



Unified Communications Using Cisco BE6000

Cisco Validated Design Guide

October 2015

© 2015 Cisco Systems, Inc. All rights reserved.





Contents

Preface	4
How to Read Commands	4
Comments and Questions.....	5
CVD Navigator	6
Use Cases	6
Scope	6
Proficiency.....	7
Introduction.....	8
Technology Use Case.....	8
Use Case: Centralized Unified Communications.....	8
Design Overview	10
Cisco Preferred Architecture.....	10
Solution Details.....	11
Cisco Unified Communications.....	11
Single Cluster Centralized Design	11
Cisco Unified Computing System.....	14
Prime collaboration Provisioning.....	14
Self Provisioning	14
Active Directory Integration	14
Cisco Voice Gateways.....	15
Dial Plan	15
Site Codes	17
Class of Service	17
Local Route Groups	19
Survivable Remote Site Telephony.....	21
Device Mobility.....	23
Extension Mobility	23
Media Resources	23
Call Admission Control.....	24
Point-to-Point Video.....	24
IM and Presence.....	24
Self Care	26
Phone Models.....	26



Deployment Details..... 28

 Preparing the Network for IP Phones..... 30

 Network Preparation Summary..... 33

 Preparing the Server for Cisco Unified CM..... 34

 Installing Cisco Unified CM..... 36

 Preparing the Platform for Cisco Unity Connection 43

 Installing Cisco Unity Connection..... 45

 Preparing the server for Cisco Unified CM IM and Presence..... 47

 Installing Cisco Unified CM IM and Presence 49

 Preparing the server for Cisco Prime Collaboration..... 51

 Installing Cisco Prime Collaboration Provisioning..... 52

 Configuring Cisco Unified CM using Cisco Prime Collaboration..... 52

 Configuring Conference Bridges and SRST..... 62

Appendix A: Product List..... 69

 Data Center or Server Room..... 69

 Headquarters Voice..... 69

 Site Voice 69

 Endpoints..... 70

Appendix B 71

 BE6000S sample network configuration..... 71



Preface

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

Documentation for Cisco Validated Designs

[Cisco Preferred Architecture \(PA\) Design Overview](#) guides help customers and sales teams select the appropriate architecture based on an organization's business requirements; understand the products that are used within the architecture; and obtain general design best practices. These guides support sales processes.

[Cisco Validated Design \(CVD\)](#) guides provide detailed steps for deploying the Cisco Preferred Architectures. These guides support planning, design, and implementation of the Preferred Architectures.

[Cisco Collaboration Solution Reference Network Design \(SRND\)](#) guide provides detailed design options for Cisco Collaboration. The SRND should be referenced when design requirements are outside the scope of Cisco Preferred Architectures.

How to Read Commands

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

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

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

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



Comments and Questions

If you would like to comment on a guide or ask questions, please email collab-mm-cvd@external.cisco.com.

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

<http://www.cisco.com/go/cvd/collaboration>



CVD Navigator

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

Use Cases

This guide addresses the following technology use cases:

- **Centralized Unified Communications**—Organizations require high-quality voice and video communications that can scale up to a thousand users using Cisco Business Edition 6000 (BE6000). They need a solution that is easy to deploy and simple to manage from a central location, without replicating costly features at their remote sites.

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

Scope

This guide covers the following areas of technology and products:

- Unified communications applications, such as IP telephony Voicemail and IM and Presence
- Virtualized servers
- Voice gateways and conference bridges
- IP telephones with remote-site survivability
- Session Initiation Protocol (SIP) signaling
- Lightweight Directory Access Protocol integration
- Cisco Prime Collaboration Provisioning (PCP)

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

Related PA Guides

[Cisco Preferred Architecture for Midmarket Voice 11.x Design](#)

Related CVD Guides

[Collaboration Edge Using Cisco Business Edition 6000](#)

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



Proficiency

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

- **CCNA Collaboration**—1 to 3 years designing, installing, and troubleshooting voice and unified communications applications, devices, and networks.



Introduction

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

To remain competitive, you need to provide reliable and consistent access to your communications resources. The importance of dependable collaboration channels inside and outside of your organization cannot be overstated. To be effective, collaboration technology must be easy to deploy and manage and intuitive to use.

Technology Use Case

Collaboration has always been an essential component of a successful organization. New pressures, heightened by a challenging global economic environment, are making organizations realize collaboration is more important than ever. Specifically, they are trying to manage operational expenses and capital expenses while increasing worker productivity and staying ahead of the competition.

You can only accomplish this “do more with less” approach 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 communication**—Collaborative applications enable real-time communication to empowered users and provide for information sharing and privacy. Because information is shared across the entire user community, its accuracy is more easily verified and corrected.
- **Accelerate through innovation**—Organizations that successfully adopt new collaborative processes are able to move faster, make better decisions, draw from a deeper base of information, and more effectively operate across time and distance barriers. As is always the case in business, either you pull ahead, or the competition will leave you behind.

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

Use Case: Centralized Unified Communications

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



This design guide enables the following capabilities:

- **Single cluster centralized design**—Makes the solution simpler to deploy and easier to manage from a centralized site while saving on infrastructure components. In the single cluster centralized design, each remote site connects to the headquarters site through a WAN and each site receives call processing features from the headquarters location.
- **Self Provisioning**—Allows an end user or administrator to add an unprovisioned phone to a Cisco Unified Communications Manager system with minimal administrative effort.
- **Lightweight Directory Access Protocol integration**—Uses an LDAP directory integration with Prime Collaboration Provisioning(PCP) for designs that require a single source of information for user management.
- **Dial Plan**—Allows you to control how Public Switched Telephony Network (PSTN) are handled for your users. Site or country specific dialling behaviours may be added using Prime Collaboration Provisioning.
- **Uniform on-net dial plan**—Uses endpoint addressing that consists of a uniform on-net dial plan containing 4-digit extensions. An optional access code and 2-digit or 3-digit site codes are available with local site 4-digit dialing.
- **Local route groups**—Uses local route groups in order to reduce the number of route patterns required to provision Session Initiation Protocol (SIP) gateways for all sites.
- **Class of service**—Provisions class of service (CoS) categories with the use of partitions and calling search spaces in order to allow emergency, local, long distance and international dialing capabilities.
- **Survivable Remote Site Telephony (SRST)**—Provides failover at each remote site by standard SRST for SIP and Skinny Client Control Protocol (SCCP) phones.
- **Device Mobility**—Uses the Device Mobility feature, which allows Cisco Unified CM to determine the physical locations of devices and apply call handling policies accordingly.
- **Server load balancing**—Load-balances phones across Cisco Unified CM redundancy groups on a phone-by-phone basis.
- **Extension Mobility**—Uses the Cisco Extension Mobility feature for all phones, which enables users to assign a Cisco Unified IP Phone as their own or move from phone-to-phone within the organization.
- **Media resources**—Provisions individual media resources, such as conference bridges for every site.
- **Call Admission Control**—Provides location-based Call Admission Control (CAC) for a typical hub-and-spoke WAN environment.
- **Voice messaging**—Provisions Cisco Unified CM for voice messaging integration and configured with PCP(Prime collaboration Provisioning).
- **Instant Messaging and Presence**—Provisions Cisco Unified CM IM and presence service integration.
- **Point-to-Point Video**—Enables automatic point-to-point video calling between two participants with video endpoints.
- **Simplified Administration**—Cisco Prime Collaboration Provisioning provides simplified, unified management for multiple services from a single interface.



Design Overview

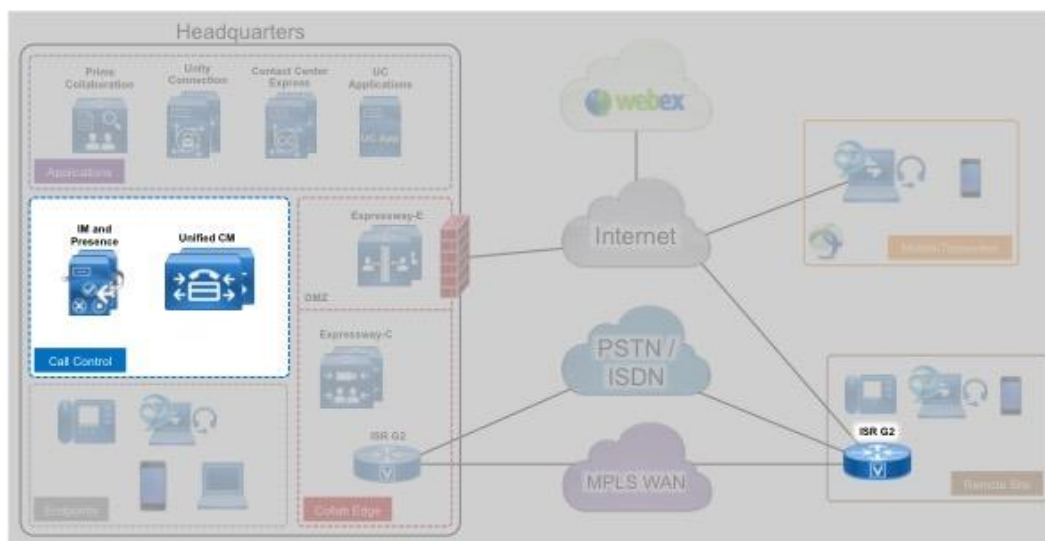
This design guide reduces cost of technology selection and implementation by recommending appropriate equipment and using methods and procedures that have been developed and tested by Cisco. Applying the guidance within this document reduces the time required for adoption of the technology and allows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

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

Cisco Preferred Architecture

Cisco Preferred Architectures provide recommended deployment models for specific market segments based on common use cases. They incorporate a subset of products from the Cisco Collaboration portfolio that is best suited for the targeted market segment and defined use cases. These deployment models are prescriptive and built to scale with an organization as its business needs change. This prescriptive approach simplifies the integration of multiple system-level components and enables an organization to select the deployment model that best addresses its business needs.

The Cisco Preferred Architecture (PA) recommends capabilities that enable organizations to realize immediate gains in productivity and add value to their current voice deployments.





Solution Details

The Unified Communications CVD includes the following components:

- Cisco Unified Communications Manager (Unified CM), for call control and SIP endpoint registrations.
- Cisco Unity Connection , for Voice messaging.
- Cisco Unified CM IM & Presence for Instant Messaging and to show presence status for endpoints.
- Cisco Prime Collaboration Provisioning for provisioning endpoints and integrating UC applications.
- Desktop (Cisco 8800 series IP phones, Cisco Jabber and Cisco Desktop Collaboration Experience DX series) and multipurpose (Cisco TelePresence SX 10 and 20 Quick Set) systems for placing and receiving calls.

Cisco Unified Communications

The products and priorities for this design were based on requirements from customers, partners, and Cisco field personnel. Your specific business requirements may be different from those in this guide, in which case, the product selection may not exactly match your needs.

Cisco Unified Communications has the following software components:

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

This guide uses a 1:1 publisher-subscriber cluster design to provide redundant call control for the target use case.

Single Cluster Centralized Design

The following single cluster centralized design model provides a highly available and scalable call-control and voicemail system capable of Unified Messaging.

The Cisco Business Edition (BE) 6000 uses a single Cisco UCS server platform for up to 1000 users. The virtualized server provides the following:

- The publisher, subscriber and TFTP functions are combined with Cisco Unity Connection on a single hardware platform in order to help lower the capital and operational expenses.
- The Cisco UCS C220 M4 hardware platform for the BE6000 is a 1 rack unit form factor.

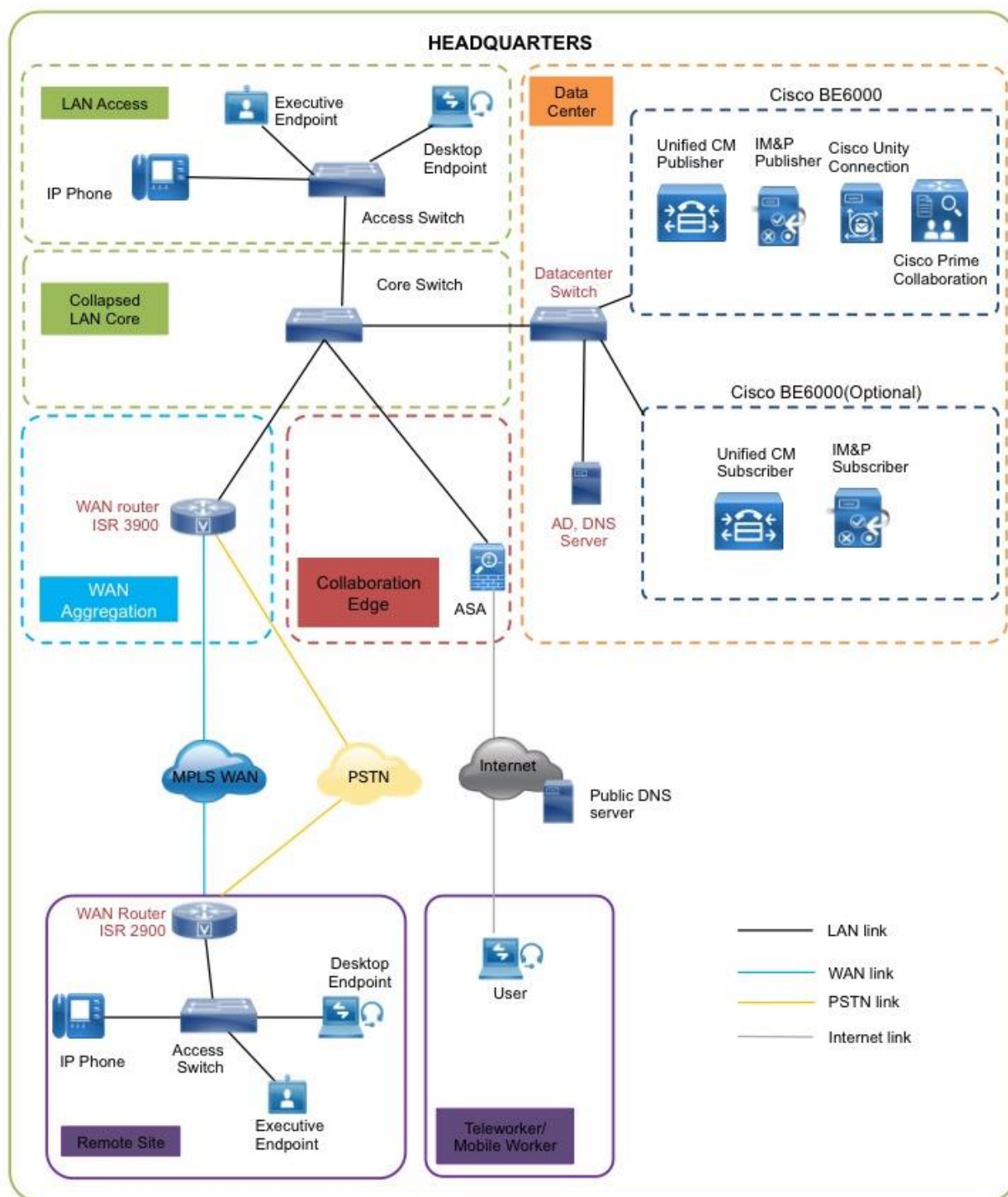


- The Cisco Business Edition 6000 supports Cisco Instant Messaging and Presence and Cisco Unified Contact Center Express on the same virtual server platform. You can also add a redundant server to this configuration if an organization requires it.

For the design model, the following features are provided:

- Connect each server to a different switch within the server room or data center in order to provide for high availability should a switch or link connection fail.
- There is sufficient capacity for multiple devices for each user. For example, you can enable a desk phone and a soft phone with enough computer telephony integration to allow a high percentage of users to have click-to-call or other applications that can remotely control their phones.
- There is additional capacity available for phones that are not assigned to a specific user, such as those in public areas, meeting rooms, storage areas, and break rooms.
- 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, 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 conferencing, contact center, video conferencing and Collaboration Edge. These advanced services are discussed in other design guides.
- Business Edition 6000S can be used for entry level centralized unified communication solutions supporting up to 150 users. Configuring the BE6000S (without preconfigured images) is discussed further in this design guide. Appendix B of this guide has a sample configuration for BE6000S.

Network Block diagram with Cisco Unified CM, Cisco Unity Connection, and Unified CM IM and Presence





The centralized design consists of a headquarters site and up to 49 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 1000 telephony users with voice messaging and Cisco Prime Collaboration Provisioning (PCP). An optional BE6000 server can be placed at the main site for redundancy and to install other applications. Each remote site takes advantage of the Cisco ISR G2 router that was deployed as part of the WAN deployment. Remote worker/mobile worker use cases leveraging Cisco Expressway C & Expressway E are discussed in detail in Collab Edge using BE6000 Design Guide.

Cisco Unified Computing System

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

For 1000 users or fewer, Cisco Business Edition (BE) 6000 is recommended. A second BE6000 server may be added for organizations that require hardware redundancy.

Cisco BE6000S provides unified communications and voice gateway functions in a single appliance, suitable for 25-150 users.

Prime collaboration Provisioning

Cisco Prime Collaboration Provisioning provides a scalable web-based solution to manage company's next-generation communication services. Prime Collaboration Provisioning manages IP communication endpoints and services in an integrated IP telephony, video, voice mail, and unified messaging environment that includes Cisco Unified Communications Manager, Cisco UCM Instant Messaging and Presence, Cisco Unity, Cisco Unity Connection systems, and Analog Gateways.

Self Provisioning

The Self-Provisioning feature allows an end user or administrator to add an unprovisioned phone to a Cisco Unified Communications Manager system with minimal administrative effort. A phone can be added by plugging it into the network and following a few prompts to identify the user. This feature enhances the out-of-box experience for end users by allowing them to directly add their desk phone or soft client without contacting the administrator. It simplifies administrator deployments by allowing them to add desk phones on behalf of an end user. The feature lets administrators and users deploy a large number of devices without interacting directly with the Cisco Unified Communications Manager Administration GUI, but from the device itself. The feature relies on the administrator preconfiguring a number of templates and profiles, so that when the phone attempts to self-provision, the necessary information is available in the system for it to create a new device.

Active Directory Integration

Active Directory integration allows you to provision users automatically from the corporate directory into the Cisco Prime Collaboration Provisioning 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 PCP each time a change occurs in the corporate directory. The other advantage is that end users are able to authenticate to PCP by using the same credentials in Active Directory, which reduces the number of passwords across the network.

Cisco Voice Gateways

Cisco Integrated Services Routers (ISR) provide gateway services to public telephone networks, audio conferencing resources resilient call control for remote sites. The combination of these voice services in a single platform offers savings over the individual components. The voice services can be provided by an ISR that also connects to the wide area data network, or they can be deployed in a standalone ISR for additional capacity and redundancy.

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

Because Cisco Integrated Services Router Generation 2 (ISR G2) have different processing capabilities based on the number of phones and the features applied, it is important to select the appropriate platform based on expected usage.

The sizing information in this guide supersedes the information from the various CVD WAN design guides because the number of SRST users determines the proper router model, as listed in the following table.

Table 1. Standalone voice gateway scaling options

	Voice gateway	Voice T1/E1	Trunk ports
50 users	Cisco 2911	4	120
50 users	Cisco 4321	8	240
100 users	Cisco 2921	6	180
100 users	Cisco 4331	12	360
250 users	Cisco 2951	8	240
730 users	Cisco 3925	12	360
1200 users	Cisco 3945	18	540
1200 users	Cisco 4431	24	720

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. PCP configures a +E.164 dial plan as part of the path selection for PSTN destinations. You can modify the dial plan to meet your specific needs. Cisco recommends using the E.164 dial plans as shown in the examples below.

**Reader Tip**

PCP can be used to deploy the default templates and to create new dial plans or Modify the existing ones.

Figure 1. +E.164 dialing for NANP with 7-digit local dialing

Route Pattern	Route Partition	
\+1911	PAR_Base	Emergency Dialing
\+911	PAR_Base	
\+[2-9]XXXXXX	PAR_PSTN_Local	Local Dialing
\+1[2-9]XX[2-9]XXXXXX	PAR_PSTN_National	National Dialing
\+[^1]!	PAR_PSTN_Intl	International Dialing
\+[^1]!#	PAR_PSTN_Intl	

Figure 2. +E.164 dialing for NANP with 10-digit local dialing

Route Pattern	Route Partition	
\+1911	PAR_Base	Emergency Dialing
\+911	PAR_Base	
\+[2-9]XX[2-9]XXXXXX	PAR_PSTN_Local	Local Dialing
\+1[2-9]XX[2-9]XXXXXX	PAR_PSTN_National	National Dialing
\+[^1]!	PAR_PSTN_Intl	International Dialing
\+[^1]!#	PAR_PSTN_Intl	

There are two configured international route patterns: one to route the variable-length dialed digits and one configured with a pound (octothorpe) in order to allow users to bypass the inter-digit timeout. The +911 and +1911 emergency route patterns are created with urgent priority to prevent inter-digit timeout delays when they are entered from a phone.

Dial Plans can be configured using PCP to suit any country. For example, for Australian Dial Plan the table below shows some Route Patterns and their respective Route Partitions.



Figure 3. +E.164 dialing for Australia

Route Pattern	Route Partition	
+106	PAR_Base	Emergency Dialing
+9106	PAR_Base	
+ [2-9]XXXXXXX	PAR_PSTN_Local	Local Dialing
\+61XXXXXXXXXX	PAR_PSTN_National	National Dialing
\+6[^1]!	PAR_PSTN_Intl	International Dialing
\+6[^1]!#	PAR_PSTN_Intl	

Site Codes

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

When you use this method, a phone in San Jose, CA can have the same 4-digit extension as one in Houston, TX without creating a numbering conflict. For example: 408-555-**1234** in San Jose and 713-555-**1234** in Houston.

For networks up to 50 sites, the dial plan consists of the following:

- One digit as an inter-site access code
- Two digits for the site code
- Four digits for the site extension

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

Figure 4. Two-digit site code format



1056

Class of Service

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



Figure 5. Calling search spaces and partitions

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

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

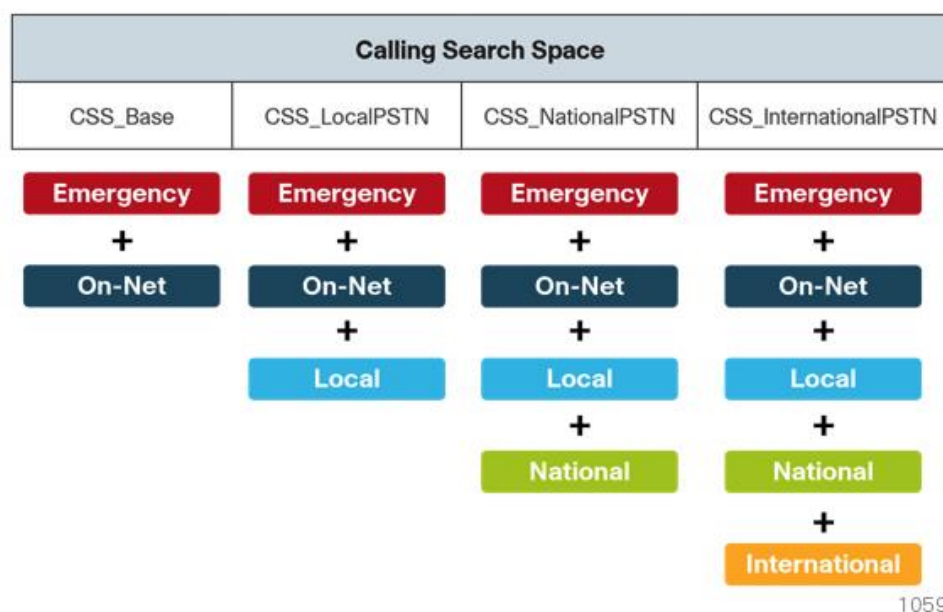
1058

With PCP's Getting Started Wizard(GSW) if administrators choose the default CSS that is defined, the auto registration partition will be defaulted to CSS_Base. This allows all devices to dial both on-net and emergency off-net numbers.

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



Figure 6. Calling capabilities for calling search spaces

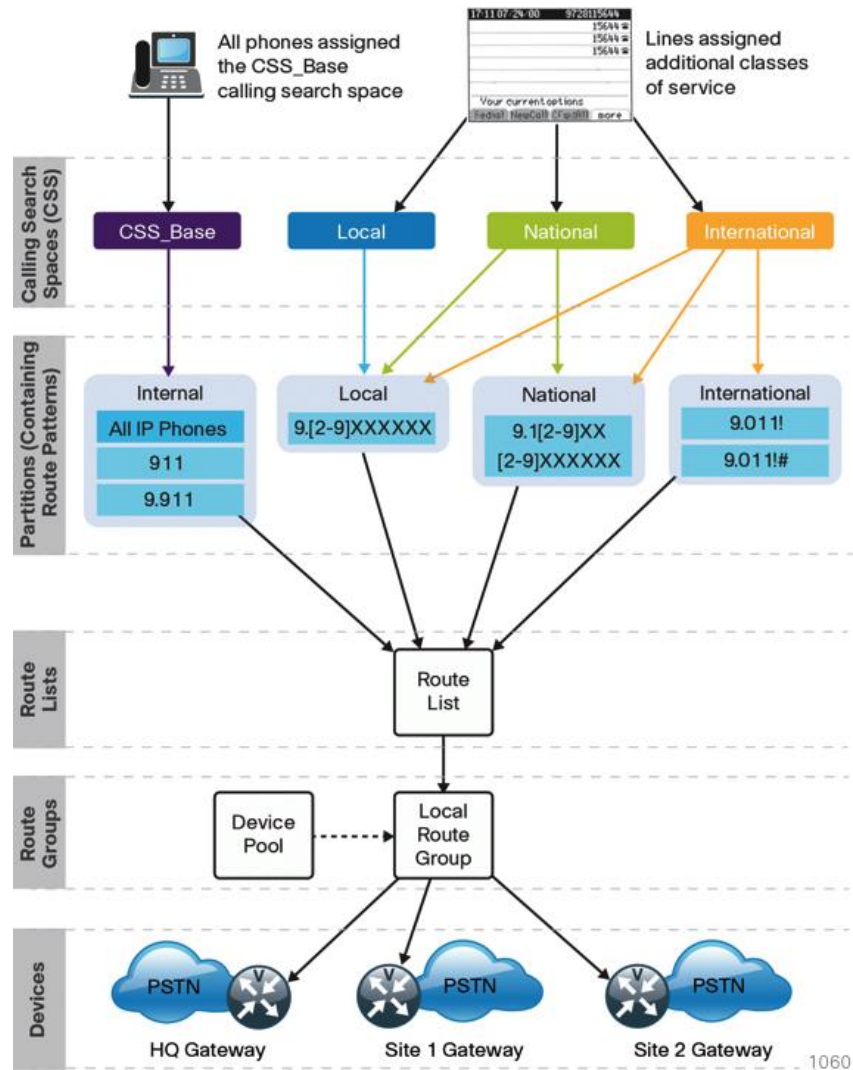


For example, if a user requires international dialing capability, their directory number would be assigned the CSS_InternationalPSTN calling search space, which includes dialing accessibility to all PSTN route patterns as well as national, local, emergency, and on-net numbers.

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.

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

Figure 7. Cisco Unified CM call routing



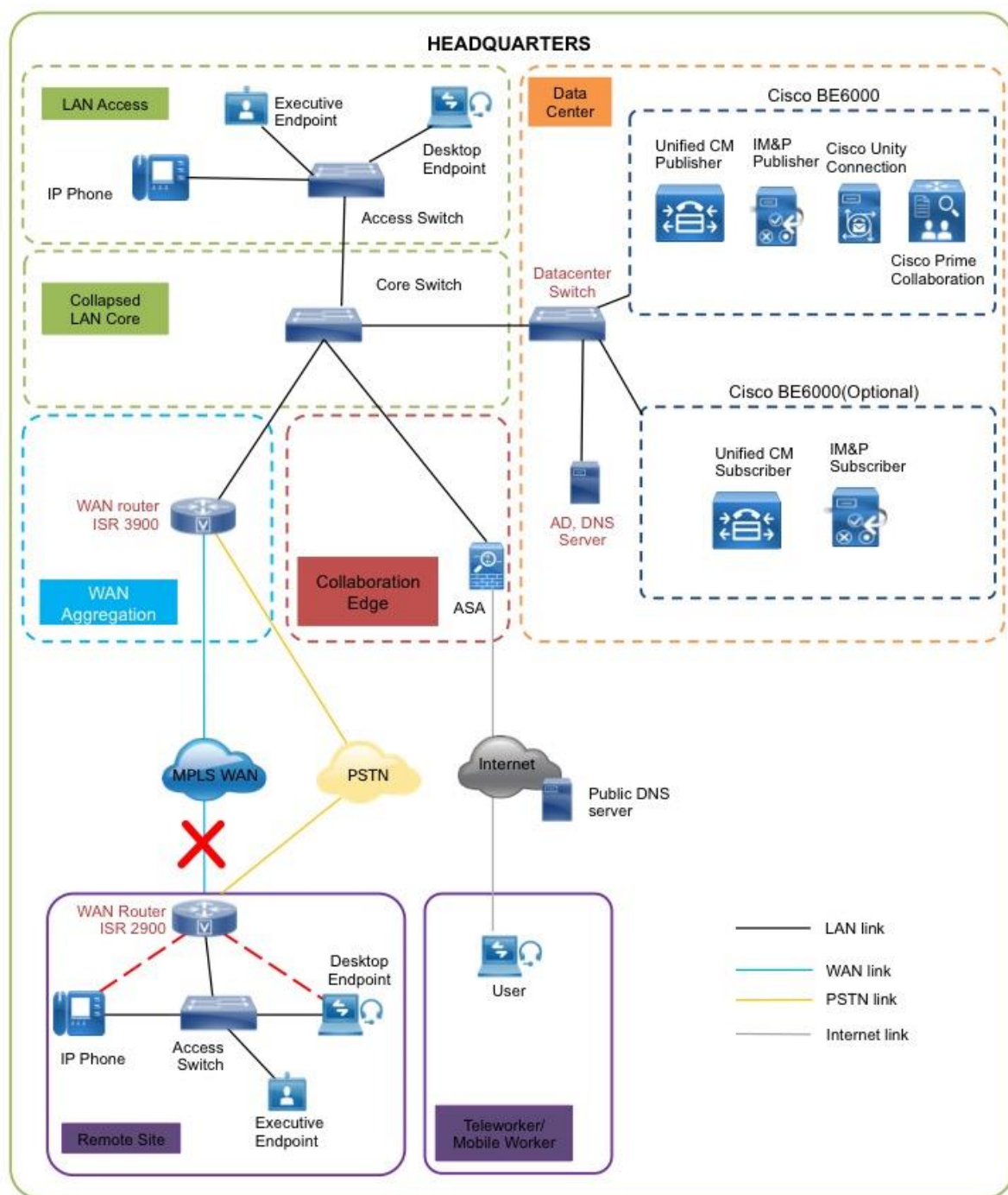
Survivable Remote Site Telephony

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 Survivable Remote Site Telephony (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 complexity.

Using the Cisco 2921 ISR router, a maximum of 100 phones are supported at a remote site. If you have more phones than a single SRST router can manage, you should consider using the higher end ISR router 3945.

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

Figure 8. SRST at a remote site



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

The Forward on No Registration feature enables the calls to remote site via the PSTN in the event of a call failure.

Device Mobility

PCP uses *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

Extension Mobility enables end users to personalize a Cisco Unified IP Phone temporarily. 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. Extension mobility can be used for hot desking and allows a user to move between floors, sites or geographic locations and utilize an available Cisco IP phone.

Media Resources

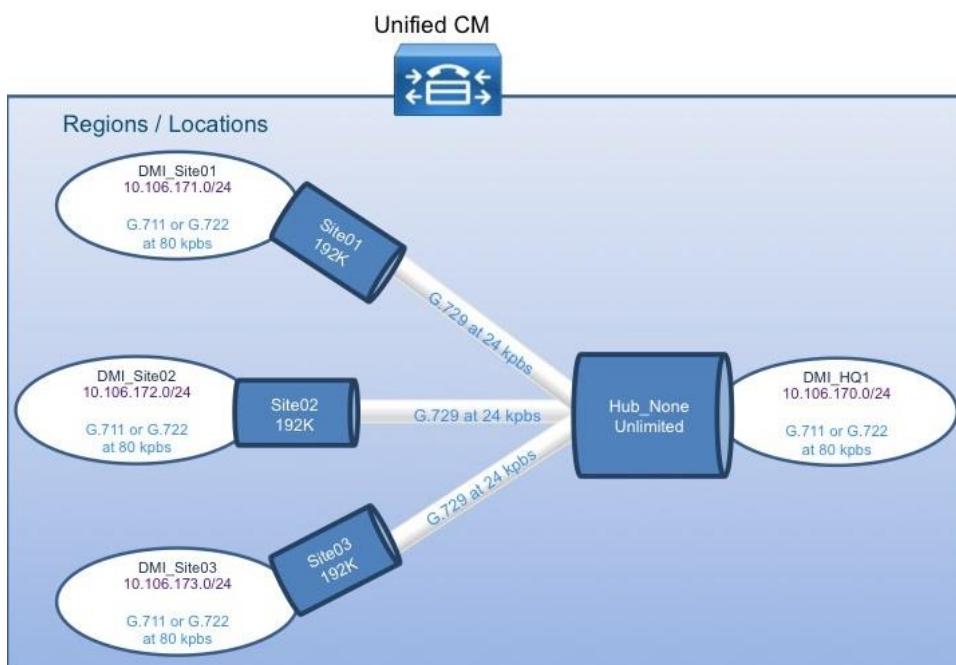
Media resources have been provisioned as part of the procedure for every site in order to ensure that remote sites use their local conference bridges and avoid unnecessary voice traffic over the WAN. The naming of the conference bridges needs to match those provisioned by PCP. The names are always CFB1<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 PCP 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.

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 to provide the correct Call Admission Control based on the speed of the link.

Figure 9. Hub-and-spoke topology for Call Admission Control



Point-to-Point Video

PCP can be used to deploy all the video models, including the DX70 and Dx80 devices.

IM and Presence

Cisco Jabber for Windows streamlines communications and enhances productivity by unifying presence, instant messaging, video, voice, voice messaging, desktop sharing, and conferencing capabilities securely into one desktop client. It offers flexible deployment models and integrates with commonly used



applications. Cisco Jabber for Windows can also be deployed in virtual environments. In a virtual environment, it supports presence, instant messaging, and desk-phone control.

Cisco Jabber solutions can be deployed using a mixture of on-premise and cloud based solutions.

The on-premises Jabber solution includes the following components:

- Unified CM IM and presence, for instant messaging and presence
- Unified CM, for audio and video call management, user and device configuration, and Jabber software phone and directory synchronization
- Cisco Unity Connection, for voice mail
- Jabber for Windows, Jabber for Mac, Jabber for iPad, Jabber for iPhone and Jabber for Android
- MS Active Directory, for client user information
- WebEx Meeting Center, for hosted meetings
- Network Time Protocol (NTP) server, for logging consistency
- Domain Name System (DNS) server, for name-to-IP resolution
- Syslog server, for logging events (optional)

This guide describes the following Cisco Jabber features:

- **Communication integration**—Use a single, intuitive interface for instant messaging with individuals and groups, IP telephony, visual voicemail, voice and web conferencing, desktop sharing, communication history, and integrated directories.
- **Presence**—View real-time availability of co-workers and colleagues within and outside the enterprise network.
- **Enterprise instant messaging**—Chat in real time by using instant messaging. Several chat modes are supported, including:
 - Point-to-point chat with co-workers inside your network, or supported federated business and personal contacts
 - Group chat, which enables multiple colleagues to communicate and collaborate in a single discussion
 - Personal instant messaging history for your reference
- **Predictive search**—Provides suggestions to you as you type in a search query and is capable of indexing your Cisco Jabber contact list, recent contacts, Microsoft Active Directory, or LDAP directory.
 - **Media escalation**—Escalate from a chat to an audio call, video call, desktop share, or web meeting. Media escalations are as easy as clicking a button.
 - **Desktop share**—Share what is on your desktop with Cisco Jabber users, as well as Cisco and other standards-based video endpoints.
 - **Integrated voice and video telephony**—A coordinated video display on the screen and voice conversation with a dedicated soft phone.



You can make, receive, and control your phone calls whether you are in or out of the office and support business-quality video communication up to high-definition (720p) and high-fidelity wideband audio. You can also use voice, video, and even desktop share when interacting with TelePresence endpoints and room-based and multipoint videoconferencing systems.

Many call-control options are available, including mute, call transfer, call forwarding, and ad-hoc conferencing. The reliability and failover features of Cisco Unified Communications Manager are supported.

- **Visual voice message access**—Access and manage your voice messages.
 - View, play back, and delete voice messages from Cisco Unity Connection.
 - Secure messaging is provided, with support for private and encrypted voice messages.

Self Care

Unified Communications Self-Care Portal is used to configure user settings for your Cisco Unified IP Phones and Jabber applications. Using Unified Communications Self Care Portal, end users can configure settings such as speed dial numbers, contact lists, phone services, and voicemail notifications. The administrator can control user access to the Self Care portal. Before a user can start using the Self Care portal, they should be added as a user to the Cisco Unified Communications Manager end user group. The URL to access the Self Care portal is <https://cucmhostname:portnumner/ucmuser>.

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.

Cisco Unified IP Phone 7800 Series is a high-fidelity voice communications portfolio designed for people-centric collaboration. It combines always-on reliability and security, full-featured easy-to-use IP telephony, and wideband audio to increase productivity, with an earth-friendly design for reduced costs. 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 Cisco IP Phone 7800 Series brings a higher quality standard, with full wideband audio support for handset, headset and speaker, to our voice-centric portfolio. A new ergonomic design includes support for larger grayscale, graphical backlit displays.

Cisco Unified IP Phone 7821 is a two-line, endpoint that is designed for information workers and managers. The Cisco IP phone 7841 is a four-line endpoint that is designed for information workers, the administrative staff and managers who have moderate level of voice communication needs. The Cisco IP



phone 7861 has 16 lines and is ideal for the users such as administrative staff, managers and agents in contact centers.

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

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



Deployment Details

A Unified Communications solution based on the BE6000 may be installed using one of the following methods-

- **Preconfigured Images** - a set of applications that have been preinstalled and configured during manufacture, allowing you to be up and running with a simple Unified Communications solution in less than an hour. Applications in this solution include Cisco PCP, Cisco UCM, Cisco IM & Presence, Cisco Unity Connection and Cisco Paging Server. For further details, please refer to the Preconfigured Image option in the BE6000 Installation Guide.
- **Config to Order** - A service provided by Cisco distribution partners to install and configure applications to customer specifications prior to delivery. For further information, please contact your Cisco distributor.
- **Standard Deployment** - The manual process for installing and configuring applications.

This design guide focuses on the standard deployment procedure.

This guide uses Cisco Prime Collaboration Provisioning (PCP) to configure, and deploy basic telephony and voice messaging services. 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.



Easy Access Configuration Sheet

The table below lists the information you will require to complete a standard deployment. Enter your details in the rightmost column. The center column lists the values used as examples throughout this CVD. Use this information to help map your requirements to the procedures detailed in this document.

Cisco UCM Installation Requirements		
Item	CVD Configuration	Site specific Configuration
NTP server IP address	10.64.58.50	
Domain Name System server IP	10.106.170.130	
Domain Name	mmcvd.ciscolabs.com	
Hostname	CUCM-Pub	
IP address	10.106.170.135	
Network mask	255.255.255.128	
Default gateway	10.106.170.129	
Administrator ID	Admin	
Password for admin	[Password]	
Security password	[Password]	
Application username	CUCMAdmin	
Password for CUCMAdmin	[Password]	
Organization	Cisco Systems, Inc	
Unit	Collaboration	
Location	Bangalore	
State	Karnataka	
Country	India	
Lightweight Directory Access protocol (LDAP) information for AD integration: Manager Distinguished name	CN=Administrator,cn=Users,dc=mmcvd,dc=ciscolabs,dc=com	
User search Base	CN=Users,dc=mmcvd,dc=ciscolabs,dc=com	
LDAP server IP address	10.106.170.130	
License files	Obtained from Cisco Licensing team	



Tech Tip

As your solution grows, you may need to acquire a security certificate from a public certification authority. Choose a domain name in this step with a valid Internet domain suffix (.com, .edu etc) to ensure that your system is ready for this requirement.



Tech Tip

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



Preparing the Network for IP Phones

PROCESS

1. [Enable DHCP option 150](#)

The campus design is voice-ready because it includes the QoS settings, VLANs, and IP subnets needed for voice endpoints. It also includes the Dynamic Host Configuration Protocol (DHCP) scopes for the voice VLANs. However, the DHCP option that automatically directs phones to Unified CM is covered in this module.

Procedure 1

Enable DHCP option 150

DHCP is used by phones to obtain an IP address, subnet mask, default gateway, domain name, DNS addresses, and TFTP server(Unified CM) information. When you are configuring DHCP for use in a Cisco Unified CM deployment, this design recommends a local 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 10.106.170.0/24, option 150: CUCM-Pub (primary), CUCM-Sub (secondary)
- In subnet 10.106.171.0/24, option 150: CUCM-Sub (secondary), CUCM-Pub (primary)

Under normal operations, a phone in subnet 10.106.170.0/24 will request TFTP services from CUCM-Pub, while a phone in subnet 10.106.171.0/24 will use CUCM-Sub. If CUCM-Pub fails, then phones from both subnets will request TFTP services from CUCM-Sub. The method for load sharing between the DHCP scopes is left up to the network administrator, because they will have the best knowledge of how many phones reside in each subnet.



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

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

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

Option 1: Enable option 150 on Microsoft DHCP server

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

- Step 1.** From the Microsoft server, open the DHCP Server Administration Tool.
- Step 2.** On the left side of the page, navigate to **[active directory name] > IPv4** (Example: ad.mmcvd.ciscolabs.com > IPv4).
- Step 3.** Right-click **IPv4**, and then choose **Set Predefined Options** from the list.
- Step 4.** Click **Add**, enter the following information, and then click **OK**:
 - Name—**TFTP Servers**
 - Data Type—**IP Address**
 - Array—Select the check box.
 - Code—**150**
 - Description—**Option 150 - TFTP Servers for CUCM**



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

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

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

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

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

Step 2. In the global configuration section, edit the DHCP pools supporting IP phones to include option 150 so the phones can find the TFTP servers at 10.106.170.136 (secondary) and 10.106.170.135 (primary).

```
ip dhcp pool wired-voice
  network 10.106.170.0 255.255.255.0
  default-router 10.106.170.1
  dns-server 10.106.170.130
  option 150 ip 10.106.170.136 10.106.170.135
  domain-name mmcvd.ciscolabs.com

ip dhcp pool wired-voice2
```



```
network 10.106.171.0 255.255.255.0
default-router 10.106.171.1
dns-server 10.106.170.130
option 150 ip 10.106.170.136 10.106.170.135
domain-name mmcvd.ciscolabs.com
```

Network Preparation Summary

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

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



Preparing the Server for Cisco Unified CM

PROCESS

1. [Configure server connectivity to the LAN](#)
2. [Prepare the server for Unified CM](#)

The BE6000 server includes a software summary in the data store that lists the applications included – so you would know the software available and what might be newer on the website

To install Cisco Unified CM, make sure you have completed the following steps before you start:

- Download the Open Virtual Archive (OVA) virtual machine template from the Cisco website at: <https://software.cisco.com/download/release.html?mdfid=286284802&flowid=74823&softwareid=283088407&release=11.0%281%29&reind=AVAILABLE&rellifecycle=&reltype=latest>
- Check the Cisco website to determine if there is a patch for your version of Cisco Unified CM: <https://software.cisco.com/download/release.html?mdfid=286284802&flowid=74823&softwareid=282074295&release=11.0%281%29&reind=AVAILABLE&rellifecycle=&reltype=latest>

Procedure 1

Configure platform connectivity to the LAN

The Cisco BE6000 server can be connected to a Cisco switch in the data center or a Cisco Catalyst switch in the server room. Please choose the option that is appropriate for your environment.

Option 1: Connect the server to a Cisco switch

- Step 1.** Log in to the Cisco switch with a username that has the ability to make configuration changes.
- Step 2.** If there is a previous configuration on the switch port where the Cisco Unified BE6000 server is connected, remove the individual commands by issuing a no in front of each one. This brings the port back to its default state.



Step 3. Configure the port as an access port.

```
interface Ethernet1/1/4
description BE6000
switchport access vlan 20
```

Option 2: Connect the BE6000 server to a Cisco Catalyst switch

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

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

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

Step 3. Configure the port as an access port.

```
interface GigabitEthernet1/0/6
description Unified CM
switchport access vlan 20
```

Procedure 2

Prepare the server for Unified CM

This BE6000 server Comes preloaded with Bootable image of Cisco Unified CM. Power on the server and start configuring

If you are deploying a secondary server then follow the steps below to deploy an OVA file in order to define the virtual machine requirements.

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

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

- On the Source page, click **Browse**, select the Cisco Unified CM OVA file downloaded from Cisco or from the datastore of the BE6000 server, click **Open**, and then click **Next**.
- On the OVF Template Details page, verify the version information, and then click **Next**:
- On the Name and Location page, in the Name box, enter the virtual machine name **CUCM-Pub**. 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 the following node, and then click **Next**.
 - **1000-user node (BE6000K)**—for a cluster of 1000 or fewer users.
- On the Disk Format page, choose **Thick Provision Eager Zeroed**, and then click **Next**.



On the Ready to Complete page, verify the settings, and then click **Finish**.

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	<p>When you click Finish, the deployment task will be started.</p> <p>Deployment settings:</p> <table> <tr> <td>OVF file:</td> <td>C:\Users\administrator\Desktop\cucm_11.0_vmv8_v1.0.o...</td> </tr> <tr> <td>Download size:</td> <td>101.5 KB</td> </tr> <tr> <td>Size on disk:</td> <td>80.0 GB</td> </tr> <tr> <td>Name:</td> <td>Cisco Unified Communications Manager (CUCM)</td> </tr> <tr> <td>Deployment Configuration:</td> <td>CUCM 1000 user node - C200</td> </tr> <tr> <td>Host/Cluster:</td> <td>localhost</td> </tr> <tr> <td>Datastore:</td> <td>datastore1 (3)</td> </tr> <tr> <td>Disk provisioning:</td> <td>Thick Provision Eager Zeroed</td> </tr> <tr> <td>Network Mapping:</td> <td>"eth0" to "VM Network"</td> </tr> </table>	OVF file:	C:\Users\administrator\Desktop\cucm_11.0_vmv8_v1.0.o...	Download size:	101.5 KB	Size on disk:	80.0 GB	Name:	Cisco Unified Communications Manager (CUCM)	Deployment Configuration:	CUCM 1000 user node - C200	Host/Cluster:	localhost	Datastore:	datastore1 (3)	Disk provisioning:	Thick Provision Eager Zeroed	Network Mapping:	"eth0" to "VM Network"
OVF file:	C:\Users\administrator\Desktop\cucm_11.0_vmv8_v1.0.o...																		
Download size:	101.5 KB																		
Size on disk:	80.0 GB																		
Name:	Cisco Unified Communications Manager (CUCM)																		
Deployment Configuration:	CUCM 1000 user node - C200																		
Host/Cluster:	localhost																		
Datastore:	datastore1 (3)																		
Disk provisioning:	Thick Provision Eager Zeroed																		
Network Mapping:	"eth0" to "VM Network"																		

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

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

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

Step 6. Select **Datastore ISO File**, click **Browse**, navigate to the location of the Cisco Unified CM bootable installation file (or browse the datastore to find the CUCM installation file), select the correct ISO image, and then click OK.

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

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

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

Installing Cisco Unified CM

PROCESS

1. [Install the first Cisco Unified CM platform](#)
2. [Install licenses and start services](#)
3. [Configure additional servers](#)
4. [Install the redundant server](#)
5. [Start services](#)
6. [Adding the secondary node in the Cisco Unified Communications Manager Group](#)



Procedure 1

Install the first Cisco Unified CM platform

Refer to the [install guide](#) document for installing the Cisco UCM

Procedure 2

Install licenses and start services

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

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

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

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

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



Tech Tip

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

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

- Name—**CUCM-Pub**
- Description—**CUCM Publisher**
- Product Type—**Unified CM**
- Hostname/IP Address—**10.106.170.135 (publisher)**
- Username—**Admin** (case-sensitive platform administrator ID)
- Password—**[password]**

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

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

If the connection is not successful, repeat [Step 4](#) through [Step 6](#) with the correct information.

Step 7. Click **Synchronize Now**.



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



Tech Tip

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

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

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

Next, you verify the licenses have been properly installed.

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

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

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

Step 13. Enter the **Username** and **Password** from the Application User Configuration page in [Step 20](#) of the previous procedure, and then click **Login**.

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

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

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



Tech Tip

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

Cisco Messaging Interface

Cisco DHCP Monitor Service

Cisco TAPS Service

Cisco Directory Number Alias Sync



Cisco Directory Number Alias Sync
 Cisco Dialed Number Analyzer Server
 Cisco Dialed Number Analyzer
 Self Provisioning IVR

Step 17. In the message window, click OK.

CM Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CalManager	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 checked="" type="checkbox"/>	Cisco Intercluster Lookup Service	Activated
<input checked="" type="checkbox"/>	Cisco Location Bandwidth Manager	Activated
<input type="checkbox"/>	Cisco Directory Number Alias Sync	Deactivated
<input type="checkbox"/>	Cisco Directory Number Alias Lookup	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
CTI Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco IP Manager Assistant	Activated
<input checked="" type="checkbox"/>	Cisco WebDialer Web Service	Activated
<input type="checkbox"/>	Self Provisioning IVR	Deactivated
CDR Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco SOAP - CDRonDemand Service	Activated
<input checked="" type="checkbox"/>	Cisco CAR Web Service	Activated

Figure 10. Recommended publisher services when using non-dedicated TFTP server

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


Procedure 3

Configure additional servers

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

- Step 1.** In the **Navigation** list at the top of the page, choose **Cisco Unified CM Administration** and then click **Go**.
- Step 2.** Navigate to **System > Server**, and then click **Add New**
- Step 3.** Select the server type as CUCM Voice/Video
- Step 4.** Enter the host name of the additional Cisco Unified CM server, a description, and then click **Save**.



Status	
 Status: Ready	
Server Information	
Server Type	CUCM Voice/Video
Host Name/IP Address*	CUCM-Sub
IPv6 Address (for dual IPv4/IPv6)	
MAC Address	
Description	Subscriber

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

- Step 5.** Navigate to **System > Application Server**, and then click **Add New**.
- Step 6.** On the first Application Server Configuration page, in Application Server Type list, choose **Cisco Unity Connection**, and then click **Next**.
- Step 7.** On the second Application Server Configuration page, in the Name box, enter **CUC**, and then in the IP Address box, enter **10.106.170.137**.
- Step 8.** In the **Available Application Users** list, select the account you created during the installation of Cisco Unified CM (Example: CUCMAdmin), move the account to **the Selected Application Users** list by clicking the **v** character, and then click **Save**.
- Step 9.** When the subscriber and Cisco Unity Connection servers have been added to the publisher's database, repeat the procedures in "Preparing the Platform for Cisco Unified CM" for each additional Unified CM server, and then return to Procedure 4, "Install the redundant server."

Procedure 4

Install the redundant server

Install the redundant server(subscriber) with the same steps as listed in Install guide

Procedure 5

Start services

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

- Step 1.** In a web browser, access the Cisco Unified CM administration interface on the publisher, and then in the center of the page, under Installed Applications, click **Cisco Unified Communications Manager**.
- Step 2.** Enter the application **Username** and **Password**, and then click **Login**.
- Step 3.** In the **Navigation** list on the top right side of the page, choose **Cisco Unified Serviceability**, and then click **Go**.
- Step 4.** Navigate to **Tools > Service Activation**.



- Step 5.** In the **Server** list, choose the next additional server, and then click **Go**.
- Step 6.** Select **Check All Services**, clear the ones that are not needed for this node, and then click **Save**.
- Step 7.** In the message window, click **OK**.

Figure 11. Recommended subscriber services when using non-dedicated TFTP servers

CM Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CallManager	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 checked="" type="checkbox"/>	Cisco Location Bandwidth Manager	Activated
<input type="checkbox"/>	Cisco Directory Number Alias Lookup	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

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

Database and Admin Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco AXL Web Service	Activated
<input checked="" type="checkbox"/>	Cisco UXL Web Service	Activated

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

Security Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CTL Provider	Activated

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

Procedure 6

Adding the secondary node in the Cisco Unified Communications Manager Group

- Step 1.** In a web browser, access the Cisco Unified CM administration interface on the publisher, and then in the center of the page, under Installed Applications, click Cisco Unified Communications Manager.
- Step 2.** Enter the application Username and Password, and then click **Login**.
- Step 3.** In the Navigation list on the top right side of the page, choose Cisco Unified CM , and then click **Go**.
- Step 4.** Navigate to System> Cisco Unified CM group.



Step 5. Select the secondary Cisco Unified Communications Manager from the Available group and click the down arrow.

Step 6. Click **save**.

Cisco Unified Communications Manager Group Members

Available Cisco Unified Communications Managers	Selected Cisco Unified Communications Managers*
	CM_10.106.170.136 CM_CUCM-Pub



Preparing the Platform for Cisco Unity Connection

Easy Access Configuration Sheet

The following information is needed for the installation:

Cisco Unity Connection Installation Requirements		
Item	CVD Configuration	Site specific Configuration
NTP server IP address	10.64.58.50	
Domain Name System server IP	10.106.170.130	
Domain Name	mmcvd.ciscolabs.com	
Hostname	CUC	
IP address	10.106.170.137	
Network Mask	255.255.255.128	
Default gateway	10.106.170.129	
Administrator ID	Admin	
Admin password	[Password]	
Security password	[Password]	
Application username	CUCAdmin	
Application password	[password]	
Organization	Cisco Systems, Inc	
Unit	Collaboration	
Location	Bangalore	
State	Karnataka	
Country	India	
Lightweight Directory Access protocol (LDAP) information for AD integration:	CN=Administrator,cn=Users,dc=mmcvd,dc=ciscolabs,dc=com	
Manager Distinguished name	CN=Users,dc=mmcvd,dc=ciscolabs,dc=com	
User search Base		
LDAP server IP address	10.106.170.130	

i	Tech Tip
The password must start with an alphabetic character and have at least six characters, and it can contain alphanumeric characters, hyphens, or underscores. The default pin generated by the PCP for Voicemail will be 054321.	



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.

The BE6000 server includes a software summary in the data store that lists the applications included – so you would know the software available and what might be newer on the website

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

- Download the Open Virtual Archive (OVA) file from the Cisco website at:
<https://software.cisco.com/download/release.html?mdfid=283062758&flowid=45673&softwareid=282074348&release=OVA-11.0&relind=AVAILABLE&rellifecycle=&reltype=latest>
- Check the Cisco website to determine if there is a patch for your version of Cisco Unified CM:
<https://software.cisco.com/download/release.html?mdfid=286286362&flowid=74882&softwareid=282074295&release=11.0%281%29&relind=AVAILABLE&rellifecycle=&reltype=latest>



Installing Cisco Unity Connection

PROCESS

1. [Install Cisco Unity Connection platform](#)
2. [Install licenses and start services](#)

Procedure 1

Install Cisco Unity Connection server

For installation of Cisco Unity Connection, refer the [install guide](#)

Procedure 2

Install licenses and start services

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

- Step 1.** In a web browser, access the Cisco Unified CM publisher, and in the center of the page, under Installed Applications, click **Cisco Prime License Manager**.
- Step 2.** On the login page, enter the following case-sensitive Cisco Unified CM application username and password, and then click **Login**:
 - User Name—**CUCMAdmin** (case-sensitive)
 - Password—**[password]**
- Step 3.** Navigate to **Inventory > Product Instances**, and then click **Add**.



Tech Tip

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

- Step 4.** Enter the following information for Cisco Unity Connection, and then click **Test Connection**:
 - Name—**CUC**
 - Description—**Unity Connection**
 - Product Type—**Unity Connection**
 - Hostname/IP Address—**10.106.170.137**



- Username—**Admin**
- Password—**[password]**

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

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

If the connection is not successful, repeat [Step 4](#) through [Step 6](#) with the correct information.

Step 7. Click **Synchronize Now**.

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

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

Step 10. Repeat [Step 9](#) for each additional license file for your installation. After all files have been installed, click **Close**.

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

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

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

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

Step 13. Enter the **Username** and **Password** you entered on the Application User Configuration page in [Step 18](#) of the previous procedure, and then click **Login**.

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

Step 15. Navigate to **Tools > Service Activation**, select **Check All Services**, and then click **Save**. In the message window, click **OK**.

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



Preparing the server for Cisco Unified CM IM and Presence

Easy Access Configuration Sheet

The following information is needed for the installation

Cisco Unified CM IM and Presence Installation requirements		
Item	CVD Configuration	Site specific Configuration
NTP server IP address	10.64.58.50	
Domain Name Sytem server IP	10.106.170.130	
Domain Name	mmcvd.ciscolabs.com	
Hostname,IP address	IMP	
IP address	10.106.170.146	
Network Mask	255.255.255.128	
Default Gateway	10.106.170.129	
Administrator ID	Admin	
Password	[Password]	
Organization	Cisco Systems, Inc	
Unit	Collaboration	
Location	Bangalore	
State	Karnataka	
Country	India	
Connectivity to First node (UCM Publisher): Hostname	CUCM-Pub	
UCM IP address	10.106.170.135	
UCM security password	[Password]	

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

The BE6000 server includes a software summary in the data store that lists the applications included – so you would know the software available and what might be newer on the website

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

- Download the Open Virtualization Archive (OVA) file from the Cisco website at:
<https://software.cisco.com/download/release.html?mdfid=286287586&flowid=74862&softwareid=282074312&release=11.0%281%29&reind=AVAILABLE&rellifecycle=&reltype=latest>



- Check the Cisco website to determine if there is a patch for your version of Cisco Unified CM IM and Presence:
<https://software.cisco.com/download/release.html?mdfid=286287586&flowid=74862&softwareid=282074312&release=11.0%281%29&reind=AVAILABLE&rellifecycle=&reltype=latest>



Installing Cisco Unified CM IM and Presence

PROCESS

1. [Install Cisco Unified CM IM and Presence](#)
2. [Start services](#)

Procedure 1

Install Cisco Unified CM IM and Presence

For installation of Cisco Unified CM IM & Presence, refer the [install guide](#)

Procedure 2

Start services

After the software is installed, use the web interface in order to complete the rest of the procedures.

- Step 1.** In a web browser, access the IP address or hostname of the Cisco Unified CM IM and Presence server, and then in the center of the page under Administrative Applications, click **Cisco Unified Communications Manager IM and Presence**.



Tech Tip

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

- Step 2.** In the **Navigation** list, click **Cisco Unified CM IM and Presence administration**, and then click **Go**.
- Step 3.** Enter the username and password of the CUCM admin.
- Step 4.** Navigate to **Tools > Service Activation**, enter the following information and then click **Save**:
- Cisco SIP Proxy—**Select**
 - Cisco Presence Engine—**Select**
 - Cisco Sync Agent—**Select**
 - Cisco XCP Connection Manager—**Select**
 - Cisco XCP Directory Service—**Select**
 - Cisco XCP Authentication Service—**Select**



IM and Presence Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco SIP Proxy	Activated
<input checked="" type="checkbox"/>	Cisco Presence Engine	Activated
<input checked="" type="checkbox"/>	Cisco Sync Agent	Activated
<input type="checkbox"/>	Cisco XCP Text Conference Manager	Deactivated
<input type="checkbox"/>	Cisco XCP Web Connection Manager	Deactivated
<input checked="" type="checkbox"/>	Cisco XCP Connection Manager	Activated
<input type="checkbox"/>	Cisco XCP SIP Federation Connection Manager	Deactivated
<input type="checkbox"/>	Cisco XCP XMPP Federation Connection Manager	Deactivated
<input type="checkbox"/>	Cisco XCP Message Archiver	Deactivated
<input checked="" type="checkbox"/>	Cisco XCP Directory Service	Activated
<input checked="" type="checkbox"/>	Cisco XCP Authentication Service	Activated

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

Performance and Monitoring Services		
	Service Name	Activation Status
<input type="checkbox"/>	Cisco Performance Monitoring Service	Deactivated

Step 5. In the message window, click OK.



Preparing the server for Cisco Prime Collaboration

Easy Access Configuration Sheet

The following information is needed for the installation:

Cisco Prime Collaboration Installation Requirements		
Item	CVD Configuration	Site specific Configuration
NTP server IP address	10.64.58.50	
Domain Name System server IP	10.106.170.130	
Domain Name	mmcvd.ciscolabs.com	
Hostname	CPC	
IP address	10.106.170.139	
Network Mask	255.255.255.128	
Default Gateway	10.106.170.129	
Globaladmin password	[Password]	
Security password	[Password]	
Root password	[password]	
Lightweight Directory Access protocol (LDAP) information for AD integration	CN=Administrator,cn=Users,dc=mmcvd,dc=ciscolabs,dc=com	
Manager Distinguished name User search Base	CN=Users,dc=mmcvd,dc=ciscolabs,dc=com	
LDAP server IP address	10.106.170.130	



Tech Tip

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

The BE6000 server includes a software summary in the data store that lists the applications included - so you would know the software available and what might be newer on the website.

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

Download the Open Virtualization Archive (OVA) file from Cisco website at:

<https://software.cisco.com/download/release.html?mdfid=286289005&flowid=75802&softwareid=286289070&release=11.0&relind=AVAILABLE&rellifecycle=&reltype=latest>



Installing Cisco Prime Collaboration Provisioning

PROCESS

1. [Install Cisco Prime Collaboration Provisioning](#)
2. [Configure Cisco Unified Communication processors using Cisco Prime Collaboration](#)

Procedure 1

Install Cisco Prime Collaboration Provisioning

For installation of Cisco Unified CM IM & Presence, refer the [install guide](#)

Configuring Cisco Unified CM using Cisco Prime Collaboration

Procedure 1

Configure Cisco Unified Communication processors using Cisco Prime Collaboration

After the software is installed, use the web interface in order to complete the rest of the procedures.

- Step 1.** In a web browser, access the IP address or hostname of the Cisco Prime Collaboration
- Step 2.** Enter the globaladmin username and password of the Cisco Prime Collaboration.
- Step 3.** When you log into Cisco Prime Collaboration Provisioning for the first time, the Getting Started wizard popup appears. On subsequent logins, you must choose Infrastructure Setup> Getting Started Wizard.
- Step 4.** If you have a configuration file that contains configuration details, it can be uploaded manually using Use Existing Configuration step or just click Begin to start the configuration.
- Step 5.** In the next step of Getting started wizard, which is Infrastructure Setup, all the unified communication server credentials are filled with an example value. Replace all the values with the specific detail of your infrastructure devices from the Before you Start table.




Tech Tip

Make sure you enter the right values, because you cant go back and change the values once you proceed.



- Unified Communications Manager
Name > CUCM-Pub
Host / IP Address > 10.106.170.135
Username > CUCMAdmin
Password > *****
Click Test connection
It should have a green check mark if not re verify the credential
- Unity Connection (optional)
Name > CUC
Host / IP Address > 10.106.170.137
Username > CUCAdmin
Password > *****
OS Administrator Name : Admin
OS Administrator Password : *****
Voicemail pilot Number : 2000
Click Test connection
It should have a green check mark if not re verify the credential
- Do not check Enable Unified Messaging (requires Exchange Server information)
- Unified IM & Presence (Optional)
Name > IMP1
Host / IP Address > 10.106.170.146
Username > CUCMAdmin
Password > *****
Click Test connection
It should have a green check mark if not re verify the credential



Getting Started With Prime Collaboration Provisioning

▼ Unified Communications Manager

* Name

CUCM-Pub

* Host / IP Address

10.106.170.135

* Username

CUCMAdmin

* Password

.....

Test Connection

✓

▼ Unity Connection (Optional)

* Name

CUC

* Host / IP Address

10.106.170.137

* Username

CUCAdmin

* Password

.....

* OS Administrator Name

Admin

* OS Administrator Password

.....

* Voicemail pilot Number

2000

Test Connection

✓

Close

Save and Continue

Click **Save and Continue**

Step 6. Add a administrative Domain name and description to the Domain creation step

Step 7. Right click on the Download an example Dial Pattern file and save and upload the dial pattern file, a green check mark is displayed on uploading the dial pattern.



Getting Started With Prime Collaboration Provisioning



Domain Creation

Step 3 of 6

A Domain is a collection of users and sites (called Service Areas) that will be managed together. A Domain could be a building, region, country, sales team or other group of individuals. Administrators can be assigned to one or more Domain Groups.

The wizard will create one Domain for you, additional Domains may be created under the Provisioning Setup menu.

* Name

Description

Dial Pattern (Optional) ⓘ

[Download an example Dial Pattern file](#)

Select a Dial Pattern file

 Browse...

Clear

Upload



Close

Save and Continue

Click Save and Continue

Step 8. Add a Service area name in the Service area Step of the GSW

- Service area> Site one
- Time Zone > Asia/Kolkata
- PSTN Gateway IP Address > 10.106.170.5
- Site Code> 810

Step 9. Add the SRST details

- IP Address >10.106.170.113
- Port >2000
- SIP Network / IP Address > 10.106.170.113
- SIP Port > 5060



Getting Started With Prime Collaboration Provisioning

Service Area

Step 4 of 6

Service Areas represent geographical boundaries in your UC network and define the **Calling Search Spaces (CSS)**, **Device Pools**, **Regions**, and **Locations** to be used for provisioning services for the users assigned to that **Service Area**.

This page sets up a basic **Service Area** with an intra-site dial plan which you can edit or extend later using the **User Provisioning Setup** page.

Domain	mmcvd.ciscolabs.com
* Service Area	<input type="text" value="site one"/>
* Time Zone	<input type="text" value="Asia/Kolkata"/>
* PSTN Gateway IP Address	<input type="text" value="10.106.170.5"/>
Site Code	<input type="text" value="810"/>

▼ Survivable Remote Site Telephony [SRST] (Optional)

IP Address	<input type="text" value="10.106.170.113"/>
Port	<input type="text" value="2000"/>
SIP Network / IP Address	<input type="text" value="10.106.170.113"/>
SIP Port	<input type="text" value="5060"/>

Step 10. Add Device Mobility details

- Subnet> 10.106.170.129
- Subnet Mask (bits size)> 25

Step 11. Add Directory Numbers details

- Click Edit and change the prefix and First number and Last Number accordingly
- Prefix >810
- First Number >8001 Last Number > 9000



▼ **Device Mobility Information (Optional)**

Subnet

Subnet Mask (bits size)

▼ **Directory Numbers** ⓘ

Show

	Prefix	First Number	Last Number	Minimum Length
<input checked="" type="radio"/>	810	8001	9000	7
<input type="radio"/>	415	1001	1050	7

Close

Save and Continue

Click **Save and Continue**

Step 12. Add Role Name in the User Role (Part 1 - Manual Service Provisioning) step of the GSW

Step 13. Role Name > Employee

Step 14. Under the Manual Service Provisioning section check or uncheck the Line and Chosen Line Depending on the kind of line needed.

Step 15. Under the Endpoint section choose the default endpoint type you want to assign to the user type Employee by clicking on the grey check mark on the right and selecting the endpoint type.

Step 16. Under the Service section choose all the services or the services you desire by clicking on the grey check mark similarly.

Step 17. Under the Service Bundle Section choose the services bundle you desire by clicking on the grey check mark.

Getting Started With Prime Collaboration Provisioning



• Manual Service Provisioning

The endpoints, services and service

• Automatic Service Provisioning

The endpoints, services and service synchronized.

Domain **mmcvd.ciscolabs.com**

* Role Name

▼ Manual Service Provisioning

Specify which services can be manually provisioned by this user role.

Lines

- ☒ Auto-Assigned Line
- ☒ Chosen Line

Endpoints

Cisco 7821
Cisco 7841
Cisco DX650

✕

☒ Extension Mobility Access ⓘ

☒ Extension Mobility Line ⓘ

☒ Line ⓘ

☒ Line on a Shared Endpoint ⓘ

☒ Enable Mobility Support ⓘ

☒ Endpoint ⓘ

☒ Remote Destination Profile Line ⓘ

☒ Remote Destination Profile ⓘ

Services

Endpoint
Line
Voicemail
User Services

Service Bundles

Click **Save and Continue**

Step 18. Under User Role (Part 2 - Automatic Service Provisioning) step of GSW check Enable auto-provisioning for this role when a user is created or synchronized

Step 19. Under Automatically Provision These Services check the Endpoint option.

- Under the Endpoint settings Check the Self provisioned endpoint option and set the maximum number of self-provisioned Endpoints a user can have > 3
- Self Provisioning IVR Directory Number > 8009400
- Starting auto-registration Directory Number > 8000001



- Ending auto-registration Directory Number > 8009000
- Select Check Line, Self-Provisioned Single Number Reach, IM and Presence, Voicemail, Extension Mobility Access, Extension Mobility Line, depending on the kind of services you desire
- Under Cisco Jabber Select check the kind of Cisco Jabber type from Cisco Jabber for BlackBerry, Desktop, Android, iPhone, Tablet.

Getting Started With Prime Collaboration Provisioning

User Role (Part 2 - Automatic Service Provisioning)

Step 5 of 6

Domain **mmcvd.ciscolabs.com**Role Name **Employee**

▼ Automatic Service Provisioning

Specify which services will be automatically provisioned when a user is created in the system with this user role.

☒ Enable auto-provisioning for this role when a user is created or synchronized

Automatically Provision These Services:

☒ Endpoint

▼ Endpoint Settings

☒ Self-Provisioned Endpoint

Maximum Number of Endpoints

Information needed to auto-register and Self Provision the endpoints. ⓘ

Self Provisioning IVR Directory Number

Starting auto-registration Directory Number

Ending auto-registration Directory Number

☐ Default Endpoint

Model

[Customize](#)

Close

Save and Continue

Click **Save and Continue**.

Step 20. Under the Directory Synchronization (LDAP Sync) step of GSW select check Use Directory (LDAP) Server to synchronize users to Prime Collaboration Provisioning.

Step 21. Under the LDAP Server

- Name > LDAP



- IP Address > 10.106.170.130
- Port > 389
- Admin Distinguished Name > Administrator
- Admin Password > *****
- LDAP User Search Base > cn=users,dc=mmcvd,dc=ciscolabs,dc=com
- LDAP Server Type > Microsoft AD Server
- Click Test Connection it should have a green check mark if not re-verify the credential.

Getting Started With Prime Collaboration Provisioning

Directory Synchronization (LDAP Sync)

Step 6 of 6

Directory Synchronization enables automatic import of users into Prime Collaboration Provisioning when they are added to your network directory server

- ☐ Do not import users. System administrators can enter user information after the wizard
☒ Use Directory (LDAP) Server to synchronize users to Prime Collaboration Provisioning

▼ LDAP Server

*Name
 *IP Address
 *Port
 *Admin Distinguished Name
 *Admin Password
 *LDAP User Search Base
 LDAP Server Type
 Use SSL ☐
 Backup Server IP
 Backup Server Port
 Test Connection ☒

Close

Save and Continue

Step 22. Under the Sync policy settings

- Mode > Authentication and Synchronization
- Re-Sync Every > days > 1
- Users Search Base > cn=users,dc=mmcvd,dc=ciscolabs,dc=com

Step 23. Under Domain LDAP settings

- Filter Query for Synchronization > Synchronize all users



Step 24. Under Service Area LDAP settings

- Filter By > Title = Employee

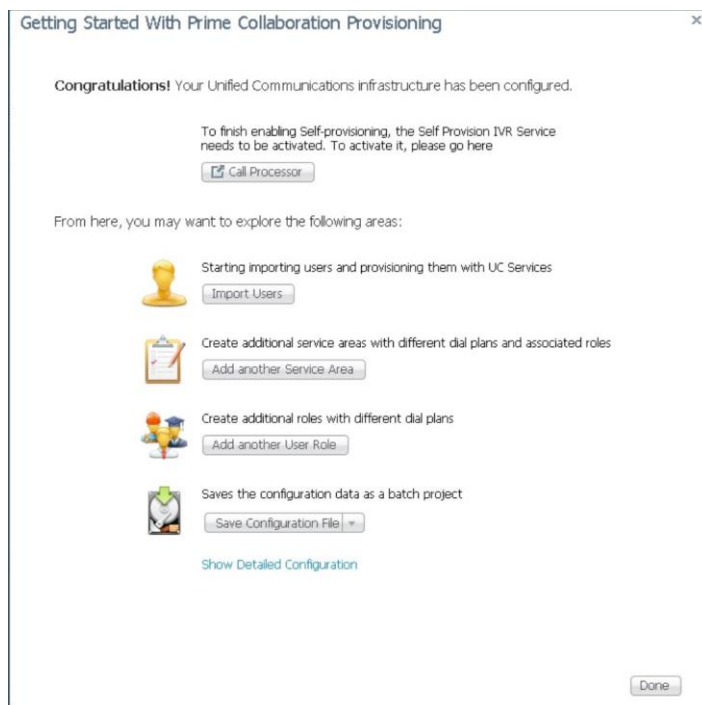
Step 25. Under Line Settings

- Select check Assign new line from the extension block.
- Select check Apply mask to LDAP synchronized telephone number.
- Click **Save** and **Continue**.

Step 26. Under the Summary of the GSW Click **Apply**

Applying the changes will take few minutes

Step 27. Click on **Import users> select from LDAP > Domain : Main > Click Import**.



Step 28. Once you are done with applying the configuration, Click **Done**.



Configuring Conference Bridges and SRST

PROCESS

1. [Configure conference bridges](#)
2. [Configure SRST for phones](#)
3. [Block voice traffic on WAN links](#)

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

Please follow the steps in this process to understand what site-specific information is required in each section of the gateway template files.

Procedure 1

Configure conference bridges

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

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 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) ships with a PVDM3-16, and the 2921 ISR with VSEC and 2951 ISR ship with a PVDM3-32. The Cisco 2900 Series ISRs have to be upgraded to a single PVDM3-64 DSP in order to allow sufficient resources for a single voice T1 and at least five 8-party conferences.

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

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

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



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

```

dspfarm profile 1 conference
  description HQ Conference Bridges
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  codec g729r8
  codec g729br8
  codec g722-64
  codec ilbc
maximum sessions 5

associate application SCCP
no shutdown

```

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

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

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

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

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

```

sccp local [interface type] [number]
sccp ccm 10.106.170.136 identifier 1 priority 1 version 7.0
sccp ccm 10.106.170.135 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 [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 PCP, 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 SRST for phones

The procedure will configure SRST for phones.

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

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

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

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

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. The example given is for 7-digit directory numbers starting with 820.

```
voice translation-rule 1
rule 1 /^[1-7]...$/ /811\0/

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

voice translation-rule 800
rule 2 /^800\(.*)//1310610\1/

voice translation-profile SRST-7-Digit
translate called 800
```

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

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

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

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



Tech Tip

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

- Step 4.** If 2-digit site codes are used for this installation, translate the inbound number to the 7-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, 2-digit site code, and the last four digits. This configuration is done under call-manager-fallback

```
call-manager-fallback
dialplan-pattern 1 311611.... extension-length 7
extension-pattern 811....
```

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.

```
call-manager-fallback
dialplan-pattern 1 311611.... extension-length 4 extension-
pattern
....
```

- Step 5.** If site codes are used for this installation, add VoIP dial peers in order to maintain dialing between sites in SRST mode. The examples given are for the access code, 2-digit site codes, 7-digit directory numbers, and 10-digit outbound PSTN numbers.

Example: Headquarters Site

```
dial-peer voice 810 voip
description 7-DIGIT DIAL to HQ in SRST
translation-profile outgoing SRST-7-Digit
destination-pattern 810....
session protocol sipv2
session target ipv4:10.106.170.136
dtmf-relay rtp-nte
codec g711ulaw
no vad
```

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

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

```
voice register pool 1
id network 10.106.170.1 mask 255.255.255.0
dtmf-relay rtp-nte sip-notify
codec g711ulaw
```



Step 7. 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 ipv4:10.106.170.136 expires 3600
  registrar ipv4:10.106.170.135 expires 3600 secondary
```

Procedure 3

Block voice traffic on WAN links

(Optional)

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



Tech Tip

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

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

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

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



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

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




Appendix A: Product List

Data Center or Server Room

Component	Product Description	Part Numbers	Software
Call Control	Cisco Business Edition 6000 with up to 1000 users	BE6M-M4-K9	11.0.1.20000-2
Unity Connection	Cisco Business Edition 6000 with up to 1000 users		11.0.1.20000-2
IM & Presence	Cisco Business Edition 6000 with up to 1000 users		11.0.1.20000-2
Prime Collaboration	Cisco Business Edition 6000 with up to 1000 users		11.0-small.ova

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	15.5.2T1
	2 Port Channelized T1/E1 and ISDN PRI High Speed WAN Interface Card (data only)	HWIC-2CE1T1-PRI	
	2-Port 3rd Gen Multiflex Trunk Voice/WAN Int. Card-T1/E1	VVIC3-2MFT-T1/E1	

Site Voice

Functional Area	Product Description	Part Numbers	Software
Remote Site Voice Router	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	15.5.2T1
	2 Port Channelized T1/E1 and ISDN PRI High Speed WAN Interface Card (data only)	HWIC-2CE1T1-PRI	
	2-Port 3rd Gen Multiflex Trunk Voice/WAN Int. Card-T1/E1	VVIC3-2MFT-T1/E1	
	SRST For 100 phones	FL-CME-SRST-100	



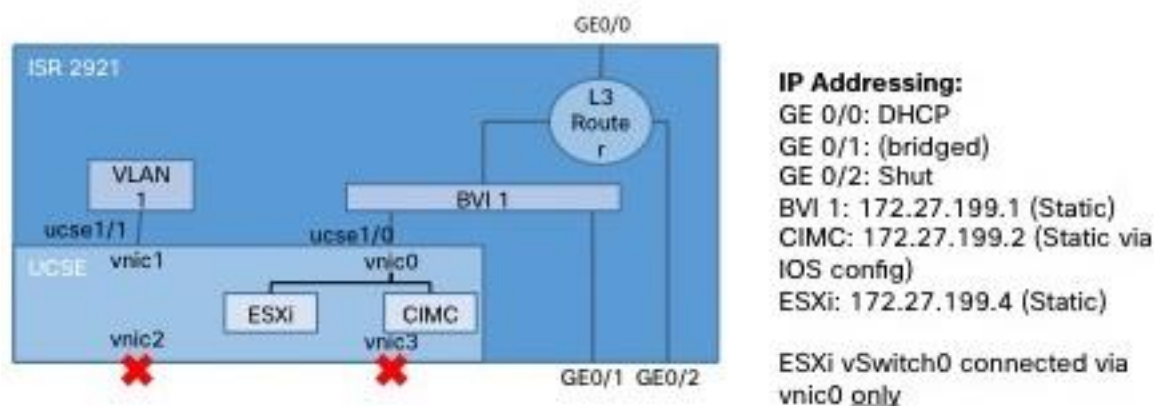
Endpoints

Functional Area	Product Description	Part Numbers	Software
Phones	Unified IP Phone 7800 Series	CP-7821-K9 CP-7841-K9 CP-7861-K9	SIP78xx.10-2-1-12
	Unified IP Phones DX600 Series	CP-DX650-K9	SIPdx650.10-2-4-46.k3
	Unified IP Phones 8800	CP-8841-K9= CP-8851-K9=	SIP88xx.10-2-2-16
Soft Client	Jabber	Cisco Jabber for Windows	Jabber_for_Windows-11.0
Soft Client	Jabber	Cisco Jabber for Mac	Jabber_for_Mac-11.0

Appendix B

BE6000S sample network configuration

Cisco BE6000S ships with preconfigured images with 172.27.x.x network as shown in the figure below



The procedure listed below gives you information on how an installation can be done for the environment where you would have a different network.

The following information is needed for the installation:

Items	CVD configuration	Site specific Configuration
NTP server IP address	10.64.58.50	
Domain Name System server IP	10.106.170.176	
Domain Name	mmcvd1.ciscolabs.com	
Hostname,IP address, network mask, and default gateway for each applications	UCM-Pub 10.106.170.185 255.255.255.128 10.106.170.129	
	Ucn1 10.106.170.186 255.255.255.128 10.106.170.129	
	Imp1 10.106.170.187 255.255.255.128 10.106.170.129	
	Pcp 10.106.170.184 255.255.255.128 10.106.170.129	



Procedure 1

Configuring Cisco BE6000S

Step 1. Change the username and password for BE6000S for the first time when you log into the Router using the command `username <newusername> privilege 15 secret <newpassword>`

Step 2. Change the domain names and the IP addresses that will be used for different applications-

```
ip domain name mmcvd1.ciscolabs.com
ip host ntp.mmcvd1.ciscolabs.com 10.64.58.50
ip host ucm-pub.mmcvd1.ciscolabs.com 10.106.170.185
ip host ucn1.mmcvd1.ciscolabs.com 10.106.170.186
ip host impl.mmcvd1.ciscolabs.com 10.106.170.187
ip host pcp.mmcvd1.ciscolabs.com 10.106.170.184
ip host s1-mmcvd1.ciscolabs.com 10.106.170.190
ip host s1-mmcvd1.ciscolabs.com.106.170.188
ip host ns.mmcvd1.ciscolabs.com 10.106.170.176
ip name-server 10.106.170.176
```

Step 3. Configure the IP address of UCM under trusted list within Voice service Voip command

```
voice service voip
ip address trusted list
ipv4 10.106.170.185
```

Step 4. Configure Gigabit interface 0/2 with the IP address that this network will be accessible from

```
interface GigabitEthernet0/2
description Access to the router
ip address 10.106.170.176 255.255.255.128
```

Step 5. Configure the sub interfaces on Gigabit interface 0/1 that will connect to the switch (for connecting the data and voice vlan on the switch)

```
interface GigabitEthernet0/2.1
description datavlan
encapsulation dot1Q 1 native
ip address 192.168.0.1 255.255.255.0
interface GigabitEthernet0/2.2
description voice vlan
encapsulation dot1Q 2
ip address 192.168.2.1 255.255.255.0
```



Step 6. Change the IP address on ucse1/0 interface

```
interface ucse1/0
description Internal interface connected to UCSE Port 0
ip unnumbered GigabitEthernet0/0
imc ip address 10.106.170.190 255.255.255.128 default-gateway
10.106.170.129
imc access-port shared-lom console
```

Step 7. Configure DNS server on this router or if you have any existing DNS server, use the IP address of the DNS server

```
ip dns server
ip dns spoofing 10.106.170.176
```

Step 8. Add a default route for routing across the networks and also for each of the applications with the same Ucse1/0 as the outgoing interface

```
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
ip route 10.106.170.184 255.255.255.255 ucse1/0
ip route 10.106.170.185 255.255.255.255 ucse1/0
ip route 10.106.170.186 255.255.255.255 ucse1/0
ip route 10.106.170.187 255.255.255.255 ucse1/0
ip route 10.106.170.188 255.255.255.255 ucse1/0
ip route 10.106.170.190 255.255.255.255 ucse1/0
```

Step 9. Add routing to the switch connecting to the router

```
ip route 192.168.2.2 255.255.255.255 GigabitEthernet0/2
```

Step 10. Update the NTP server address with local NTP server address.

Step 11. Access the ESXI and follow the install steps listed in the preparing application sections to complete the Installation of applications on the BE6000S server blade.



Feedback

Please send comments and suggestions about this guide to collab-mm-cvd@external.cisco.com.



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.

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. 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)