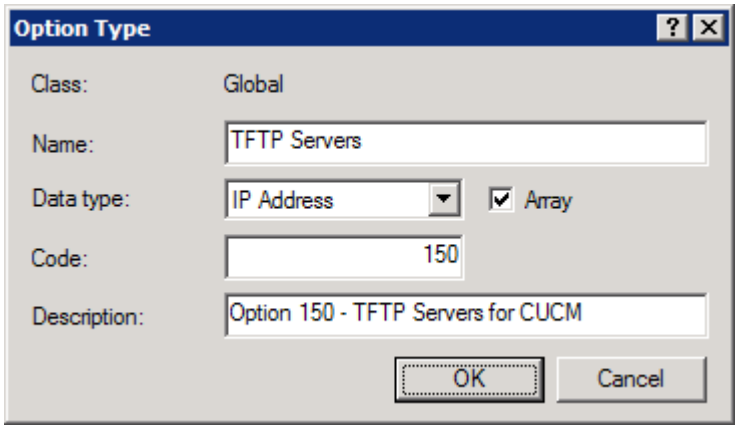
Step 1: From the Microsoft server, open the DHCP Server Administration Tool.

Step 2: On the left side of the page, navigate to **[active directory name] > IPv4** (Example: ad.cisco.local > IPv4).

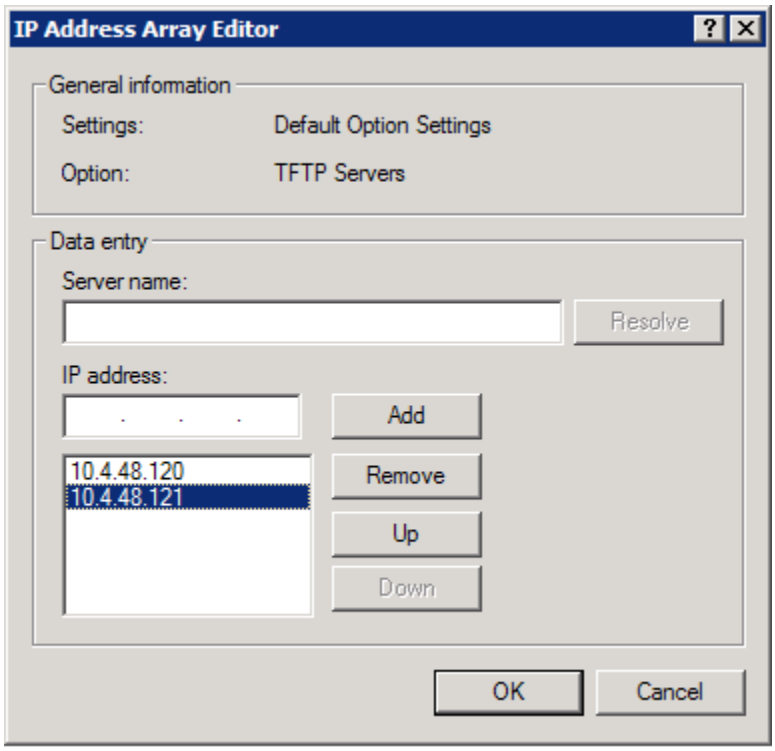
Step 3: Right-click **IPv4**, and then choose **Set Predefined Options** from the list.

Step 4: Click **Add**, enter the following information, and then click **OK**:

- Name–**TFTP Servers**
- Data Type–**IP Address**
- Array–**Select**
- Code–**150**
- Description–**Option 150 - TFTP Servers for CUCM**



Step 5: Click **Edit Array**, add up to two IP addresses for your TFTP servers, and then click **OK**.



Step 6: On the Predefined Options and Value page, verify the information, and then click **OK**.

Option 2: Enable option 150 using Cisco IOS DHCP server feature

Use the following commands in order to enable option 150 in the appropriate DHCP pools in Cisco IOS devices.

Step 1: Log in to the device with a username that has the ability to make configuration changes.

Step 2: In the global configuration section, edit the DHCP pools supporting IP phones to include option 150 so the phones can find the TFTP servers at 10.4.48.121 (secondary) and 10.4.48.120 (primary):

```
ip dhcp pool wired-voice
  network 10.5.2.0 255.255.255.0
  default-router 10.5.2.1
  dns-server 10.4.48.10
  option 150 ip 10.4.48.121 10.4.48.120
  domain-name cisco.local

ip dhcp pool wired-voice2
  network 10.5.4.0 255.255.255.0
  default-router 10.5.4.1
  dns-server 10.4.48.10
  option 150 ip 10.4.48.121 10.4.48.120
  domain-name cisco.local
```

Phone Models

For decades, traditional phone systems have provided basic dial tone and voicemail services, but there is little they can offer in terms of advanced communication features. Organizations who lead the way in technological innovation expect the next generation of handsets to provide features that will transform the way they operate their business. Even as they lead the way with new tools and technology, they want to cut costs by eliminating expensive wiring to every desktop and lowering electricity usage. The high cost of energy and the push for a greener planet is causing organizations to rethink every aspect of their business to see if they can lower their carbon footprint.

At the other end of the spectrum, cost-conscious organizations want to lower costs by saving money in nonessential areas of their business. Most employees only need a simple telephone handset. Even a character-based display screen is too expensive for their budgets. Aging phones systems have been discontinued, and spare parts are getting harder to find. These challenges are causing organizations to search for a cost-effective solution to their telephony needs.

Several new Cisco Unified IP Phones have been introduced over the last few years to address the high-end and cost-conscious business models. Cisco Unified IP Phones 9951 and 9971 support video telephony by adding a USB camera to a high-end color phone. This allows customers to meet face-to-face with others in their organization by using the simple interface of a telephone. The color screens are larger with higher resolution than other models, and they support more tilt options to allow better viewing of the video images. They support Bluetooth and USB to give the end user more flexibility when choosing headsets. Cisco Unified IP Phone 9971 supports Wi-Fi connectivity, which frees users from the constraints of a hardwired telephone infrastructure within their buildings. Cisco Unified IP Phone 8945 also supports video telephony with a built-in camera and a high-resolution color display. Cisco Unified IP Phone 8900 Series and 9900 Series have a deep-sleep power-save option, which can reduce power consumption by up to 90 percent compared to the normal operation of the phone. This design recommends Unified IP Phone 8945 for a four-line video phone and Unified IP Phone 9971 for a five-line, video, and Wi-Fi–enabled phone.

Cisco Unified IP Phone 6900 Series are inexpensive and durable alternatives for organizations that want to lower their capital outlay. These basic phone models provide essential calling functionality and still maintain the inherent flexibility of an IP-based endpoint, which operates from an existing Ethernet port for power and connectivity. Unified IP Phone 6900 Series use less power because they have either small, character-based screens or no display at all. The higher-end models, starting with Cisco Unified IP Phone 6921 and above, also support a deep-sleep mode, which uses 50 percent less power in the off-hours.

Cisco Unified IP Phone 6901 is recommended for a single-line, cost-effective phone. However, this phone does not have a display, so it cannot support the XML applications that are required in order to run Cisco Extension Mobility to dynamically assign users to the device. Organizations that require this phone for break areas, lobbies, hallways, or other areas have to manually configure Unified IP Phone 6901 after the rest of the phones are provisioned by using the steps outlined in this guide. For XML-capable phones, this design recommends Unified IP Phone 6921 for two lines, Unified IP Phone 6945 for four lines, and Unified IP Phone 6961 for six lines.

Cisco Unified Wireless IP Phone 7925 is recommended for mobility, Cisco Unified IP Conference Station 7937 is recommended for conference rooms, and the Cisco IP Communicator software client is recommended to provide a desktop computer solution.

The phones take full advantage of the Cisco recommended QoS settings by using Class Selector 3 (CS3) for signaling, Assured Forwarding 41 (AF41) for video, and Expedited Forwarding (EF) for voice. These settings are recommended for Cisco Medianet because they provide optimum voice and video quality while maintaining the integrity of the data flows within the network. Whether the phones are running Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP), they can also use SRST at the remote sites in order to provide survivability in the case of a WAN outage.

Cisco Unified IP Phone 7900 Series are also available as an alternative for users who do not need the high-end features of the Unified IP Phone 8900 and 9900 Series phones, but require more functionality than what is found in the Unified IP Phone 6900 Series models.

Network Preparation Summary

To ensure that your phones are registered at the correct time, you need to deploy DHCP option 150 and select your IP phone models before you perform the deployment procedures found in the next process.

PROCESS

Preparing the Platform for Cisco Unified CM

1. Configure platform connectivity to the LAN
2. Prepare the server for Unified CM

For a quick and easy installation experience, it is essential to know up front what information you will need. To install Cisco Unified CM, make sure you have completed the following steps before you start:

- If you are installing on a new virtual machine, download the Open Virtual Archive (OVA) file from the Cisco website at:
  http://software.cisco.com/download/release.html?mdfid=284510097&flowid=37562&softwareid=283088407&release=9.1(1)&relind=AVAILABLE&rellifecycle=&reltype=latest

  For an installation using ESXi 4.1, choose the latest OVA file with vmv7 in the name. For example: **cucm_9.1_vmv7_v1.6.ova**

  For an installation using ESXi 5.0 or higher, choose the latest OVA file with vmv8 in the name. For example: **cucm_9.1_vmv8_v1.6.ova**
- Check the Cisco website to determine if there is a patch for your version of Cisco Unified CM:
  http://software.cisco.com/download/release.html?mdfid=284510097&flowid=37562&softwareid=282074295&release=9.1(1)&relind=AVAILABLE&rellifecycle=&reltype=latest

Procedure 1 Configure platform connectivity to the LAN

The Cisco Unified CM server can be connected to a Cisco Nexus switch in the data center or a Cisco Catalyst switch in the server room. In both cases, QoS policies are added to the ports in order to maintain voice quality during the setup and configuration of calls. Please choose the option that is appropriate for your environment.

Option 1: Connect the Cisco Unified CM server to a Cisco Nexus 2248UP switch

Step 1: Log in to the Cisco Nexus switch with a username that has the ability to make configuration changes.

Step 2: If there is a previous configuration on the switch port where the Cisco Unified CM server is connected, remove the individual commands by issuing a **no** in front of each one. This brings the port back to its default state.

Step 3: Configure the port as an access port and apply the QoS policy.

```
interface Ethernet107/1/4
 description Unified CM
 switchport access vlan 148
 spanning-tree port type edge
 service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

Tech Tip

When deploying a dual-homed Cisco Nexus 2248 switch, this configuration is applied to both Nexus 5548 switches.

Option 2: Connect the Cisco Unified CM server to a Cisco Catalyst 3750-X Series switch

To ensure that signaling traffic is prioritized appropriately, you must configure the Cisco Catalyst access switch port where the Cisco Unified CM server is connected to trust the differentiated services code point (DSCP) markings. The easiest way to do this is to clear the interface of any previous configuration and then apply the egress QoS macro that was defined in the access-switch platform configuration of the Campus Wired LAN Design Guide.

Step 1: Log in to the Cisco Catalyst switch with a username that has the ability to make configuration changes.

Step 2: Clear the interface's configuration on the switch port where the Cisco Unified CM server is connected.

```
default interface GigabitEthernet1/0/6
```

Step 3: Configure the port as an access port and apply the egress QoS policy.

```
interface GigabitEthernet1/0/6
 description Unified CM
 switchport access vlan 148
 switchport host
 macro apply EgressQoS
```

Procedure 2 Prepare the server for Unified CM

The following table describes the server scaling options for Cisco Unified CM.

Table 5 - Cisco Unified CM virtual machine scaling options

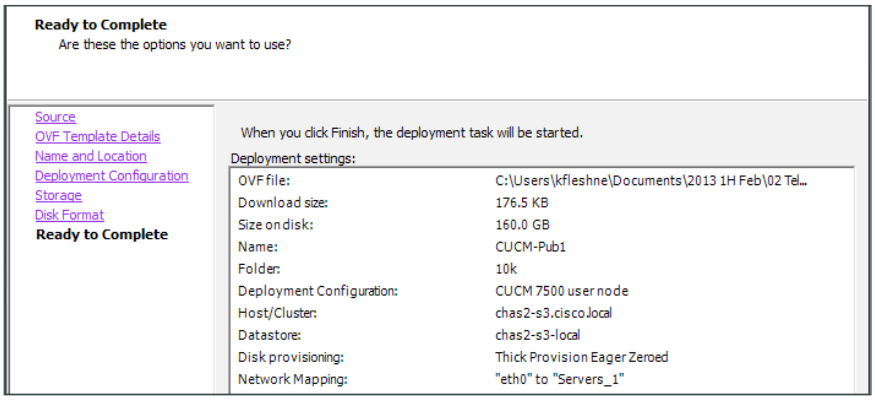
	1000-user node (BE 6000)	2500-user node	7500-user node
Virtual CPUs	2	1	2
CPU speed	800 MHz	800 MHz	3600 MHz
RAM	4 GB	4 GB	6 GB
Hard disk	80 GB	80 GB	110 GB
VMware ESXi	4.0, 4.1, 5.0	4.0, 4.1, 5.0	4.0, 4.1, 5.0
OS support	RHE Linux 5 (32-bit)	RHE Linux 5 (32-bit)	RHE Linux 5 (32-bit)
Total users	500 or fewer	500 to 2500	2500 to 10,000

Follow the steps below to deploy an OVA file in order to define the virtual machine requirements.

Step 1: Open VMware vSphere Client, click on the server hardware you want to use for this install, and then navigate to **File > Deploy OVF Template**.

Step 2: In the Deploy OVF Template wizard, enter the following information:

- On the Source page, click **Browse**, select the Cisco Unified CM OVA file that you downloaded from Cisco, click **Open**, and then click **Next**.
- On the OVF Template Details page, verify the version information, and then click **Next**:
- On the Name and Location page, in the Name box, enter the virtual machine name **CUCM-Pub1**. In the Inventory Location tree, select the location to deploy the server, and then click **Next**.
- On the Deployment Configuration page, in the Configuration list, select one of the following nodes, and then click **Next**.
  - **1000-user node (BE6K)**—For a cluster of 500 or fewer users.
  - **2500-user node**—For a cluster of 500 to 2500 users.
  - **7500-user node**—For a cluster of 2500 to 10,000 users.
- On the Storage page, choose the correct location for the virtual machine files, and then click **Next**.
- On the Disk Format page, choose **Thick Provision Eager Zeroed**, and then click **Next**.
- On the Ready to Complete page, verify the settings, and then click **Finish**.

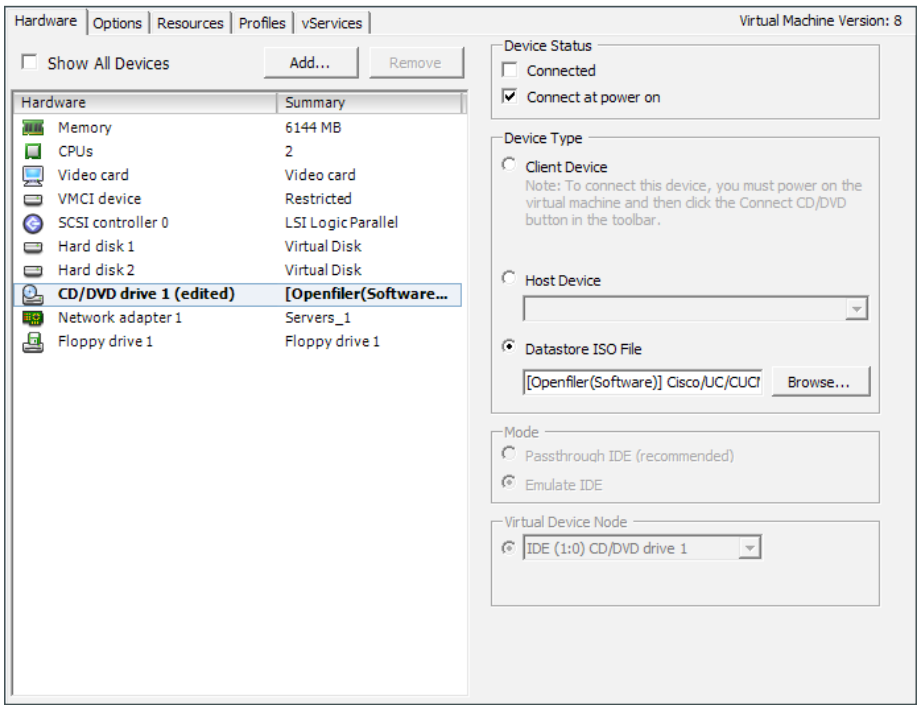


Step 3: In the message window, click **Close**.

Step 4: After the virtual machine is created, click on the server name (Example: CUCM-Pub1), navigate to the **Getting Started** tab, and then click **Edit virtual machine settings**.

Step 5: On the Hardware tab, select **CD/DVD Drive 1**, and then select **Connect at power on**.

Step 6: Select **Datastore ISO File**, click **Browse**, navigate to the location of the Cisco Unified CM bootable installation file, select the correct ISO image, and then click **OK**.



Step 7: On the Getting Started tab, click **Power on virtual machine**.

Step 8: Click the **Console** tab, and then watch the server boot.

After the ISO loads, the virtual machine is prepared for installation.

PROCESS

Installing Cisco Unified CM

1. Install the first Cisco Unified CM platform
2. Install licenses and start services
3. Configure additional servers
4. Install the remaining Unified CM platforms
5. Start services

The following information is needed for the installation:

- Time zone for the server
- Host name, IP address, network mask, and default gateway
- Domain Name System (DNS) server IP addresses
- Administrator ID and password
- Organization, unit, location, state, and country
- Network Time Protocol (NTP) server IP addresses
- Security password
- Application username and password
- Lightweight Directory Access Protocol (LDAP) information for integration with Microsoft's Active Directory:
    - Manager Distinguished Name (read access required)
    - User Search Base
    - Host name or IP address and port number for the LDAP server

When users are created in Active Directory, either the telephone number or the IP phone attribute is mandatory. Otherwise, the users cannot be imported into Cisco Unity Connection.

Complete the tasks listed below before you start the installation:

- In DNS, configure Cisco Unified CM host names
- Obtain license files from the Cisco licensing system
- On the PC or Mac used for administration, install an archive program for opening .tar files

For standard deployments, this design recommends that you configure Cisco Unified CM to use IP addresses rather than host names. However, during the initial installation of the publisher node in a Unified CM cluster, the publisher is referenced in the server table by the host name you provided for the system. When new subscribers are added to a publisher, the initial use of host names makes it easier to identify the servers for troubleshooting purposes. The host names will be changed to IP addresses later in this guide.

Each subscriber should be added to this server table one device at a time, and there should be no definitions for non-existent subscribers at any time, other than for the new subscribers being installed.

Procedure 1 Install the first Cisco Unified CM platform

This procedure is for installing the first Cisco Unified CM platform. If this is not the first Unified CM platform, skip ahead to Procedure 4 “Install the remaining Unified CM platforms.”

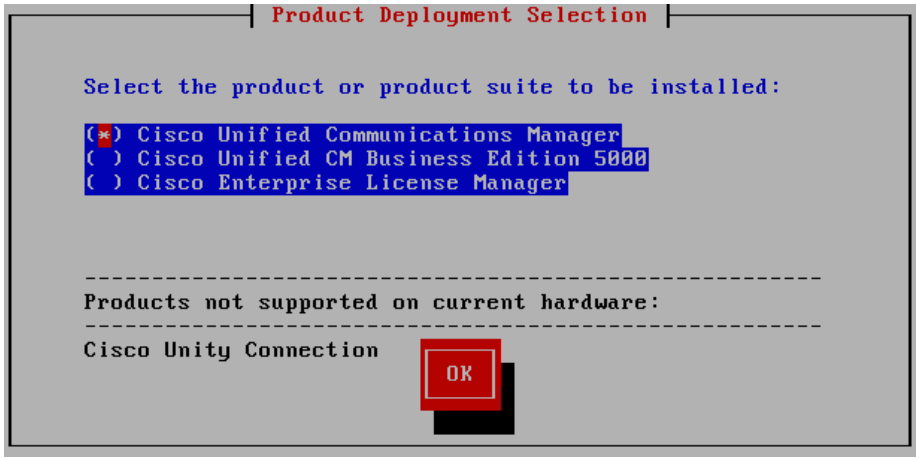
After the ISO/DVD loads, continue the installation on the server console.

Step 1: On the DVD Found page, choose **Yes**.

Step 2: If the media check passes, choose **OK**.

If the media check does not pass, contact Cisco Technical Assistance Center or your local representative in order to replace the media, and then repeat Step 1.

Step 3: On the Product Deployment Selection page, choose **Cisco Unified Communications Manager**, and then choose **OK**.



Step 4: On the Proceed with Install page, verify that the version is correct, and then choose **Yes**.

Step 5: On the Platform Installation Wizard page, choose **Proceed**.

Step 6: On the Apply Patch page, choose **No**.

Step 7: If the Import Windows Data page is displayed, choose **No**.

Step 8: On the Basic Install page, choose **Continue**.

Step 9: On the Timezone Configuration page, use the arrow keys to select the correct time zone, and then choose **OK**.

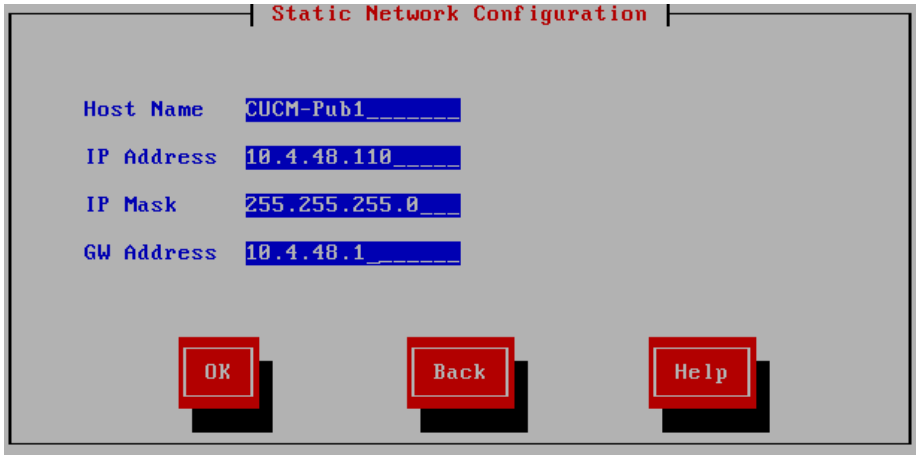
Step 10: On the Auto Negotiation Configuration page, choose **Continue**.

Step 11: On the MTU Configuration page, choose **No**.

Step 12: On the DHCP Configuration page, choose **No**.

Step 13: On the Static Network Configuration page, enter the following information, and then choose **OK**:

- Host Name–**CUCM-Pub1** first node (publisher)
- IP Address–**10.4.48.110**
- IP Mask–**255.255.255.0**
- GW Address–**10.4.48.1**



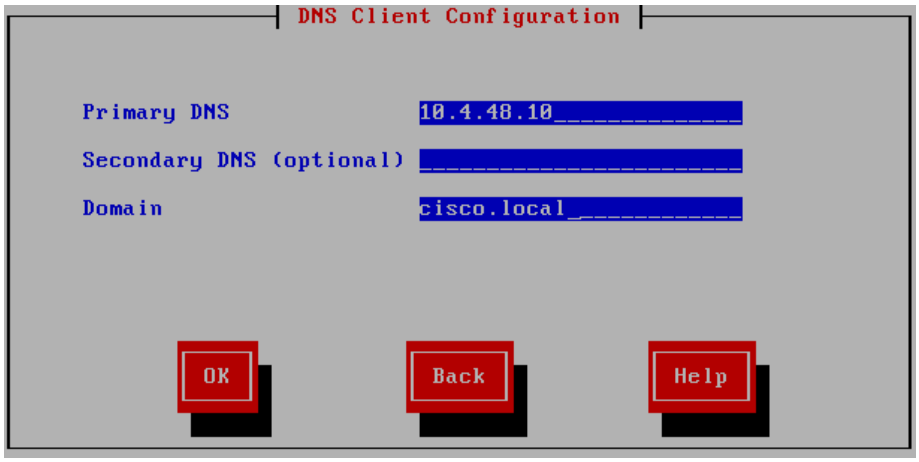
Tech Tip

During the software installation, the server performs a reverse DNS lookup on the name and IP address entered above. The installation halts if the lookup does not succeed, so please verify your server information is properly entered into DNS and the associated pointer records are created beforehand.

Step 14: On the DNS Client Configuration page, choose **Yes**.

Step 15: Enter the following information, and then choose **OK**:

- Primary DNS–**10.4.48.10**
- Domain–**cisco.local**

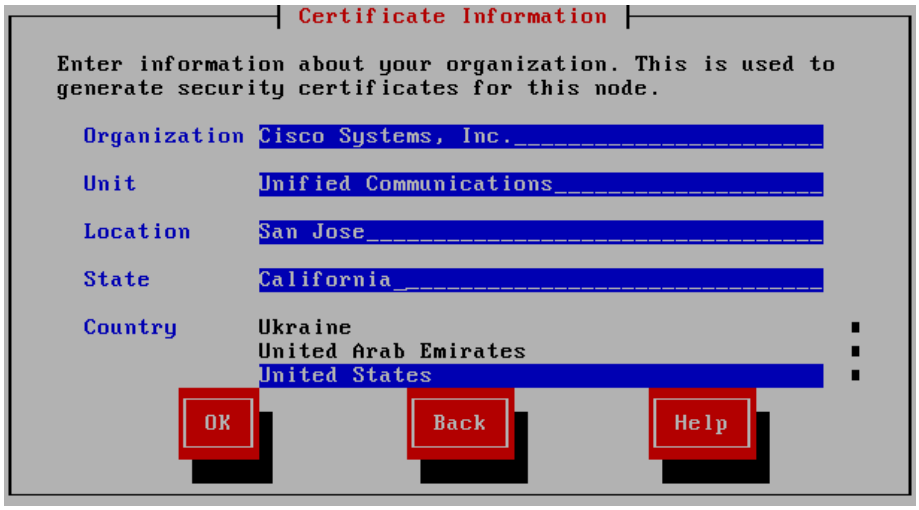


Step 16: On the Administrator Login Configuration page, enter the following information, and then choose **OK**:

- Administrator ID—**Admin**
- Password—**[password]**
- Confirm Password—**[password]**

> **Tech Tip**
>
> The password must start with an alphabetic character, have at least six characters, and can contain alphanumeric characters, hyphens, or underscores.

Step 17: On the Certificate Information page, enter the details that will be used to generate the certificate used for secure communications, and then choose **OK**.



Step 18: On the First Node Configuration page, choose **Yes**.

Step 19: On the Network Time Protocol Client Configuration page, next to the NTP Server 1 prompt, enter **10.4.48.17**, add up to four more NTP host names or IP addresses, and then choose **OK**.

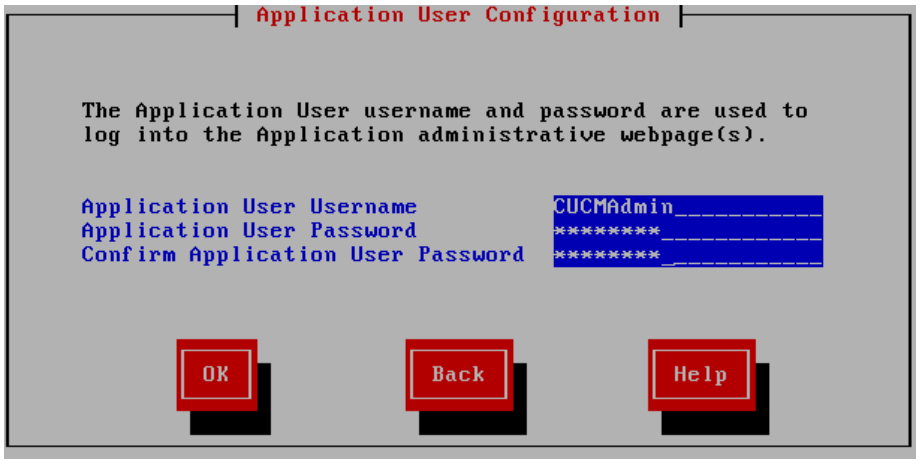
Step 20: On the Security Configuration page, enter a security password, confirm the password, and then choose **OK**.

You use the security password during the remaining nodes installation process.

Step 21: On the SMTP Host Configuration page, choose **No**.

Step 22: On the Application User Configuration page, enter the following information, and then choose **OK**:

- Application User Username—**CUCMAdmin**
- Application User Password—**[password]**
- Confirm Application User Password—**[password]**



Step 23: On the Platform Configuration Confirmation page, choose **OK**.

The system finishes the rest of the installation process without user input. The system reboots a few times during installation. The process can take 60 minutes or more, depending on your server hardware.

After the software has finished installing, the login prompt appears on the console.

Step 24: In vSphere Client, navigate to the virtual machine's **Getting Started** tab, and then click **Edit virtual machine settings**.

Step 25: On the Hardware tab, select **CD/DVD Drive 1**.

Step 26: Clear **Connect at power on**, and then click **OK**.

Procedure 2 Install licenses and start services

After the first Unified CM platform is installed, there are several configuration steps that have to be completed in order to prepare the publisher for the remaining servers.

Step 1: In a web browser, access the IP address or hostname of the publisher, and then in the center of the page, under Installed Applications, click **Cisco Enterprise License Manager**.

Step 2: On the login page, enter the following application username and password from Step 22, and then click **Login**:

- User Name—**CUCMAdmin** (case-sensitive)
- Password—**[password]**

Step 3: Navigate to **Inventory > Product Instances**, and then click **Add**.

> **Tech Tip**
>
> The username and password for adding the product instances is the case-sensitive platform administrator ID that was created when installing the server software.

Step 4: Enter the following information for Cisco Unified CM, and then click **Test Connection**:

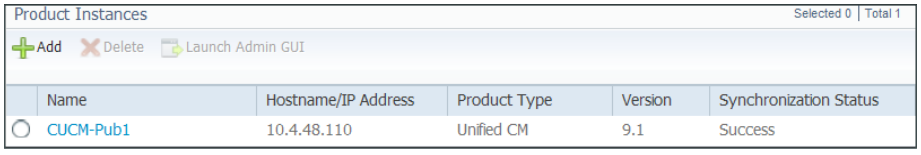
- Name–**CUCM-Pub1**
- Description–**CUCM Publisher**
- Product Type–**Unified CM**
- Hostname/IP Address–**10.4.48.110** (publisher)
- Username–**Admin** (case-sensitive platform administrator ID from Step 16)
- Password–**[password]**

Step 5: In the message window, click **OK**.

Step 6: If the connection is successful, click **OK**.

If the connection is not successful, repeat Step 4 through Step 6 with the correct information.

Step 7: Click **Synchronize Now**.



Step 8: Navigate to **License Management > Licenses**, and then select **Other Fulfillment Options > Fulfill Licenses from File**.

> **Tech Tip**
>
> Extract the .bin file from the .zip before trying to install the license in the next step. The installation process returns an error if you try to install the .zip file.

Step 9: On the Install License File page, click **Browse**, locate the directory that contains the license files you obtained prior to installation, select the .bin file, click **Open**, and then click **Install**. A message confirms that the license was successfully installed.

Step 10: Repeat Step 8 through Step 9 for each additional license file for your installation. After all files have been installed, click **Close**.

Next, you verify the licenses have been properly installed.

Step 11: Navigate to **Monitoring > License Usage**, and then confirm the status is In Compliance.

If there is a problem, please notify your Cisco representative in order to obtain new license files.

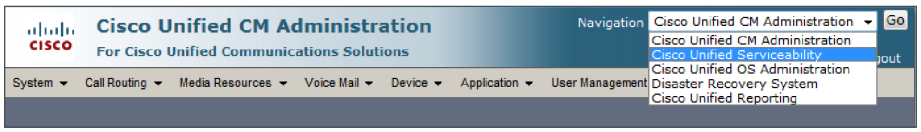
License Usage

Type	Product Scope	Required	Installed	Unused	Status
Enhanced (9.0)	Unified CM	0	10000	10000	In Compliance

Step 12: In a web browser, access the IP address or hostname of the publisher, and in the center of the page, under Installed Applications, click **Cisco Unified Communications Manager**.

Step 13: Enter the **Username** and **Password** from the Application User Configuration page in Step 22 of the previous procedure, and then click **Login**.

Step 14: In the **Navigation** list at the top of the page, choose **Cisco Unified Serviceability**, and then click **Go**.



Step 15: Navigate to **Tools > Service Activation**, in the **Server** list, choose **CUCM-Pub1**, and then click **Go**.

Tech Tip

If you will have more than 1250 phones in your cluster, dedicated TFTP servers are recommended, and the TFTP service is not activated on the first node (publisher).

Step 16: Select **Check All Services**, clear the ones that are not needed for this node, and then click **Save**.

Tech Tip

You may safely disable the following services if you don't plan to use them:

Cisco Messaging Interface

Cisco DHCP Monitor Service

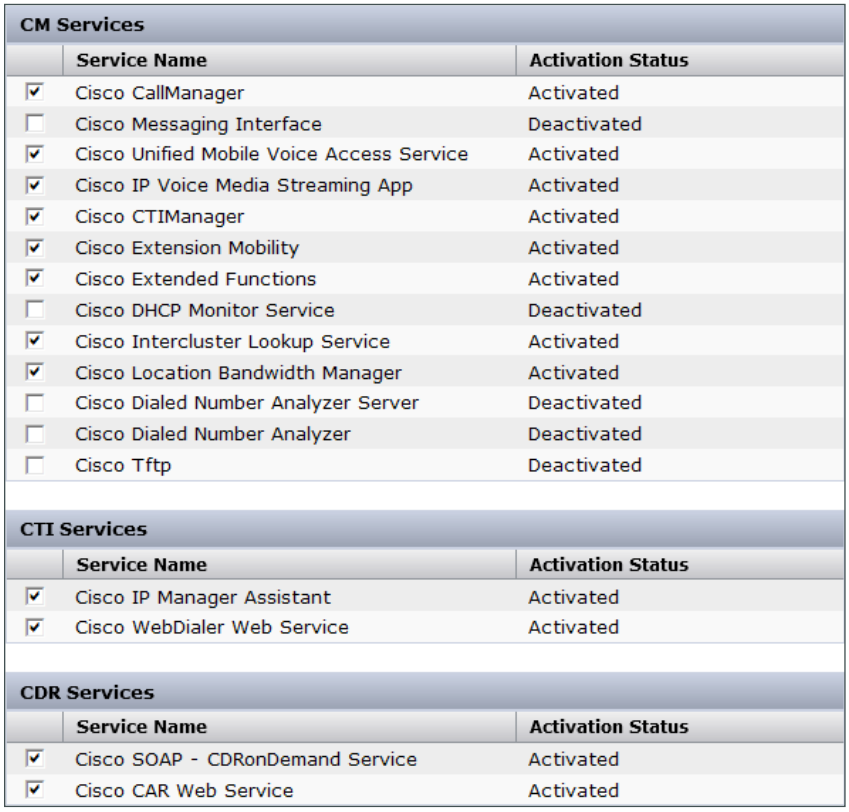
Cisco TAPS Service

Cisco Dialed Number Analyzer Server

Cisco Dialed Number Analyzer

Step 17: In the message window, click **OK**.

Figure 16 – Recommended publisher services when using dedicated TFTP servers



CM Services

	Service Name	Activation Status
☑	Cisco CallManager	Activated
☐	Cisco Messaging Interface	Deactivated
☑	Cisco Unified Mobile Voice Access Service	Activated
☑	Cisco IP Voice Media Streaming App	Activated
☑	Cisco CTIManager	Activated
☑	Cisco Extension Mobility	Activated
☑	Cisco Extended Functions	Activated
☐	Cisco DHCP Monitor Service	Deactivated
☑	Cisco Intercluster Lookup Service	Activated
☑	Cisco Location Bandwidth Manager	Activated
☐	Cisco Dialed Number Analyzer Server	Deactivated
☐	Cisco Dialed Number Analyzer	Deactivated
☐	Cisco Tftp	Deactivated

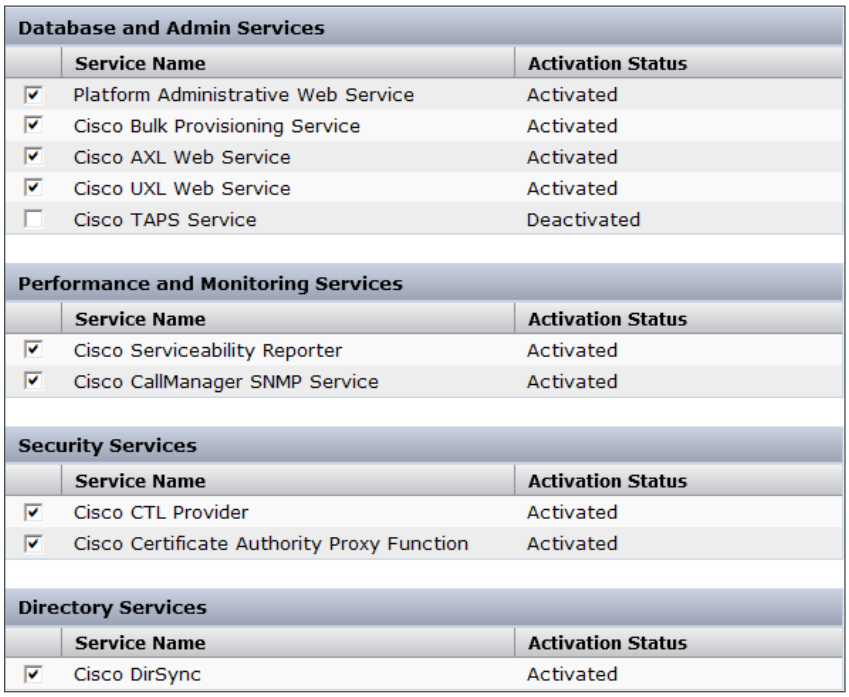
CTI Services

	Service Name	Activation Status
☑	Cisco IP Manager Assistant	Activated
☑	Cisco WebDialer Web Service	Activated

CDR Services

	Service Name	Activation Status
☑	Cisco SOAP - CDROnDemand Service	Activated
☑	Cisco CAR Web Service	Activated

Figure 17 – Recommended publisher services (continued)



Database and Admin Services

	Service Name	Activation Status
☑	Platform Administrative Web Service	Activated
☑	Cisco Bulk Provisioning Service	Activated
☑	Cisco AXL Web Service	Activated
☑	Cisco UXL Web Service	Activated
☐	Cisco TAPS Service	Deactivated

Performance and Monitoring Services

	Service Name	Activation Status
☑	Cisco Serviceability Reporter	Activated
☑	Cisco CallManager SNMP Service	Activated

Security Services

	Service Name	Activation Status
☑	Cisco CTL Provider	Activated
☑	Cisco Certificate Authority Proxy Function	Activated

Directory Services

	Service Name	Activation Status
☑	Cisco DirSync	Activated

Activating services may take a few minutes to complete, so please wait for the page to refresh before you continue.

Procedure 3 Configure additional servers

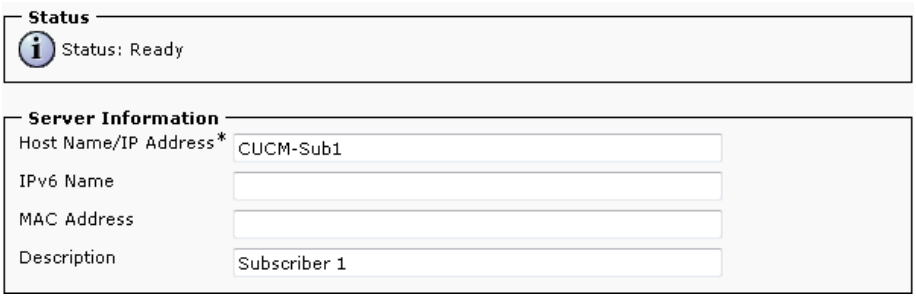
After installing the licenses and starting the services, the subscribers, TFTP and voicemail servers must be added to the publisher. When new subscribers and TFTP servers are added to a publisher, the initial use of host names makes it easier to identify the servers for troubleshooting purposes. The host names will be changed to IP addresses later in this guide.

Please do not add servers that will not be installed prior to running the CUCC tool.

Step 1: In the **Navigation** list at the top of the page, choose **Cisco Unified CM Administration**, and then click **Go**.

Step 2: Navigate to **System > Server**, and then click **Add New**.

Step 3: Enter the host name of the additional Cisco Unified CM server, a description, and then click **Save**.



Step 4: For each additional subscriber and TFTP server, click **Add New**, and then repeat Step 3, using the appropriate information.

Host Name/IP Address	Description
CUCM-Pub1	Publisher
CUCM-Sub1	Subscriber 1
CUCM-Sub2	Subscriber 2
CUCM-Sub3	Subscriber 3
CUCM-Sub4	Subscriber 4
CUCM-TFTP1	TFTP Server 1
CUCM-TFTP2	TFTP Server 2

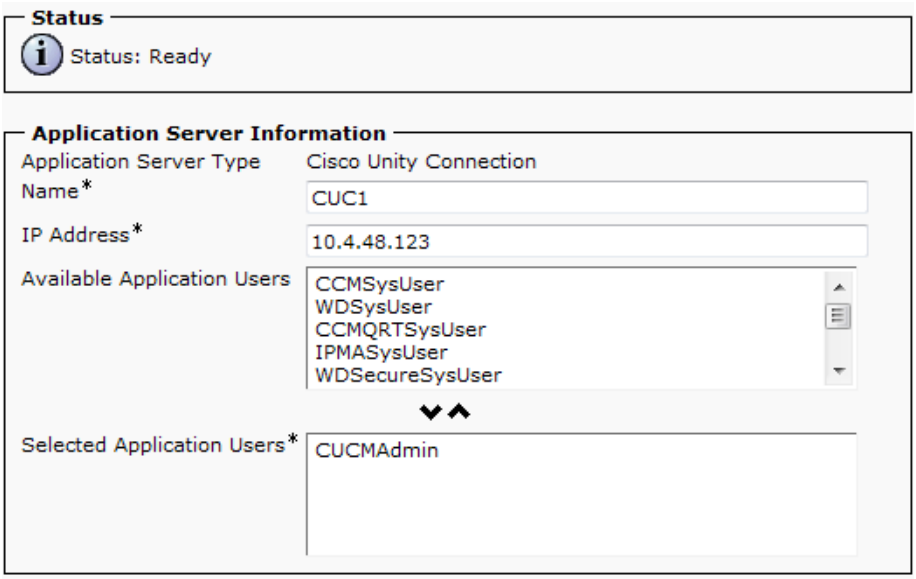
The next several steps add Cisco Unity Connection as an application server to the cluster.

Step 5: Navigate to **System > Application Server**, and then click **Add New**.

Step 6: On the first Application Server Configuration page, in Application Server Type list, choose **Cisco Unity Connection**, and then click **Next**.

Step 7: On the second Application Server Configuration page, in the Name box, enter **CUC1**, and then in the IP Address box, enter **10.4.48.123**.

Step 8: In the **Available Application Users** list, select the account you created during the installation of Cisco Unified CM (Example: CUCMAdmin), move the account to the **Selected Application Users** list by clicking the **v** character, and then click **Save**.



Step 9: When all the subscriber, TFTP and Cisco Unity Connection servers have been added to the publisher's database, repeat the procedures in "Preparing the Platform for Cisco Unified CM" for each additional Unified CM server, and then return to Procedure 4 "Install the remaining Unified CM platforms".

Procedure 4 Install the remaining Unified CM platforms

This procedure installs the remaining Cisco Unified CM subscriber and TFTP servers in a cluster.

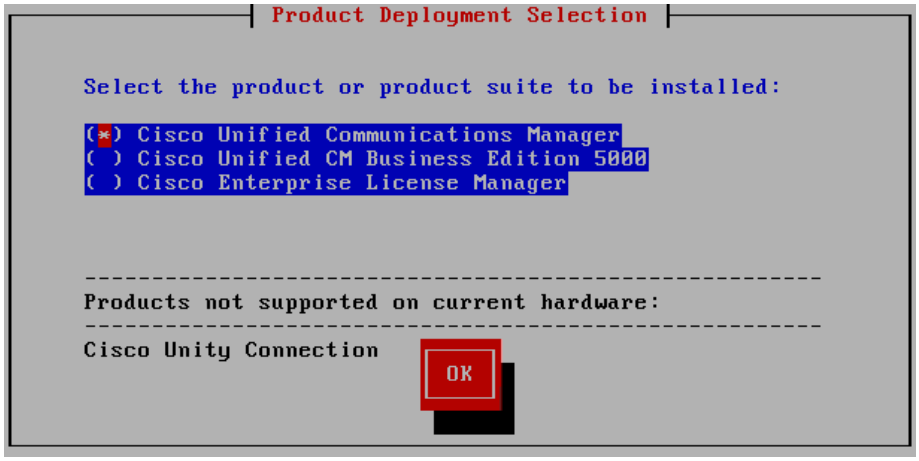
After the DVD loads, continue the installation on the server console.

Step 1: If you have not done so already, on the DVD Found page, choose **Yes**.

Step 2: If the media check passes, choose **OK**.

If the media check does not pass, contact Cisco Technical Assistance Center or your local representative in order to replace the media, and then repeat Step 1.

Step 3: On the Product Deployment Selection page, choose **Cisco Unified Communications Manager**, and then choose **OK**.



Step 4: On the Proceed with Install page, verify that the version is correct, and then choose **Yes**.

Step 5: On the Platform Installation Wizard page, choose **Proceed**.

Step 6: On the Apply Patch page, choose **No**.

Step 7: On the Basic Install page, choose **Continue**.

Step 8: On the Timezone Configuration page, use the arrow keys to select the correct time zone, and then choose **OK**.

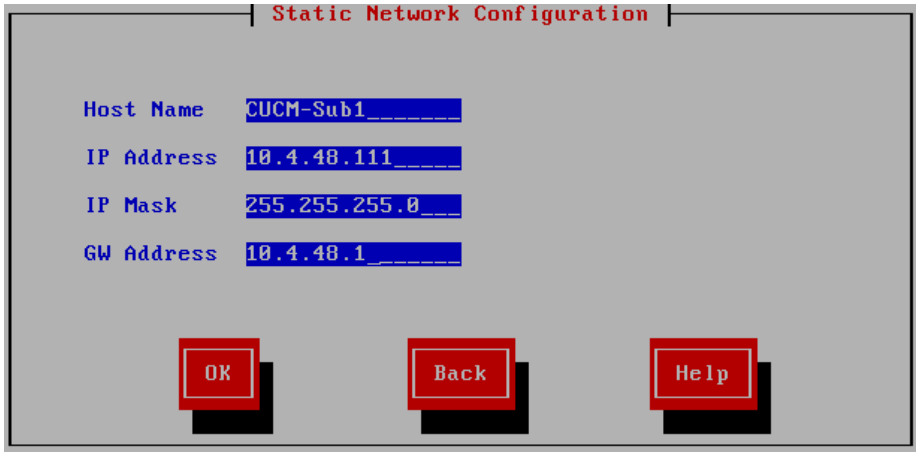
Step 9: On the Auto Negotiation Configuration page, choose **Continue**.

Step 10: On the MTU Configuration page, choose **No**.

Step 11: On the DHCP Configuration page, choose **No**.

Step 12: On the Static Network Configuration page, enter the following information, and then choose **OK**:

- Host Name–**CUCM-Sub1** second node (subscriber 1)
- IP Address–**10.4.48.111**
- IP Mask–**255.255.255.0**
- GW Address–**10.4.48.1**



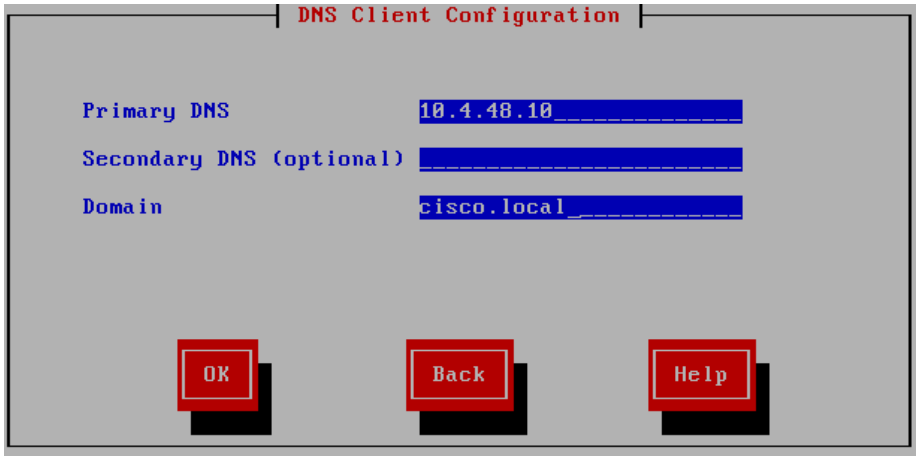
Tech Tip

During the software installation, the server performs a reverse DNS lookup on the name and IP address entered above. The installation halts if the lookup does not succeed, so please verify your server information is properly entered into DNS and the associated pointer records are created beforehand.

Step 13: On the DNS Client Configuration page, choose **Yes**.

Step 14: Enter the following information, and then choose **OK**:

- Primary DNS–**10.4.48.10**
- Domain–**cisco.local**

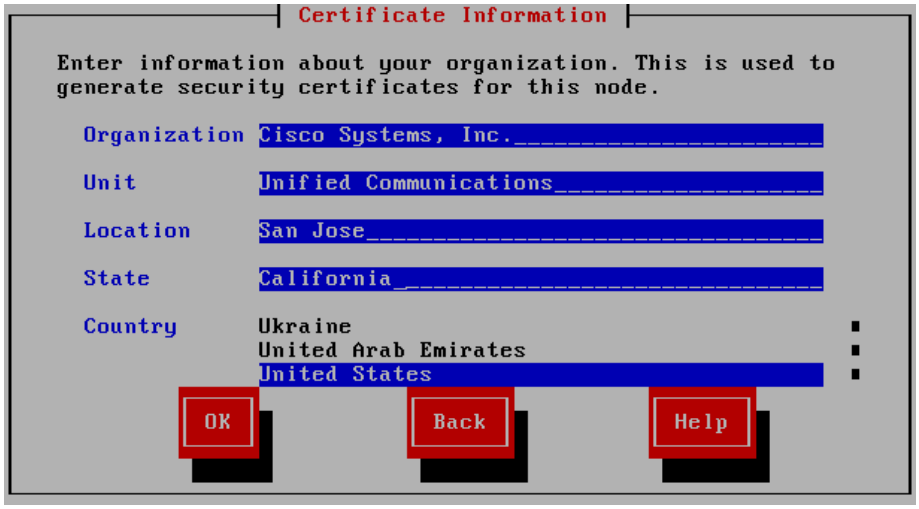


Step 15: On the Administrator Login Configuration page, enter the following information, and then choose **OK**:

- Administrator ID—**Admin**
- Password—**[password]**
- Confirm Password—**[password]**

> **Tech Tip**
>
> The password must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, or underscores.

Step 16: On the Certificate Information page, enter the details that will be used to generate the certificate used for secure communications, and then choose **OK**.



Step 17: On the First Node Configuration page, choose **No**.

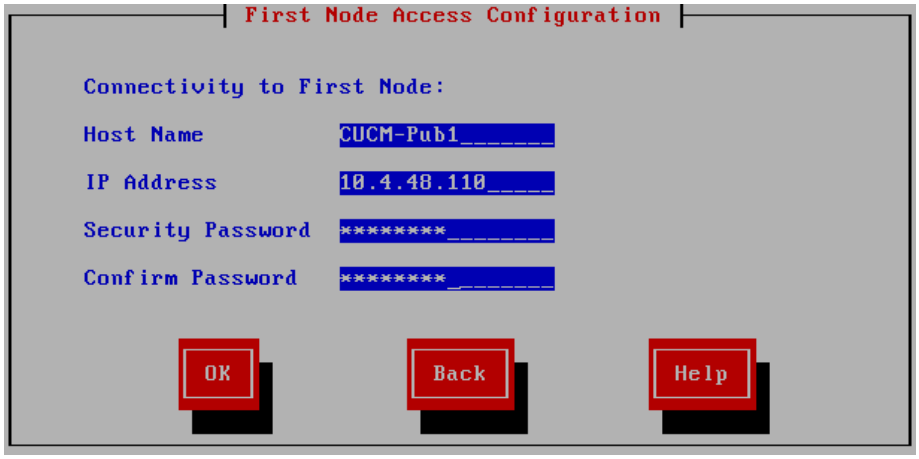
> **Tech Tip**
>
> Before proceeding with the remaining nodes installation, ensure that the first node has finished installing and the subscribers have been added under the publisher's **System > Server** menu using the Cisco Unified CM administration interface.

Step 18: On the First Node Configuration page, read the warning, and then choose **OK** to acknowledge you have installed the first node and verified that it is reachable from the network.

Step 19: On the Network Connectivity Test Configuration page, choose **No**.

Step 20: On the First Node Access Configuration page, enter the following information, and then choose **OK**:

- Host Name–**CUCM-Pub1** (name of publisher)
- IP Address–**10.4.48.110** (IP address of publisher)
- Security Password–**[password]** (from publisher)
- Confirm Password–**[password]**



Step 21: On the SMTP Host Configuration page, choose **No**.

Step 22: On the Platform Configuration Confirmation page, choose **OK**.

The system finishes the rest of the installation process without user input. The system reboots a few times during installation. The process can take 60 minutes or more, depending on your hardware.

After the software has finished installing, the login prompt appears on the console.

Step 23: In vSphere Client, navigate to the virtual machine's **Getting Started** tab, and then click **Edit virtual machine settings**.

Step 24: On the Hardware tab, select **CD/DVD Drive 1**.

Step 25: Clear **Connect at power on**, and then click **OK**.

Procedure 5 Start services

After the software installation completes, the services must be started from the publisher.

Step 1: In a web browser, access the Cisco Unified CM administration interface on the publisher, and then in the center of the page, under Installed Applications, click **Cisco Unified Communications Manager**.

Step 2: Enter the application **Username** and **Password**, and then click **Login**.

Step 3: In the **Navigation** list on the top right side of the page, choose **Cisco Unified Serviceability**, and then click **Go**.

Step 4: Navigate to **Tools > Service Activation**.

Step 5: In the **Server** list, choose the next additional server, and then click **Go**.

> **Tech Tip**
>
> If you will have more than 1250 phones in your cluster, dedicated TFTP servers are recommended, and the TFTP service is not activated on the subscriber nodes in the cluster. This design also recommends that you disable the Cisco CallManager service on the dedicated TFTP servers in order to save CPU processing.

Step 6: Select **Check All Services**, clear the ones that are not needed for this node, and then click **Save**.

Step 7: In the message window, click **OK**.

Figure 18 - Recommended subscriber services when using dedicated TFTP servers

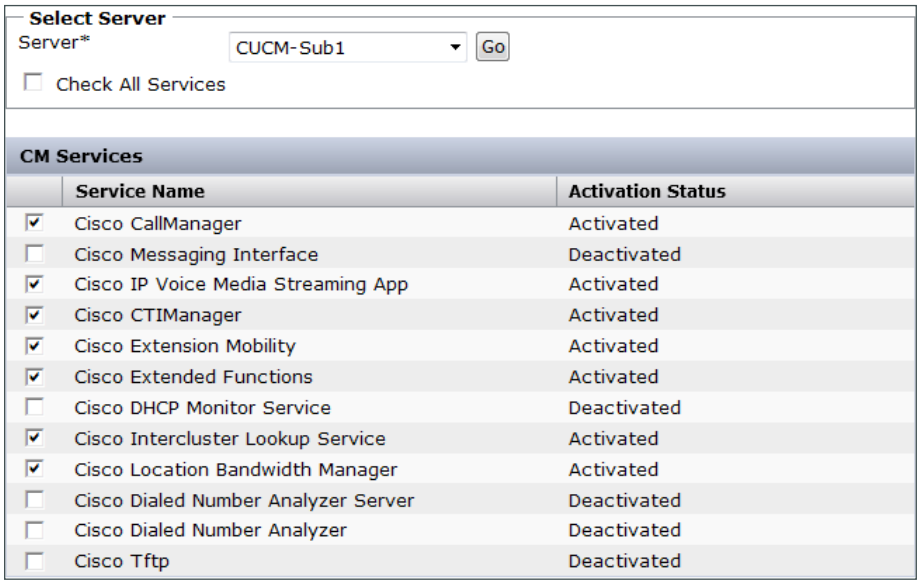
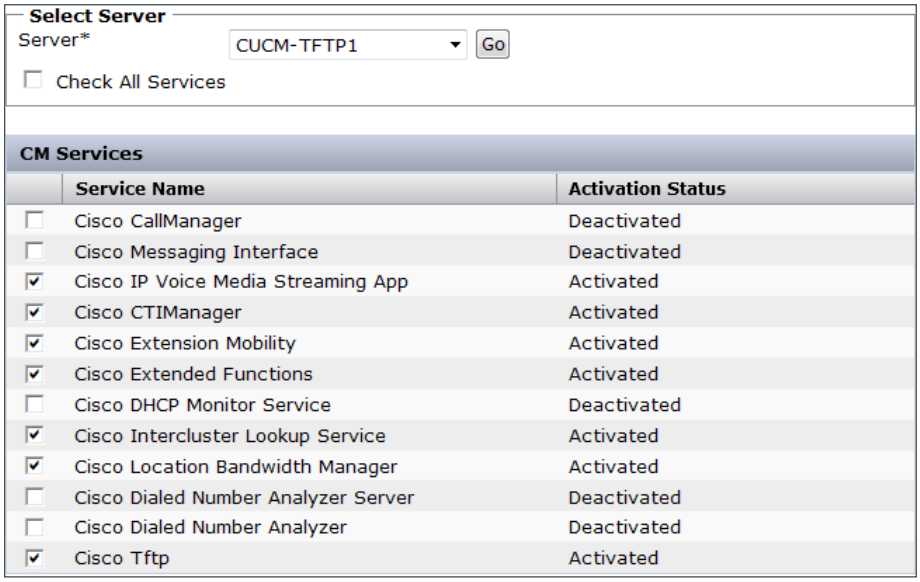


Figure 19 - Recommended dedicated TFTP services with Cisco CallManager deactivated



Activating services may take a few minutes to complete, so please wait for the page to refresh before continuing.

Step 8: Repeat this procedure for the rest of the subscriber and TFTP servers, using the appropriate information for each device.

PROCESS

Preparing the Platform for Cisco Unity Connection

1. Configure platform connectivity to the LAN
2. Prepare the server for Unity Connection

Cisco Unity Connection is used as the voicemail platform for the unified communications foundation. It is configured as a simple voicemail-only system that uses a single server.

For a quick and easy installation experience, it is essential to know up-front what information you will need. To install Cisco Unity Connection, make sure you have completed the following steps before you start:

- Download the Open Virtual Archive (OVA) file from the Cisco website at: http://software.cisco.com/download/release.html?mdfid=283062758&flowid=31846&softwareid=282074348&release=OVA-9.1&relind=AVAILABLE&rellifecycle=&reltype=latest

  For an installation using ESXi 4.1, choose the latest OVA file with vmv7 in the name. For example: **CUC_9.1_vmv7_v1.5.ova**

  For an installation using ESXi 5.0 or higher, choose the latest OVA file with vmv8 in the name. For example: **CUC_9.1_vmv8_v1.5.ova**

- Check the Cisco website to determine if there is a patch for your version of Cisco Unity Connection: http://software.cisco.com/download/release.html?mdfid=284603371&flowid=37563&softwareid=282074295&release=9.1(1)&relind=AVAILABLE&rellifecycle=&reltype=latest

Procedure 1 Configure platform connectivity to the LAN

The Cisco Unity Connection server can be connected to a Cisco Nexus switch in the data center or a Cisco Catalyst switch in the server room. In both cases, QoS policies are added to the ports in order to maintain voice quality during the setup and configuration of calls. Please choose the option that is appropriate for your environment.

Option 1: Connect the Cisco Unity Connection server to a Cisco Nexus 2248UP switch

Step 1: Log in to the Cisco Nexus switch with a username that has the ability to make configuration changes.

Step 2: If there is a previous configuration on the switch port where the Cisco Unity Connection server is connected, remove the individual commands by issuing a **no** in front of each one. This brings the port back to its default state.

Step 3: Configure the port as an access port and apply the QoS policy.

```
interface Ethernet107/1/14
 description Unity Connection
 switchport access vlan 148
 spanning-tree port type edge
 service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

Tech Tip

When deploying a dual-homed Cisco Nexus 2248 switch, this configuration is applied to both Nexus 5548 switches.

Option 2: Connect the Cisco Unity Connection server to a Cisco Catalyst 3750-X Series switch

To ensure that signaling traffic is prioritized appropriately, you must configure the Cisco Catalyst access switch port where the Cisco Unity Connection server is connected to trust the DSCP markings. The easiest way to do this is to clear the interface of any previous configuration and then apply the egress QoS macro that was defined in the access-switch platform configuration of the Campus Wired LAN Design Guide.

Step 1: Log in to the Cisco Catalyst switch with a username that has the ability to make configuration changes.

Step 2: Clear the interface's configuration on the switch port where the Cisco Unity Connection server is connected.

```
default interface GigabitEthernet1/0/16
```

Step 3: Configure the port as an access port and apply the egress QoS policy.

```
interface GigabitEthernet1/0/16
 description Unity Connection
 switchport access vlan 148
 switchport host
 macro apply EgressQoS
```

Procedure 2 Prepare the server for Unity Connection

The following tables describe the server scaling options for Cisco Unity Connection.

Table 6 - Cisco Unity Connection virtual machine scaling options

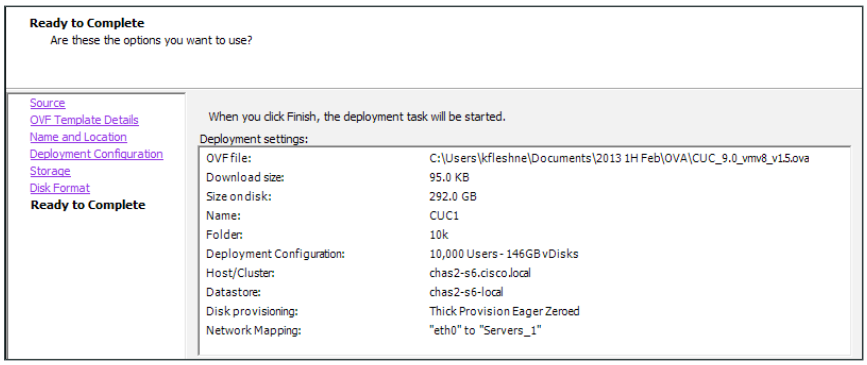
	1000 users	5000 users	10,000 users
Virtual CPUs	1	2	4
CPU speed	2.13 GHz	5.06 GHz	10.12 GHz
RAM	4 GB	6 GB	6 GB
Hard disk	160 GB	200 GB	300 GB (2)
VMware ESXi	4.0, 4.1, 5.0	4.0, 4.1, 5.0	4.0, 4.1, 5.0
OS support	RHE Linux 5 (32-bit)	RHE Linux 5 (32-bit)	RHE Linux 5 (32-bit)
Total users	1000 or fewer	1000 to 5000	5000 to 10,000

Follow the steps below to deploy an OVA file in order to define the virtual machine (VM) requirements.

Step 1: Open VMware vSphere Client, click on the server hardware you want to use for this install, and then navigate to **File > Deploy OVF Template**.

Step 2: In the Deploy OVF Template wizard, enter the following information:

- On the Source page, next to the Deploy from a file or URL box, click **Browse**, select the Cisco Unity Connection OVA file that you downloaded from Cisco, click **Open**, and then click **Next**.
- On the OVF Template Details page, verify the version information, and then click **Next**:
- On the Name and Location page, in the Name box, enter the virtual machine name **CUC1**. In the **Inventory Location** tree, select the location to deploy the server, and then click **Next**.
- On the Deployment Configuration page, in the Configuration list, select one of the following options, and then click **Next**:
  - **1000 users**—For 1000 users or fewer.
  - **5000 users**—For 1000 to 5000 users.
  - **10,000 users**—For 5000 users or more.
- On the Storage page, select the destination for the virtual machine files, and then click **Next**.
- On the Disk Format page, choose **Thick Provisioned Eager Zeroed**, and then click **Next**.
- On the Ready to Complete page, verify the settings, and then click **Finish**.



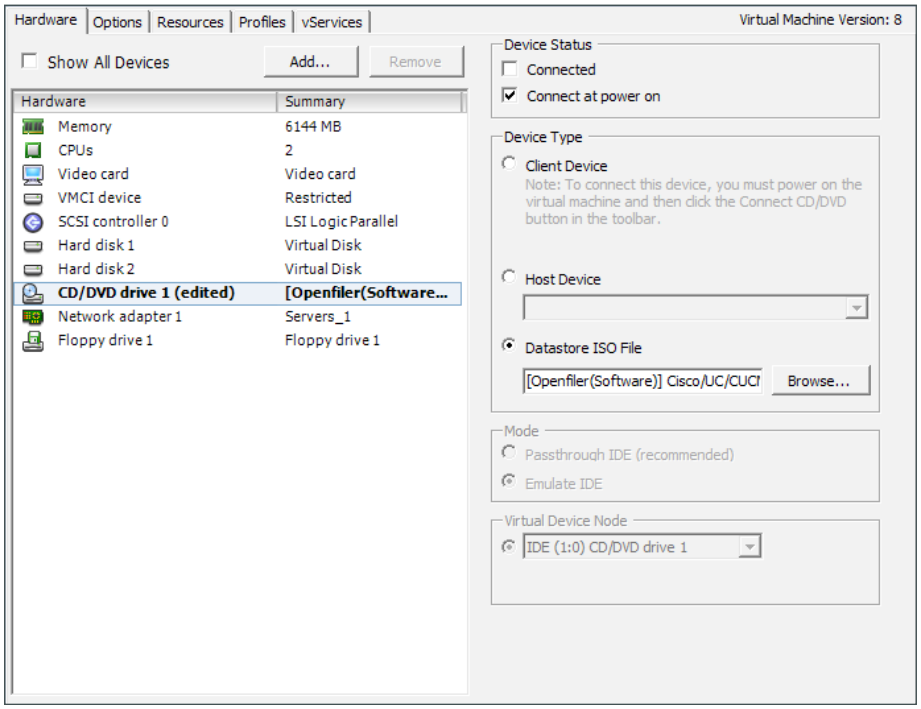
Step 3: In the message window, click **Close**.

Step 4: After the virtual machine is created, navigate to the **Getting Started** tab, and then click **Edit virtual machine settings**.

Step 5: On the Hardware tab, select **CD/DVD Drive 1**, and then select **Connect at power on**.

> **Tech Tip**
>
> Cisco Unity Connection shares the same ISO image with Cisco Unified Communications Manager.

Step 6: Select **Datastore ISO File**, click **Browse**, navigate to the location of the Cisco Unity Connection bootable installation file, select the correct ISO image, and then click **OK**.



Step 7: On the Getting Started tab, click **Power on virtual machine**.

Step 8: Click the **Console** tab, and then watch the virtual machine boot.

The virtual machine is prepared for installation.

PROCESS

Installing Cisco Unity Connection

1. Install Cisco Unity Connection platform
2. Install licenses and start services

The following information is needed for the installation:

- Time zone for the server
- Host name, IP address, network mask, and default gateway
- DNS IP addresses
- Administrator ID and password
- Organization, unit, location, state and country
- Network Time Protocol (NTP) server IP addresses
- Security password
- Application username and password
- LDAP information for integration with a Lightweight Directory Access Protocol server:
  - Manager Distinguished Name (read access required)
  - User Search Base (for example: The User Search Base in domain cisco.local is cn=users, dc=cisco, dc=local)
  - Host name or IP address and port number for the LDAP server

When users are created in Active Directory, either the telephone number or the IP phone attribute is mandatory. Otherwise, the users cannot be imported into Cisco Unity Connection.

Complete the tasks listed below before you start the installation:

- In DNS, configure the Cisco Unity Connection host name (CUC1)
- Obtain license files from the licensing system prior to installing Cisco Unity Connection

Procedure 1 Install Cisco Unity Connection platform

After the ISO/DVD loads, continue the installation on the server console.

Step 1: On the DVD Found page, choose **Yes**.

Step 2: If the media check passes, choose **OK**.

If the media check does not pass, contact Cisco Technical Assistance Center or your local representative in order to replace the media, and then repeat Step 1.

Step 3: On the Product Deployment Selection page, choose **Cisco Unity Connection**, and then choose **OK**.

Step 4: On the Proceed with Install page, verify that the version is correct, and then choose **Yes**.

Step 5: On the Platform Installation Wizard page, choose **Proceed**.

Step 6: On the Apply Patch page, choose **No**.

Step 7: On the Basic Install page, choose **Continue**.

Step 8: On the Timezone Configuration page, use the arrow keys to select the correct time zone, and then choose **OK**.

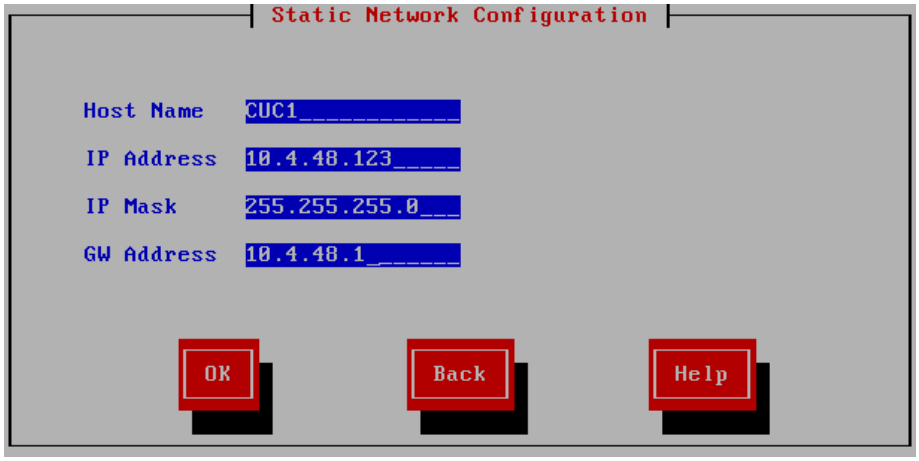
Step 9: On the Auto Negotiation Configuration page, choose **Continue**.

Step 10: On the MTU Configuration page, choose **No**.

Step 11: On the DHCP Configuration page, choose **No**.

Step 12: On the Static Network Configuration page, enter the following information, and then choose **OK**:

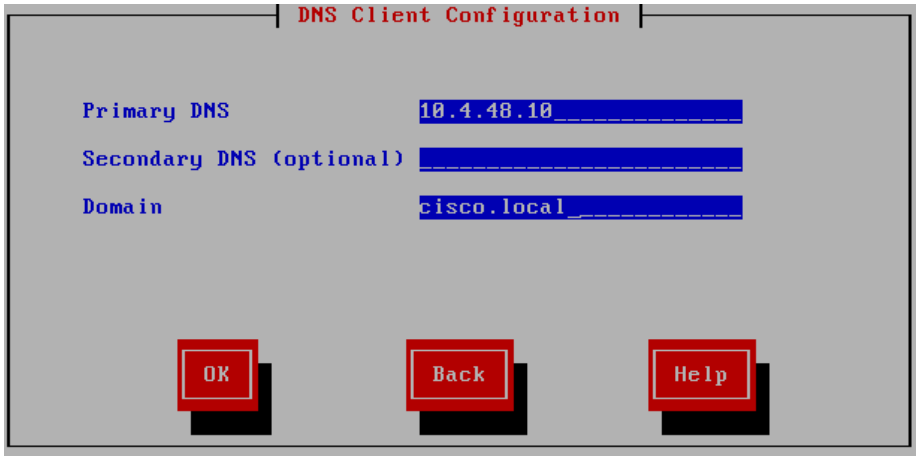
- Host Name–**CUC1**
- IP Address–**10.4.48.123**
- IP Mask–**255.255.255.0**
- GW Address–**10.4.48.1**



Step 13: On the DNS Client Configuration page, choose **Yes**.

Step 14: Enter the following information, and then choose **OK**:

- Primary DNS–**10.4.48.10**
- Domain–**cisco.local**

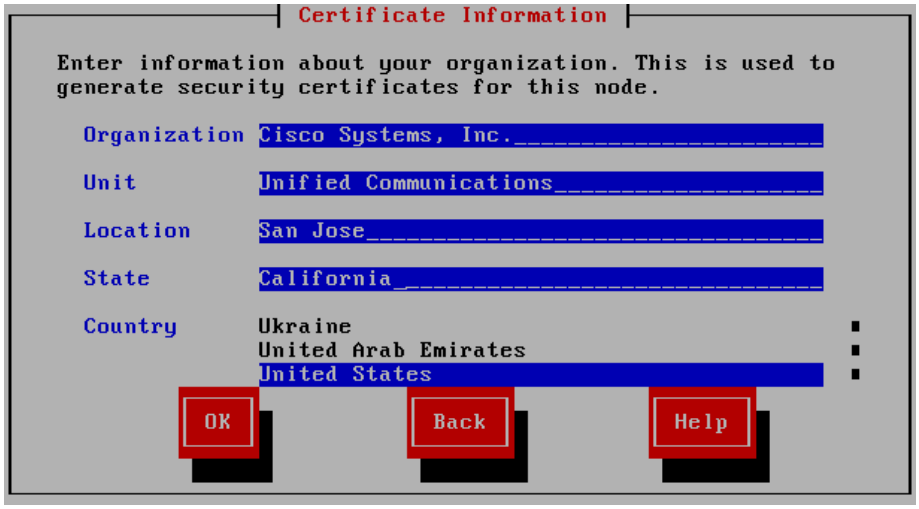


Step 15: On the Administrator Login Configuration page, enter the following information, and then choose **OK**:

- Administrator ID–**Admin**
- Password–**[password]**
- Confirm Password–**[password]**

> **Tech Tip**
>
> The password must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores.

Step 16: On the Certificate Information page, enter the details that will be used to generate the certificate used for secure communications, and then choose **OK**.



Step 17: On the First Node Configuration page, choose **Yes**.

Step 18: On the Network Time Protocol Client Configuration page, for the NTP host name or IP address, enter **10.4.48.17**, add up to four more NTP host names or IP addresses, and then choose **OK**.

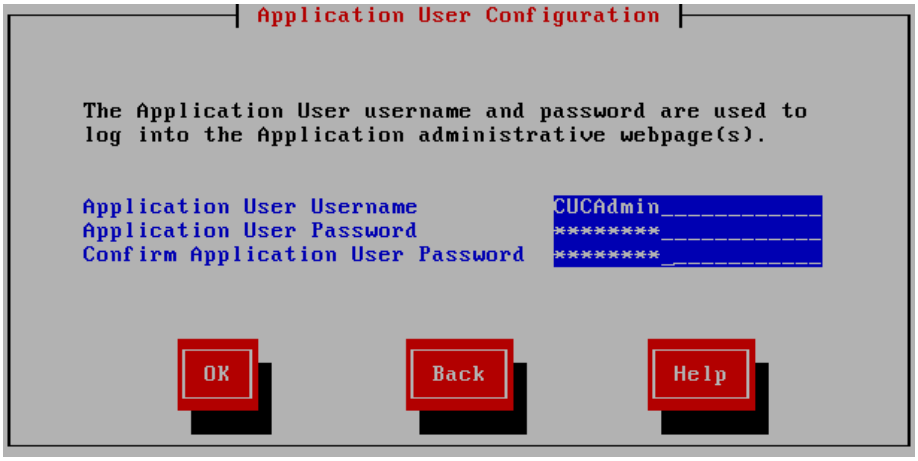
Step 19: On the Security Configuration page, enter a security password, confirm the password, and then choose **OK**.

You use this password in the future if you add another Cisco Unity Connection node.

Step 20: On the SMTP Host Configuration page, choose **No**. You can configure mail notifications at a later stage, if desired.

Step 21: On the Application User Configuration page, enter the following information, and then choose **OK**:

- Application User Username—**CUCAdmin**
- Application User Password—**[password]**
- Confirm Application User Password—**[password]**



Step 22: On the Platform Configuration Confirmation page, choose **OK**.

The system finishes the rest of the installation process without user input. The system reboots a few times during installation. The process can take 60 minutes or more, depending on your hardware.

After the software has finished loading, the login prompt appears on the console.

Step 23: In the vSphere Client, navigate to the virtual machine's **Getting Started** tab, and then click **Edit virtual machine settings**.

Step 24: On the Hardware tab, select **CD/DVD Drive 1**.

Step 25: Clear **Connect at power on**, and then click **OK**.

Procedure 2 Install licenses and start services

After the Unity Connection platform is installed, there are several configuration steps that have to be completed in order to add the licenses and start the services.

Step 1: In a web browser, access the Cisco Unified CM publisher, and in the center of the page, under Installed Applications, click **Cisco Enterprise License Manager**.

Step 2: On the login page, enter the following case-sensitive Cisco Unified CM application username and password, and then click **Login**:

- User Name—**CUCMAdmin** (case-sensitive)
- Password—**[password]**

Step 3: Navigate to **Inventory > Product Instances**, and then click **Add**.

> **Tech Tip**
>
> The username and password for adding the Product Instances is the case-sensitive platform administrator ID that was entered when installing the server software.

Step 4: Enter the following information for Cisco Unity Connection, and then click **Test Connection**:

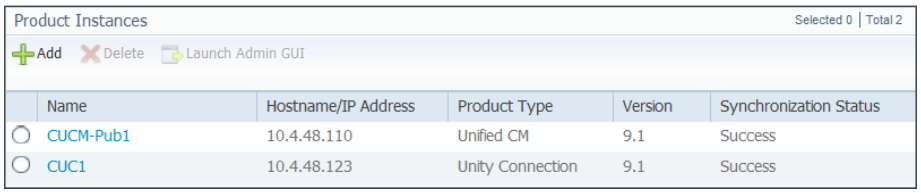
- Name–**CUC1**
- Description–**Unity Connection**
- Product Type–**Unity Connection**
- Hostname/IP Address–**10.4.48.123**
- Username–**Admin** (platform administrator ID from Step 15)
- Password–**[password]**

Step 5: In the message window, click **OK**.

Step 6: If the connection is successful, click **OK**.

If the connection is not successful, repeat Step 4 through Step 6 with the correct information.

Step 7: Click **Synchronize Now**.



Step 8: Navigate to **License Management > Licenses**, and then select **Other Fulfillment Options > Fulfill Licenses from File**.

Step 9: On the Install License File page, click **Browse**, locate the directory that contains the license files you obtained prior to installation, select the .bin file, click **Open**, and then click **Install**.

Step 10: Repeat Step 9 for each additional license file for your installation. After all files have been installed, click **Close**.

Next, you verify that the licenses have been properly installed.

Step 11: Navigate to **Monitoring > License Usage**, and then confirm the status is In Compliance.

If there is a problem, please notify your Cisco representative in order to obtain new license files.

License Usage

Type	Product Scope	Required	Installed	Unused	Status
Enhanced (9.0)	Unified CM	0	10000	10000	In Compliance
Basic Messaging (9.0)	Unity Connection	0	10000	10000	In Compliance

Step 12: In a web browser, access the Cisco Unity Connection server, and then in the center of the page, under Installed Applications, click **Cisco Unity Connection**.

Step 13: Enter the **Username** and **Password** you entered on the Application User Configuration page in Step 21 of the previous procedure, and then click **Login**.

Step 14: In the **Navigation** list, choose **Cisco Unified Serviceability**, and then click **Go**.

Step 15: Navigate to **Tools > Service Activation**.

Step 16: Select **Check All Services**, and then click **Save**. In the message window, click **OK**.

Activating services may take a few minutes to complete, so please wait for the page to refresh before you continue.

PROCESS

Configuring Cisco Unified CM and Cisco Unity Connection

1. Configure Cisco Unified CM server and site
2. Synchronize the LDAP database
3. Change host names to IP addresses
4. Configure the Unity Connection server

After all of the Cisco Unified CM and Cisco Unity Connection servers have been installed, start the server configurations using the Cisco Unified Configurator for Collaboration (CUCC) tool, which is available in a Windows and Mac version. The different versions can be downloaded from the following URLs:

- Windows: http://cvddocs.com/fw/Rel2-430-a
- Mac: http://cvddocs.com/fw/Rel2-430-b

System version 3.0 supports Cisco Unified CM and Cisco Unity Connection versions 8.5, 8.6, 9.0, and 9.1.

The Cisco Unified CM template consists of a series of comma-separated values (CSV) files that contain the base configuration for the cluster. This configuration is modified for your specific environment, based on information entered into the tool.

Please choose the correct number of servers for your installation. Choosing a number that is higher than the installed servers can cause unpredictable results when running the tool.

Procedure 1 Configure Cisco Unified CM server and site

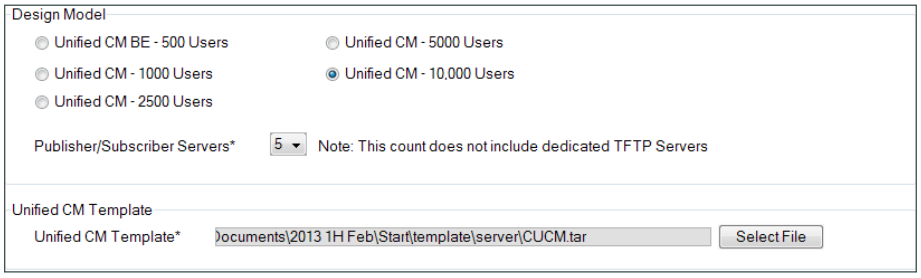
Step 1: Unzip the CUCC software package to a folder on your PC or Mac, change to the directory, and then double-click **CUCC**.

Step 2: Read the Terms of use page and if you agree, click **Accept**.

Step 3: Navigate to **Server Deployment > New CUCM Server and Site**, and then enter the information that fits your type of installation. For example:

- Design Model–**Unified CM - 10,000 Users**
- Publisher/Subscriber Servers list–**5**

Step 4: In the Unified CM Template section, click **Select File**, choose the default template called **CUCM.tar**, and then click **Next**.



Step 5: On the Server and Site Information page, enter the following information:

- First Unified CM node–**CUCM-Pub1** (Publisher)
- Second Unified CM node–**CUCM-Sub1** (Subscriber 1)
- Third Unified CM node–**CUCM-Sub2** (Subscriber 2)
- Fourth Unified CM node–**CUCM-Sub3** (Subscriber 3)
- Fifth Unified CM node–**CUCM-Sub4** (Subscriber 4)
- Check to enable synchronizing users with LDAP–**Selected**
- Check to save all data for future sessions–**Selected**

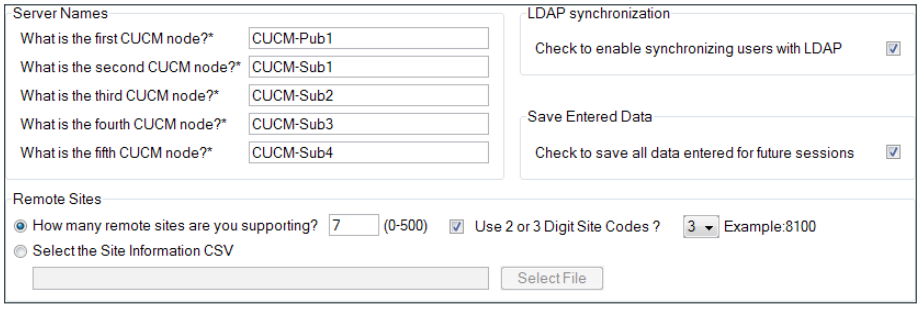
Tech Tip

The server node names that you enter on this page need to be exactly the same (including case) as specified during installation.

Step 6: In the Remotes Sites section, if you do not have a Site Information comma-separated variables (CSV) file, enter the following information, and then click **Next**:

- How many remote sites are you supporting–**7**
- Use 2 or 3 Digit Site Codes–**Selected**
- Site Code–**3**

If you have your own Site Information CSV file, choose the **Select the Site Information CSV** radio button, and then click **Select File**. Choose the .csv file from the ./template/site directory, click **Open**, and then, click **Next**.



There are two sample Site Information files in the ./template/site directory. The first one has 3-digit site codes and the second one does not have site codes. Use these sample files as a starting point for your sites to make data entry faster on the Site Information page.

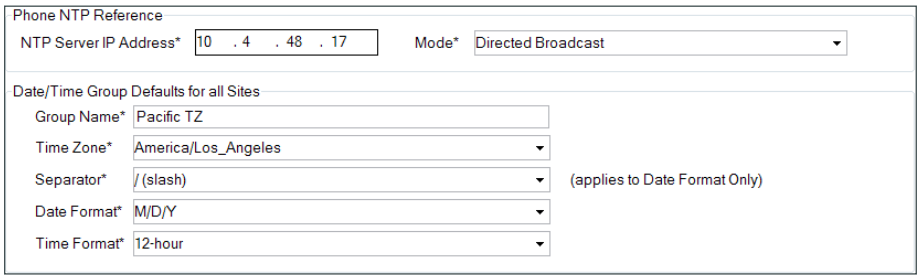
Step 7: On the Phone NTP and Date/Time Group Defaults page, enter the following information, and then click **Next**:

- NTP Server IP Address–**10.4.48.17**
- Mode–**Directed Broadcast**
- Group Name–**Pacific TZ**
- Time Zone–**Americas/Los_Angeles**
- Separator–**/ (slash)**
- Date Format–**M/D/Y**
- Time Format–**12-hour**

Reader Tip

The Date/Time Group Name and Time Zone are used as the default settings for the Site Information page. These values can be modified per site, as required for your installation.

The rest of the fields are the defaults for all Date/Time Groups created by CUCC, but their values cannot be modified on subsequent pages.



Step 8: On the Site Information page, enter the correct information for each corresponding site, and then click **Next**:

- Site Name–**HQ1**
- DMI subnet–**10.4.0.0**
- DMI subnet Mask–**17**
- SIP Gateway 1–**10.4.48.138**
- SIP Gateway 2–**10.4.48.139**
- Location Audio Kbps– (leave blank for HQ, which means unlimited)
- Site Code–**8100**
- Date/Time Group Name–**Pacific TZ**
- Time Zone–**America/Los_Angeles**

Site Name*	DMI Subnet*	DMI subnet Mask*	SIP Gateway 1*	SIP Gateway 2	Location Audio Kbps	Site Codes*	Date/Time Group Name*	Time Zone*
HQ1	10.4.0.0	17	10.4.48.138	10.4.48.139		8510	Pacific TZ	America/Los_Angeles
RS200	10.5.0.0	21	10.5.7.30		96	8511	Pacific TZ	America/Los_Angeles
RS203	10.5.48.0	21	10.5.53.28		192	8514	Mountain TZ	America/Denver
RS206	10.5.8.0	21	10.5.12.28	10.5.12.29	96	8517	Central TZ	America/Chicago
RS210	10.5.144.0	21	10.255.255.210		192	8521	Eastern TZ	America/New_York
RS211	10.5.152.0	21	10.255.255.211	10.255.253.2...	96	8522	Alaska TZ	America/Juneau
RS221	10.5.104.0	21	10.255.251.221		192	8526	Pacific_2 TZ	America/Los_Angeles
RS222	10.5.112.0	21	10.255.252.222	10.255.253.2...	384	8527	Alaska TZ	America/Juneau

Step 9: In the LDAP System Information section, choose the following options from the lists:

- LDAP Server Type–**Microsoft Active Directory**
- LDAP Attribute for User ID–**sAMAccountName**

Step 10: If you want to filter the LDAP users, create a custom filter. In the LDAP Custom Filter section, enter the following information:

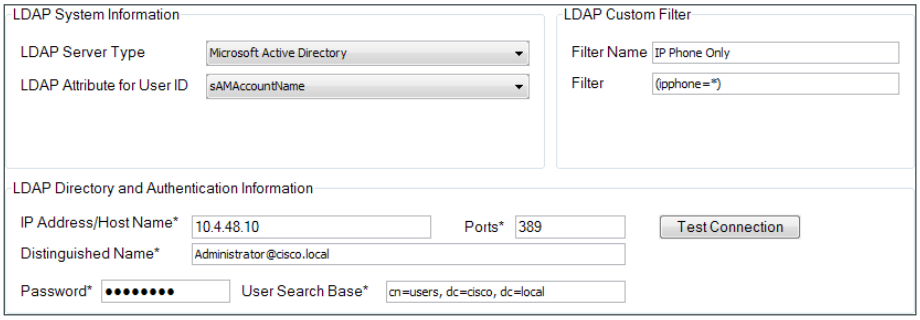
- Filter Name–**IP Phones Only**
- Filter–**(ipphone=*)**

In this example, an LDAP filter is created that limits the selection of users to the entries that contain information in the ipphone field. If the ipphone field is blank, the user is not synchronized.

Step 11: In the LDAP Directory and Authentication Information section, enter the following information:

- IP Address/Host Name–**10.4.48.10**
- Port–**389**
- Distinguished Name–**Administrator@cisco.local**
- Password–**[password]**
- User Search Base–**cn=users, dc=cisco, dc=local**

Step 12: Click **Test Connection.** This verifies connectivity to the LDAP server and confirms the credentials entered are valid. On the Connection Test page, click **OK**.



Step 13: If the LDAP server information is correct, click **Next**.

If it is not correct, fix the information, and then repeat Step 12 and Step 13.

Tech Tip

If configured, the phone number field populates the user's telephone number field in the Cisco Unified CM directory. This field is synchronized from Active Directory from either the ipPhone attribute or the telephoneNumber attribute, whichever is selected.

Typically, the telephoneNumber attribute contains the user's E.164-formatted number and the ipPhone attribute contains the user's extension. It is recommended to use the ipPhone attribute, provided that it is configured with the user's correct extension.

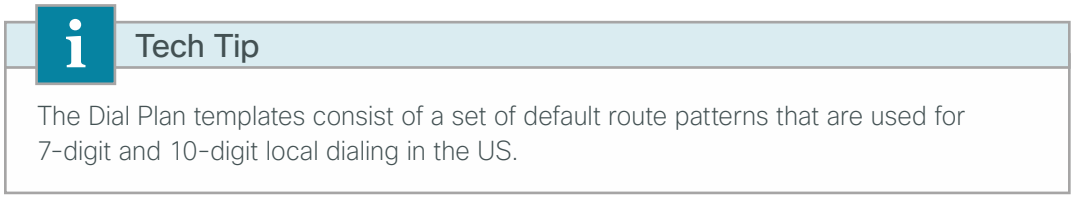
Step 14: On the Field Mapping Information page, choose the following options, and then click **Next**:

- Phone Number—**ipPhone**
- Mail ID—**mail**
- Middle Name—**middleName**

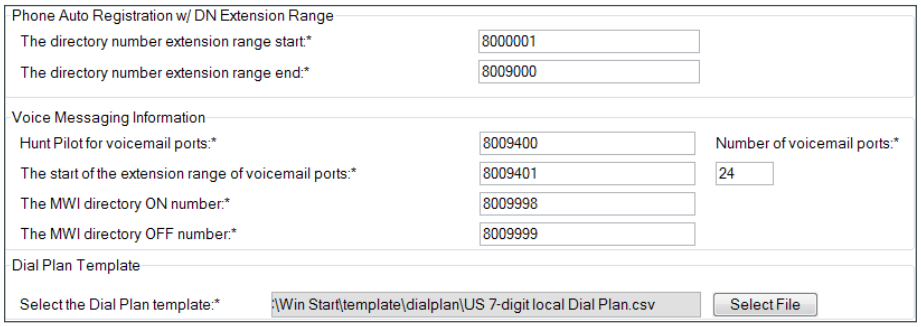
Unified CM User Fields	LDAP/CSV User Fields
User ID*	sAMAccountName
Phone Number*	ipPhone
Department	department
Mail ID	mail
First Name	First name
Middle Name	middleName
Last Name	Last name
Manager User ID	mananger

Step 15: On the Unified CM Dial-Plan page, enter the following information:

- Directory number extension range start–**8000001**
- Directory number extension range end–**8009000**
- Hunt Pilot for voicemail ports–**8009400**
- Start of the extension range of voicemail ports–**8009401**
- Number of voicemail ports–**24**
- MWI directory ON number–**8009998**
- MWI directory OFF number–**8009999**



Step 16: In the Dial Plan Template section, click **Select File**, choose the correct template for your installation, and then click **Next**. For example: **US 7-digit local Dial Plan.csv**.



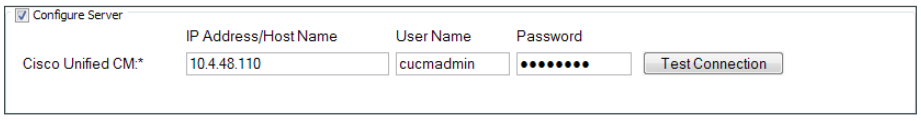
Step 17: The Summary Information page provides a summary of all inputs entered into CUCC up to this point. If the information shown is correct, click **Next**.

If any of the information shown is incorrect, click **Back**, and then correct it.

Step 18: On the Configuration Information page, if you want to update the Cisco Unified CM publisher in real-time, select **Configure Server**, and then enter the following information:

- IP Address/Host Name–**10.4.48.110** (publisher)
- User Name–**cucmadmin**
- Password–**[password]**

Step 19: Click **Test Connection**. This verifies connectivity to the Cisco Unified CM server and confirms the credentials entered are valid. On the Connection Test page, click **OK**.



Step 20: If you want to create a package file that you can use at a later date in order to update a Cisco Unified CM server, select **Export File**, and then click **Save As**.

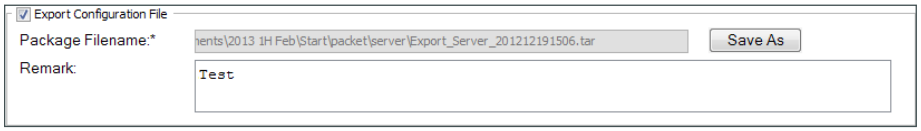
If you do not want to save a package file, skip to Step 23.

Step 21: On the Save dialog box, accept the default file name or enter a file name of your own choosing, and then click **Save**.

Step 22: Enter a **Remark**, which is then saved with the package file.

Tech Tip

The saved package file can be used at a later time to update a Cisco Unified CM server with the **Server Deployment > Modify UCM Server and Site** option of CUCC.



Step 23: If you want to create a gateway template for each voice gateway entered on the Site Information page, select **Gateway Template**, and then click **Save As**.

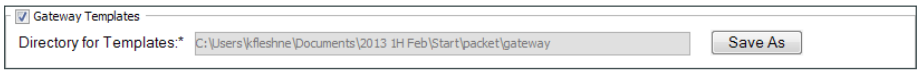
If you do not want to create gateway templates, skip to Step 25.

Step 24: On the Save dialog box, accept the default directory name or navigate to a new directory of your own choosing, and then click **Save**.

Tech Tip

The gateway template default directory is .\packet\gateway and they have a standard naming format of: SIP_[Site_Name]_GWY.txt. The files are generated with the site-specific information known to CUCC. However, they do not include the hardware and carrier-specific details about your individual voice gateway routers.

The template files are modified with your specific information and then copied into your voice gateway routers when following the procedures and steps in the "Configuring Conference Bridges, PSTN, Dial Peers, and SRST" process later in this guide.



Step 25: After choosing your configuration method from the options listed in the previous steps, click **Configure**.

Step 26: In the message window, click **Yes**.

CUCC displays its progress on the Update Information page and a log file called new_server.log with date/time stamps is created in the .\log directory. If you selected Gateway Templates, a log file called export_gateway.log is created in the same location.

CUCC updates approximately 2.5 sites and 5 gateways per minute. This means an installation with 50 sites and 100 gateways takes twenty minutes and an installation with 500 sites and 1000 gateways takes more than three hours to complete.

Please wait for the update to complete before proceeding.

Procedure 2 Synchronize the LDAP database

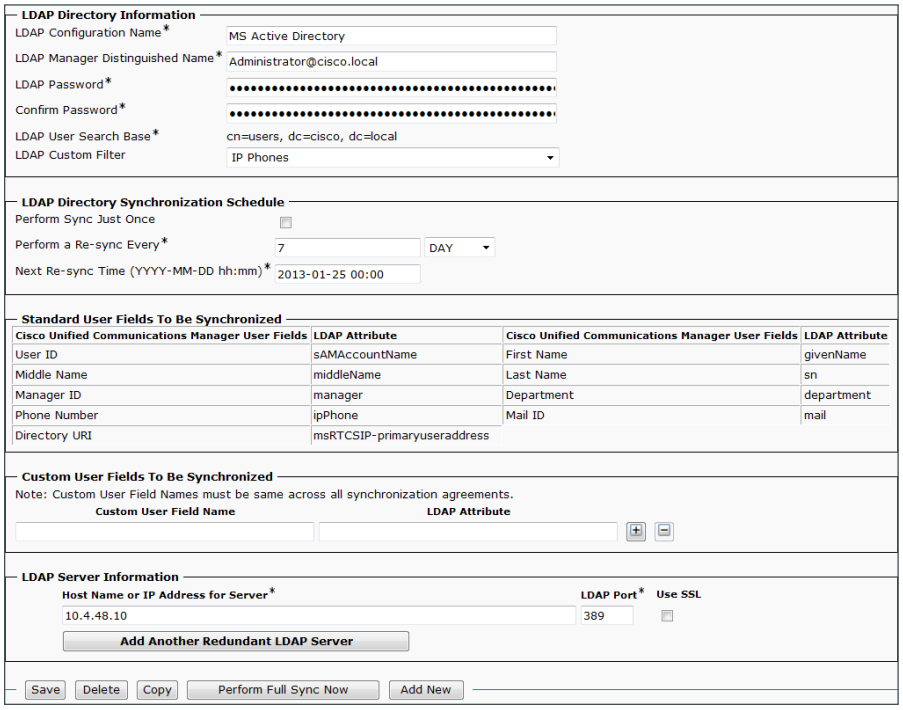
If you have chosen to update the Cisco Unified CM server and you are using LDAP, you must manually synchronize the LDAP database and perform several additional steps before the first phase of CUCC is complete.

If you are not using LDAP, please skip to Procedure 3 "Change host names to IP addresses."

Step 1: From the Cisco Unified CM administration page, navigate to **System > LDAP > LDAP Directory**, and then click **Find**.

Step 2: Click the name of LDAP directory that you created with CUCC (Example: MS Active Directory).

Step 3: Click **Perform Full Sync Now**, and then on the dialog box that appears, click **OK**. The user import process begins.



The Cisco Unified CM synchronization LDAP process reads approximately 200 users per minute. This means an installation with 1,000 users takes five minutes and an installation with 10,000 users takes more than fifty minutes to complete.

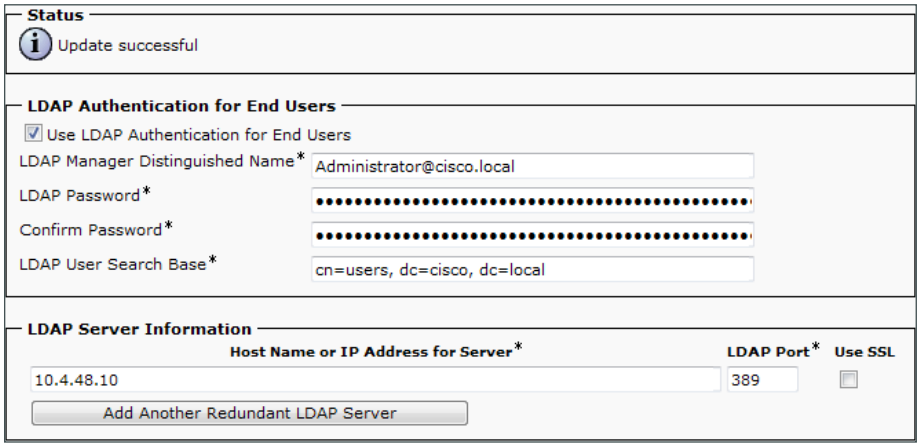
Please wait until the LDAP synchronization completes before continuing.

Step 4: To confirm the users have been synchronized, navigate to **User Management > End User**, and then click **Find**.

Verify the number of users equals the number you expect. If not, please repeat this step until the remaining users have been synchronized before continuing.

Step 5: Navigate to **System > LDAP > LDAP Authentication**, enter the following information, and then click **Save**:

- LDAP Password–**[password]**
- Confirm Password–**[password]**



Tech Tip

LDAP authentication is used for features such as Extension Mobility in order to validate the user credentials with the LDAP database.

Step 6: In the Status section, verify that the message "Update successful" appears. If not, enter the correct information on this page until the update is successful.

Procedure 3 Change host names to IP addresses

The next set of steps changes the Cisco Unified CM publisher, subscriber, and TFTP server host names to IP addresses, which removes the dependency on DNS for day-to-day operation of the phones.

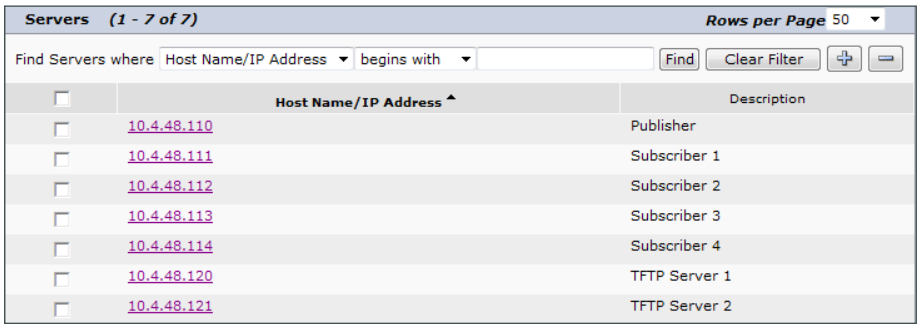
Step 1: Navigate to **System > Server**, and then click **Find**.

Step 2: Select **CUCM-Pub1**, change the **Host Name/IP Address** to **10.4.48.110** and the **Description** to **Publisher**, click **Save**, and on the dialog box that appears, click **OK**.

Step 3: In the **Related Links** list, choose **Back to Find/List**, and then click **Go**.

Step 4: Select **CUCM-Sub1**, change the **Host Name/IP Address** to **10.4.48.111** and the **Description** to **Subscriber 1**, click **Save**, and on the dialog box that appears, click **OK**.

Step 5: Repeat Step 3 and Step 4 for the rest of the subscriber and TFTP servers.



Step 6: Return to the CUCC program, click **Continue**, and then click **Finish**.

This completes the first phase of the CUCC program.

Procedure 4 Configure the Unity Connection server

After the running the first phase of CUCC, the next set of steps will continue the configuration of the Cisco Unity Connection server by using the administration interface.

Step 1: In a web browser, access the Cisco Unity Connection administration interface, and in the center of the page, under Installed Applications, click **Cisco Unity Connection**.

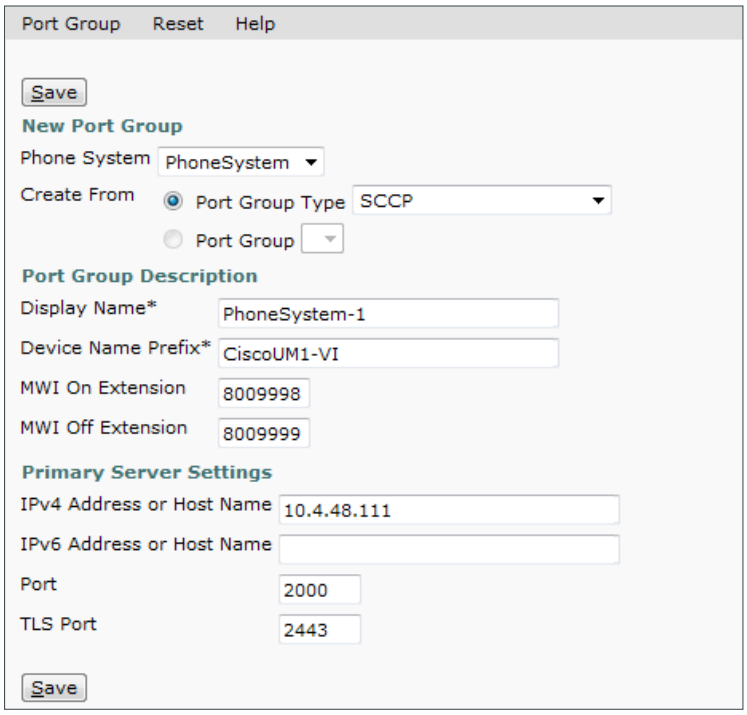
Step 2: Enter the application administrator **Username** and **Password**, and then click **Login**.

Step 3: In the left column, navigate to **Telephony Integrations > Phone System**, and then select **PhoneSystem**.

Step 4: At the top of the page, in the **Related Links** list, choose **Add Port Group**, and then click **Go**.

Step 5: On the New Port Group page, enter the following information, then click **Save**:

- Phone System–**PhoneSystem**
- Create From: Port Group Type–**SCCP**
- Display Name–**PhoneSystem-1**
- Device Name Prefix field–**CiscoUM1-VI**
- MWI On Extension–**8009998**
- MWI Off Extension–**8009999**
- IPv4 Address or Host Name–**10.4.48.111** (subscriber 1)



Step 6: From the top of the Port Group Basics page, navigate to **Edit > Servers**.

Step 7: In the Cisco Unified CM Servers section, click **Add**, and then enter the following information on the first row:

- Order–**0**
- IPv4 Address or Host Name–**10.4.48.111** (subscriber 1)

In the new second row, enter the following:

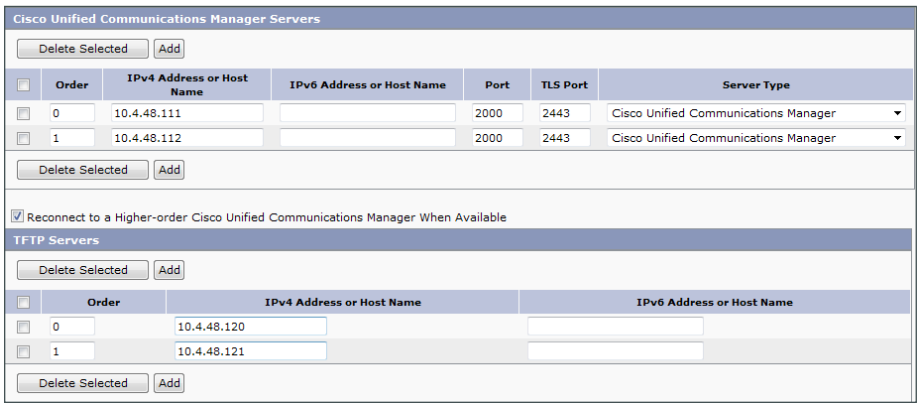
- Order–**1**
- IPv4 Address or Host Name–**10.4.48.112** (subscriber 2)

Step 8: In the TFTP Servers section, click **Add**, and then enter the following information in the first row:

- Order—**0**
- IP Address or Host Name—**10.4.48.120** (TFTP 1)

In the new second row, enter the following:

- Order—**1**
- IP Address or Host Name—**10.4.48.121** (TFTP 2)



Step 9: At the bottom of the page, click **Save**.

For the changes to take effect, you must restart the Connection Conversation Manager service.

Step 10: At the top of the page, in the **Navigation** list, choose **Cisco Unity Connection Serviceability**, and then click **Go**.

Step 11: Navigate to **Tools > Service Management**, under the Critical Services section, locate **Connection Conversation Manager**, and then click **Stop**.

Step 12: On the dialog box, click **OK**.

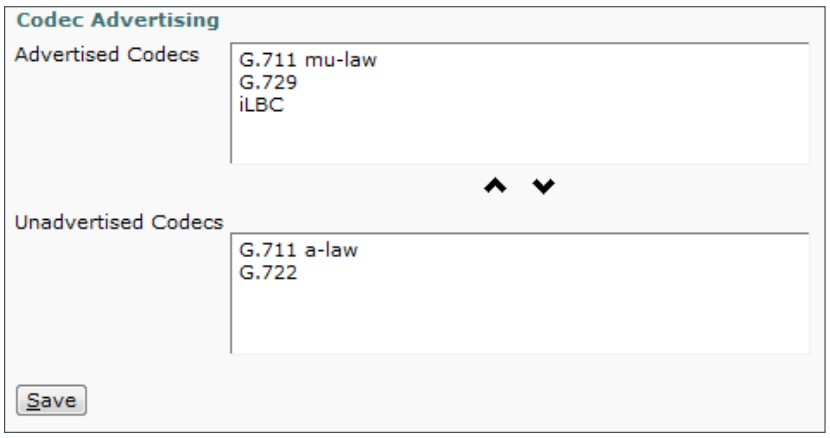
Step 13: After the page refreshes, locate **Connection Conversation Manager**, and then click **Start**.

Step 14: Wait several minutes, and then at the top of the page, click **Refresh**. Confirm the **Service Status** has changed from **Service in Transition** to **Started**.

Step 15: At the top of the page, in the **Navigation** list, choose **Cisco Unity Connection Administration**, and then click **Go**.

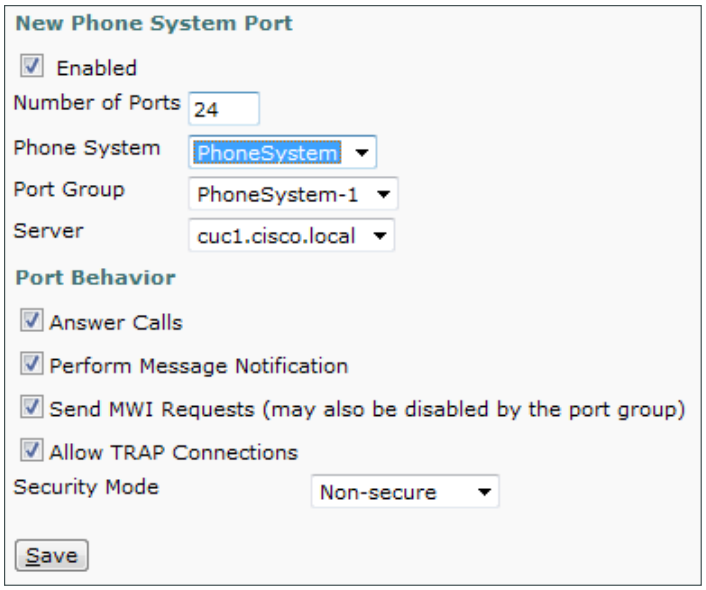
Step 16: On the left side of the page, navigate to **Telephony Integrations > Port Group**, and then select **PhoneSystem-1**.

Step 17: At the top of the page, navigate to **Edit > Codec Advertising**, use **^** to move **iLBC** from the **Unadvertised Codecs** list to the **Advertised Codecs** list, and then click **Save**.



Step 18: Navigate to **Telephony Integrations > Port**, and then click **Add New**.

Step 19: In **Number of Ports**, enter the licensed ports, and then click **Save**.

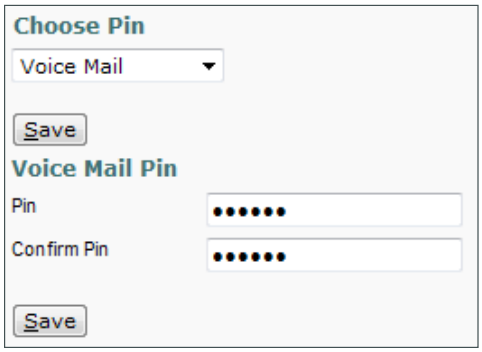


Step 20: Navigate to **Telephony Integrations > Port Group**, and then select **PhoneSystem-1**.

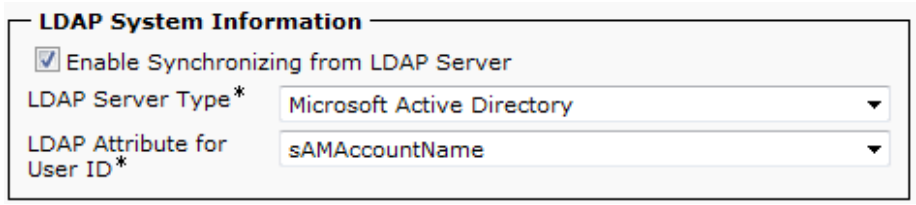
Step 21: If **Reset Status** shows **Reset Required**, click **Reset**.

Step 22: Navigate to **Templates > User Templates**, and then select the **voicemailusertemplate** template.

Step 23: From the top of the page, navigate to **Edit > Change Password**, and then in the **Choose Pin** list, choose **Voice Mail**. In **Pin** and **Confirm Pin**, enter a default PIN of at least six numeric characters for accessing voicemail from a telephone, and then click **Save**.



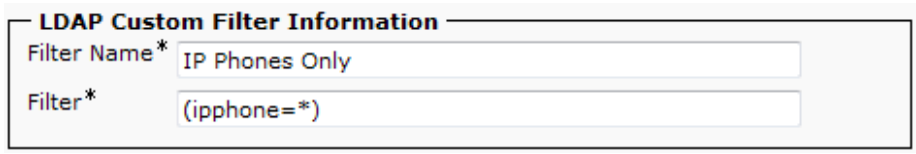
Step 24: Navigate to **System Settings > LDAP > LDAP Setup**, select **Enable Synchronizing from LDAP Server**, and then click **Save**.



Step 25: Navigate to **System Settings > LDAP > LDAP Custom Filter**, and then click **Add New.**

Step 26: On the LDAP Filter Configuration page, enter the following values, and then click **Save**:

- Filter Name—**IP Phones Only**
- Filter—**(ipphone=*)**



Step 27: Navigate to **System Settings > LDAP > LDAP Directory Configuration**, and then click **Add New**.

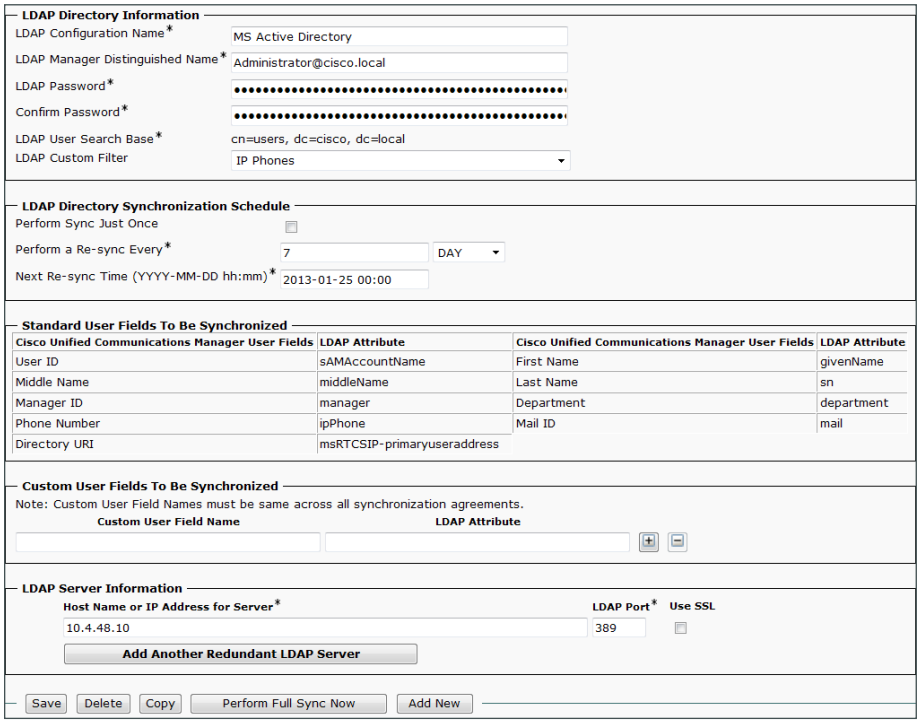
Step 28: From the LDAP Directory Configuration page, enter the following information, and then click **Save**:

- LDAP Configuration Name–**MS Active Directory**
- LDAP Manager Distinguished Name–**Administrator@cisco.local**
- LDAP Password–**[password]**
- Confirm Password–**[password]**
- LDAP User Search Base–**cn=users, dc=cisco, dc=local**
- LDAP Custom Filter–**IP Phones Only**
- Phone Number–**ipPhone**
- Host name or IP address for server of the LDAP server–**10.4.48.10**
- LDAP Port–**389**

Tech Tip

Ensure that the attribute selected from the **Phone Number** list matches the attribute selected from the **Phone Number** list inside CUCC.

This field is synchronized from Active Directory from either the ipPhone attribute or the telephoneNumber attribute, whichever is selected. Typically, the telephoneNumber attribute contains the user's E.164 formatted number and the ipPhone attribute contains the user's extension. It is recommended to use the ipPhone attribute, provided that it is configured with the user's correct extension.

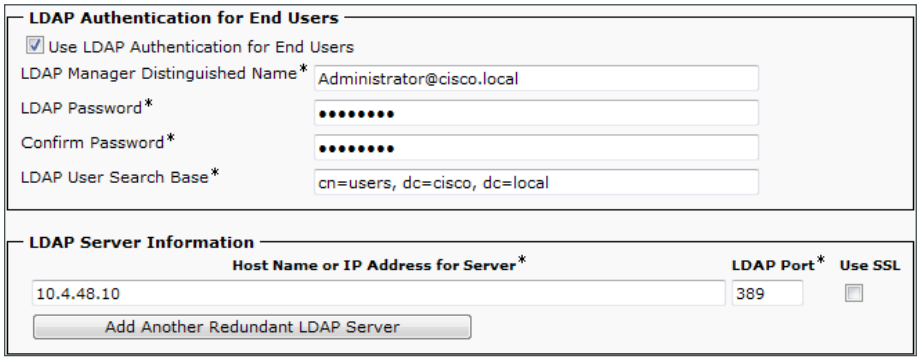


Step 29: After you have saved the information for the first time, a new set of buttons appears at the bottom of the page. Click **Perform Full Sync Now**, and then on the dialog box, click **OK**.

Step 30: Navigate to **System Settings > LDAP > LDAP Authentication**.

Step 31: Select **Use LDAP Authentication for End Users**, enter the following information, and then click **Save**:

- Use LDAP Authentication for End Users–**Select**
- LDAP Manager Distinguished Name–**Administrator@cisco.local**
- LDAP Password–**[password]**
- Confirm Password–**[password]**
- LDAP User Search Base–**cn=users, dc=cisco, dc=local**
- Host name or IP address for server of the LDAP server–**10.4.48.10**
- LDAP Port–**389**



Step 32: Navigate to **Users > Import Users**.

Step 33: In the **Find End Users In** list, choose **LDAP Directory**, and then click **Find**.

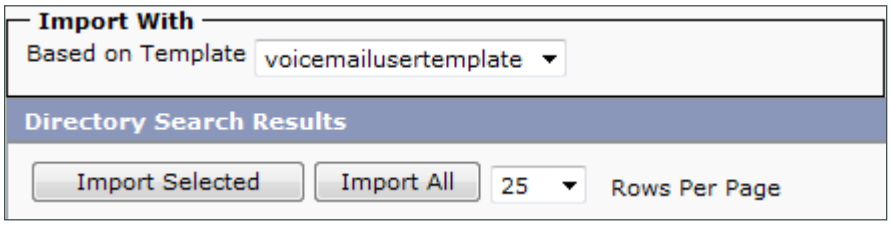
The Cisco Unity Connection LDAP synchronization process reads approximately 500 users per minute. This means an installation with 1,000 users takes two minutes and an installation with 10,000 users takes twenty minutes to complete.

In order to correctly import all of the LDAP users, you must wait for the sync to complete before continuing with the next steps in this procedure.

Step 34: In the Based on Template list, choose **voicemailusertemplate**.

Step 35: If you created an LDAP custom filter in order to limit your selection, click **Import All**, and then in the message box, click **OK**.

If you have not used an LDAP custom filter, select the users that require a voice messaging mailbox, and then click **Import Selected**.



Step 36: In the status box that appears at the top of the page, ensure that all users are imported successfully and there are no failures.

Cisco Unity Connection imports approximately 60 users per minute. This means an installation with 1,000 users takes seventeen minutes and an installation with 10,000 users takes almost three hours to complete.

Please wait for the update to complete before proceeding.

PROCESS

Configuring Users, Device Profiles, and IP Phones

1. Configure user and device profiles
2. Deploy IP phones

After the Cisco Unified CM and Cisco Unity Connection servers are configured, the next set of steps updates the users with Unified CM specific information and creates their user device profiles for extension mobility. Since the users have already been synchronized with LDAP, you will use the Modify section of the CUCC tool in order to update their information.

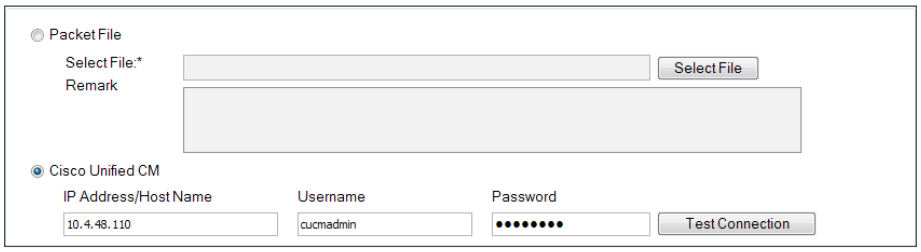
After updating the users and device profiles, the IP phones must have extension mobility enabled. They will also be updated with the correct home device pool and calling search space for their specific location. To log in to the phone, the users will enter their LDAP User ID and the default PIN of '112233'.

Procedure 1 Configure user and device profiles

Step 1: On the CUCC main page, navigate to **Server Deployment > Modify CUCM and CUC Users and Device Profiles**.

Step 2: On the Data Source page, select **Cisco Unified CM**, and then enter the following information:

- IP Address–**10.4.48.110** (publisher)
- Username–**cucmadmin**
- Password–**[password]**



Step 3: Click **Test Connection**. This verifies connectivity to the Cisco Unified CM server and confirms the credentials entered are valid. On the Connection Test page, click **OK**.

Step 4: If the test is successful, click **Next**.

If the test is not successful, repeat Step 2 with the correct information.

After CUCC is done reading the user information from Cisco Unified CM, the first five users are displayed. The first three columns are auto-generated from the source data, and the information they contain cannot be changed.

Step 5: If you want to sort the users, click the heading of the different columns. The sorted column heading turns a light blue color, and a small arrow at the top indicates the direction of the sort.

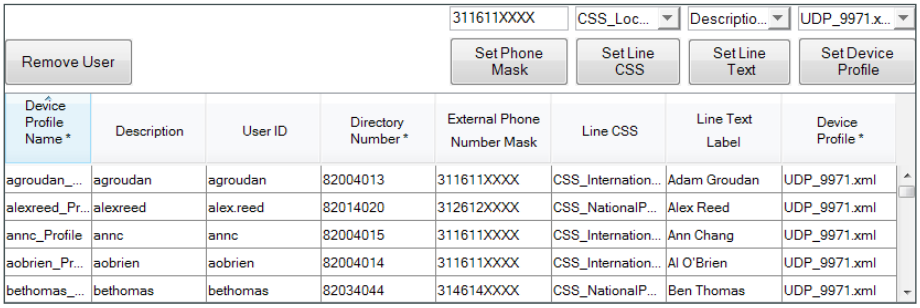
Step 6: Some user IDs that were exported may not need user device profiles. If you want to remove them from the list, select those **User IDs**, and then click **Remove Users**.

Tech Tip

Use the **<Shift>** key to select multiple users at one time or the **<Ctrl>** key to pick individual users from the list at any time during data entry.

Step 7: For each user device profile, populate the **Directory Number**, **External Phone Number Mask**, **Line CSS**, **Line Text Label** and **Device Profile** fields as follows, and then click **Next**:

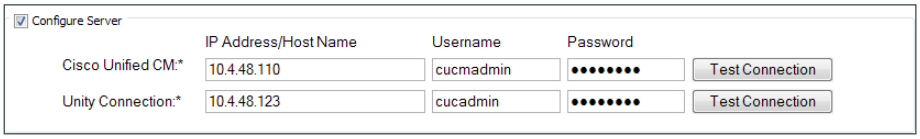
- **Directory Number**–This is the number that was synchronized from the ipPhone field in the LDAP directory. (Required)
- **External Phone Number Mask**–This value is used to create the direct inward-dialing number for the user or a main office number. This also appears on the black stripe at the top of the IP phone's display. Enter the phone number mask (for example, 311611XXXX) into the text box at the top of the column, and then click **Set Phone Mask**.
- **Line CSS**–This defines the class of restriction, or type of numbers, the user is allowed to call. The calling search spaces (CSS) defined during the import process is viewed in Cisco Unified CM Administration, under **Call Routing > Class of Control > Calling Search Space**. In the list at the top of the column, select the **Line CSS**, and then click **Set Line CSS**.
- **Line Text Label**–This is the label that is displayed on the phone. Although any alphanumeric string is allowed, it is recommended to use **FirstName, LastName**. In the list at the top of the column, select a text label format option, and then click **Set Line Text**.
- **Device Profile**–This is the device profile associated with the user device profile. In the list at the top of the column, select the device profile, and then click **Set Device Profile**. (Required)



Step 8: On the Configuration Information page, select **Configure Server**, and then enter the following information:

- Cisco Unified CM IP Address–**10.4.48.110** (publisher)
- Cisco Unified CM Username–**cucmadmin**
- Cisco Unified CM Password–**[password]**
- Cisco Unity Connection IP Address–**10.4.48.123**
- Cisco Unity Connection Username–**cucadmin**
- Cisco Unity Connection Password–**[password]**

Step 9: Next to each server, click **Test Connection**. This verifies connectivity to the servers and confirms the credentials entered are valid. On the Connection Test page, click **OK**.



Step 10: If you want to create a package file for the information entered, select **Export File**, and then click **Save As**.

If you do not want to create a package file, skip to Step 13.

Step 11: In the Save window, accept the default file name or enter a file name of your own choosing, and then click **Save**.

Step 12: Enter a **Remark**, which is then saved with the package file.

Step 13: After choosing your preferred method from the options in the steps above, click **Configure**.

Step 14: In the message window, click **Yes**.

Step 15: When the program is done updating users, click **Finish**.

The tool displays its progress on the Update Information page and a log file called modify_user.log with date/time stamps is created in the .\log directory.

CUCC updates approximately 850 users per hour. This means an installation with 1000 users will take seventy minutes and an installation with 10,000 users will take almost twelve hours to complete.

This completes the second phase of the CUCC program.

Procedure 2 Deploy IP phones

This procedure will enable extension mobility on the list of phones. It will also update the phones with the proper home device pool and default calling search space, based on their IP address in the network. The home device pool defines the Cisco Unified Communications Manager redundancy group, local route group, region, media resource group list, location, SRST reference, and physical location for each phone.

Within the network services layer, DHCP option 150 instructs the IP phones to connect to the Cisco Unified CM TFTP server for its initial configuration file and to auto-register with the default pair of Unified CM subscriber servers. Do not proceed with this procedure until all IP phones have registered.

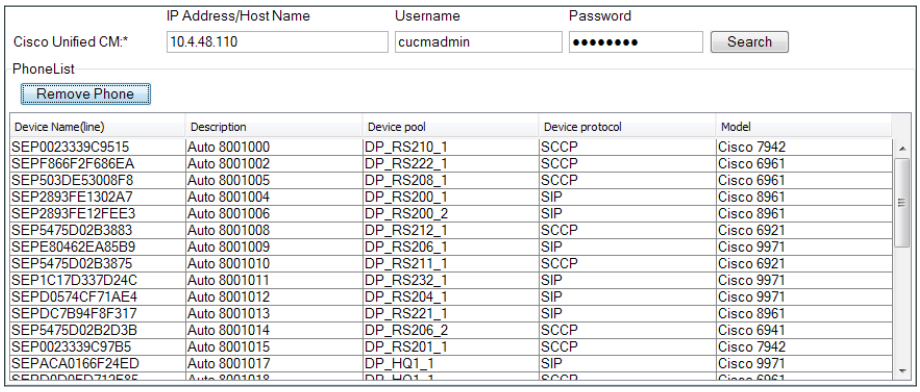
Step 1: Connect the IP phones to the network so they begin the automatic registration process. Depending on the size of your installation and the number of remote sites, this can take several hours to complete.

Please wait for the phones to register before continuing.

Step 2: From the CUCC main page, navigate to **Phone Deployment > Phone Deployment**, enter the following information, and then click **Search**:

- IP Address/Host Name–**10.4.48.110** (publisher)
- Username–**cucmadmin**
- Password–**[password]**

Step 3: If there are any phones that do not need to be updated, select them, and then click **Remove Phone**.



Step 4: After removing the unwanted phones, click **Configure**.

Step 5: In the message window, click **Yes**.

CUCC displays its progress in a blue message window and a log file called phone.log with date/time stamps is created in the .\log directory.

CUCC updates and restarts approximately 30 phones a minute. This means an installation with 1000 phones will take thirty-five minutes and an installation with 10,000 phones will take more than five hours to complete.

Please wait for the phone configuration to complete before continuing.

Step 6: In the message window at the end of the configuration step, click **OK**.

Step 7: Exit out of the CUCC program by clicking the **X** on the right side of the title bar. On the "Do you really want to quit" message, click **Yes**.

This completes the third phase of the CUCC program. Allow several minutes for the remaining phones to finish restarting with the Cisco Unified CM cluster.

After the users and IP phones are updated in Cisco Unified CM, the configuration of the gateways, conference bridges, public switched telephone network (PSTN) interfaces and Survivable Remote Site Telephony (SRST) services can begin.

PROCESS

Preparing a Standalone Voice Router for Services

1. Configure the standalone voice gateway
2. Configure Layer 2 connectivity to the LAN
3. Configure Layer 3 connectivity to the LAN

This process only applies to the deployment of a standalone voice router. If an existing WAN router is being used for voice services, please proceed to the next process, "Configuring Conference Bridges, PSTN, Dial Peers, and SRST."

Procedure 1 Configure the standalone voice gateway

This procedure only applies to standalone voice routers. If integrating voice services into an existing WAN router, skip ahead to the next process, "Configuring Conference Bridges, PSTN, Dial Peers, and SRST."

Within this design, there are features and services that are common across all standalone voice routers. These features and services simplify and secure the management of the solution.

As networks scale in the number of devices to maintain, it poses an operational burden to maintain local user accounts on every device. A centralized authentication, authorization and accounting (AAA) service reduces operational tasks per device and provides an audit log of user access, for security compliance and root cause analysis. When AAA is enabled for access control, AAA controls all management access to the network infrastructure devices (SSH and HTTPS).

Reader Tip

The AAA server used in this architecture is the Cisco Authentication Control System (ACS). For details about ACS configuration, see the Device Management Using ACS Design Guide.

Secure HTTP (HTTPS) and Secure Shell (SSH) Protocol are secure replacements for the HTTP and Telnet protocols. They use Secure Sockets Layer (SSL) and Transport Layer Security (TLS) in order to provide device authentication and data encryption.

Secure management of the network device is enabled through the use of the SSH and HTTPS protocols. Both protocols are encrypted for privacy, and the nonsecure protocols, Telnet and HTTP, are turned off.

IP Multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. Using IP Multicast is much more efficient than multiple individual unicast streams or a broadcast stream that would propagate everywhere. IP telephony Music on Hold and IP video broadcast streaming are two examples of IP Multicast applications.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an IGMP message to their local multicast router. In a traditional IP Multicast design, the local router consults another router in the network that is acting as a rendezvous point (RP) in order to map the receivers to active sources so they can join the multicast streams. In this design, which is based on sparse mode multicast operation, Auto RP is used to provide a simple yet scalable way to provide a highly resilient RP environment.

Step 1: Log in to the device with a username that has the ability to make configuration changes.

Step 2: Configure the device host name in order to make it easy to identify the device.

```
hostname [hostname]
```

Step 3: Enable password encryption.

```
username admin password [password]
enable secret [password]
service password-encryption
aaa new-model
```

Tech Tip

The local login account and password provides basic access authentication to a router, providing only limited operational privileges. The enable secret password secures access to the device configuration mode and prevents the disclosure of plain text passwords when viewing configuration files.

Step 4: If you are using AAA service to control management access, enable TACACS+ as the primary protocol on the infrastructure devices, and then define a local AAA user database on each network infrastructure device. This provides a fallback authentication source in case the centralized TACACS+ server is unavailable.

```
tacacs server TACACS-SERVER-1
 address ipv4 10.4.48.15
 key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
 server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa authorization console
ip http authentication aaa
```

Step 5: Specify the transport preferred none on vty lines in order to prevent errant connection attempts from the CLI prompt. Without this command, if the ip name-server is unreachable, long timeout delays may occur for mistyped commands.

```
ip domain-name cisco.local
ip ssh version 2
no ip http server
ip http secure-server
line vty 0 15
 transport input ssh
 transport preferred none
```

Step 6: When synchronous logging of unsolicited messages and debug output is turned on, console log messages are displayed on the console after interactive CLI output is displayed or printed. When you enable synchronous logging, you can continue typing at the device console when debugging is enabled.

```
line con 0
 logging synchronous
```

Step 7: Enable Simple Network Management Protocol (SNMP). This allows a Network Management System to manage the network infrastructure devices. SNMPv2c is configured both for a read-only and a read-write community string.

```
snmp-server community cisco RO
snmp-server community cisco123 RW
```

Step 8: If you use a network with centralized operation support and you want to increase network security by limiting the networks that can access the device, use an access list. In this example, only devices on the 10.4.48.0/24 network are able to access the device via SSH or SNMP.

```
access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
 access-class 55 in
!
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
```

Tech Tip

If you configure an access-list on the vty interface, you may lose the ability to use SSH to log in from one router to the next for hop-by-hop troubleshooting.

Step 9: Program network devices to synchronize to a local NTP server in the network, and then configure console messages, logs, and debug output to provide time stamps on output.

```
ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Tech Tip

The Network Time Protocol (NTP) is designed to synchronize a network of devices. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the organization's network. The local NTP server typically references a more accurate clock feed from an outside source.

Step 10: Enable IP Multicast routing on the platforms in the global configuration mode.

```
ip multicast-routing
```

Step 11: Configure every Layer 3 switch and router to discover the IP Multicast RP with autorp. This configuration provides for future scaling and control of the IP Multicast environment and can change based on network needs and design.

```
ip pim autorp listener
```

Step 12: Enable all Layer 3 interfaces in the network for sparse mode multicast operation.

```
ip pim sparse-mode
```

Procedure 2 Configure Layer 2 connectivity to the LAN

This procedure only applies to standalone voice routers. If you are integrating voice services into an existing WAN router, advance to the next process, "Configuring Conference Bridges, PSTN, Dial Peers, and SRST."

This procedure describes four different options for connecting your standalone voice router to the LAN:

1. EtherChannel to Cisco Nexus switches in the data center
2. EtherChannel to a Cisco Catalyst switch in the server room or remote-site distribution layer
3. EtherChannel to a Cisco Catalyst switch in the remote-site access layer
4. Single link to a Cisco Catalyst switch in the remote-site access layer

Layer 3 EtherChannels are used to interconnect the voice routers to the access or distribution layers in the most resilient method possible. If your voice router is deployed at a location with no distribution layer and you are using a non-stacked access layer, a single Layer 3 link will be used. In the case of connecting to a Nexus switch, this guide assumes the use of Enhanced virtual Port Channel (EvPC).

Please choose the option that is appropriate for your installation.

Option 1: EtherChannel from the voice router to the Cisco Nexus data center switches

The physical interfaces that are members of an EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order reduces errors because most of the commands entered to a port-channel interface are copied to its members interfaces and do not require manual replication.

Tech Tip

This example outlines the steps to configure a port channel between two dual-homed Cisco Nexus 2248TP-Es switch connected to two Cisco Nexus 5548UP switches by using EvPC. Step 3 and Step 4 are repeated on both Nexus 5548UP switches in order to ensure connectivity to the voice router.

Step 1: Configure the port-channel interface on the router.

```
interface Port-channel 1
 description EtherChannel link to DC5548UP
 no shutdown
```

Step 2: Configure the physical interfaces to tie to the logical port-channel by using the channel-group command. The number for the port-channel and channel-group must match. Not all router platforms can support Link Aggregation Control Protocol (LACP) in order to negotiate with the switch, so EtherChannel is configured statically.

```
interface GigabitEthernet 0/0
 description DC2248TP-E Eth106/1/5
interface GigabitEthernet 0/1
 description DC2248TP-E Eth107/1/5
interface range GigabitEthernet 0/0, GigabitEthernet 0/1
 channel-group 1
 no shutdown
```

Step 3: Connect the router EtherChannel uplinks to separate dual-homed Cisco Nexus Fabric Extenders in the data center, and then configure two physical interfaces to be members of the EtherChannel. Not all connected router platforms can support LACP to negotiate with the switch, so EtherChannel is configured statically.

```
interface Ethernet 106/1/5
 description HQ-3945-VG1 Gig0/0
interface Ethernet 107/1/5
 description HQ-3935-VG1 Gig0/1
interface Ethernet 106/1/5, Ethernet 107/1/5
 channel-group 70
```

Step 4: Define this port as a spanning tree edge in order to allow the voice router to bypass the wait times associated with spanning tree convergence. For simplicity, the voice gateway is placed in the same VLAN as Cisco Unified Communications Manager.

```
interface port-channel 70
 spanning-tree port type edge
 switchport access vlan 148
```

Option 2: EtherChannel from the voice router to the Cisco Catalyst server room or remote-site distribution switch

Step 1: Configure the port-channel interface on the router.

```
interface Port-channel 20
 description EtherChannel link to RS200-D3750X
 no shutdown
```

Step 2: Configure the EtherChannel member interfaces on the router.

```
interface GigabitEthernet 0/0
 description RS200-D3750X Gig1/0/18
interface GigabitEthernet 0/1
 description RS200-D3750X Gig2/0/18
interface range GigabitEthernet 0/0, GigabitEthernet 0/1
 channel-group 20
 no shutdown
```

Step 3: Configure the EtherChannel member interfaces on the Cisco Catalyst switch.

```
interface GigabitEthernet 1/0/18
 description RS200-3925-VG Gig0/0
interface GigabitEthernet 2/0/18
 description RS200-3925-VG Gig0/1
interface range GigabitEthernet 1/0/18, GigabitEthernet 2/0/18
 macro apply EgressQoS
 channel-group 20 mode on
 logging event link-status
 logging event bundle-status
```

Step 4: Configure the port-channel interface on the Cisco Catalyst switch.

```
interface Port-channel 20
 description EtherChannel link to RS200-3925-VG
 switchport access vlan 106
 switchport mode access
 spanning-tree portfast
 logging event link-status
```

Option 3: EtherChannel from the voice router to the remote-site access switch

Step 1: Configure the port-channel interface on the router.

```
interface Port-channel 3
 description EtherChannel link to RS203-A3750X
 no shutdown
```

Step 2: Configure the EtherChannel member interfaces on the router.

```
interface GigabitEthernet 0/0
 description RS203-A3750X Gig1/0/20
interface GigabitEthernet 0/1
 description RS203-A3750X Gig2/0/20
interface range GigabitEthernet 0/0, GigabitEthernet 0/1
 channel-group 20
 no shutdown
```

Step 3: Clear the EtherChannel member interfaces' configuration on the access switch.

```
default interface range GigabitEthernet 1/0/20, GigabitEthernet 2/0/20
```

Step 4: Configure the EtherChannel member interfaces on the access switch.

```
interface GigabitEthernet 1/0/20
 description RS203-2921-VG Gig0/0
interface GigabitEthernet 2/0/20
 description RS203-2921-VG Gig0/1
interface range GigabitEthernet 1/0/20, GigabitEthernet 2/0/20
 macro apply EgressQoS
 channel-group 3 mode on
 logging event link-status
 logging event bundle-status
```

Step 5: Configure the port-channel interface on the access switch.

```
interface Port-channel 3
 description EtherChannel link to RS203-2921-VG
 switchport access vlan 64
 switchport mode access
 ip arp inspection trust
 spanning-tree portfast
 logging event link-status
```

Option 4: Single link from the voice router to the remote-site access switch

Step 1: Configure the interface on the on the router.

```
interface GigabitEthernet 0/0
 description RS213-A3560X Gig0/20
 no shutdown
```

Step 2: Clear the interface's configuration on the access switch.

```
default interface GigabitEthernet 0/20
```

Step 3: Configure the interface on the access switch.

```
interface GigabitEthernet 0/20
 switchport access vlan 64
 switchport host
 ip arp inspection trust
 macro apply EgressQoS
 logging event link-status
```

Procedure 3 Configure Layer 3 connectivity to the LAN

This procedure only applies to standalone voice routers. If integrating voice services into an existing WAN router, skip ahead to the next process, "Configuring Conference Bridges, PSTN, Dial Peers, and SRST."

This procedure describes configuration of Layer 3 connectivity for the standalone voice router.

Step 1: Configure the IP address on voice router.

```
interface [type][number]
 ip address [LAN network] [LAN network netmask]
 ip pim sparse-mode
```

Step 2: Configure the IP default gateway on voice router.

```
ip route 0.0.0.0 0.0.0.0 [default gateway]
```

PROCESS

Configuring Conference Bridges, PSTN, Dial Peers, and SRST

1. Configure conference bridges
2. Configure the PSTN interface
3. Configure IOS dial-peers for VoIP
4. Configure IOS dial-peers for POTS
5. Configure SRST for SCCP phones
6. Configure SRST for SIP phones
7. Block voice traffic on WAN links

The procedures in this process are required for all voice routers.

If you chose to create the gateway templates in the first phase of the CUCC tool, the files must be modified for your hardware interfaces, server IP address and carrier parameters before you copy them into the voice gateway routers. Unless the location was changed by the user, the individual gateway files are located in the .\packet\ gateway directory using a naming format of: SIP_[Site_Name]_GWY.txt. Please follow the steps in this process to understand what site-specific information is required in each section of the gateway template files.

Procedure 1 Configure conference bridges

All routers need a minimum of a packet voice digital signal processor (DSP) module (PVDM3-64) in order to create five 8-party conference bridge resources along with the DSPs needed for voice gateway services. If your organization needs more gateway or conference resources, you will need additional DSPs. The router requires additional DSPs and configuration if hardware-based transcoding is needed. By default, calls to Cisco Unity Connection are transcoded in the server.

The router at the main site can provide unified communications gateway functions. Therefore, it should be configured with sufficient DSPs and a T1/E1 voice/WAN interface card (VWIC) for the PSTN primary rate interface (PRI) configurations.

The Cisco 3945 and 3925 Integrated Services Routers with voice security (VSEC) ship with a PVDM3-64, so they have enough DSPs to handle one voice T1 and five 8-party conferences. If the remote site uses E1, they will have enough DSPs for only four 8-party conferences. The Cisco 2911 Integrated Services Router (ISR) with VSEC ships with a PVDM3-16, and the 2921 ISR with VSEC and 2951 ISR with VSEC ship with a PVDM3-32. The Cisco 2900 Series ISRs have to be upgraded to a single PVDM3-64 DSP in order to allow sufficient resources for a single voice T1 and at least five 8-party conferences.

Apply the following configuration in the HQ router in order to register the five conference-bridge resources as the highest priority on the primary subscriber and as the second priority on the backup subscriber. The same configuration is used in the remote-site routers if conferencing resources are needed.

Tech Tip

The IOS commands are listed under the **Conference Bridge** section in the template file for each voice gateway.

The hardware and IP address-specific information in square brackets must be modified in the gateway template file before the commands can be successfully copied into the router. Use the examples in this section to help you understand what is needed in each area of the configuration.

Step 1: Configure the DSP services on the voice card.

```
voice-card 0
  dspfarm
  dsp services dspfarm
```

Step 2: Configure the dspfarm profile for a conference bridge with a maximum of **5** sessions and a list of the acceptable codecs.

```
dspfarm profile 1 conference
  description HQ Conference Bridges
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  codec g729r8
  codec g729br8
  codec g722-64
  codec ilbc
  maximum sessions 5
  associate application SCCP
  no shutdown
```

Step 3: Configure which interface is used to register to the Cisco Unified CM. If you are adding voice configuration to an existing router, use the Loopback 0 interface.

```
ccm-manager sccp local loopback 0
```

If you are using a standalone voice router, use the interface connecting to the LAN.

```
ccm-manager sccp local [interface type][number]
```

Step 4: Configure the SCCP gateway interface to connect to the Cisco Unified CM servers used for subscription. If a large number of conference bridges are implemented, the priority of the subscriptions should be balanced appropriately by alternating the IP addresses of the Unified CM subscribers in the cluster. Set the version to 7.0 and above.

```
sccp local [interface type][number]
sccp ccm 10.4.48.111 identifier 1 priority 1 version 7.0
sccp ccm 10.4.48.112 identifier 2 priority 2 version 7.0
sccp ccm 10.4.48.113 identifier 3 priority 3 version 7.0
sccp ccm 10.4.48.114 identifier 4 priority 4 version 7.0
sccp
```

Step 5: Bind the interface for the conference bridge to the one used by the SCCP applications. Group the servers created in Step 4 and associate them with the profile for the conference bridge. Again if a large number of conference bridges are implemented, the priority should be balanced appropriately. Register the conference bridge with Cisco Unified CM, set the switchback method to graceful, and then wait 60 seconds.

```
sccp ccm group 1
  bind interface [interface type][number]
  associate ccm 1 priority 1
  associate ccm 2 priority 2
  associate ccm 3 priority 3
  associate ccm 4 priority 4
  associate profile 1 register CFB1HQ1
  switchback method graceful
  switchback interval 60
```

Tech Tip

The Cisco Unified CM configuration for the conference bridge was completed with CUCC, so the registration name must match the name uploaded into the cluster by the tool. The names are always CFB1<*Site Name*> and CFB2<*Site name*>, if there are two. For example, if the headquarters site is HQ1, the conference bridge names are CFB1HQ1 and CFB2HQ1.

Procedure 2 Configure the PSTN interface

The PSTN interface card is specific to your carrier, and it must be added to the router configuration. At the headquarters site, this is very likely a T1 or E1 PRI interface. The recommended T1/E1 PRI voice interface card for the Cisco ISR routers is the VWIC3-2MFT-T1/E1.

Whichever PSTN interface option you choose for your locations, SIP is the recommended signaling protocol to connect the gateway to Cisco Unified CM at the headquarters and remote sites. SIP provides a common dial-plan configuration when a site is connected to Unified CM and in a fail-over scenario when the servers cannot be reached.

Tech Tip

The IOS commands are listed under the **PSTN Interface** section in the template file for each voice gateway.

The hardware-specific information in square brackets must be modified in the gateway template file before the commands can be successfully copied into the router. Use the examples in this section to help you understand what is needed in each area of the configuration.

Step 1: Using the voice interface card recommended above, configure the card type in the global configuration section.

```
card type t1 0 0
```

Step 2: Configure the global ISDN switch type for this router.

```
isdn switch-type primary-ni
```

Step 3: Bind the control and media interface for SIP. If you are adding voice configuration to an existing router, use the Loopback 0 interface.

```
voice service voip
  sip
    bind control source-interface loopback 0
    bind media source-interface loopback 0
```

If you are using a standalone voice router, use the interface connecting to the LAN.

```
voice service voip
  sip
    bind control source-interface [interface type][number]
    bind media source-interface [interface type][number]
```

Step 4: Create the list of voice codecs supported in the VoIP dial-peers.

```
voice class codec 1
  codec preference 1 g711ulaw
  codec preference 2 g711alaw
  codec preference 3 g729r8
  codec preference 4 ilbc
```

Step 5: Enable each VWIC to use the network for clock timing.

```
network-clock-participate wic 0
```

Step 6: Enable the PRI group on each T1 which you further configure in the next step.

```
controller T1 0/0/0
  Description PSTN PRI
  cablelength short 110
  pri-group timeslots 1-24
  no shutdown
```

Step 7: After enabling each T1 controller to support PRI, configure the newly created serial interface or interfaces with the correct ISDN switch type, and then enable voice.

```
interface Serial0/0/0:23
  no ip address
  encapsulation hdlc
  isdn switch-type primary-ni
  isdn incoming-voice voice
  no cdp enable
  no shutdown
```

Procedure 3 Configure IOS dial-peers for VoIP

This procedure creates the SIP dial peers for inbound calls from the PSTN to the Cisco Unified CM subscribers.

The following is an example for a North American, SIP gateway configuration for the headquarters site. The PSTN provider is sending 10 digits on inbound calls for each site. In some locations, the carrier will send four or seven digits, and the destination patterns for the SIP Trunk to Cisco Unified CM VoIP dial-peers will have to be modified to correctly match the incoming digits. The remote-site gateways are similar; with the exception of the destination patterns of some dial peers and the interface where the gateway control and media is bound.

Tech Tip

The IOS commands are listed under the **Dial Peers - VoIP** section in the template file for each voice gateway.

The carrier and IP address-specific information in square brackets must be modified in the gateway template file before the commands can be successfully copied into the router. Use the examples in this section to help you understand what is needed in each area of the configuration.

Step 1: Create the SIP dial peers for inbound calls destined for Cisco Unified CM. Configure dial peers for each subscriber in the cluster. Prioritize the dial peers to maintain an appropriate balance across all gateways. In the preferred order, include the codecs specified in Step 4 of the previous procedure. The destination pattern matches the ten digits coming in from the PSTN provider.

```
dial-peer voice 100 voip
  description SIP TRUNK to CUCM-Sub1
  preference 1
  destination-pattern 310610....
  voice-class codec 1
  session protocol sipv2
  session target ipv4:10.4.48.111
  incoming called-number .
!
dial-peer voice 101 voip
  description SIP TRUNK to CUCM-Sub2
  preference 2
  destination-pattern 310610....
  voice-class codec 1
  session protocol sipv2
  session target ipv4:10.4.48.112
  incoming called-number .
!
dial-peer voice 102 voip
  description SIP TRUNK to CUCM-Sub3
  preference 3
  destination-pattern 310610....
  voice-class codec 1
  session protocol sipv2
  session target ipv4:10.4.48.113
  incoming called-number .
!
dial-peer voice 103 voip
  description SIP TRUNK to CUCM-Sub4
  preference 4
  destination-pattern 310610....
  voice-class codec 1
  session protocol sipv2
  session target ipv4:10.4.48.114
  incoming called-number .
```

Toll fraud prevention is enabled by default in the version of Cisco IOS used for this configuration. The four VoIP dial-peer commands listed above permit call signaling from the Cisco Unified CM servers, but they prevent other call agents from contacting your gateways. Use the **show ip address trusted list** command in the router to view the trusted list.

Reader Tip

For more information about this topic, read the Toll Fraud Prevention Enhancement notes at the following URL: http://www.cisco.com/en/US/docs/ios/15_1/release/notes/151-2TNEWF.html#wp43627

Procedure 4 Configure IOS dial-peers for POTS

This procedure creates the basic telephone service (also known as *POTS*) dial peers for outbound emergency, local, national and international calls from Cisco Unified CM subscribers to the PSTN.

Tech Tip

The IOS commands are listed under the **Dial Peers - POTS** section in the template file for each voice gateway.

The hardware-specific information in square brackets must be modified in the gateway template file before the commands can be successfully copied into the router. Use the examples in this section to help you understand what is needed in each area of the configuration.

Step 1: Strip the leading 9, and only forward the digits that are expected by the carrier. For international dialing, which is variable in length, prefix the 011 needed by the long-distance carrier in order to properly route the call.

```
dial-peer voice 1911 pots
 description EMERGENCY
 preference 1
 destination-pattern 911
 port 0/0/0:23
 forward-digits 3
!
dial-peer voice 19911 pots
 description EMERGENCY WITH LEADING 9
 preference 1
 destination-pattern 9911
 port 0/0/0:23
 forward-digits 3
!
dial-peer voice 17 pots
 description LOCAL 7 DIGIT
 preference 1
 destination-pattern 9[2-9]......
 port 0/0/0:23
 forward-digits 7
!
dial-peer voice 111 pots
 description LONG DISTANCE 11 DIGIT
 preference 1
 destination-pattern 91[2-9]..[2-9]......
 port 0/0/0:23
 forward-digits 11
!
```

```
dial-peer voice 19011 pots
 description INTERNATIONAL VARIABLE LENGTH
 preference 1
 destination-pattern 9011T
 incoming called-number .
 direct-inward-dial
 port 0/0/0:23
 prefix 011
```

Step 2: Depending on the number of POTS circuits that are needed, multiple PSTN circuits may be required. In this case, additional dial peers are created to utilize these lines, and preferences are set to tell Cisco IOS which lines to use first.

If more than two circuits are used on a router, modify the 'dial-peer voice', 'preference', and 'port' fields in each group of commands. This example aligns the first numeral in the 'dial-peer voice' number with the 'preference' for that dial peer. The port field matches the physical interface of the additional PSTN circuit.

In the case below 'preference 2' is used so the dial peers become 'dial-peer voice 2**** pots'. This pattern can be extended to 'preference 3' and 'dial-peer voice 3**** pots' and so on if necessary. Also, remember to modify the 'port' configuration to the correct PSTN physical interface.

```
dial-peer voice 2911 pots
 description EMERGENCY
 preference 2
 destination-pattern 911
 port 0/0/1:23
 forward-digits 3
!
dial-peer voice 29911 pots
 description EMERGENCY WITH LEADING 9
 preference 2
 destination-pattern 9911
 port 0/0/1:23
 forward-digits 3
!
dial-peer voice 27 pots
 description LOCAL 7 DIGIT
 preference 2
 destination-pattern 9[2-9]......
 port 0/0/1:23
 forward-digits 7
!
dial-peer voice 211 pots
 description LONG DISTANCE 11 DIGIT
 preference 2
 destination-pattern 91[2-9]..[2-9]......
 port 0/0/1:23
 forward-digits 11
!
```

```
dial-peer voice 29011 pots
 description INTERNATIONAL VARIABLE LENGTH
 preference 2
 destination-pattern 9011T
 incoming called-number .
 direct-inward-dial
 port 0/0/1:23
 prefix 011
```

Procedure 5 Configure SRST for SCCP phones

The procedure will configure SRST for SCCP phones. If you are not using SCCP phones at remote sites, please skip this procedure.

SRST is a valuable feature to help you maintain the use of remote-site phones during an unexpected WAN outage at a remote location. The phones will register with the remote-site gateway when they cannot reach the central-site Cisco Unified CM servers. The SRST configuration in a router is customizable to a certain extent in order to allow the basic phone features to work in a similar fashion as they do on the central-site cluster. There are configuration steps for SCCP phones, and the next procedure contains a different group of steps for SIP phones. The two types of phones can coexist on the same SRST gateway as long as both sets of commands are entered.

An SRST feature license is required for all phones that will register with the router when it is in fallback mode. Each phone will consume one seat. SCCP and SIP phones can coexist on the same router by using the same feature license.

If sites codes are used for this installation, the **dialplan-pattern** command transforms the 10-digit E164 PSTN number into the unique 7-digit or 8-digit directory number on the phone. The **extension-length** and **extension-pattern** keywords in the SRST feature allow you to identify the last four digits of the E164 number. You create additional dial peers in order to maintain 7-digit or 8-digit dialing between sites with site codes.

For networks with 90 sites or less, the dial plan consists of the following:

- One digit as an inter-site access code
- Two digits for the site code to accommodate up to 90 sites
- Four digits for the site extension

The format is 8 + SS + XXXX, where 8 is the on-net access code, SS is a 2-digit site code from 10-99, and XXXX is a 4-digit extension number, giving a total of seven digits.

For networks with greater than 90 sites, the dial plan consists of the following:

- One digit as an inter-site access code
- Three digits for the site code to accommodate up to 900 sites
- Four digits for the site extension

The format is 8 + SSS + XXXX, where 8 is the on-net access code, SSS is a 3-digit site code of 100-999, and XXXX is a 4-digit extension number, giving a total of eight digits.

To allow the users to maintain 4-digit dialing between the phones at each remote site, a voice translation rule and profile are associated with incoming calls. The voice translation profile is only active when the phones are in SRST mode.

If sites codes are not used for this installation, the **dialplan-pattern** command transforms the 10-digit E164 PSTN number into the unique 4-digit directory number on the phone. The **extension-length** and **extension-pattern** keywords allow you to identify the last four digits of the E164 number. Voice translation rules and profiles are not needed for installations that do not use site codes.

Tech Tip

The IOS commands are listed under the **SRST voice translation commands** section in the template file for each voice gateway. These commands are only needed if site codes are used in your installation.

Step 1: If site codes are used, create a voice translation rule and a voice translation profile in the global area of the router. The first part of the translation rule—between the first set of forward slashes—matches a 4-digit number that starts with a 1 through 7. The second part of the rule—between the second set of forward slashes—prepends the unique site code to the 4-digit dialed number. The translation-profile called SRST-4-Digit applies the translation rule to the number called by the user. The example given is for 8-digit directory numbers starting with 8200.

```
voice translation-rule 1
 rule 1 /^[1-7]...$/ /8200\0/

voice translation-profile SRST-4-Digit
 translate called 1
```

Tech Tip

The IOS commands are listed under the **SRST for SCCP** section in the template file for each voice gateway.

The carrier and SRST license-specific information in square brackets must be modified in the gateway template file before the commands can be successfully copied into the router. Use the examples in this section to help you understand what is needed in each area of the configuration.

Step 2: Assign the SRST interface to the source address of the router closest to the phones using the default SCCP port of 2000. Allow 50 phones to register, and use dual-line support to allow transfers and conferencing. These are the four basic commands to enable SCCP SRST.

If you are integrating SRST features into a preexisting router, use the IP address of the gateway's Loopback 0 interface.

```
call-manager-fallback
  ip source-address 10.5.7.12 port 2000
  max-ephones 50
  max-dn 35 dual-line
```

Tech Tip

When the command **max-ephones 50** is executed, a license agreement appears. To activate this feature, you must accept the agreement. Be aware of this when copy and pasting or scripting the deployment of these features, as configuration cannot continue until this agreement is accepted.

Step 3: Enhance the user experience in SCCP fallback mode by adding a secondary dial tone when the number 9 is pressed, and then allow the user to perform a supervised transfer (full consultation). Configure eight 3-way conference calls for ad hoc conferencing.

```
secondary-dialtone 9
transfer-system full-consult
max-conferences 8 gain -6
```

Step 4: If site codes are used for this installation, translate the inbound number to the directory number for the phone. When a call arrives from the PSTN carrier, the call is directed to the correct phone, based on the access code, site code, and the last four digits. Apply the translation profile for incoming calls when phones are in SRST mode. The example given is for 3-digit site codes, 8-digit directory numbers, and 10-digit inbound numbers from the PSTN.

```
dialplan-pattern 1 311611.... extension-length 8 extension-pattern 8200....
translation-profile incoming SRST-4-Digit
```

If site codes are not used for this installation, configure the translated number to match the 4-digit directory number for the phone. When a call arrives from the PSTN carrier, the call is directed to the correct phone, based on the last four digits. The example given is for 4-digit directory numbers and 10-digit inbound numbers from the PSTN.

```
dialplan-pattern 1 311611.... extension-length 4 extension-pattern ....
```

Step 5: If site codes are used for this installation, add IOS POTS dial peers in order to maintain dialing between sites in SRST mode. The examples given are for 3-digit site codes, 8-digit directory numbers, and 11-digit outbound PSTN numbers.

Example: Headquarters Site

```
dial-peer voice 8100 pots
 description 8-DIGIT DIAL to HQ in SRST
 preference 1
 destination-pattern 8100....
 port 0/0/0:23
 prefix 1310610
```

Example: Remote Site 203

```
dial-peer voice 8203 pots
 description 8-DIGIT DIAL to RS203 in SRST
 preference 1
 destination-pattern 8203....
 port 0/0/0:23
 prefix 1314614
```

Repeat this step for each additional remote site. Use an appropriate dial-peer number, description, destination pattern, and prefix.

Procedure 6 Configure SRST for SIP phones

The procedure will configure SRST for SIP phones. If you are not using SIP phones at remote sites, please skip this section.

If sites codes are used for this installation, the **dialplan-pattern** command transforms the 10-digit E164 PSTN number into the unique 7-digit or 8-digit directory number on the phone. The **extension-length** and **extension-pattern** keywords allow you to identify the last four digits of the E164 number. You create additional dial peers in order to maintain 7-digit or 8-digit dialing between sites with site codes.

For networks with 90 sites or less, the dial plan consists of the following:

- One digit as an inter-site access code
- Two digits for the site code to accommodate up to 90 sites
- Four digits for the site extension

The format is 8 + SS + XXXX, where 8 is the on-net access code, SS is a 2-digit site code from 10-99, and XXXX is a 4-digit extension number, giving a total of seven digits.

For networks with greater than 90 sites, the dial plan consists of the following:

- One digit as an inter-site access code
- Three digits for the site code to accommodate up to 900 sites
- Four digits for the site extension

The format is 8 + SSS + XXXX, where 8 is the on-net access code, SSS is a 3-digit site code of 100-999, and XXXX is a 4-digit extension number, giving a total of eight digits.

To allow the users to maintain 4-digit dialing between the phones at each remote site, a voice translation rule and profile are associated with incoming calls. The voice translation profile is only active when the phones are in SRST mode.

If sites codes are not used for this installation, the **dialplan-pattern** command transforms the 10-digit E164 PSTN number into the unique 4-digit directory number on the phone. The **extension-length** and **extension-pattern** keywords allow you to identify the last four digits of the E164 number. Voice translation rules and profiles are not needed for installations that do not use site codes.

Tech Tip

The IOS commands are listed under the **SRST voice translation commands** section in the template file for each voice gateway. These commands are only needed if site codes are used in your installation.

Step 1: If site codes are used, create a voice translation rule and a voice translation profile in the global area of the router. The first part of the translation rule—between the first set of forward slashes—matches a 4-digit number that starts with a 1 through 7. The second part of the rule—between the second set of forward slashes—prepends the unique site code to the 4-digit dialed number. The translation-profile called SRST-4-Digit applies the translation rule to the number called by the user. The example given is for 8-digit directory numbers starting with 8200.

```
voice translation-rule 1
 rule 1 /^[1-7]...$/ /8200\0/

voice translation-profile SRST-4-Digit
 translate called 1
```

Tech Tip

The IOS commands are listed under the **SRST for SIP** section in the template file for each voice gateway.

The carrier, IP address and SRST license-specific information in square brackets must be modified in the gateway template file before the commands can be successfully copied into the router. Use the examples in this section to help you understand what is needed in each area of the configuration.

Step 2: Create the SIP back-to-back user agent and SIP registrar functionality. Change the SIP registrar expiration timer to 600 seconds.

```
voice service voip
 allow-connections sip to sip
 sip
  registrar server expires max 600 min 60
```

Step 3: Assign the following characteristics to SIP phones globally: the system message on the bottom of certain phones, the maximum directory numbers, and the maximum number of pools allowed on the SRST router.

```
voice register global
 system message "SIP SRST Service"
 max-dn 200
 max-pool 50
```

Tech Tip

When the command **max-pool 50** is executed, a license agreement appears. To activate this feature, you must accept the agreement. Be aware of this when copy and pasting or scripting the deployment of these features, as configuration cannot continue until this agreement is accepted.

Step 4: If site codes are used for this installation, translate the inbound number to the directory number for the phone. When a call arrives from the PSTN carrier, the call is directed to the correct phone, based on the access code, site code, and the last four digits. The example given is for 3-digit site codes, 8-digit directory numbers, and 10-digit inbound numbers from the PSTN.

```
dialplan-pattern 1 311611.... extension-length 8 extension-pattern 8200....
```

If site codes are not used for this installation, configure the translated number to match the 4-digit directory number for the phone. When a call arrives from the PSTN carrier, the call is directed to the correct phone, based on the last four digits. The example given is for 4-digit directory numbers and 10-digit inbound numbers from the PSTN.

```
dialplan-pattern 1 311611.... extension-length 4 extension-pattern ....
```

Step 5: If site codes are used for this installation, add IOS POTS dial peers in order to maintain dialing between sites in SRST mode. The examples given are for 3-digit site codes, 8-digit directory numbers, and 11-digit outbound PSTN numbers.

Example: Headquarters Site

```
dial-peer voice 8100 pots
 description 8-DIGIT DIAL to HQ in SRST
 preference 1
 destination-pattern 8100....
 port 0/0/0:23
 prefix 1310610
```

Example: Remote Site 203

```
dial-peer voice 8203 pots
 description 8-DIGIT DIAL to RS203 in SRST
 preference 1
 destination-pattern 8203....
 port 0/0/0:23
 prefix 1314614
```

Repeat this step for each additional remote site. Use an appropriate dial-peer number, description, destination pattern, and prefix.

Step 6: Configure the voice register pool for the defined IP address range. If your IP address ranges are not contiguous, you may create multiple pools. The id network is the IP subnet for the voice VLAN. Create a voice pool for each voice subnet implemented at the remote site. In this example, we are using two voice subnets. Use **rtp-nte sip-notify** for the **dtmf-relay** parameter, and use the G711 ulaw codec for all calls.

```
voice register pool  1
 id network 10.5.2.0 mask 255.255.255.0
 dtmf-relay rtp-nte sip-notify
 codec g711ulaw
```

Step 7: If site codes are used, apply the translation profile for incoming calls in each voice register pool.

```
 translation-profile incoming SRST-4-Digit
```

Step 8: Identify the IP address of the Cisco Unified CM subscriber 1 and subscriber 2 as the external registrars, using the default expiration of 3600 seconds that is defined in the cluster.

```
sip-ua
 registrar ipv4:10.4.48.111 expires 3600
 registrar ipv4:10.4.48.112 expires 3600 secondary
```

Procedure 7 Block voice traffic on WAN links

(Optional)

In some cases, an administrator may want to force IP phones into SRST mode when a failover to a backup WAN link occurs. Implementing this blocking avoids transmitting voice over a lossy link, and it decreases the cost of a failure by reducing data usage while maintaining the dial tone that end-users expect. This configuration can be applied to the backup router of a dual router design or to the secondary link of a single router design. This configuration can also be used on any WAN interface when centralized voice registrations are not wanted at a particular remote site.

Tech Tip

The IOS commands are listed under the **Optional - Block Voice on WAN** section in the template file for each voice gateway.

The hardware-specific information in square brackets must be modified in the gateway template file before the commands can be successfully copied into the router. Use the examples in this section to help you understand what is needed in each area of the configuration.

Step 1: Configure the access list that blocks SIP: 5060 (TCP/UDP), Secure SIP: 5061 (TCP/UDP), SCCP: 2000 (TCP), Secure SCCP: 2443 (TCP), standard RTP ports: 16384-32767 (UDP), and allow all other traffic.

```
ip access-list extended ACL-VOIP-CONTROL
 deny tcp any any eq 5060
 deny udp any any eq 5060
 deny tcp any any eq 5061
 deny udp any any eq 5061
 deny tcp any any eq 2000
 deny tcp any any eq 2443
 deny udp any any range 16384 32767
 permit ip any any
```

Step 2: Apply the access control list to the WAN interface to which the administrator wishes to block voice traffic.

```
interface Tunnel10
 ip access-group ACL-VOIP-CONTROL in
 ip access-group ACL-VOIP-CONTROL out
```

The Cisco Unified CM system installation is now complete.

Appendix A: Product List

Data Center or Server Room

Functional Area	Product Description	Part Numbers	Software
Virtual Servers	Cisco UCS C240 M3 C-Series Solution Pak for unified communications applications	UCUCS-EZ-C240M3S	9.1(1a) ESXi 5.0
	Cisco UCS C220 M3 C-Series Solution Pak for unified communications applications	UCUCS-EZ-C220M3S	
	Cisco UCS C220 M3 for Business Edition 6000	UCSC-C220-M3SBE	

Headquarters Voice

Functional Area	Product Description	Part Numbers	Software
Headquarters Voice Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.2(4)M3 securityk9 license ipbasek9 license uck9 license
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	
	Security Paper PAK for Cisco 3900 Series	SL-39-SEC-K9	
	IP Base Paper PAK for Cisco 3900 series	SL-39-IPB-K9	
	Unified Communications Paper PAK for Cisco 3900 Series	SL-39-UC-K9	
	2 Port Channelized T1/E1 and ISDN PRI High Speed WAN Interface Card (data only)	HWIC-2CE1T1-PRI	
	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card-T1/E1	VWIC2-2MFT-T1/E1	

Remote Site Voice

Functional Area	Product Description	Part Numbers	Software
Remote Site Voice Routers	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	15.2(4)M3 securityk9 license ipbasek9 license uck9 license
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Security Paper PAK for Cisco 2900 Series	SL-29-SEC-K9	
	IP Base Paper PAK for Cisco 2900 series	SL-29-IPB-K9	
	Unified Communications Paper PAK for Cisco 2900 Series	SL-29-UC-K9	
	2 Port Channelized T1/E1 and ISDN PRI High Speed WAN Interface Card (data only)	HWIC-2CE1T1-PRI	
	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card-T1/E1	VWIC2-2MFT-T1/E1	
	Cisco 881 Voice Router with FXS, BRI and FXO	C881-V-K9	15.2(4)M3 advancedip license uck9 license
	Unified Communication Paper PAK for Cisco 881 and 887	SL-8XX-UC-K9	
	Cisco SRST880 Advanced IP Services License	SL-SRST880-AIS	

Endpoints

Functional Area	Product Description	Part Numbers	Software
Phones	Unified IP Phone with six lines, video, color, Wi-Fi, Bluetooth, USB	CP-9971	SIP9971.9-3-2-10
	Unified IP Phone with four lines, video, color	CP-8945	SIP8941_8945.9-3-2-12
	Unified IP Conference Phone	CP-7937G	APPS37SCCP.1-4-4-0
	Unified IP Wireless Phone with six lines, color, Bluetooth	CP-7926G	CP7926G-1.4.3SR1.2
	Unified IP Phone with twelve lines	CP-6961	SCCP69xx.9-3-1-3
	Unified IP Phone with four lines	CP-6945	SCCP6945.9-3-1-3
	Unified IP Phone with two lines	CP-6921	SCCP69xx.9-3-1-3
	Unified IP Phone with one line	CP-6901	SCCP6901.9-3-1-2
	IP Communicator for Windows PC with eight lines	IPCOMM86-SW	–

Data Center Core

Functional Area	Product Description	Part Numbers	Software
Core Switch	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5596UP-FA	NX-OS 5.2(1)N1(3) Layer 3 License
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2	
	Cisco Nexus 5548 up to 48-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5548UP-FA	
	Cisco Nexus 5548 Layer 3 Switching Module	N55-D160L3	
	Cisco Nexus 5500 Layer 3 Enterprise Software License	N55-LAN1K9	
	Cisco Nexus 5500 Storage Protocols Services License, 8 ports	N55-8P-SSK9	
Ethernet Extension	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	–
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	
	Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender	N2K-C2232PP-10GE	

Server Room

Functional Area	Product Description	Part Numbers	Software
Stackable Ethernet Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 ports	WS-C3750X-48T-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Ethernet Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 ports	WS-C3560X-48T-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 ports	WS-C3560X-24T-S	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.4.0.SG(15.1-2SG) IP Base license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.2.1SE(15.0-1EX1) IP Base license
	Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports	WS-C3850-24P	
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	
	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(2)SE2 LAN Base license
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

Appendix B: Device Configuration Files

To view the configuration files from the CVD lab devices that we used to test this guide, please go to the following URL:
http://cvddocs.com/fw/Rel2-425

Feedback

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

B-0000430-2 11/13