



# Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to <http://www.cisco.com/go/sba>

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.





# Telephony Using Cisco UCM Deployment Guide

● ● ● SMART BUSINESS ARCHITECTURE

August 2012 Series

# Preface

## Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

## Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

**month year** Series

For example, the series of guides that we released in August 2012 are the “August 2012 Series”.

You can find the most recent series of SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>

## How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). 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 shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

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

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100  
100 100 100
```

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 [SBA feedback form](#).

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

# Table of Contents

<b>What's In This SBA Guide.....</b>	<b>1</b>
Cisco SBA Collaboration.....	1
Route to Success .....	1
About This Guide .....	1
<b>Introduction.....</b>	<b>2</b>
Design Goals .....	2
Business Overview .....	3
Technical Overview .....	3
<b>Network Infrastructure Module .....</b>	<b>5</b>
Business Overview.....	5
Technical Overview .....	5
Deployment Details .....	5
Preparing the Network for IP Phones .....	5

<b>Cisco Unified Communications Manager Module.....</b>	<b>8</b>
Business Overview.....	8
Technical Overview .....	8
Deployment Details .....	20
Preparing the Platform for Cisco Unified CM.....	20
Installing Cisco Unified CM .....	23
Preparing the Platform for Cisco Unity Connection .....	32
Installing Cisco Unity Connection.....	35
Configuring Cisco Unified CM and Cisco Unity Connection .....	39
Configuring Users, Device Profiles, and IP Phones.....	49
Preparing a Standalone Voice Router for Services.....	51
Configuring Gateways, Conference Bridges, PSTN, and SRST.....	56
<b>Appendix A: Product List .....</b>	<b>64</b>
<b>Appendix B: Changes.....</b>	<b>68</b>

# What's In This SBA Guide

## Cisco SBA Collaboration

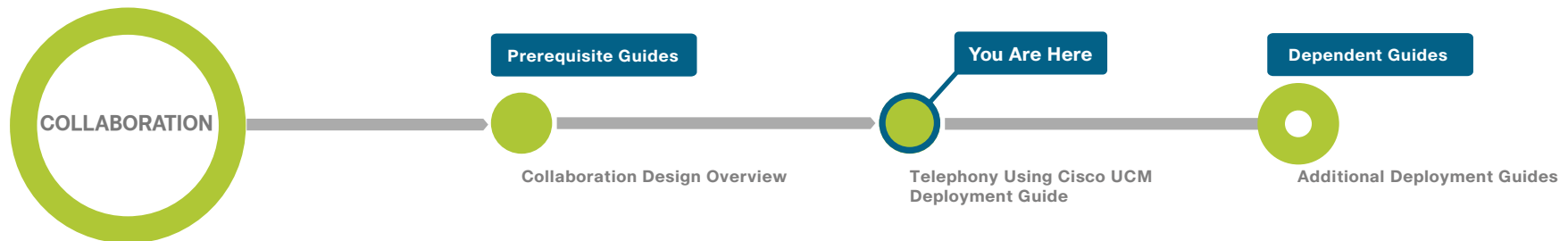
Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Collaboration is a design incorporating unified communications, video collaboration, and web conferencing. By building upon the hierarchical model of network foundation, network services, and user services, Cisco SBA Collaboration provides dependable delivery of business applications and services.

## Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.



## About This Guide

This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>

# Introduction

Cisco Smart Business Architecture (SBA) is a comprehensive design for networks with up to 10,000 users. Cisco SBA incorporates LAN, WAN, wireless, security, WAN optimization, and unified communication technologies, which are tested together as a solution. This solution-level approach simplifies the system integration normally associated with multiple technologies, allowing you to select the modules that solve your organization's problems rather than worrying about the technical details.

Cisco SBA is a platform that is easy to configure, deploy, and manage. The platform does the following:

- Provides a solid foundation
- Makes initial deployment fast and easy
- Accelerates your ability to easily deploy additional services
- Avoids the need to reengineer the network as the organization grows

To enhance the architecture, a number of supplemental guides address specific functions, technologies, or features that may be important to solving your business needs.

This guide includes detailed information about the following:

- The Network Infrastructure module provides guidance on how to prepare your network and plan for a Cisco Unified Communications deployment.
- The Cisco Unified Communications Manager module describes how to install Cisco Unified Communications Manager (Unified CM) for call control and Cisco Unity Connection for voicemail services. It also covers how the integrated services in your existing routers help you use the embedded resources in the network foundation in order to support a Cisco Unified Communications deployment without reengineering the core network.
- Appendix A provides the complete list of products used in the lab testing of this design, as well as the software revisions used on the products in the system.

## Design Goals

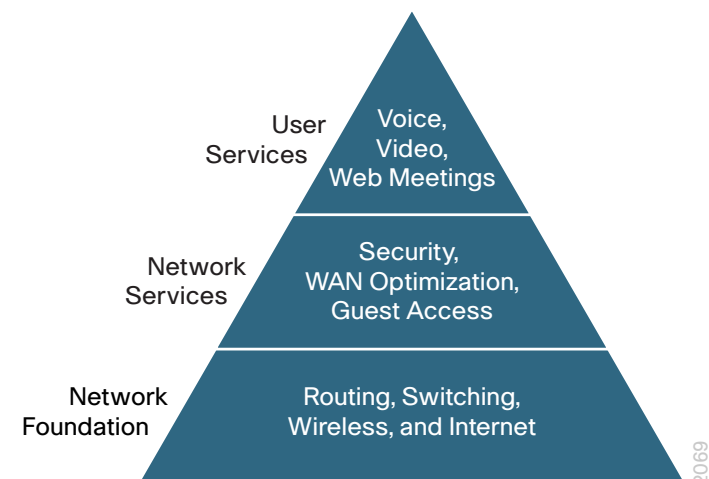
From the beginning, one of the primary concepts of this design has been the modular concept. The deployment process was divided into modules according to the following principles:

- **Ease of use**—A top requirement was to develop a design that could be deployed with minimal configuration and day-two management.
- **Cost-effective**—Another critical requirement in the selection of products was to meet the budget guidelines for an organization.
- **Flexibility and scalability**—As the organization grows, so too must its infrastructure. Products selected needed to have the ability to grow or be repurposed within the architecture.
- **Reuse**—The goal, when possible, was to reuse the same products throughout the various modules in order to minimize the number of products required for spares.

Cisco SBA for Collaboration was designed using a structured process to help ensure the stability of voice, video, and web conferencing for business processes and assets.

The architecture is broken down into three modular, yet interdependent, components. They are the network foundation, network services, and user services, with the interdependency being hierarchical in nature. The top layers rely on the ones below as depicted in the following diagram:

Figure 1 - Smart Business Architecture





## Business Overview

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 technology investments and reduce your overall operational costs.

### Provide Reliable Access to Organization Resources

Collaboration is critical to an organization's ability to operate and compete. Online workforce-enablement tools only offer benefit if the data network provides reliable access to information resources. Collaboration tools rely on a high-speed, low-latency network platform in order to provide an effective user experience. However, as networks become more complex, they become more susceptible to reduced availability, performance degradation, configuration errors, maintenance and upgrade outages, or hardware and software faults.

### Minimize Time Required to Select and Absorb Technology Investments

New technology can impose significant costs, including the time required to select the proper equipment, the investment in the equipment, and the time and workforce outlay required to deploy the new technology and establish operational readiness. Matching the correct equipment to solve business problems with the right mix of scalability, growth, and cost is difficult with the number of choices in the market. When new technology is introduced, it takes time to understand how the technology operates and to ascertain how to effectively integrate the new technology into the existing infrastructure. Over time, the methods and procedures used to deploy a new technology are refined to become more efficient and accurate.

## Reduce Operational Costs

Organizations constantly pursue opportunities to reduce network operational costs without negatively impacting the network's effectiveness for the end users. Operational costs include not only the price of the physical operation (power, cooling, etc.), but also the labor required to staff an IT department that monitors and maintains the voice network. Additionally, voice outages and performance issues impose costs that are more difficult to quantify, in the form of loss of productivity and interruption of business continuity.

## Technical Overview

This guide is designed to address three primary needs of an organization:

- To provide reliable access to an organization's Cisco Unified CM resources
- To minimize the time required to select and absorb communication technology
- To reduce configuration and operational costs across all areas of the communications infrastructure

This deployment 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. The Cisco SBA design ensures support for Cisco Unified Communications solutions from the onset.

Cisco Unified Communications has two software components. The first is Cisco Unified CM, which is the hub for interconnecting and managing IP telephony and other communication applications. The second is Cisco Unity Connection, which provides services such as voicemail, voicemail integration with your email inbox, and many other productivity features.

## Server Hardware

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 platform based on expected usage:

- For 500 users or fewer, Cisco Unified Communications Manager Business Edition 6000 on a Cisco Unified Computing System (UCS) C200 M2 High-Density Rack-Mount server is recommended. A second Cisco UCS server is added to the Cisco Unified CM Business Edition 6000 for organizations that need server redundancy.
- For 500 to 1000 users, two standalone Cisco MCS 7835 Unified Communications Manager appliances and a Cisco MCS 7835 Media Convergence Server for Cisco Unity Connection are recommended.
- For 1000 to 2500 users, four standalone Cisco MCS 7835 Unified Communications Manager appliances and a Cisco MCS 7835 Media Convergence Server for Cisco Unity Connection are recommended.
- For 2500 to 5000 users, five standalone Cisco MCS 7845 Unified Communications Manager appliances and a Cisco MCS 7845 Media Convergence Server for Cisco Unity Connection are recommended.
- For 5000 to 10,000 users, seven standalone Cisco MCS 7845 Unified Communications Manager appliances and a Cisco MCS 7845 Media Convergence Server for Cisco Unity Connection are recommended.
- For virtualized applications with 2500 users or less, two Cisco UCS C200 M2 High-Density Rack-Mount servers are recommended.
- For virtualized applications greater than 2500 users, two Cisco UCS C210 M2 High-Density Rack-Mount servers are recommended.

## Voice Gateways

Voice gateways provide the connectivity to the outside world, 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:

- For remote sites with up to 4 phones, the Cisco 880 SRST Series ISR is recommended
- For remote sites with 5 to 50 phones, the Cisco 2911 ISR is recommended
- For remote sites with 50 to 100 phones, the Cisco 2921 ISR is recommended
- For remote sites with 100 to 250 phones, the Cisco 2951 ISR is recommended
- For remote sites with 250 to 700 phones, the Cisco 3925 ISR is recommended
- For remote sites with 700 to 1200 phones, the Cisco 3945 ISR is recommended



# Network Infrastructure Module

Designing a long-lasting network infrastructure is a lot like designing a home from the ground up. The products used in the home and the individual design have to be selected with a clear understanding of what you need today, as well as a vision of where you are heading in the future. If you are planning to have children, building a three bedroom home today will save money over trying to add new bedrooms at a later date. The same argument holds true for your network infrastructure. The more items you can anticipate up front and accommodate into your design, the more money you will save down the road.

## Business Overview

When voice, video, and web conferencing are added to your network for the first time, a proper network foundation investment will make it much less expensive to implement. You do not want to replace or add more foundational equipment every time you deploy a new technology. You want to use your original investment in the network infrastructure as long and efficiently as possible. Starting with a comprehensive blueprint will lead to the right components in the network from the beginning.

## Technical Overview

The Cisco SBA guides are the blueprints you need to create a resilient network infrastructure that will last a long time, even as you add new technology. If you followed the Cisco SBA—Borderless Networks guides, you are in great shape to add unified communications to your network infrastructure. Cisco Unified Communications deployments are significantly simplified by the product selections and configurations in the other Cisco SBA deployment guides. The original equipment selections were chosen with Cisco Unified Communications in mind, so you will not have to make wholesale changes when you deploy a new technology, for example:

- Access switches provide Power over Ethernet (PoE) for phone deployments without the need for a local power outlet.
- The entire network is preconfigured with quality of service (QoS) to support high-quality voice and video traffic.

- The choice of the headquarters router in the Cisco SBA—Borderless Networks WAN deployment guides support the public switched telephone network (PSTN) gateway function, as well as the conference bridge resources with the addition of packet voice digital signal processor (DSP) modules, which are also called PVDMS.
- The wireless network is preconfigured for voice devices, providing IP telephony over 802.11 Wi-Fi at the headquarters and remote sites.
- The *Cisco SBA—Solutions Teleworking—Cisco Virtual Office Deployment Guide* is ready to provide “soft” phones and regular “hard” phones via VPN. These are plugged directly into the Cisco ASA 5505 Series Adaptive Security Appliances (ASA), which provides PoE on two ports and connectivity to the Cisco ASA 5500 at the headquarters site.
- For remote sites, the Cisco ISR G2 provides voice service during a WAN outage or loss of connectivity to the headquarters site. A simple Survivable Remote Site Telephony (SRST) configuration is used within the router and automatically takes over during a failure. As mentioned previously, voice services such as SRST can be deployed in an existing WAN router or in a standalone gateway for additional capacity and resiliency.

## Deployment Details

This module presents the detailed procedures to prepare your network and 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

Cisco SBA 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, since 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.

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

**Step 1:** Login 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
```

## About 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. The 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. The Cisco Unified IP Phone 9971 supports Wi-Fi connectivity, which frees users from the constraints of a hardwired telephone infrastructure within their buildings. The Cisco Unified IP Phone 8945 also supports video telephony with a built-in camera and a high-resolution color display. The 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 the Unified IP Phone 8945 for a four-line video phone and the 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. The 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 the Cisco Unified IP Phone 6921 and above, also support a deep-sleep mode, which uses 50 percent less power in the off-hours.

The 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 the Unified IP Phone 6901 after the rest of the phones are provisioned using the steps outlined in this guide. For XML-capable phones, this design recommends the Unified IP Phone 6921 for two lines, the Unified IP Phone 6945 for four lines, and the 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 SBA 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.

## 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 module.

# Cisco Unified Communications Manager Module

The Cisco Unified Communications Manager (Unified CM) module uses the Cisco Smart Business Configurator for Collaboration (SBCC) 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.

## Business Overview

Collaboration has always been an essential component of a successful organization. New pressures, heightened by a challenging global economic environment, are making collaboration more important than ever. Specifically, businesses 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.

## Technical Overview

Cisco SBA is a prescriptive architecture that delivers an easy-to-use, flexible, and scalable network with wired, wireless, security, WAN optimization, and unified communication components. It eliminates the challenges of integrating the various network components by using a standardized design that is reliable and offers comprehensive support.

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.

The business challenges mentioned previously are addressed with technologies, 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. The Cisco SBA platform is designed to support collaboration services, such as unified communications and video, without forklift upgrades to the underlying infrastructure components.

Cisco Unified Communications has the following software components running on standalone or virtualized appliances:

- 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.
- Voicemail is considered part of the Cisco Unified CM foundation and is provided by the Cisco Unity Connection appliance.

The following options are used in this guide:

- A dedicated TFTP server for clusters with more than 1250 phones and two dedicated TFTP servers for 5000 or more phones.
- A 1:1 subscriber redundancy in all configurations except for the smallest installations of 500 phones or less.
- Hardware redundancy for installations of more than 1000 phones when servers are virtualized on Cisco UCS platforms.

Building on the Cisco SBA platform, the following servers provide a highly available and scalable call-control and voicemail system capable of email client integration:

- Cisco Unified Communications Manager Business Edition 6000 uses a single-server instance running on a virtual server for up to 500 users. These servers provide 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.
  - Even though they are not covered in this guide, 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.
- The selection of Cisco MCS 7835 for up to 2500 users provides a balance between flexibility for future services and cost. These servers provide the following:
  - With one Cisco Unified CM server acting as a publisher and TFTP server and another server acting as a subscriber/TFTP server, the cluster will scale up to 1000 users with capacity to spare.
  - For medium-sized organizations with up to 2500 users, configure one Cisco Unified CM server 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 “Deploying Conference Bridges, Gateways and SRST” process, the conference bridges and dial-peers are configured with the two subscriber servers.

- Cisco Unity Connection deployed on a Cisco MCS 7835 platform supports up to 2500 users with voice mailboxes accessible through the phone or integrated into their email client.
- The Cisco Unified CM servers and the Cisco Unity Connection server can also be virtualized onto the Cisco UCS C210 M2 hardware platform. 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 2 - 1:1 subscriber redundancy with Cisco Unified CM groups for 1000 and 2500 users*

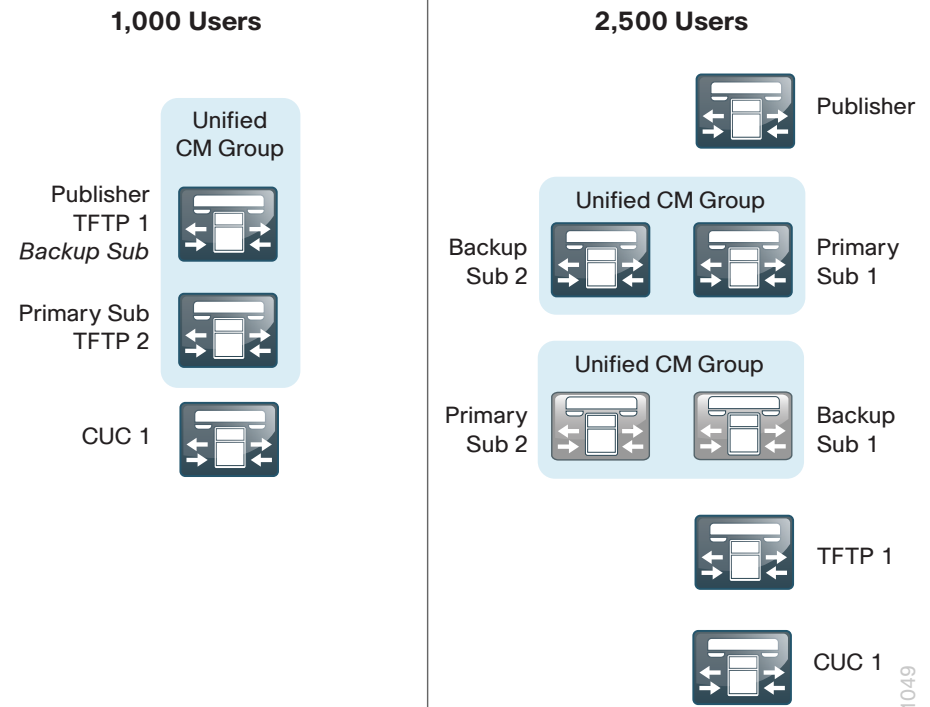
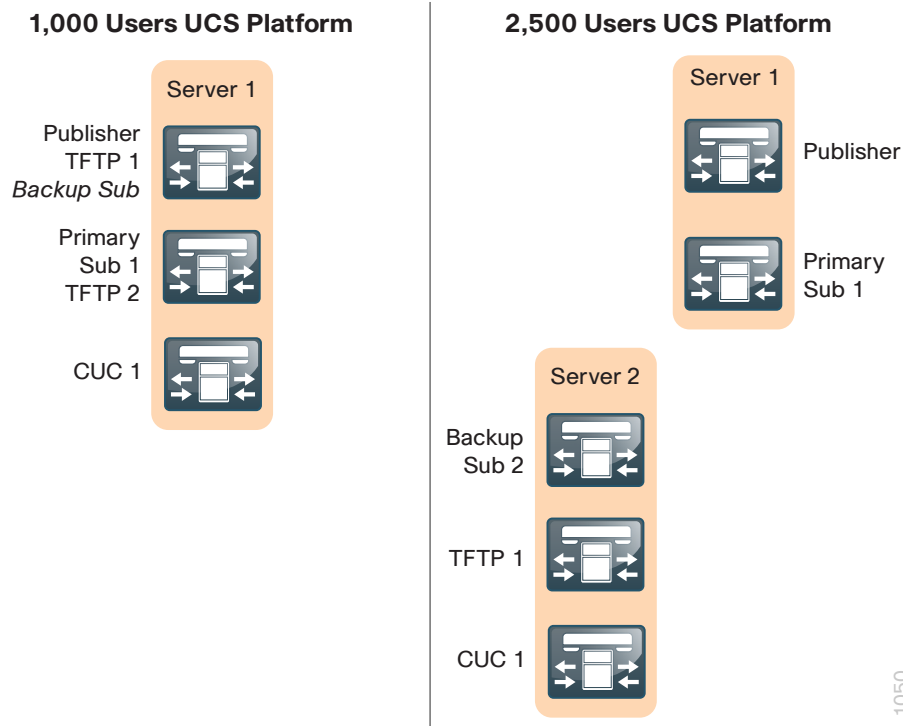




Figure 3 - Hardware platform redundancy for 2500 users



- The selection of Cisco MCS 7845 for 2500 to 10,000 users provides larger organizations the computing power and advanced features for future services and cost. These servers provide the following:
  - Configuring one Cisco Unified CM server as a publisher, two as subscribers, and two as dedicated TFTP servers allows 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 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 deployed on a Cisco MCS 7845 platform supports up to 10,000 users with voice mailboxes accessible through the phone or integrated into their email client.
- The Cisco Unified CM servers and the Cisco Unity Connection server can also be virtualized onto the Cisco UCS C210 M2 hardware platform. 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 4 - 1:1 subscriber redundancy with Cisco Unified CM groups for 5000 and 10,000 users

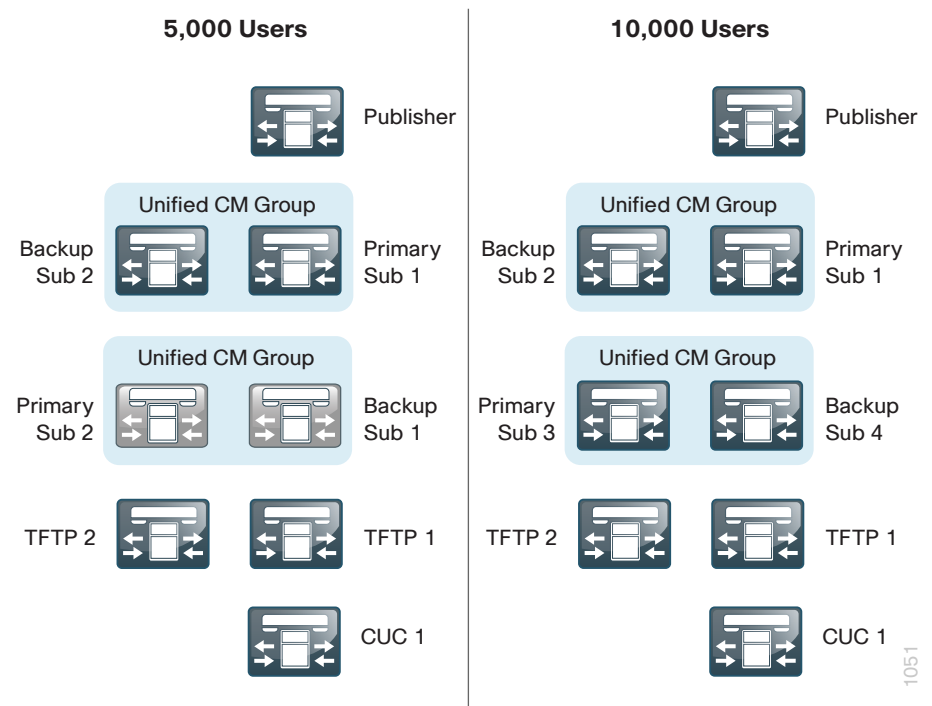
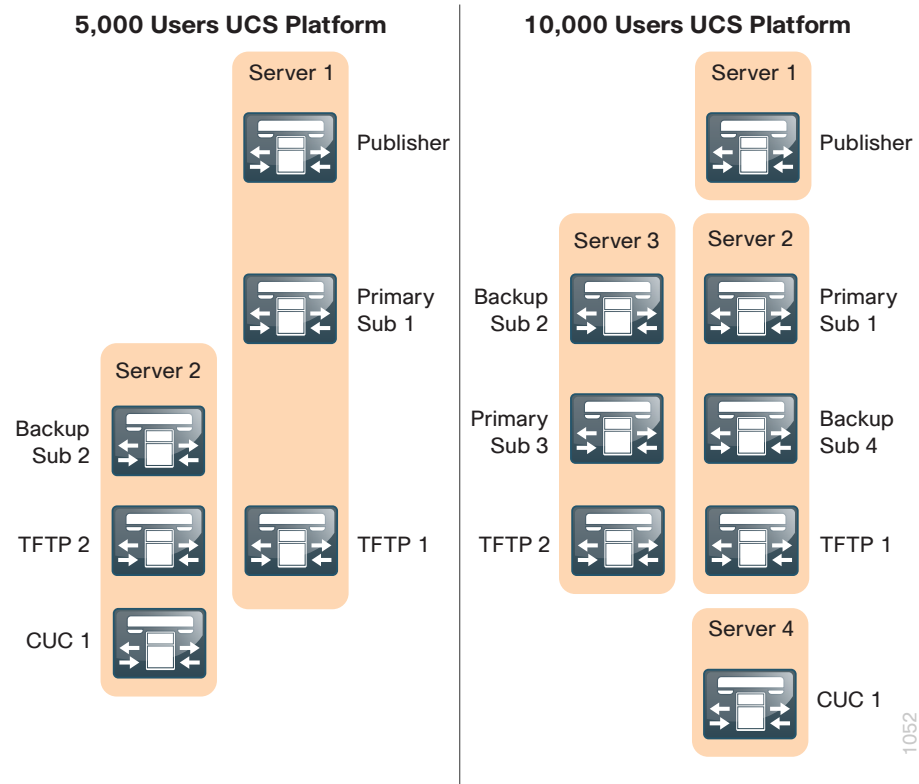




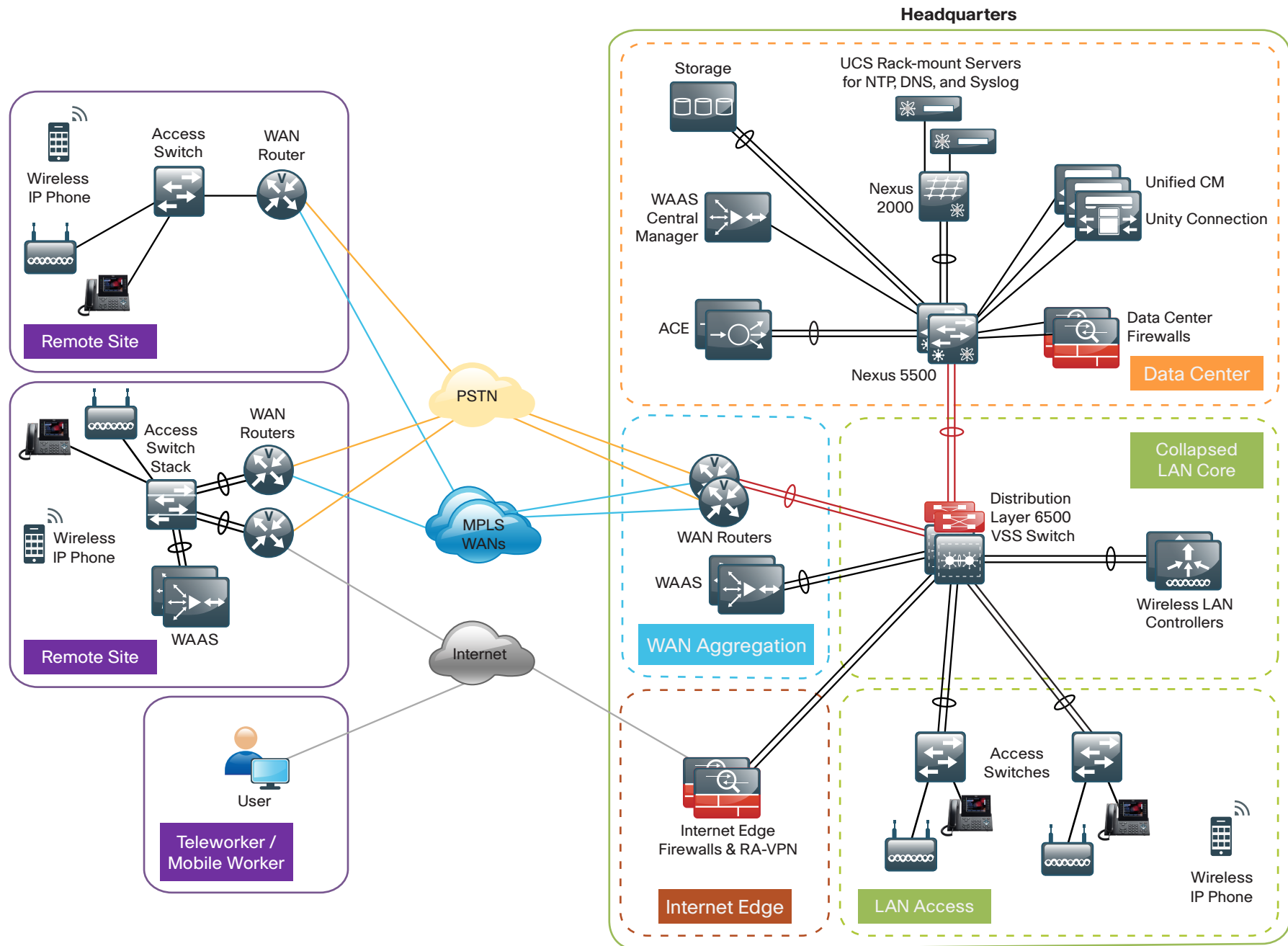
Figure 5 - Hardware platform redundancy for 5000 and 10,000 users



For all of the scaling options, the following features are provided:

- Connect each server to a different switch within the server farm or data center 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. Please contact your Cisco representative or local partner for additional information on these services.

Figure 6 - Cisco SBA design with Cisco Unified CM foundation



2079

The Cisco SBA 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 module.

This guide includes the following Cisco Unified CM features:

- Automatically registers phones for quick and easy deployment
- Integrates an Active Directory feature in both Cisco Unified CM and Cisco Unity Connection for designs that require a single source of information for user management
- Allows you to choose between two North American Numbering Plans as part of the path selection for PSTN destinations
- Uses endpoint addressing that consists of a uniform on-net dial plan containing an access code, site codes, and four-digit extensions
- Provisions SIP gateways for all sites
- Provides SRST for SIP and SCCP phones
- Uses the Device Mobility feature, which allows Cisco Unified CM to determine the physical locations of devices
- Uses the Cisco Extension Mobility feature, which enables users to assign a Cisco Unified IP Phone as their own
- Provisions individual media resources, such as conference bridges and software media termination points, for every site
- Automatically provisions Cisco Unified CM for Voice Messaging integration and documents the Cisco Unity Connection configuration
- Provides locations-based Call Admission Control

## 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 SBCC, 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.



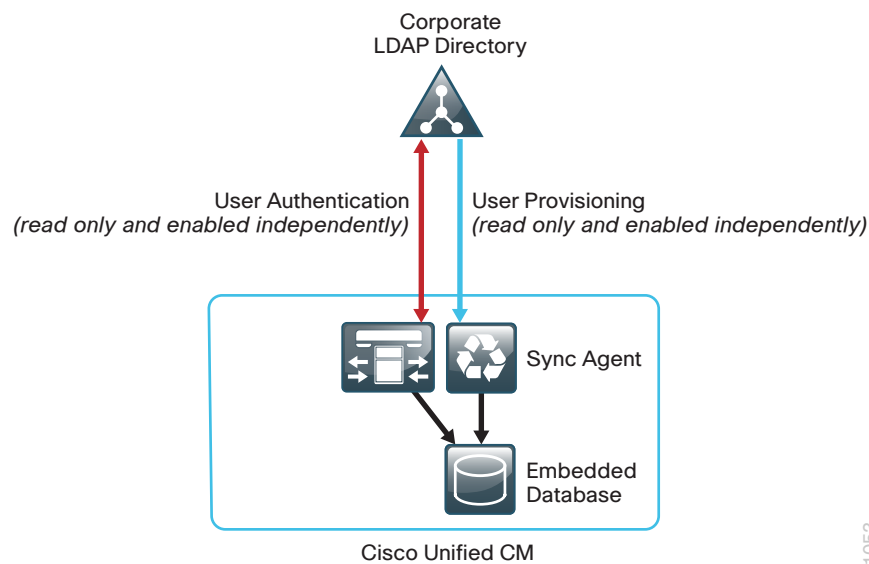
### Tech Tip

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 7 - Directory integration with Cisco Unified CM



1053

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. Cisco SBCC 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 SBCC 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 8 - 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

Emergency Dialing

Local Dialing

National Dialing

International Dialing

1054

Figure 9 - 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

Emergency Dialing

Local Dialing

National Dialing

International Dialing

1055

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 9.911 emergency 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 four-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.

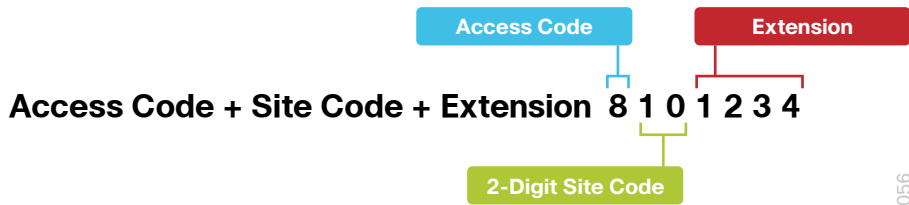
When you use this method, a phone in San Jose, CA can have the same 4-digit extension as one in Houston, TX without creating a numbering conflict. For example: 408-525-1234 in San Jose and 713-448-1234 in Houston.

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

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

Figure 10 - 2-digit site code format

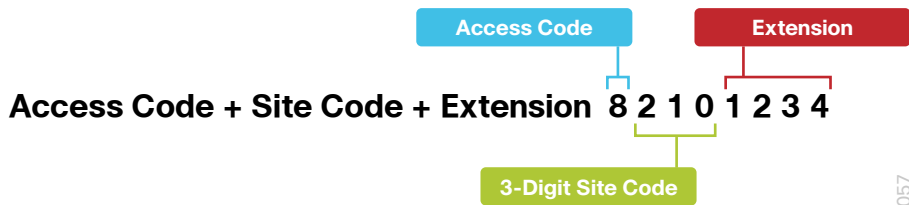


For networks with greater than 90 sites, the dial plan consists of the following:

- 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

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

Figure 11 - 3-digit site code format



When site codes are used, Cisco SBCC creates a new partition, calling search space, and translation pattern per site to allow 4-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 12 - Calling search spaces and partitions

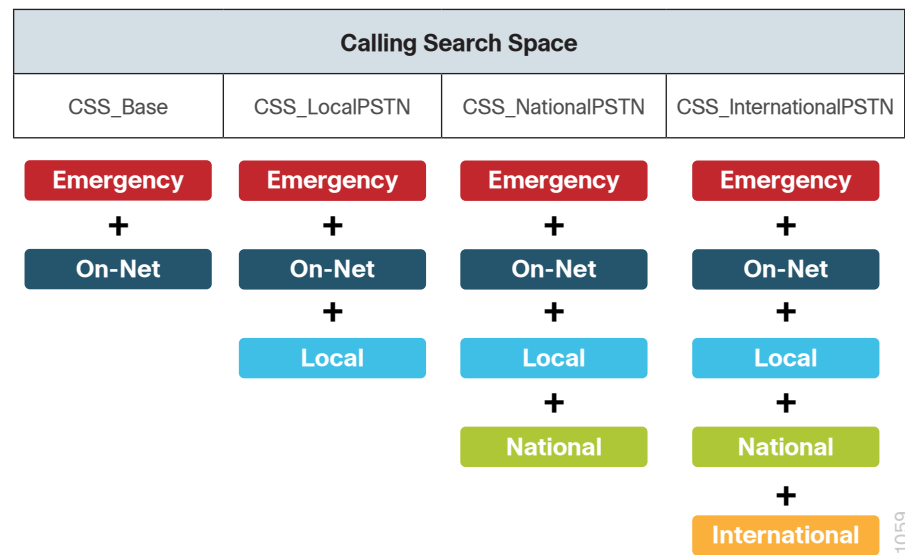
	Calling Search Space	Route Partition 1	Route Partition 2	Route Partition 3
1	CSS_Base	PAR_Base	—	—
2	CSS_LocalPSTN	PAR_PSTN_Local	—	—
3	CSS_NationalPSTN	PAR_PSTN_Local	PAR_PSTN_National	—
4	CSS_InternationalPSTN	PAR_PSTN_Local	PAR_PSTN_National	PAR_PSTN_Intl

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

With Cisco SBCC, 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 seven-digit or local ten-digit, national, and international dialing capabilities.

Figure 13 - Calling capabilities for calling search spaces



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.

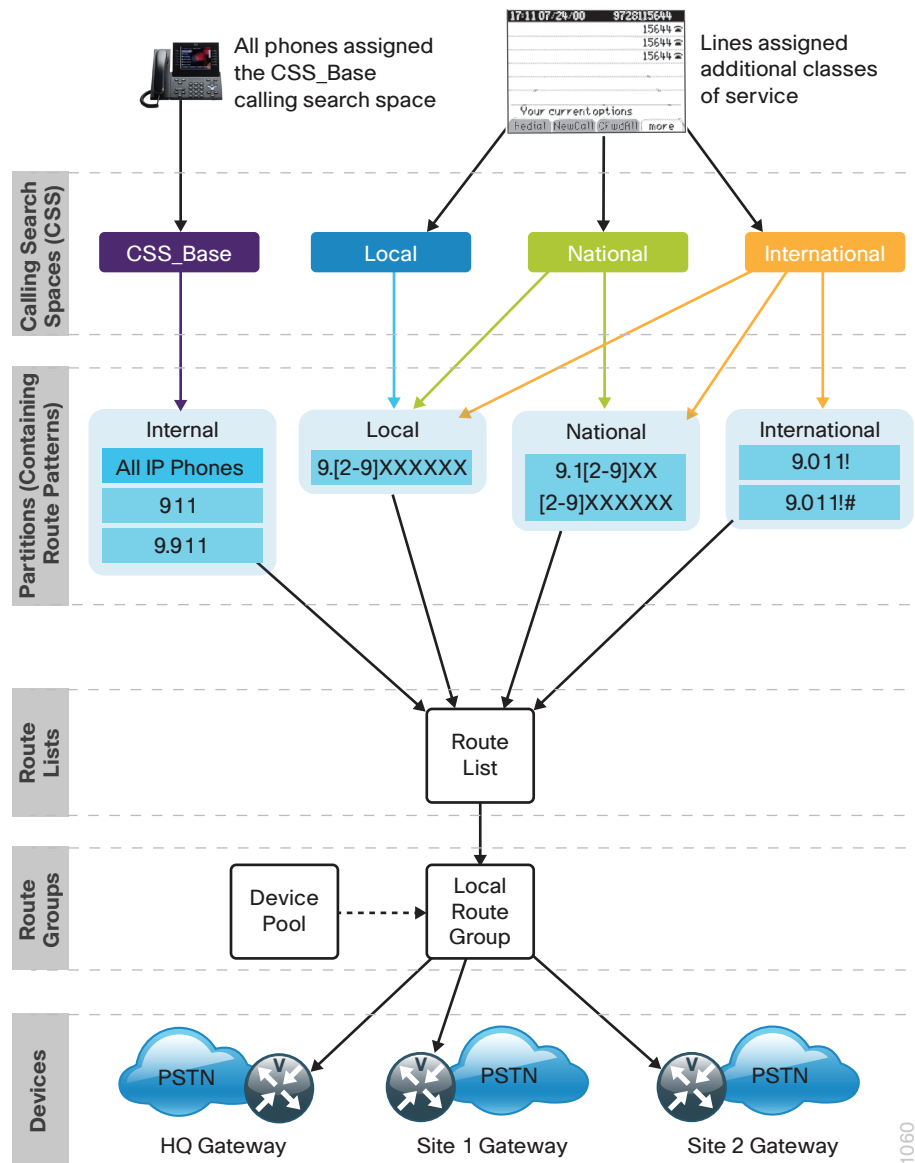
Local Route Groups

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.

Cisco SBCC 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 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 14 - 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.

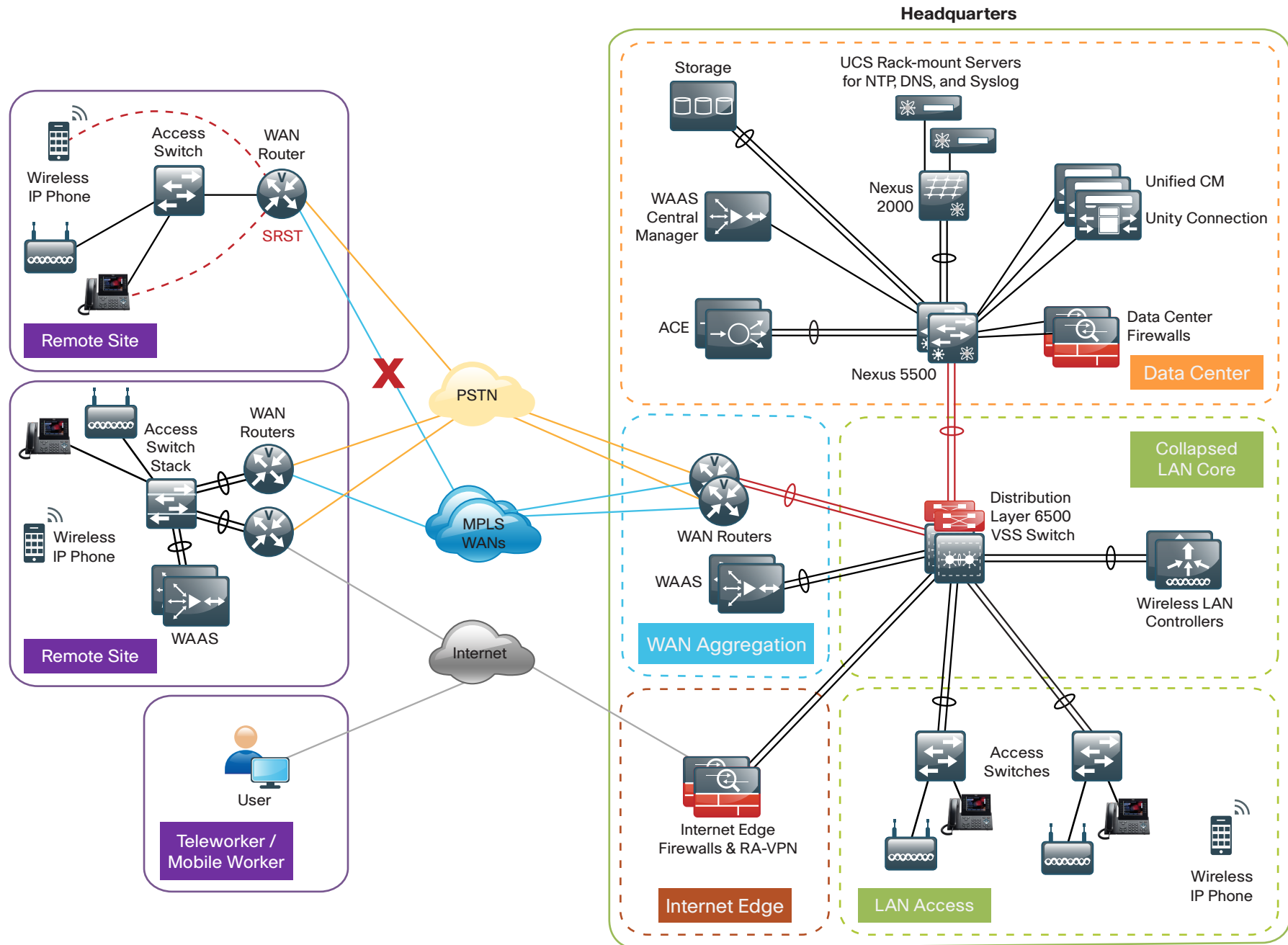
At a remote site with more than one PSTN gateway, configure SRST on the router with the most voice ports. If only one router has PSTN interfaces, SRST must be configured on the router to reduce complications.

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](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 in the Cisco SBA design when the WAN is down.

Figure 15 - Cisco SBA design with SRST at a remote site



1061

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

Cisco SBCC 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.

## Extension Mobility

Cisco SBCC 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 Cisco SBCC 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 SBCC will have a default PIN of '112233'.

## Media Resources

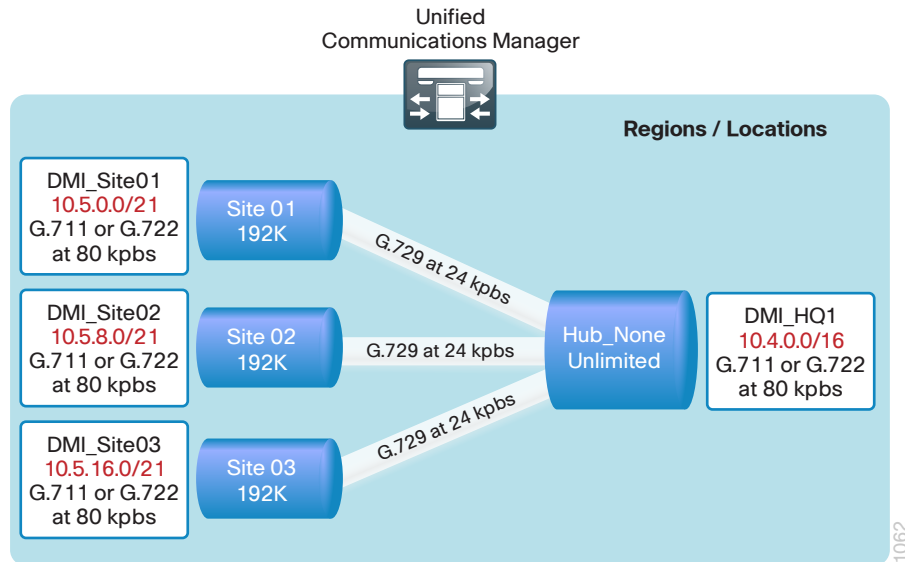
Media resources have been provisioned as part of the procedure for every site in order to ensure that remote sites use their local conference bridges and avoid unnecessary voice traffic over the WAN. The naming of the conference bridges needs to match those provisioned by Cisco SBCC. The names are always 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 Cisco SBCC 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 SBCC default voice bandwidth setting for inter-site calls. For sites with only 500 users, the default setting is two inter-site calls (48 kbps), all the way up to sites with 10,000 users which default to eight inter-site calls (192 kbps). The amount of bandwidth in and out of each site can be modified within SBCC, 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 Cisco SBCC to provide the correct Call Admission Control based on the speed of the link.

Figure 16 - Hub-and-spoke topology for Call Admission Control



The remaining sections of this module include step-by-step instructions for installing, configuring and deploying Cisco Unified Communications for basic telephony and simple voice messaging, including the following:

- Platform preparation and software installation for Cisco Unified CM
- Server and site configuration
- Platform preparation and software installation for Cisco Unity Connection
- User and device profile configuration
- IP phone deployment

## Deployment Details

The following procedures allow for the parallel installation of Cisco Unified CM and Cisco Unity Connection servers. They are installed on different virtual machines or standalone servers.

Please note, however, that at certain points of the installation process, some steps must occur prior to proceeding with others. In order to save time, the software installation can also proceed in parallel with running Cisco SBCC, but certain steps require access to the Cisco Unified CM administration pages.

### Process

Preparing the Platform for Cisco Unified CM

1. Prepare a virtual machine for Unified CM
2. Prepare a server for Cisco 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://www.cisco.com/cisco/software/release.html?mdfid=283782839&lowid=26422&softwareid=283088407&release=8.6\(1\)&reind=AVAILABLE&rellifecycle=&reltype=latest](http://www.cisco.com/cisco/software/release.html?mdfid=283782839&lowid=26422&softwareid=283088407&release=8.6(1)&reind=AVAILABLE&rellifecycle=&reltype=latest)
- Check the Cisco website to determine if there is a patch for your version of Cisco Unified CM:  
[http://www.cisco.com/cisco/software/release.html?mdfid=283782839&lowid=26422&softwareid=282074295&release=8.6\(2\)&reind=AVAILABLE&rellifecycle=&reltype=latest](http://www.cisco.com/cisco/software/release.html?mdfid=283782839&lowid=26422&softwareid=282074295&release=8.6(2)&reind=AVAILABLE&rellifecycle=&reltype=latest)

If you are installing a virtual machine, follow the steps in Procedure 1, "Prepare a virtual machine for Unified CM."

If you are installing a standalone server, follow the steps in Procedure 2, "Prepare a server for Cisco Unified CM."

## Procedure 1 Prepare a virtual machine for Unified CM

If you are installing a virtual machine, follow the steps below to deploy an OVA file in order to define the virtual machine requirements for Cisco Unified CM.

The Cisco Unified CM OVA file defines the following virtual machine for a 2500-user node:

- Number of virtual CPUs—1 (800 MHz reservation)
- Amount of RAM—4 GB (4 GB reservation)
- Hard disk—1 x 80 GB
- VMware ESXi support—ESXi 4.0 or ESXi 4.1 (VM version 7)
- OS support—Red Hat Enterprise Linux 5 (32-bit)

The Cisco Unified CM OVA file defines the following virtual machine for a 7500-user node:

- Number of virtual CPUs—2 (3600 MHz reservation)
- Amount of RAM—6 GB (6 GB reservation)
- Hard disk—2 x 80 GB
- VMware ESXi support—ESXi 4.0 or ESXi 4.1 (VM version 7)
- OS support—Red Hat Enterprise Linux 5 (32-bit)

**Step 1:** Open the VMware vSphere client, and then navigate to **File > Deploy OVF Template**.

**Step 2:** Next to the **Deploy from a file or URL** box, click the **Browse** button, find the location of the Cisco Unified CM OVA file that you downloaded from Cisco, and then click **Next**.

**Step 3:** On the OVF Template Details page, verify the version information, and then click **Next**.

When you are deploying a cluster of less than 2500 users, select the 2500-user node. If you are deploying a cluster of 2500 users or more, select the 7500-user node.

**Step 4:** In the Deploy OVF Template wizard, enter the following information:

- 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, choose either the 2500-user node or the 7500-user node, and then click **Next**.
- On the Disk Format page, choose **Thick provisioned format**, and then click **Next**.
- On the Ready to Complete page, verify the settings, and then click **Finish**.

**Ready to Complete**  
Are these the options you want to use?

[Source](#)  
[OVF Template Details](#)  
[Name and Location](#)  
[Deployment Configuration](#)  
[Disk Format](#)  
**Ready to Complete**

When you click Finish, the deployment task will be started.

Deployment settings:

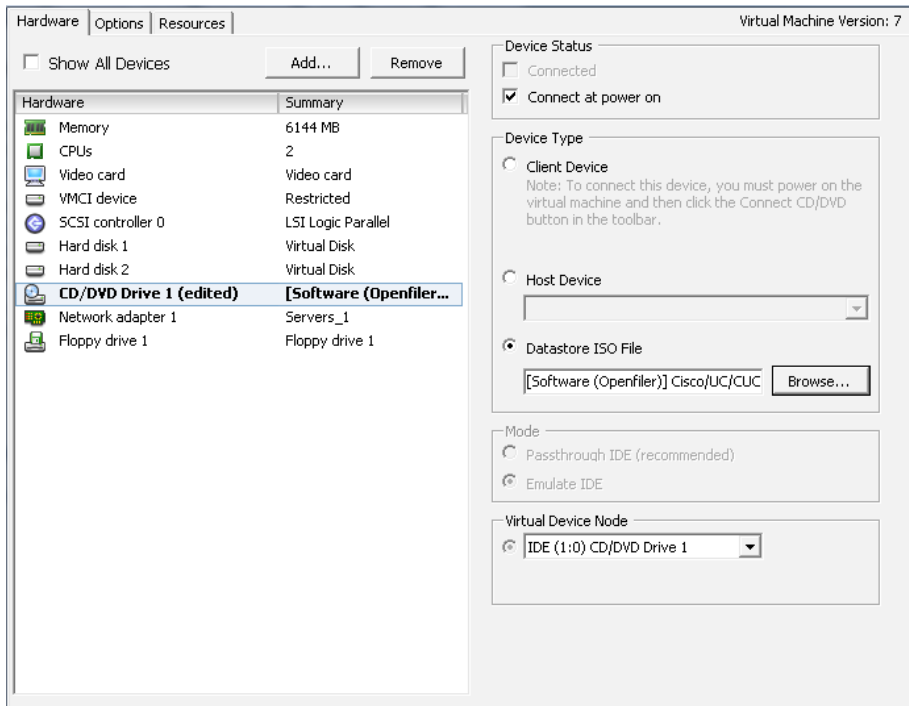
OVF file:	C:\Users\kfleshne\Downloads\cucm_8.6_vmv7_v1.5.ova
Download size:	176.5 KB
Size on disk:	576.0 KB
Name:	CUCM-Pub1
Folder:	Enterprise
Deployment Configuration:	CUCM 7500 user node
Host/Cluster:	chas2-s3.cisco.local
Datastore:	datastore1 (2)
Disk Format:	Thick Provisioning
Network Mapping:	"eth0" to "Servers_1"

**Step 5:** After the virtual machine is created, navigate to the Getting Started tab, and then choose **Edit virtual machine settings**.

**Step 6:** On the Hardware tab, choose **CD/DVD Drive 1**.

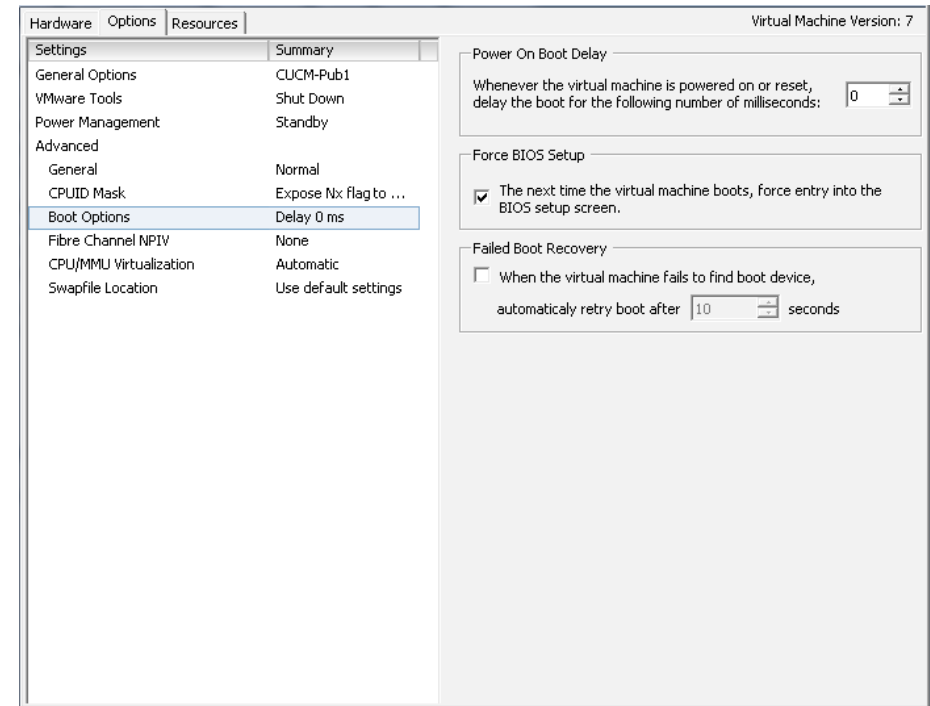
**Step 7:** Select the **Connect at power on** check box.

**Step 8:** Select **Datastore ISO File**, click **Browse**, and then navigate to the location of the Cisco Unified CM bootable installation file.



**Step 9:** On the Options tab, choose **Boot Options**.

**Step 10:** Select the **The next time the virtual machine boots, force entry into the BIOS setup screen** check box, and then click **OK**.

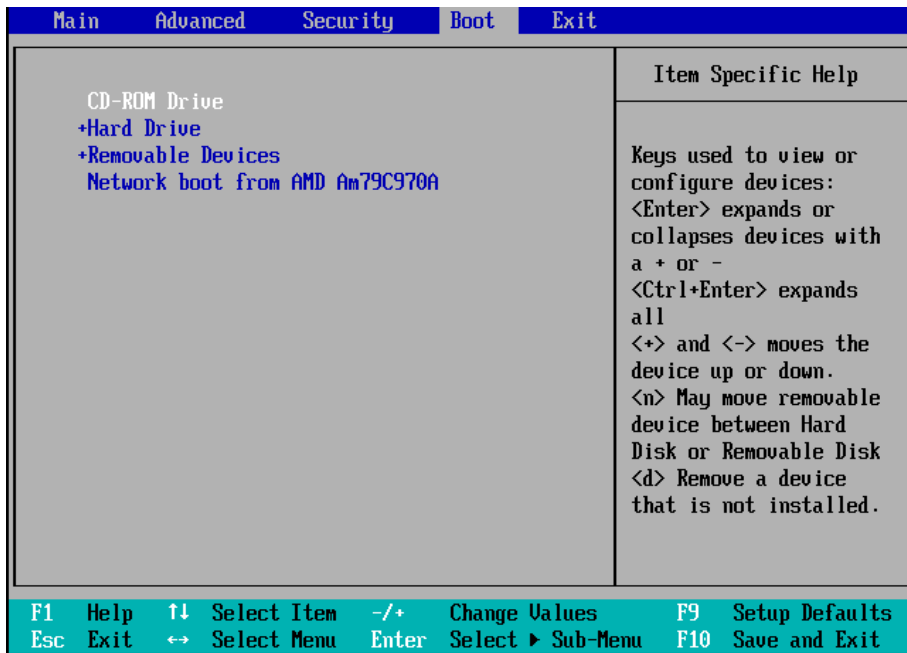


**Step 11:** Navigate to the Getting Started tab, choose **Power on the virtual machine**, and then click the Console tab. Watch the server boot.

**Step 12:** After the machine boots into the **PhoenixBIOS Setup Utility**, use the right arrow key to move to the Boot tab.



**Step 13:** Edit the boot order with the + and - keys in order to make **CD-ROM Drive** the first item and **Hard Drive** the second.



**Step 14:** Press the **F10** key. The BIOS settings are saved, and you exit the PhoenixBIOS Setup Utility.

**Step 15:** In the Setup Confirmation dialog box, select **Yes**, and then press **Enter**. The virtual machine boots from the datastore ISO file.

**Step 16:** After the ISO file loads from the virtual DVD drive, follow the procedures in "Installing Cisco Unified CM" to complete the installation.

**Step 3:** Power on the server. It boots from the DVD.

**Step 4:** After the DVD loads, follow the procedures in "Installing Cisco Unified CM" to complete the installation.

## Process

### Installing Cisco Unified CM

1. Install the first Cisco Unified CM platform
2. Install the remaining Unified CM platforms

This process is the same whether you are installing in a virtual environment or on a standalone server.

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
- 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.

## Procedure 2 Prepare a server for Cisco Unified CM

**Step 1:** Physically install the server and attach the monitor, keyboard, and network cable.

**Step 2:** Insert the Cisco Unified CM DVD into the DVD drive.

Complete the tasks listed below before you start the installation:

- Configure Cisco Unified CM host names in DNS
- Obtain license files from the Cisco licensing system
- On the PC 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 2 “Install the remaining Unified CM platforms.”

**Step 1:** On the DVD Found page, choose **Yes**. A media check is performed.

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

If the media check does not pass, select another DVD or ISO file, 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:** If you are installing on a standalone server, on the Auto Negotiation Configuration page, choose **Yes**.

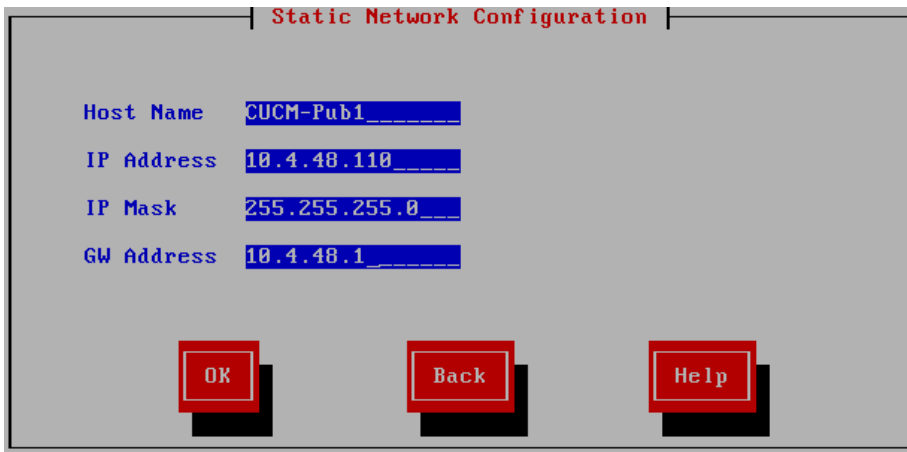
If you are deploying a virtual machine, on the Auto Negotiation Configuration page, choose **Continue**.

**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**

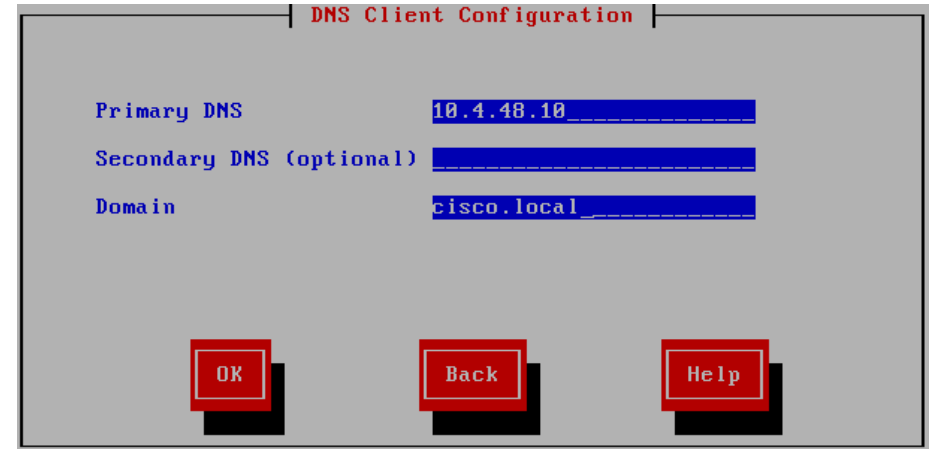


The image shows the 'Static Network Configuration' screen. It has a title bar with the text 'Static Network Configuration'. Below the title bar, there are four fields: 'Host Name' with the value 'CUCM-Pub1', 'IP Address' with '10.4.48.110', 'IP Mask' with '255.255.255.0', and 'GW Address' with '10.4.48.1'. At the bottom of the screen, there are three buttons: 'OK', 'Back', and 'Help'.

**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**



The image shows the 'DNS Client Configuration' screen. It has a title bar with the text 'DNS Client Configuration'. Below the title bar, there are three fields: 'Primary DNS' with the value '10.4.48.10', 'Secondary DNS (optional)' which is empty, and 'Domain' with 'cisco.local'. At the bottom of the screen, there are three buttons: 'OK', 'Back', and 'Help'.

**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**.

The screenshot shows the 'Certificate Information' configuration page. At the top, it says 'Enter information about your organization. This is used to generate security certificates for this node.' Below this are several fields: 'Organization' (Cisco Systems, Inc.), 'Unit' (Unified Communications), 'Location' (San Jose), 'State' (California), and 'Country' (Ukraine, United Arab Emirates, United States). At the bottom are three buttons: 'OK', 'Back', and 'Help'.

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

**Step 19:** On the Network Time Protocol Client Configuration page, select **Yes**, and 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 20:** On the Database Access Security Configuration page, enter a security password, confirm the password, and then choose **OK**.

You will 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]**

The screenshot shows the 'Application User Configuration' page. It says 'The Application User username and password are used to log into the Application administrative webpage(s)'. Below this are three fields: 'Application User Username' (CUCMAdmin), 'Application User Password' (\*\*\*\*\*), and 'Confirm Application User Password' (\*\*\*\*\*). At the bottom are three buttons: 'OK', 'Back', and 'Help'.

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

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

**Step 24:** If you deployed a virtual server, return to the VMware vSphere client. You must disable the CD/DVD drive.

If you deployed a standalone server skip ahead to Step 28

**Step 25:** From the vSphere client, navigate to the virtual machine's Getting Started tab, and then choose **Edit virtual machine settings**.

**Step 26:** On the Hardware tab, choose **CD/DVD Drive 1**.

**Step 27:** Clear the **Connect at power on** check box, and then click **OK**.

**Step 28:** Use your web browser to access the Cisco Unified CM administration interface, and in the center of the page, under **Installed Applications**, click the **Cisco Unified Communications Manager** link.



### Tech Tip

If you receive a warning about the website's security certificate, ignore it and continue to the website page.

**Step 29:** Enter the **Username** and **Password** from the Application User Configuration page in Step 22, and then click **Login**.

**Step 30:** Navigate to **System > Licensing > License File Upload**.

**Step 31:** Click **Upload License File**, and then browse to the directory that contains the license files you obtained prior to installation.

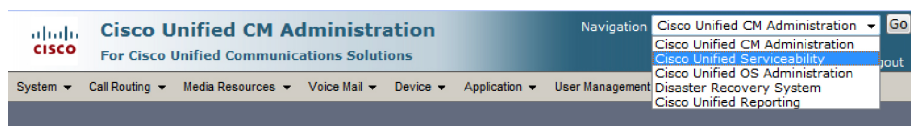
**Step 32:** Select the file, and then click **Upload**. The file transfers to the server.

**Step 33:** When the file is uploaded, click **Continue**. You return to the License File Upload page.

**Step 34:** Repeat Step 31, Step 32 and Step 33 until all the necessary files are uploaded.

**Step 35:** Navigate to **System > Licensing > License Unit Report**. Verify that the licenses are valid and the unit counts are correct. If there is a problem, please notify your Cisco representative to obtain new license files.

**Step 36:** In the **Navigation** list, choose **Cisco Unified Serviceability**, and then click **Go**.



**Step 37:** 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 38:** Select the **Check All Services** check box, clear the ones that are not needed for this node, and then click **Save**. In the dialog box, click **OK**.



### 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

Figure 17 - Recommended Publisher services when using dedicated TFTP servers

**Select Server**  
 Server\*    
☐ Check All Services

CM Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CallManager	Activated
<input type="checkbox"/>	Cisco Messaging Interface	Deactivated
<input checked="" type="checkbox"/>	Cisco Unified Mobile Voice Access Service	Activated
<input checked="" type="checkbox"/>	Cisco IP Voice Media Streaming App	Activated
<input checked="" type="checkbox"/>	Cisco CTIManager	Activated
<input checked="" type="checkbox"/>	Cisco Extension Mobility	Activated
<input checked="" type="checkbox"/>	Cisco Extended Functions	Activated
<input type="checkbox"/>	Cisco DHCP Monitor Service	Deactivated
<input type="checkbox"/>	Cisco Dialed Number Analyzer Server	Deactivated
<input type="checkbox"/>	Cisco Dialed Number Analyzer	Deactivated
<input type="checkbox"/>	Cisco Tftp	Deactivated

CTI Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco IP Manager Assistant	Activated
<input checked="" type="checkbox"/>	Cisco WebDialer Web Service	Activated

CDR Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco SOAP - CDRonDemand Service	Activated
<input checked="" type="checkbox"/>	Cisco CAR Web Service	Activated

Database and Admin Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Platform SOAP Services	Activated
<input checked="" type="checkbox"/>	Cisco AXL Web Service	Activated
<input checked="" type="checkbox"/>	Cisco UXL Web Service	Activated
<input checked="" type="checkbox"/>	Cisco Bulk Provisioning Service	Activated
<input type="checkbox"/>	Cisco TAPS Service	Deactivated


Performance and Monitoring Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco Serviceability Reporter	Activated
<input checked="" type="checkbox"/>	Cisco CallManager SNMP Service	Activated

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

**Step 39:** In the **Navigation** list at the top of the page, choose **Cisco Unified CM Administration**, and then click **Go**.

**Step 40:** Navigate to **System > Server**, and then click **Add New**.

**Step 41:** Enter the host name of the additional Cisco Unified CM server, and then click **Save**.

**Status**  
 Status: Ready

**Server Information**  
 Host Name/IP Address\*   
 IPv6 Name   
 MAC Address   
 Description

**Step 42:** For each additional subscriber and TFTP server, click **Add New**, and then repeat Step 41.

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

**Step 43:** Navigate to **System > Application Server**, and then click **Add New**.

**Step 44:** On the first Application Server Configuration page, in **Application Server Type**, choose **Cisco Unity Connection**, and then click **Next**.

**Step 45:** 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 46:** In the **Available Application Users** list, select the account you created during the installation of Cisco Unified CM (CUCMadmin), move the account to the **Selected Application Users** list by clicking the **v** character, and then click **Save**.

**Status**  
Status: Ready

**Application Server Information**

Application Server Type: Cisco Unity Connection

Name\*: CUC1

IP Address\*: 10.4.48.123

Available Application Users: CCMSysUser, WDSysUser, CCMQRTSysUser, IPMASysUser, WDSecureSysUser

Selected Application Users\*: CUCMAdmin

**Step 47:** 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 2 "Install the remaining Unified CM platforms".

The Cisco Unity Connection platform is prepared and installed in a subsequent process below.

## Procedure 2 Install the remaining Unified CM platforms

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

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

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

If the media check does not pass, select another DVD or ISO file, and then repeat Step 1.

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

**Product Deployment Selection**

Select the product or product suite to be installed:

- (\*) Cisco Unified Communications Manager
- ( ) Cisco Unity Connection
- ( ) Cisco Unified CM Business Edition 5000

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:** If you are installing on a standalone server, on the Auto Negotiation Configuration page, choose **Yes**.

If you are deploying a virtual machine, 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**

Static Network Configuration

Host Name **CUCM-Sub1**

IP Address **10.4.48.111**

IP Mask **255.255.255.0**

GW Address **10.4.48.1**

**OK** **Back** **Help**

**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**

DNS Client Configuration

Primary DNS **10.4.48.10**


Secondary DNS (optional)

Domain **cisco.local**

**OK** **Back** **Help**

**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**.

Certificate Information

Enter information about your organization. This is used to generate security certificates for this node.

Organization **Cisco Systems, Inc.**

Unit **Unified Communications**

Location **San Jose**

State **California**

Country **United States**

**OK** **Back** **Help**

**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 **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]**

First Node Access Configuration

Connectivity to First Node:

Host Name CUCM-Pub1

IP Address 10.4.48.110

Security Password \*\*\*\*\*

Confirm Password \*\*\*\*\*

OK Back Help

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

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

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

**Step 23:** If you deployed a virtual server, return to the VMware vSphere client. You must disable the CD/DVD drive.

If you deployed a standalone server, skip ahead to Step 27.

**Step 24:** From the vSphere client, navigate to the virtual machine's Getting Started tab, and then choose **Edit virtual machine settings**.

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

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

**Step 27:** Use your web browser to access the Cisco Unified CM administration interface on the publisher, and then in the center of the page, under **Installed Applications**, click the **Cisco Unified Communications Manager** link.

**Step 28:** Enter the application **Username** and **Password**, and then click **Login**.

**Step 29:** In the **Navigation** list on the top right side of the page, choose **Cisco Unified Serviceability**, and then click **Go**.

**Step 30:** Navigate to **Tools > Service Activation**.

**Step 31:** 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 32:** Select the **Check All Services** check box, clear the ones that are not needed for this node, and then click **Save**. In the dialog box, click **OK**.

Figure 18 - Recommended Subscriber services when using dedicated TFTP servers

**Select Server**  
 Server\*    
☐ Check All Services

CM Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CallManager	Activated
<input type="checkbox"/>	Cisco Messaging Interface	Deactivated
<input checked="" type="checkbox"/>	Cisco IP Voice Media Streaming App	Activated
<input checked="" type="checkbox"/>	Cisco CTIManager	Activated
<input checked="" type="checkbox"/>	Cisco Extension Mobility	Activated
<input checked="" type="checkbox"/>	Cisco Extended Functions	Activated
<input type="checkbox"/>	Cisco DHCP Monitor Service	Deactivated
<input type="checkbox"/>	Cisco Dialed Number Analyzer Server	Deactivated
<input type="checkbox"/>	Cisco Dialed Number Analyzer	Deactivated
<input type="checkbox"/>	Cisco Tftp	Deactivated

Figure 19 - Recommended dedicated TFTP services with Cisco CallManager deactivated

**Select Server**  
 Server\*    
☐ Check All Services

CM Services		
	Service Name	Activation Status
<input type="checkbox"/>	Cisco CallManager	Deactivated
<input type="checkbox"/>	Cisco Messaging Interface	Deactivated
<input checked="" type="checkbox"/>	Cisco IP Voice Media Streaming App	Activated
<input checked="" type="checkbox"/>	Cisco CTIManager	Activated
<input checked="" type="checkbox"/>	Cisco Extension Mobility	Activated
<input checked="" type="checkbox"/>	Cisco Extended Functions	Activated
<input type="checkbox"/>	Cisco DHCP Monitor Service	Deactivated
<input type="checkbox"/>	Cisco Dialed Number Analyzer Server	Deactivated
<input type="checkbox"/>	Cisco Dialed Number Analyzer	Deactivated
<input checked="" type="checkbox"/>	Cisco Tftp	Activated

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

**Step 33:** Repeat Procedure 2 "Install the remaining Unified CM platforms" 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. Prepare a VM for Unity Connection
2. Prepare a 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:

- If you are installing on a new virtual machine, download the Open Virtual Archive (OVA) file from the Cisco website at:  
<http://www.cisco.com/cisco/software/release.html?mdfid=283062758&flowid=31846&softwareid=282074348&release=OVA-8.6&relind=AVAILABLE&rellifecycle=&reltype=latest>
- Check the Cisco website to determine if there is a patch for your version of Cisco Unity Connection: [http://www.cisco.com/cisco/software/release.html?mdfid=283819608&flowid=31849&softwareid=282074295&release=8.6\(2a\)SU1&relind=AVAILABLE&rellifecycle=&reltype=latest](http://www.cisco.com/cisco/software/release.html?mdfid=283819608&flowid=31849&softwareid=282074295&release=8.6(2a)SU1&relind=AVAILABLE&rellifecycle=&reltype=latest)

If you are using a virtual machine, follow the steps in Procedure 1, "Prepare a VM for Unity Connection."

If you are using a standalone server, locate the Cisco Unity Connection DVD that shipped with your order, and then follow the steps in Procedure 2, "Prepare a server for Unity Connection."

## Procedure 1 Prepare a VM for Unity Connection

If you are installing Cisco Unity Connection on VMware, follow the steps below to deploy an OVA file in order to define the virtual machine (VM) requirements.

The Cisco Unity Connection OVA file defines the following virtual machine for up to 5000 users:

- Number of virtual CPUs—2 (5.06 GHz Reserved)
- Amount of RAM—6 GB
- Hard disk—1 x 200 GB (aligned at 64KB blocks)
- OS support—Red Hat Enterprise Linux 5 (32-bit)
- VMware ESXi support—ESXi 4.0 or ESXi 4.1 (VM version 7)

The Cisco Unity Connection OVA file defines the following virtual machine for up to 10,000 users:

- Number of virtual CPUs—4 (10.12 GHz Reserved)
- Amount of RAM—6 GB
- Hard disk—2 x 146 GB (aligned at 64KB blocks)
- OS support—Red Hat Enterprise Linux 5 (32-bit)
- VM ware ESXi support—ESXi 4.0 or ESXi 4.1 (VM version 7)

**Step 1:** Open the VMware vSphere client, and then navigate to **File > Deploy OVF Template**.

**Step 2:** Next to the **Deploy from a file or URL** box, click the **Browse** button, find the location of the Cisco Unity Connection OVA file that you downloaded from Cisco, and then click **Next**.

**Step 3:** On the OVF Template Details page, verify the information, and then click **Next**.

If you are deploying Cisco Unity Connection for less than 5000 users, select the virtual machine for up to 5000 users. If you are deploying Unity Connection for 5000 users or more, select the virtual machine for up to 10,000 users.

**Step 4:** In the Deploy OVF Template wizard, enter the following information:

- 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, from the menu, in the **Configuration** list, choose either 5000 users or 10,000 users, and then click **Next**.
- On the Disk Format page, choose **Thick provisioned format**, and then click **Next**.
- On the Ready to Complete page, verify the settings, and then click **Finish**.

**Ready to Complete**  
Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Users\kfleshne\Downloads\CUC_8.6.2_vmv7_v1.5.ova
Download size:	95.0 KB
Size on disk:	292.0 GB
Name:	CUC1
Deployment Configuration:	10,000 Users - 146GB vDisks
Host/Cluster:	chas2-s6.cisco.local
Datastore:	datastore1 (S)
Disk Format:	Thick Provisioning
Network Mapping:	"eth0" to "Servers_1"

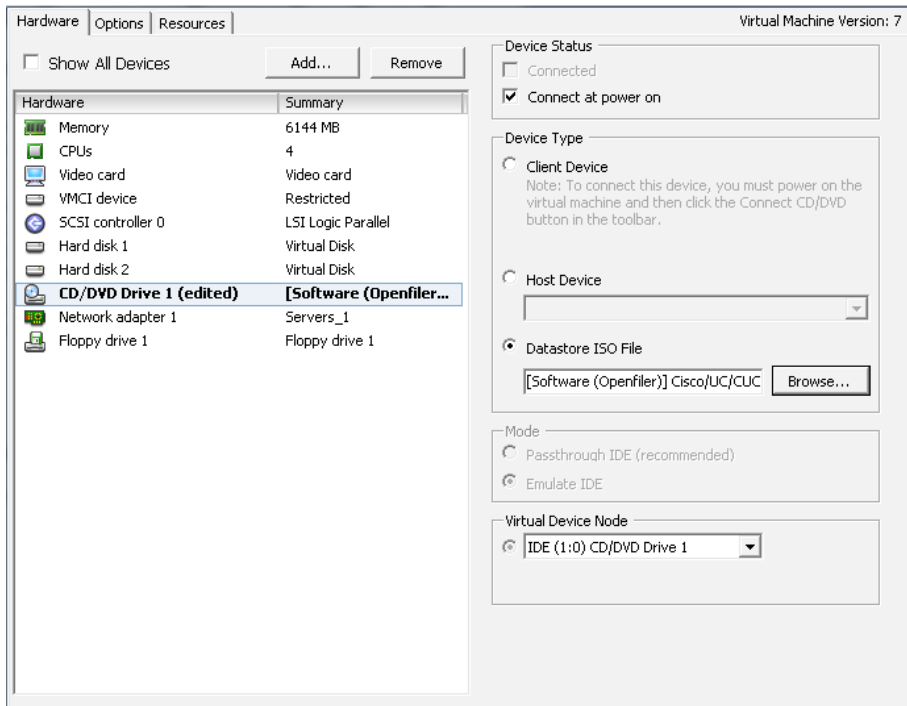
Source  
[OVF Template Details](#)  
[Name and Location](#)  
[Deployment Configuration](#)  
[Disk Format](#)  
**Ready to Complete**

**Step 5:** After the virtual machine is created, navigate to the Getting Started tab, and then choose **Edit virtual machine settings**.

**Step 6:** On the Hardware tab, choose **CD/DVD Drive 1**.

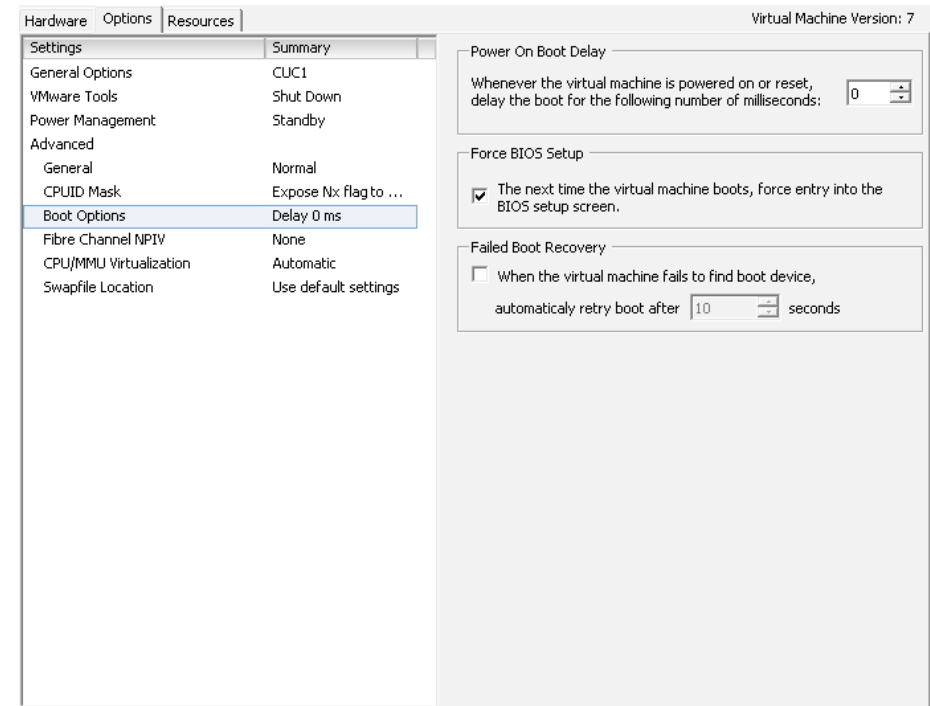
**Step 7:** Select the **Connect at power on** check box.

**Step 8:** Select **Datastore ISO File**, click **Browse**, and then navigate to the location of the Cisco Unity Connection bootable installation file.



**Step 9:** On the Options tab, choose **Boot Options**.

**Step 10:** Select the **The next time the virtual machine boots, force entry into the BIOS setup screen** check box, and then click **OK**.

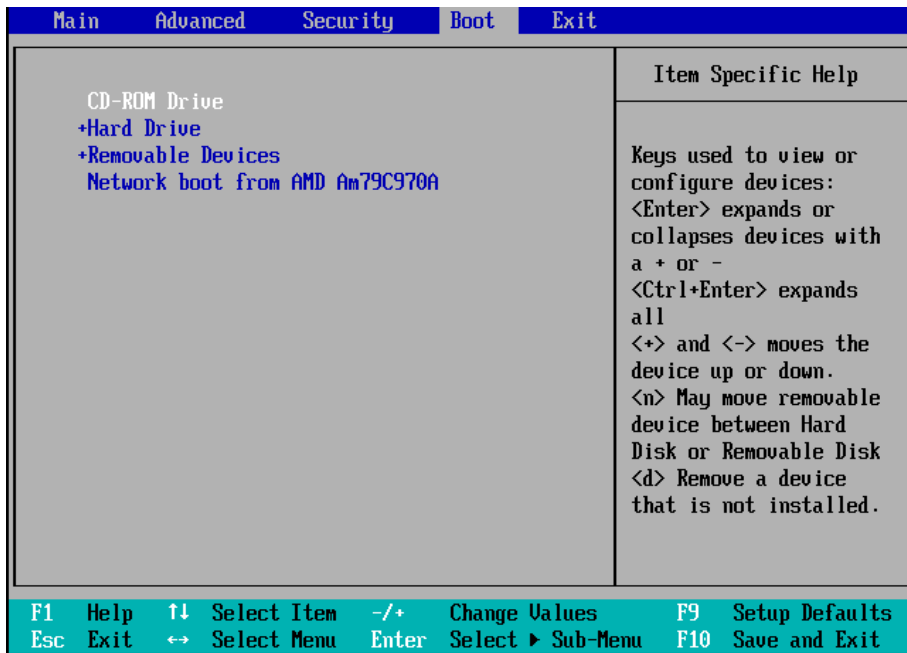


**Step 11:** On the Getting Started tab, choose **Power on the virtual machine**, and then click on the Console tab. Watch the server boot.

**Step 12:** After the machine boots into the **PhoenixBIOS Setup Utility**, use the right arrow key to move to the **Boot** tab.



**Step 13:** Edit the boot order with the + and - keys in order to make **CD-ROM Drive** the first item and **Hard Drive** the second.



**Step 14:** Press the **F10** key. The BIOS settings are saved and you exit the PhoenixBIOS Setup Utility.

**Step 15:** In the Setup Confirmation dialog box, select **Yes**, and then press **Enter**.

**Step 16:** After the datastore ISO file loads from the virtual DVD drive, follow the procedures in “Installing Cisco Unity Connection” to complete the installation.

**Step 2:** Insert the Cisco Unity Connection DVD into the DVD drive.

**Step 3:** Power on the server. It boots from the DVD.

**Step 4:** After the DVD loads, follow the procedures in “Installing Cisco Unity Connection” to complete the installation.

## Process

### Installing Cisco Unity Connection

#### 1. Install Cisco Unity Connection platform

This process is the same whether you are installing in a virtual environment or on a standalone server.

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.

## Procedure 2 Prepare a server for Unity Connection

**Step 1:** Physically install the server, and then attach the monitor, keyboard, and network cable.

Complete the tasks listed below before you start the installation:

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

## Procedure 1 Install Cisco Unity Connection platform

**Step 1:** On the DVD Found page, choose **Yes**. A media check is performed.

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

If the media check does not pass, select another DVD or ISO file, 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:** If you are installing on a standalone server, on the Auto Negotiation Configuration page, choose **Yes**.

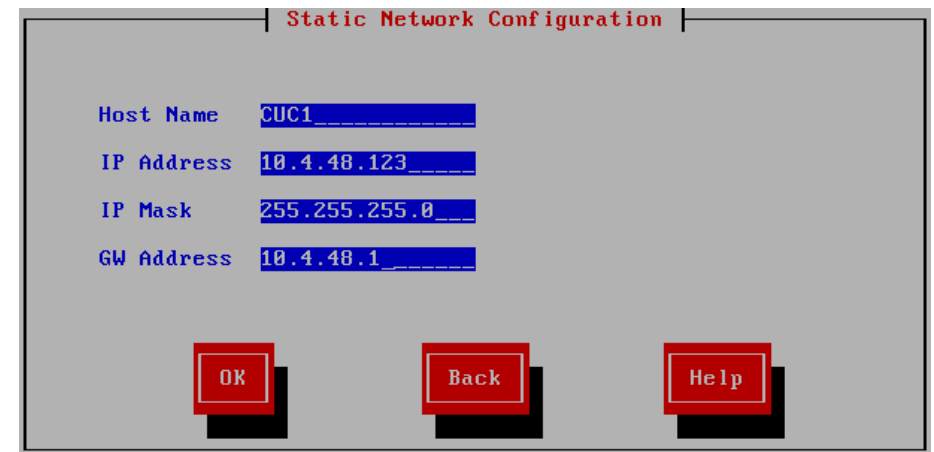
If you are deploying a virtual machine, on the Auto Negotiation Configuration page, choose **Continue**.

**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**:

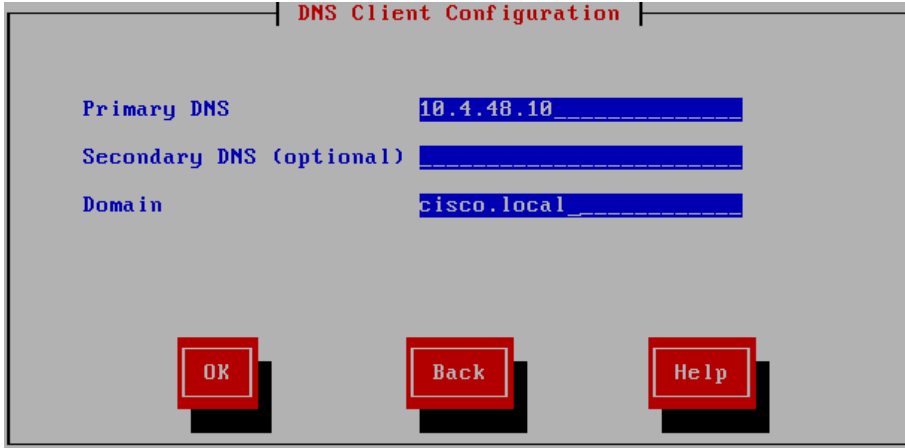
- Host Name—**CUC1**
- IP Address—**10.4.48.123**
- IP Mask—**255.255.255.0**
- GW Address—**10.4.48.1**



**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 **Yes**.


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

You will 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**.

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

**Step 23:** If you deployed a virtual server, return to the VMware vSphere client. You must disable the CD/DVD drive.


If you deployed a standalone server, skip ahead to Step 27.

**Step 24:** From the vSphere client, navigate to the virtual machine's Getting Started tab, and then choose **Edit virtual machine settings**.

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

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

**Step 27:** Use your web browser to access the Cisco Unity Connection Administration interface, and in the center of the page, under **Installed Applications**, click the **Cisco Unity Connection** link.

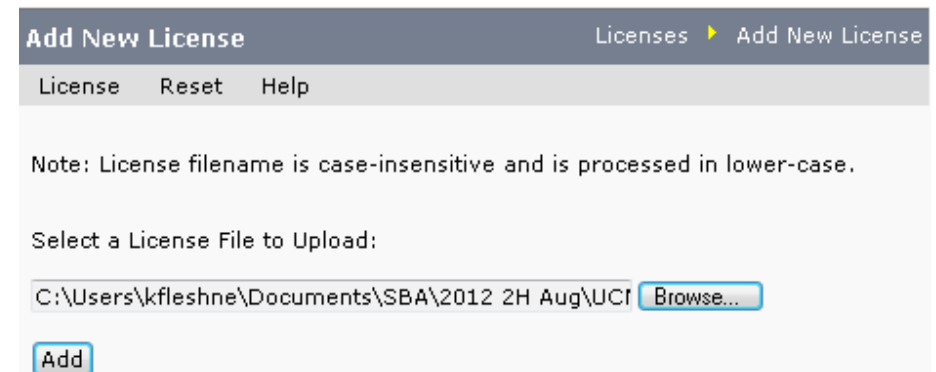
**Tech Tip**

If you receive a warning about the website's security certificate, ignore it and continue to the website page.

**Step 28:** Enter the **Username** and **Password** you entered on the Application User Configuration page in Step 21, and then click **Login**.

**Step 29:** Navigate to **System Settings > Licenses**, and then click **Add New**.

**Step 30:** Using the **Browse** button, locate the license file obtained prior to installation, and then click **Add**.



**Step 31:** Select the check box next to the previously obtained license file, clear the **CUCdemo.lic** check box, and then click **Install Selected**.

**Step 32:** Close the confirmation window, and then in the License Count section, verify the **Value** is correct for each of the licenses you purchased.

License Files

Install Selected

Delete Selected

Add New

	Installed	File Name
<input type="checkbox"/>	No	<a href="#">CUCdemo.lic</a>
<input checked="" type="checkbox"/>	Yes	<a href="#">unity_cuc8.lic</a>

Install Selected

Delete Selected

Add New

Choose Server

Server Name: cuc1

License Count

Licensed Seats For	Feature Name	Value	Used	Unused	Cluster Limit
Users with voice mailboxes	LicSubscribersMax	50	0	50	50
Users with IMAP or Single Inbox access to voice messages	LicIMAPSubscribersMax	50	0	50	50
Cisco Unity Inbox users	LicVMISubscribersMax	50	0	50	50
TTS and ASR (advanced) users	LicAdvancedUserMax	50	0	50	50
Voice ports	LicVoicePortsMax	16	0	16	-
Text-to-speech sessions	LicRealspeakSessionsMax	16	0	16	-
Voice-recognition sessions	LicUnityVoiceRecSessionsMax	16	0	16	-
SpeechView Standard users	LicSTTSubscribersMax	0	0	0	0
SpeechView Professional users	LicSTTProSubscribersMax	0	0	0	0

**Step 33:** In the **Navigation** list, choose **Cisco Unified Serviceability**, and then click **Go**.

**Step 34:** Navigate to **Tools > Service Activation**.

**Step 35:** Select the **Check All Services** check box, and then click **Save**. In the dialog box, 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 by using the Cisco Smart Business Configurator for Collaboration (SBCC) tool, which is available on the Cisco SBA web site.

## Procedure 1

### Configure Cisco Unified CM server and site

**Step 1:** Unzip the Cisco SBCC software package to a folder on your PC, change to the directory, and then double-click **SBCC.exe**.

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

**Step 3:** Navigate to **Server Deployment > New UCM Server and Site**, select the desired **Deployment Model**, and then in the **Publisher/Subscriber Servers** list, choose the correct number of servers for your installation.

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 will be modified for your specific environment based on information entered into the tool.

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

Deployment Model

☐ Unified CM BE - 500 Users
 ☐ Unified CM - 5000 Users
 ☐ Unified CM - 1000 Users
 ☒ Unified CM - 10,000 Users
 ☐ Unified CM - 2500 USers

Publisher/Subscriber Servers\*  Note: This count does not include dedicated TFTP Servers

---

Unified CM Template

Unified CM Template\*

**Step 5:** On the Server and Site Information page, enter the following information, and then click **Next**:

- 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)
- How many remote sites are you supporting—**7**
- Use 2 or 3 Digit Site Codes—**Selected**
- Site Code—**3**
- Check to enable synchronizing users with LDAP—**Selected**
- Check to save all data for future sessions—**Selected**

i

### Tech Tip

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

Server Names

What is the first CUCM node?\*

What is the second CUCM node?\*

What is the third CUCM node?\*

What is the fourth CUCM node?\*

What is the fifth CUCM node?\*

---

LDAP synchronization

Check to enable synchronizing users with LDAP ☒

---

Save Entered Data

Check to save all data entered for future sessions ☒

---

Remote Sites

☒ How many remote sites are you supporting?  (0-500)
 ☒ Use 2 or 3 Digit Site Codes?  Example: 8100

☐ Select the Site Information CSV

**Step 6:** 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**

Site name*	DMI subnet*	DMI subnet mask*	SIP Gateway 1*	SIP Gateway 2	Location Audio Kbps	Site Code
HQ1	10.4.0.0	17	10.4.48.138	10.4.48.139		8100
RS200	10.5.0.0	21	10.5.7.30		96	8200
RS203	10.5.48.0	21	10.5.53.28		192	8203
RS206	10.5.8.0	21	10.5.12.28	10.5.12.29	96	8206
RS210	10.5.144.0	21	10.255.255.210		192	8210
RS211	10.5.152.0	21	10.255.255.211	10.255.253.211	96	8211
RS221	10.5.104.0	21	10.255.251.221		192	8221
RS222	10.5.112.0	21	10.255.252.222	10.255.253.222	384	8222



**Step 7:** 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 8:** 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 9:** 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 10:** Click **Test Connection**. This verifies connectivity to the LDAP server and confirms the credentials entered are valid. In the Connection Test dialog box, press **OK**.

LDAP System Information

LDAP Server Type **Microsoft Active Directory**

LDAP Attribute for User ID **sAMAccountName**

LDAP Custom Filter

Filter Name **IP Phones Only**

Filter **(ipphone=\*)**


LDAP Directory and Authentication Information

IP Address/Host Name\* **10.4.48.10** Ports\* **389** **Test Connection**

Distinguished Name\* **Administrator@cisco.local**

Password\* **••••••••** User Search Base\* **cn=users, dc=cisco, dc=local**

**Step 11:** If the LDAP server information is correct, click **Next**.



**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 12:** On the Field Mapping Information page, choose the following options from the three lists, 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	manager

**Step 13:** On the Unified CM Dial-Plan page, enter the following information:

- Directory number extension range start—**8000000**
- 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**

The Dial Plan templates consist of a set of default route patterns which are used for 7-digit and 10-digit local dialing in the US.

**Step 14:** In the Dial Plan Template section, click **Select File**, choose the correct template for your installation, and then click **Next**.

Phone Auto Registration w/ DN Extension Range		
The directory number extension range start.*	<input type="text" value="8000000"/>	
The directory number extension range end.*	<input type="text" value="8009000"/>	
Voice Messaging Information		
Hunt Pilot for voicemail ports.*	<input type="text" value="8009400"/>	Number of voicemail ports.*
The start of the extension range of voicemail ports.*	<input type="text" value="8009401"/>	<input type="text" value="24"/>
The MWI directory ON number.*	<input type="text" value="8009998"/>	
The MWI directory OFF number.*	<input type="text" value="8009999"/>	
Dial Plan Template		
Select the Dial Plan template.*	<input type="text" value="CC\SBCC Start\template\dialplan\US 10-digit local Dial Plan.csv"/>	<input type="button" value="Select File"/>

**Step 15:** In the Phone NTP and Date/Time Group Information sections, enter the following information, and then click **Next**:

- NTP Server IP Address—**10.4.48.17**
- Mode—**Directed Broadcast**
- Group Name—**[Group Name]**
- Time Zone—**[Time Zone]**
- Separator—**/ (slash)**
- Date Format—**M/D/Y**
- Time Format—**12-Hour**

Phone NTP Reference	
NTP Server IP Address*	<input type="text" value="10 . 4 . 48 . 17"/>
Mode*	<input type="text" value="Directed Broadcast"/>
Date/Time Group Information	
Group Name*	<input type="text" value="Pacific Time Zone"/>
Time Zone*	<input type="text" value="America/Los_Angeles"/>
Separator*	<input type="text" value="/ (slash)"/>
Date Format*	<input type="text" value="M/D/Y"/>
Time Format*	<input type="text" value="12-hour"/>

**Step 16:** The Summary Information page provides a summary of all inputs entered into Cisco SBCC up to this point. If all information shown is correct, click **Next**.

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

**Step 17:** 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**
- User Name—**cucmadmin**
- Password—**[password]**

**Step 18:** Click **Test Connection**. This verifies connectivity to the Cisco Unified CM server and confirms the credentials entered are valid. In the Connection Test dialog box, click **OK**.

<input checked="" type="checkbox"/> Configure Server			
Cisco Unified CM.*	IP Address/Host Name	User Name	Password
	<input type="text" value="10.4.48.110"/>	<input type="text" value="cucmadmin"/>	<input type="password" value="••••••"/>
<input type="button" value="Test Connection"/>			

**Step 19:** 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 22.

**Step 20:** In the Save dialog box, accept the default file name or enter a file name of your own choosing, and then, click **Save**.

**Step 21:** 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 Cisco SBCC.

☒ **Export File**

Package Filename\*: A:\2012 2H Aug\SBCC\SBCC Start\packet\server\Export\_Server\_201206221040.tar **Save As**

Remark: SBCC Test

**Step 22:** After choosing your configuration method from the options listed in the previous steps, click **Configure**.

Cisco SBCC displays its progress on the Update Information page. Please wait until you see the LDAP window before continuing with the next set of steps. Depending on the speed of your publisher, the update can take up to five minutes to complete.

## 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 Cisco SBCC is complete. If you are not using LDAP, please skip ahead 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 SBCC. For example, **MS Active Directory**.

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

**LDAP Directory Information**

LDAP Configuration Name\* MS Active Directory

LDAP Manager Distinguished Name\* Administrator@cisco.local

LDAP Password\* .....

Confirm Password\* .....

LDAP User Search Base\* cn=users, dc=cisco, dc=local

LDAP Custom Filter IP Phones

**LDAP Directory Synchronization Schedule**

Perform Sync Just Once ☐

Perform a Re-sync Every\* 7 DAY

Next Re-sync Time (YYYY-MM-DD hh:mm)\* 2012-05-30 00:00

**User Fields To Be Synchronized**

Cisco Unified Communications Manager User Fields	LDAP User Fields	Cisco Unified Communications Manager User Fields	LDAP User Fields
User ID	sAMAccountName	First Name	givenName
Middle Name	middleName	Last Name	sn
Manager ID	manager	Department	department
Phone Number	ipPhone	Mail ID	mail

**LDAP Server Information**

Host Name or IP Address for Server\* 10.4.48.10 LDAP Port\* 389 Use SSL ☐

**Add Another Redundant LDAP Server**

— **Save** **Delete** **Copy** **Perform Full Sync Now** **Add New** —

**Step 4:** You must confirm all users have been synchronized from Active Directory. Navigate to **User Management > End User**, and then click **Find**.

This process may take a few minutes to complete, depending on the number of users synchronized.

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

- LDAP Password—[password]
- Confirm Password—[password]

**Status**  
 Update successful

**LDAP Authentication for End Users**  
☒ Use LDAP Authentication for End Users  
 LDAP Manager Distinguished Name\* Administrator@cisco.local  
 LDAP Password\* .....  
 Confirm Password\* .....  
 LDAP User Search Base\* cn=users, dc=cisco, dc=local

**LDAP Server Information**  
 Host Name or IP Address for Server\* 10.4.48.10 LDAP Port\* 389 Use SSL ☐  
 Add Another Redundant LDAP Server



### 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.

## 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 an IP address, 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 in 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 in the dialog box that appears, click **OK**.

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

Servers (1 - 7 of 7)			Rows per Page 50
Find Servers where Host Name/IP Address begins with Find Clear Filter			
<input type="checkbox"/>	Host Name/IP Address ^	Description	
<input type="checkbox"/>	10.4.48.110	Publisher	
<input type="checkbox"/>	10.4.48.111	Subscriber 1	
<input type="checkbox"/>	10.4.48.112	Subscriber 2	
<input type="checkbox"/>	10.4.48.113	Subscriber 3	
<input type="checkbox"/>	10.4.48.114	Subscriber 4	
<input type="checkbox"/>	10.4.48.120	TFTP Server 1	
<input type="checkbox"/>	10.4.48.121	TFTP Server 2	

**Step 6:** Return to the Cisco SBCC program, in the LDAP window, click **Continue**, and then click **Finish**.

This completes the first phase of the Cisco SBCC program.

## Procedure 4 Configure the Unity Connection server

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

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

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

**Step 3:** In the left hand 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**:

- 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)

Port Group
Reset
Help

Save

### New Port Group

Phone System
PhoneSystem

Create From
☒ Port Group Type
SCCP

☐ Port Group

### Port Group Description

Display Name\*
PhoneSystem-1

Device Name Prefix\*
CiscoUM1-VI

MWI On Extension
8009998

MWI Off Extension
8009999

### Primary Server Settings

IPv4 Address or Host Name
10.4.48.111

IPv6 Address or Host Name

Port
2000

TLS Port
2443

Save

**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)

Cisco Unified Communications Manager Servers
Delete Selected
Add

	Order	IPv4 Address or Host Name	IPv6 Address or Host Name	Port	TLS Port	Server Type
<input type="checkbox"/>	0	10.4.48.111		2000	2443	Cisco Unified Communications Manager
<input type="checkbox"/>	1	10.4.48.112		2000	2443	Cisco Unified Communications Manager

Delete Selected
Add

☒ Reconnect to a Higher-order Cisco Unified Communications Manager When Available

TFTP Servers
Delete Selected
Add

	Order	IPv4 Address or Host Name	IPv6 Address or Host Name
<input type="checkbox"/>	0	10.4.48.120	
<input type="checkbox"/>	1	10.4.48.121	

Delete Selected
Add

**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, select **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:** In 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 **Starting** to **Started**.

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

**Step 16:** On the left hand 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**.

**Codec Advertising**

**Advertised Codecs**

- G.711 mu-law
- G.729
- iLBC

^ v

**Unadvertised Codecs**

- G.711 a-law
- G.722

**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**.

**New Phone System Port**

☒ **Enabled**

**Number of Ports** 24

**Phone System** PhoneSystem

**Port Group** PhoneSystem-1

**Server** cuc1.cisco.local

**Port Behavior**

☒ **Answer Calls**

☒ **Perform Message Notification**

☒ **Send MWI Requests (may also be disabled by the port group)**

☒ **Allow TRAP Connections**

**Security Mode** Non-secure

**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 Password** list, choose **Voice Mail**. In **Password** and **Confirm Password**, 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 the **Enable Synchronizing from LDAP Server** check box, 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 Cisco SBCC.

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.

**LDAP Directory Information**

LDAP Configuration Name\*

LDAP Manager Distinguished Name\*

LDAP Password\*

Confirm Password\*

LDAP User Search Base\*

LDAP Custom Filter

**LDAP Directory Synchronization Schedule**

Perform Sync Just Once ☐

Perform a Re-sync Every\*  DAY

Next Re-sync Time (YYYY-MM-DD hh:mm)\*

**User Fields To Be Synchronized**

Cisco Unified Communications Manager User Fields	LDAP User Fields	Cisco Unified Communications Manager User Fields	LDAP User Fields
User ID	sAMAccountName	First Name	givenName
Middle Name	middleName	Last Name	sn
Manager ID	manager	Department	department
Phone Number	ipPhone	Mail ID	mail

**LDAP Server Information**

Host Name or IP Address for Server\*  LDAP Port\*  Use SSL ☐

**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 in the dialog box, click **OK**.

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

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

- 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**

**LDAP Authentication for End Users**

☒ Use LDAP Authentication for End Users

LDAP Manager Distinguished Name\*

LDAP Password\*

Confirm Password\*

LDAP User Search Base\*

**LDAP Server Information**

Host Name or IP Address for Server\*  LDAP Port\*  Use SSL ☐

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

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

**Find**

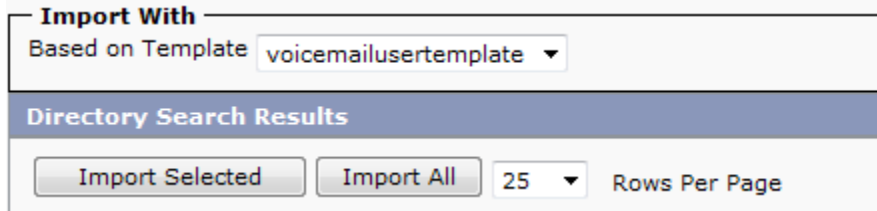
Find End Users In

Where  Begins With

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

**Step 35:** If you created an LDAP custom filter to limit your selection, click **Import All**.

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. This may take several minutes, depending on the number of users being imported.

## 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 Cisco SBCC 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 login to the phone, the users will enter their LDAP User ID and the default PIN of '112233'.

## Procedure 1

### Configure user and device profiles

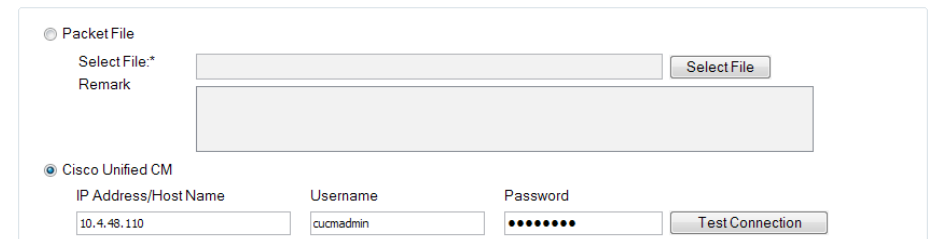
**Step 1:** From the Cisco SBCC main page, navigate to **Server Deployment > Modify CUCM and CUC Users and Device Profiles**.

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

- IP Address—**10.4.48.110**
- 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. In the Connection Test dialog box, click **OK**.

**Step 4:** Click **Next**. Cisco SBCC reads the user information from Cisco Unified CM. Depending on the size of the user database and the speed of the publisher, this may take several minutes to complete.



**Step 5:** After Cisco SBCC is done reading the user information from Cisco Unified CM, the first five users are displayed.

**Step 6:** 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.

The first three columns are auto-generated from the source data and the information they contain cannot be changed.

**Step 7:** Some users that were exported as part of the list 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

You may use the <Shift> key to highlight multiple users at one time or the <Ctrl> key to pick individual users from the list at any time during data entry.

**Step 8:** For each user device profile (UDP), populate the **Directory Number**, **External Phone Number Mask**, **Line CSS**, **Line Text Label** and **Device Profile** fields as follows, and then click **Configure**:

- **Directory Number**—This is the number that was synchronized from the iPhone 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)

Device Profile Name *	Description	User ID	Directory Number *	External Phone Number Mask	Line CSS	Line Text Label	Device Profile *
agroudan_Profile	agroudan	agroudan	85114013	311611XXXX	CSS_Internati...	Adam Groudan	UDP_9971.xml
annc_Profile	annc	annc	85114015	311611XXXX	CSS_Internati...	Ann Chang	UDP_9971.xml
aobrien_Profile	aobrien	aobrien	85114014	311611XXXX	CSS_Internati...	Alan OBrien	UDP_9971.xml
bethomas_Profile	bethomas	bethomas	85144044	314614XXXX	CSS_Internati...	Ben Thomas	UDP_9971.xml
callejas_Profile	callejas	callejas	85144043	314614XXXX	CSS_Internati...	Arlindo Callejas	UDP_9971.xml

**Step 9:** On the Configuration Information page, select **Configure Server**, and then enter the following information:

- Cisco Unified CM IP Address—**10.4.48.110**
- 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 10:** Click **Test Connection**. This verifies connectivity to the servers and confirms the credentials entered are valid. In the Connection Test dialog box, click **OK**.

☒ Configure Server

	IP Address/Host Name	Username	Password	
Cisco Unified CM:*	10.4.48.110	cucmadmin	••••••••	<input type="button" value="Test Connection"/>
Unity Connection:*	10.4.48.123	cucadmin	••••••••	<input type="button" value="Test Connection"/>

**Step 11:** 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 14.

**Step 12:** In the Save window, accept the default file name or enter a file name of your own choosing, and then click **Save**.

**Step 13:** Enter a **Remark**, which is then saved with the package file.

☒ Export File

Folder Name: \*

Remark:

**Step 14:** After choosing your preferred method from the options in the steps above, click **Configure**.

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

This completes the second phase of the Cisco SBCC 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. 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 Cisco SBA 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, this can take more than 60 minutes to complete.

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

- IP Address/Host Name—**10.4.48.110**
- Username—**cucmadmin**
- Password—**[password]**

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

IP Address/Host Name	Username	Password
10.4.48.110	cucmadmin	••••••••

Search

PhoneList

Remove Phone

Device Name(line)	Description	Device pool	Device protocol	Model
SEP0023339C9515	Auto 8001000	DP_RS210_1	SCCP	Cisco 7942
SEP866F2F686EA	Auto 8001002	DP_RS222_1	SCCP	Cisco 6961
SEP503DE53008F8	Auto 8001005	DP_RS208_1	SCCP	Cisco 6961
SEP2893FE1302A7	Auto 8001004	DP_RS200_1	SIP	Cisco 8961
SEP2893FE12FEE3	Auto 8001006	DP_RS200_2	SIP	Cisco 8961
SEP5475D02B3883	Auto 8001008	DP_RS212_1	SCCP	Cisco 6921
SEP80462EA85B9	Auto 8001009	DP_RS206_1	SIP	Cisco 9971
SEP5475D02B3875	Auto 8001010	DP_RS211_1	SCCP	Cisco 6921
SEP1C17D337D24C	Auto 8001011	DP_RS232_1	SIP	Cisco 9971
SEP00574CF71AE4	Auto 8001012	DP_RS204_1	SIP	Cisco 9971
SEPDC7B94F8F317	Auto 8001013	DP_RS221_1	SIP	Cisco 8961
SEP5475D02B2D3B	Auto 8001014	DP_RS206_2	SCCP	Cisco 6941
SEP0023339C97B5	Auto 8001015	DP_RS201_1	SCCP	Cisco 7942
SEPACA0166F24ED	Auto 8001017	DP_HQ1_1	SIP	Cisco 9971
SEP000000000000	Auto 8001018	DP_HQ1_1	SCCP	Cisco 6961

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

**Step 5:** On the first dialog box, click **Yes**, and then on the second dialog box, click **OK**.

**Step 6:** After this phase of the tool is complete, exit out of the Cisco SBCC program by clicking the **Red X** on the right side of the title bar. In the dialog box, click **Yes**.

This completes the third phase of the Cisco SBCC program. Allow a several minutes for the phones to reset and reregister 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 Gateways, Conference Bridges, PSTN, 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 Gateways, Conference Bridges, PSTN, 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. For details about ACS configuration, see the *Cisco SBA—Device Management using ACS Deployment 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 login 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 Gateways, Conference Bridges, PSTN, and SRST”.

This procedure describes different options for connecting your standalone voice router to the LAN. Options are provided for connecting to Cisco Nexus switches in the data center and for connecting to Cisco Catalyst switches in the server room, remote-site distribution layer, or remote-site access layer switches. 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).

### 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 Nexus 2248TP-Es connected to two Nexus 5548UPs using EvPC. Step 1 and Step 4 are repeated on both 5548UPs 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 the 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 Gateways, Conference Bridges, PSTN 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 Gateways, Conference Bridges, PSTN, and SRST

1. Configure conference bridges
2. Configure PSTN interfaces
3. Configure SRST for SCCP phones
4. Configure SRST for SIP phones
5. Block voice traffic on WAN links

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

#### 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 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 subscriber and as the second priority on the publisher. The same configuration is used in the remote-site routers if conferencing resources are needed.

**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 [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 [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
```

**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 [type] [number]
  associate ccm 1 priority 1
  associate ccm 2 priority 2
  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 Cisco SBCC, 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 PSTN interfaces

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.

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.

**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.

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

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



### Reader Tip

Toll fraud prevention is enabled by default in the version of Cisco IOS used for this configuration. The following two dial-peer commands permit call signaling from both 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.

For more information about this topic, search for **Toll Fraud Prevention Enhancement** on [cisco.com](http://cisco.com).

**Step 8:** 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. The destination pattern will match the ten digits coming in from the PSTN provider.

```
dial-peer voice 100 voip
  description SIP TRUNK to 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 SUB2
  preference 2
  destination-pattern 310610....
  voice-class codec 1
  session protocol sipv2
  session target ipv4:10.4.48.112
  incoming called-number .
!
```

**Step 9:** Create the basic telephone service (also known as *POTS*) dial peers for outbound emergency, local, national and international calls to the PSTN. Strip the leading 9, and only forward the digits that are expected by the carrier. For international dialing, which are variable in length, prefix the 011 needed by the long-distance carrier in order to properly route the call.

```
dial-peer voice 1911 pots
  preference 1
  destination-pattern 911
  port 0/0/0:23
  forward-digits 3
!
```

```
dial-peer voice 19911 pots
  preference 1
  destination-pattern 9911
  port 0/0/0:23
  forward-digits 3
!
dial-peer voice 17 pots
  preference 1
  destination-pattern 9[2-9].....
  port 0/0/0:23
  forward-digits 7
!
dial-peer voice 111 pots
  preference 1
  destination-pattern 91[2-9]..[2-9].....
  port 0/0/0:23
  forward-digits 11
!
dial-peer voice 19011 pots
  preference 1
  destination-pattern 9011T
  incoming called-number .
  direct-inward-dial
  port 0/0/0:23
  prefix 011
```

**Step 10:** 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
  preference 2
  destination-pattern 911
  port 0/0/1:23
  forward-digits 3
!
dial-peer voice 29911 pots
  preference 2
  destination-pattern 9911
  port 0/0/1:23
  forward-digits 3
!
dial-peer voice 27 pots
  preference 2
  destination-pattern 9[2-9].....
  port 0/0/1:23
  forward-digits 7
!
dial-peer voice 211 pots
  preference 2
  destination-pattern 91[2-9]..[2-9].....
  port 0/0/1:23
  forward-digits 11
!
dial-peer voice 29011 pots
  preference 2
  destination-pattern 9011T
  incoming called-number .
  direct-inward-dial
  port 0/0/1:23
  prefix 011
```

### Procedure 3

### 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 section.

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.

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.

**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.

```
voice translation-rule 1
  rule 1 /^[1-7]...$/ /8511\0/
```

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

**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 or declined.

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

```
dialplan-pattern 1 311611.... extension-length 8 extension-
pattern 8511....
```

Apply the translation profile for incoming calls when phones are in SRST mode.

```
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 10-digit call arrives from the PSTN carrier, the call is directed to the correct phone, based on the last four digits.

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

## Procedure 4 **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.

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.

**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.

```
voice translation-rule 1
  rule 1 /^[1-7]...$/ /8511\0/
```

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

**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 or declined.

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

```
dialplan-pattern 1 311611.... extension-length 8 extension-  
pattern 8511....
```

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 10-digit call arrives from the PSTN carrier, the call is directed to the correct phone, based on the last four digits.

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

**Step 5:** 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
```

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

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

**Step 6:** 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 5

## 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.

**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
```

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
Call Control	Cisco Media Convergence Server 7845-I3 for Unified Communications Manager up to 10,000 users	MCS7845I3-K9-CMD3A	8.6(2a)SU1
	Cisco Media Convergence Server 7835-I3 for Unified Communications Manager up to 2500 users	MCS7835I3-K9-CMD3A	
Voice Messaging	Cisco Media Convergence Server 7845-I3 for Unity Connection up to 10,000 users	MCS7845I3-K9-UCC2	8.6(2a)SU1
	Cisco Media Convergence Server 7835-I3 for Unity Connection up to 2500 users	MCS7835I3-K9-UCC2	
Call Control Virtual Servers	Cisco UCS C210 M2 General-Purpose Rack-Mount Server for unified communications applications	UCS-C210M2-VCD2	8.6(2a)SU1 ESXi4.1
	Cisco UCS C200 M2 High-Density Rack-Mount Server for unified communications applications	UCS-C200M2-VCD2	
	Unified CMBE6K UCS C200M2 for Unified Communications Manager up to 500 users	UCS-C200M2-BE6K	

## 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	15.1(4)M4 securityk9 datak9 uck9
	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	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-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	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	15.1(4)M4 securityk9 datak9 uck9
	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	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-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	HWIC-2CE1T1-PRI	
	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card-T1/E1	VWIC2-2MFT-T1/E1	
Remote Site Voice Routers	Cisco 881 SRST Ethernet Security Router with FXS FXO 802.11n FCC Compliant	C881SRST-K9	15.1(4)M2 voice

## Endpoints

Functional Area	Product Description	Part Numbers	Software
Phones	Unified IP Phone with six lines, video, color, Wi-Fi, Bluetooth, USB	CP-9971	—
	Unified IP Phone with four lines, video, color	CP-8945	—
	Unified IP Conference Phone	CP-7937G	—
	Unified IP Wireless Phone with six lines, color, Bluetooth	CP-7926G	—
	Unified IP Phone with twelve lines	CP-6961	—
	Unified IP Phone with four lines	CP-6945	—
	Unified IP Phone with two lines	CP-6921	—
	Unified IP Phone with one line	CP-6901	—
	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 5.1(3)N1(1a) 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	

Functional Area	Product Description	Part Numbers	Software
Ethernet Extension	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	—
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	
	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(1)SE2 IP Base
	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(1)SE2 IP Base
	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	3.3.0.SG(15.1-1SG) IP Base
	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 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(1)SE2 IP Base
	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	

Functional Area	Product Description	Part Numbers	Software
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(1)SE2 IP Base
	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(1)SE2 LAN Base
	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: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We added server scaling and Cisco Unified CM redundancy options for customers with up to 5000 and 10,000 users.
- We added support for dual SIP gateways at each site.
- We added support for dual IOS conference bridges at each site.
- We added support for Phone NTP Reference and Time Zone.
- We added support for site codes in Cisco SBCC and SRST.
- We added support for importing site information from a .csv file.
- We added support for Location audio bandwidth per site.
- We added support for Dial Plan templates.
- We added support for saving all entries in the Cisco SBCC tool.
- We added a feedback option in the Cisco SBCC tool.
- We added support for standalone voice gateways at each site.
- We added support for blocking voice traffic on backup WAN interfaces.
- We changed the dial plan information in order to align it with new telephony integration guides. This change ensures the voice guides use a common set of extension numbers and dialing rules.
- We updated the software on the voice infrastructure equipment and the endpoints to the latest shipping versions.

## Notes

## Feedback

Click [here](#) to provide feedback to Cisco SBA.



## SMART BUSINESS ARCHITECTURE

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.



**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](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)