Newer Cisco SBA Guides Available

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

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

Room-System Video Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series

Preface

Who Should Read This Guide

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

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

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

Release Series

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

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

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

month year Series

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

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

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

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

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

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

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

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

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

Comments and Questions

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

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

Table of Contents

What's In This SBA Guide

Cisco SBA Collaboration

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

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

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

Route to Success

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

About This Guide

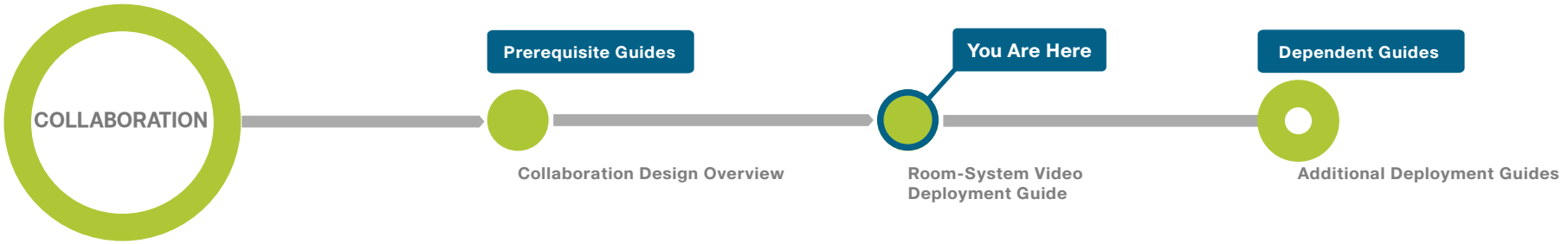
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

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

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

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

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



Introduction

Business Overview

Businesses around the world are struggling with escalating travel costs. Growing corporate expense accounts reflect the high price of travel, but travel also takes a toll on the health and well-being of employees and their families. The time away from home and the frustration levels experienced from lost luggage, navigating through airport terminals, and driving in unfamiliar cities are burdens many employees must endure weekly.

Organizations are under increasing pressure to reduce the amount of time it takes to make informed decisions concerning their business operations. Often, the only way to solve a difficult problem is to fly an expert to the location to see the issue and discuss it with the people at the site. When an expert cannot see what is being described, the resolution of a complex problem often takes much longer.

Work-at-home programs can save organizations money by reducing the amount of office space required, but some managers find the programs undesirable because they like to see their staff on a regular basis. At the same time, remote workers often feel isolated from their departments because they do not spend enough face time with their peers and they feel disconnected from the decision-making process. This isolation can lead to lower job performance and less job satisfaction from employees who do not work at the organization's main location. Human resource departments find it is difficult and expensive to interview candidates for a position if the prospective employee is not in the same city as the hiring manager.

Audio conferences can help in certain situations, but the face-to-face interaction during video collaboration meetings helps to boost information retention, promotes increased attention span, and reduces participant confusion. The nonverbal cues experienced in a visual meeting are sometimes more important than what is actually spoken.

Technology Overview

With Cisco video collaboration solutions, your organization can reap the budgetary and productivity gains that a remote workforce allows—without compromising the benefits of face-to-face interaction.

Adoption of Cisco's comprehensive video collaboration strategy affects the way business is conducted across an organization. Among the benefits:

- **Helping you make decisions faster**—Cisco multipurpose room systems enable all parties to share ideas, show detailed images, and take action more quickly. Rapid decision-making helps organizations bring new products to market or resolve customer service concerns sooner than their competitors.
- **Providing immediate access to experts—**Cisco immersive systems enable you to take advantage of the expertise of a few people across your entire organization without their having to travel. Peripherals, like document cameras and wireless hand-held cameras, can bring complex problems alive for an expert in another location. Training, translating, consulting, and troubleshooting can also happen in real time. With video streaming and archiving solutions, you can record and store an expert's knowledge for easy accessibility by anyone at any time.
- **Bringing the organization closer together—**Multiple remote offices do not have to mean that team members are isolated. Cisco multipurpose room systems, executive systems, and personal systems help to create a virtual meeting room for collaboration and sharing, which keeps everyone up to date with the same information.
- **Improving work/life balance for employees**—An employee can use Cisco personal systems to attend meetings or work from home instead of sitting in rush-hour traffic. Video participation allows people to maintain a balance between work and personal lives, save the organization travel costs, and protect the environment by reducing their carbon foot prints.

Video Collaboration Components

A camera, microphone, monitor, speaker, and codec are the five essential components that constitute a video collaboration solution. The camera and microphone capture the image and sound at one location. The codec converts the video and audio into a digital signal and compresses it before sending it out over the network. At the other end, the codec decompresses the signal and feeds the picture to a monitor and the sound to a speaker.

A video call can incorporate two or more units, with many options for advanced functionality. Depending on your application requirements and budget, Cisco provides you with numerous choices for your video collaboration solution. There is a system for every workspace, from boardrooms to desktops and from field locations to manufacturing floors. If you choose a vendor with a common set of platforms and infrastructure components, all of the systems you implement will work together easily.

Network Considerations

Cisco recommends running your video collaboration traffic over an IP network rather than a public ISDN network. If you already have an IP network in place for voice, your natural next step is to deploy video over IP. Many organizations run video systems in a mixed environment as they move from older systems to newer ones based on IP. As older systems migrate off of ISDN, you will realize significant quality improvements and cost savings.

Running video over a converged IP network allows unified communications to become a reality. IP offers lower costs, easier management, remote monitoring, and control from across the network. It also provides higher bandwidth for calls, enabling superior audio and video quality while providing tighter integration into the corporate IT mainstream.

With an IP network based on Cisco® Smart Business Architecture (SBA), the ongoing costs of running video calls are minimal because you only have to pay for maintenance and technical support. When return on investment (ROI) for the initial deployment is met, any additional calls are essentially free. Because there is no incremental cost involved, employees and managers are more likely to use the technology. As usage goes up, payback times go down, further boosting the ROI.

Cisco Medianet

The Cisco Medianet is network-aware, device-aware, and media-aware. Medianet extends the network boundary to include the endpoints in order to scale, optimize, and enhance the performance of collaboration components. The Media Services Interface is middleware running in routers, switches and endpoints within the Cisco SBA platform that makes applications aware of the network and the network aware of the applications. The infrastructure components combine with the media services and management interface to allow customers to run interactive video, unified communications, streaming video, and video surveillance over a common IP network.

Voice and video applications are raising new requirements in terms of higher bandwidth, lower latency, and predictable jitter. The Cisco SBA platform components are uniquely positioned to understand the source and destination of voice and video streams, as well as the ever-changing capacity characteristics of the connection. A medianet can also apply the necessary media transformations by using transcoders, as well as change media and signal encoding by using session border controllers to adapt to changing network conditions. This helps enable a new degree of interoperability between previously incompatible collaboration endpoints while ensuring a consistent quality of experience.

Solution Details

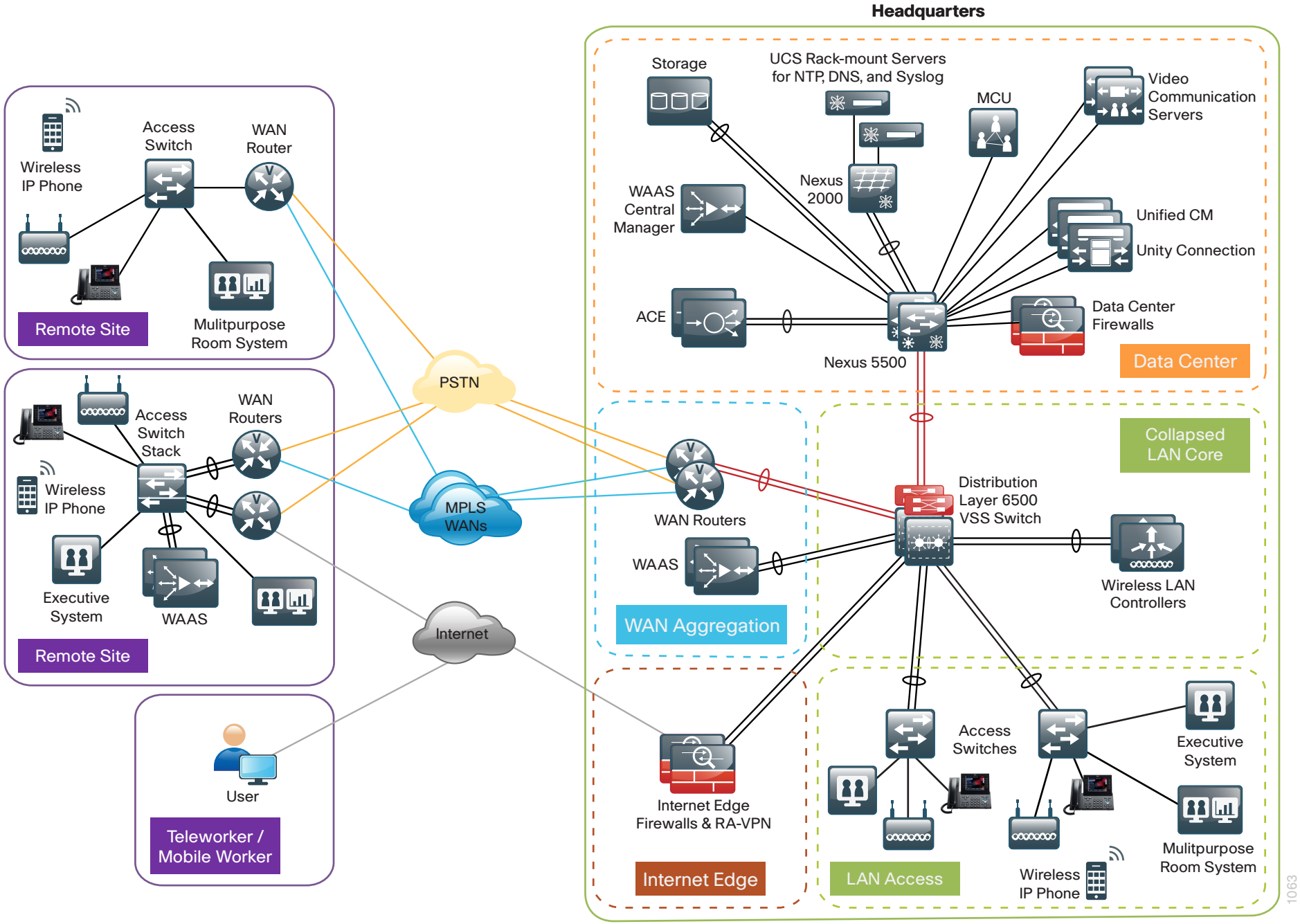
To allow the most flexibility with conference rooms of varying sizes and peripheral equipment, Cisco recommends multipurpose room systems for organizations. Cisco TelePresence Profile Series endpoints offer the highest-quality video and audio and work in a variety of room sizes, plus they can accommodate the peripherals needed for effective video collaboration among your locations. They scale from 128 kbps Quarter Common Intermediate Format (QCIF) resolutions up to 1080p30 at 5 Mbps per screen.

The Cisco TelePresence Profile 55 is ideal for single-screen use cases. A dual-screen Profile 65 works best when you require additional display real estate. The Cisco TelePresence EX90 is recommended for executive desktops and personal room systems when a single person will be using them.

The room-system video solution for Cisco SBA includes the following components (shown in Figure 1):

- Video call agent for seamless call control
- Multipurpose and executive room systems for placing calls
- High-definition multipoint control unit (MCU) for reservationless and scheduled conferences
- Network Time Protocol (NTP) server for logging consistency
- Domain Name System (DNS) server for name-to-IP resolution
- Syslog server for logging events (optional)

Figure 1 - Room-system video in Cisco SBA foundation



Cisco TelePresence Video Communication Server

Cisco TelePresence Video Communication Server (VCS) supports Session Initiation Protocol (SIP), and the configurations in this document use SIP as the signaling protocol for the endpoints. If your organization has fewer than 2500 users, you should deploy a single VCS unless you require resiliency for your video call agent. For an organization with 2500 to 10,000 connected users, Cisco recommends that you deploy a VCS cluster with at least two call agents for scalability and redundancy. VCS peers in a cluster share bandwidth usage as well as routing, zone, and other configuration amongst themselves. Endpoints can register to any of the peers in the cluster; if they lose connection to their initial peer, they can re-register to another peer in the cluster. The advantages of a VCS cluster are as follows:

- Increase the capacity of your VCS deployment compared with a single VCS
- Provide redundancy in the rare case that a VCS becomes inaccessible due to a network or power outage, or while it is in maintenance mode during a software upgrade

Call licensing is carried out on a per-cluster basis. Any traversal or non-traversal call licenses that have been installed on a cluster peer are available for use by any peer within the cluster. If a cluster peer becomes unavailable, the call licenses installed on that peer will remain available to the rest of the cluster peers for two weeks from the time the cluster lost contact with the peer. This will maintain the overall license capacity of the cluster. However, note that each peer is limited by its physical capacity of 500 non-traversal calls, 100 traversal calls, and 2500 registration licenses.

Cisco TelePresence Multipoint Control Unit

Reservationless and scheduled conferencing use the high-definition MCU to ensure endpoints can communicate in a single conference at the highest possible bit rates and resolutions without loss of quality. The MCU lets customers purchase high-definition endpoints knowing they can continue to use their standard-definition systems without replacing all of them at the same time.

There are several different models of MCU that support different capacities, but they are all configured in a similar fashion as outlined below. An MCU should be located as close as possible to the endpoints that use it the majority of the time; this reduces the WAN bandwidth and delay between the callers and the conference bridge. For instance, if video conference calls are needed in the United States, Europe, and Asia—where most of the endpoints will be local, due to time-zone differences—Cisco recommends placing one MCU in each of the given geographies.

QoS and Bandwidth Control

The room-system video solution has been tested over the Cisco SBA reference design, and it uses the medianet quality-of-service (QoS) and bandwidth-control settings that Cisco recommends. Interactive video traffic is marked as assured forwarding 41 (AF41) to give it a higher priority across the network. Cisco VCS controls the bandwidth for calls among locations. The default call settings within the devices themselves handle the bandwidth for calls within a location.

The Cisco SBA Borderless Networks foundation design is configured to allow 23 percent of the available WAN bandwidth for video calls. The remote sites have 6 Mbps of bandwidth into the Cisco IOS® Multiprotocol Label Switching (MPLS) cloud, and the headquarters (HQ) site has 10 Mbps. Using the default settings in this guide, one 384 kbps call can be placed to each remote site and four can be made to and from the HQ location. If you will need to accommodate more calls locations, you will need additional bandwidth.

Per the medianet guidelines, the conference and scheduling resources are centralized in the geographic data centers. The access, WAN, and campus networks are medianet-enabled, using highly available designs and localized services in the remote sites whenever possible. The advantage of bringing Cisco video technologies to the Cisco SBA–validated blueprint is that the initial foundation work remains intact, because the architecture was originally designed with video communication in mind.

Deployment Details

This deployment guide focuses on multipurpose room systems and multipoint conferencing, which are the key components in helping customers realize the full benefits of virtual collaboration.

Process

Configuring Cisco TelePresence Video Communication Server

1. Configure VCS connectivity to the LAN
2. Prepare the Cisco VCS platform
3. Configure the Cisco VCS
4. Configure a VCS cluster master peer
5. Prepare a VCS cluster non–master platform
6. Configure a VCS cluster non–master peer
7. Configure VCS subzones
8. Configure VCS default bandwidth

The Cisco TelePresence Video Communication Server (VCS) is used for call control and bandwidth control. Before getting started, you need to collect certain information specific to your site. You can fill in the following table.

Table 1 - Information you need before configuring Cisco VCS

Item	Cisco SBA configuration	Site-specific details
IPV4 address	10.4.48.130	
IPV4 subnet	255.255.255.0	
IPV4 default gateway	10.4.48.1	
System name	VCSc1	
DNS server address	10.4.48.10	
DNS local host name	VCSc1	
DNS domain name	cisco.local	
NTP server address	10.4.48.17	
Time zone	Pacific -8	
SNMP community name	cisco	
Remote syslog server	10.4.48.13	

Procedure 1 Configure VCS connectivity to the LAN

The VCS can be connected to a Nexus switch in the Data Center or a Catalyst switch in the Server Room. In both cases, QoS policies are added to the ports to maintain video quality during conferences. Please choose the option that is appropriate for your environment.

Option 1. Connect the VCS to a Nexus 2248UP

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

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

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

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

Tech Tip

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

Option 2. Connect the VCS to a Catalyst 3750-X

To ensure that video traffic is prioritized appropriately, you must configure the Catalyst access switch port where the VCS is connected to trust the Differentiated Services Code Point (DSCP) markings. The easiest way to do this is to clear the interface of any previous configuration and then, apply the egress QoS macro that was defined in the access-switch platform configuration of the *SBA—LAN Deployment Guide*.

Step 1: Login to the 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 VCS is connected.

```
default interface GigabitEthernet1/0/9
```

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

```
interface GigabitEthernet1/0/9
 description VCS
 switchport access vlan 148
 switchport host
 macro apply EgressQoS
```

Procedure 2 Prepare the Cisco VCS platform

In the following steps, set the initial configuration by using a PC connected to the Cisco VCS DATA port via a serial cable.

Step 1: Connect the Ethernet LAN cable from the LAN1 port on the front of the unit to your network.

Step 2: Connect the supplied serial cable from the DATA port on the front of the unit to the serial port on a PC.

Step 3: Use terminal emulation software such as PuTTY and configure the serial port on the PC as follows:

- Baud rate—115200
- Data bits—8
- Parity—none
- Stop bits—1
- Flow control—none

Step 4: Turn on the power switch on the back right of the unit (adjacent to the power cable).

Step 5: Press the power button on the back left of the unit. Wait until:

- The green PWR LED on the front of the unit is a steady green color (it may flash briefly during power-up).
- The red ALM LED on the front of the unit has gone out.
- The default IP address (192.168.0.100) is showing in the display panel on the front of the unit.

The terminal emulator program on the PC displays the VCS's startup information. After approximately 4 minutes, you will see the login prompt.

Step 6: Enter the username admin

Step 7: Enter the default password TANDBERG

Step 8: At the prompt, run the install wizard.

```
Run install wizard [n]: y
```

Tech Tip

For security reasons, you are advised to change the admin password from the default of TANDBERG when using the install wizard.

Step 9: Follow the prompts to specify the settings.

```
Do you wish to change the system password? [n]: y
Password for your admin account: [password]
Type the password again: [password]
Whether you want to use IPv4, IPv6 or Both: IPV4
The LAN 1 IP address: 10.4.48.130
The LAN 1 IPv4 subnet mask: 255.255.255.0
The IP default gateway: 10.4.48.1
The Ethernet speed: auto
Whether you want to use SSH: y
Whether you want to use Telnet: n
```

After the install wizard is finished, you are prompted to log in again.

Step 10: Log in with the username **admin** and the new **[password]**.

Step 11: When you see the install wizard prompt again, enter **n** to skip the wizard.

Step 12: Restart the system in order for the new settings take effect (required).

```
xCommand restart
```

Tech Tip

For security reasons, you are advised to change the root password from the default of TANDBERG.

After the system restarts, log in as **root** to change the password for the root account.

Step 13: Log in again with the username **root**.

Step 14: Enter the default root password **TANDBERG**.

Step 15: After logging in, type the **passwd** command.

Step 16: Enter the new password **[password]**.

Step 17: When prompted, retype the password **[password]**.

Step 18: Type the **exit** command. This logs you out of the root account.

Step 19: Disconnect the serial cable and store it in a safe place.

Procedure 3 Configure the Cisco VCS

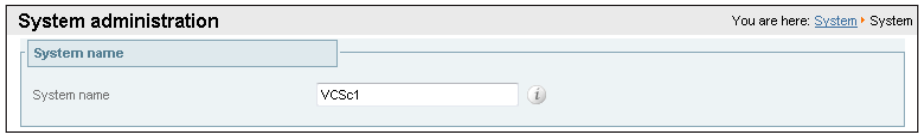
The rest of the configuration of the Cisco VCS is done using a standard web browser. You use the information collected in Table 1 at the beginning of this Cisco VCS configuration process to fill in the fields. This is the information you need to configure a basic VCS system for use with SIP endpoints.

Step 1: Open a browser window, and type the IP address of Cisco VCS: **10.4.48.130**

Step 2: Select **Administrator login**, enter the following values, and then click **Login**:

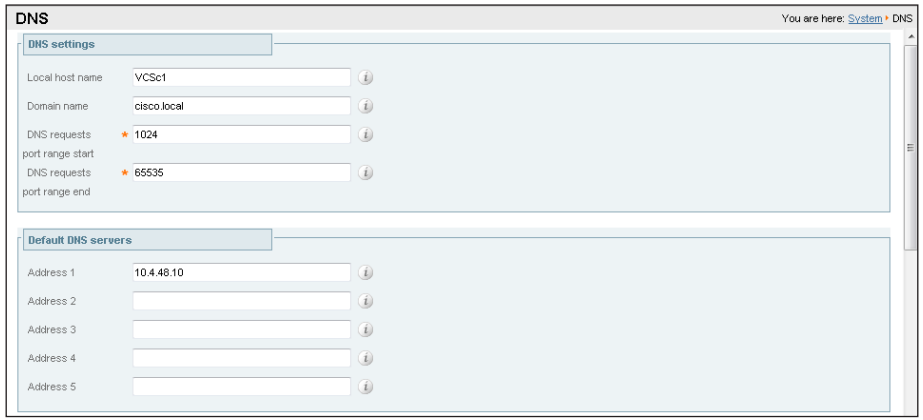
- Username—**admin**
- Password—**[password]**

Step 3: Navigate to **System** > **System**, in the **System name** box, enter **VCSc1**, and then click **Save**.



Step 4: Navigate to **System > DNS,** enter the following values, and then click **Save**:

- Local host name—**VCSc1**
- Domain name—**cisco.local**
- DNS requests port range start—**1024**
- DNS requests port range end—**65535**
- Address 1—**10.4.48.10**

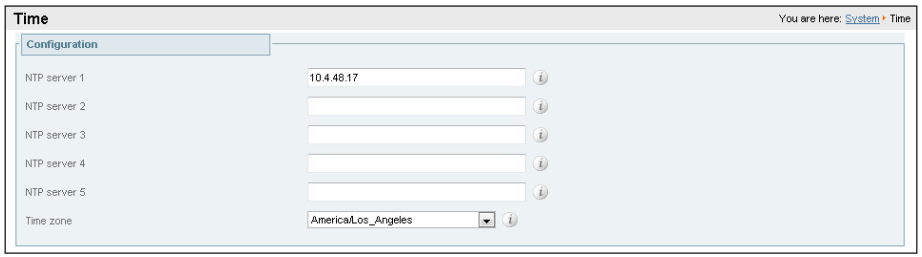


Tech Tip

You can use address fields 2 through 5 for alternate DNS server addresses (for resilience purposes) or, alternatively, for DNS server addresses that serve different types of lookup data (for example, ENUM lookups).

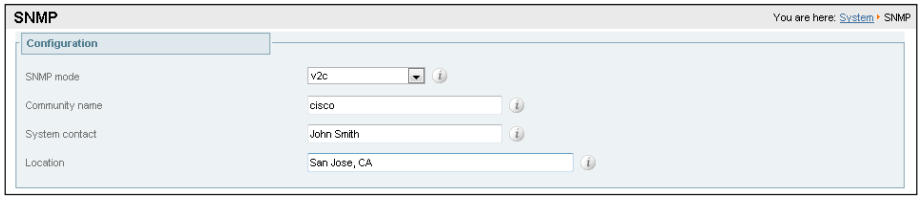
Step 5: Navigate to **System > Time,** enter the following values, and then click **Save**:

- NTP server—**10.4.48.17**
- Time zone—**America/Los_Angeles**



Step 6: Navigate to **System > SNMP**, enter the following values, and then click **Save**:

- SNMP mode—**v2c**
- Community name—**cisco**
- System contact—**John Smith** (optional)
- Location—**San Jose, CA** (optional)



Tech Tip

QoS is needed to put the media and signaling traffic into the low-latency queues defined in the *Cisco SBA—LAN Deployment Guide*. The QoS settings give the video packets a higher priority over non–real-time traffic in the data queues.

The Differentiated Service markings match the medianet-recommended settings for interactive video traffic in Cisco SBA.

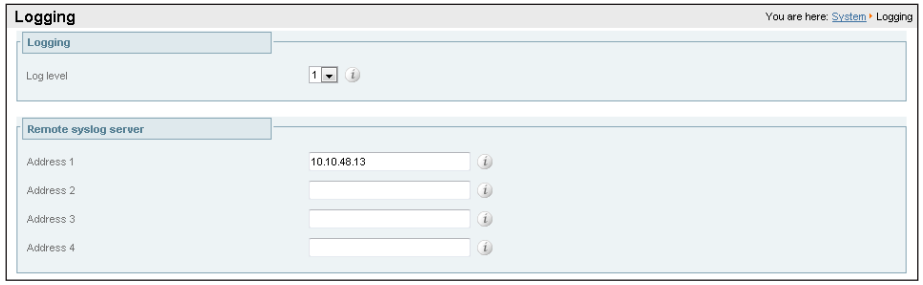
Step 7: Navigate to **System > Quality of Service**, enter the following values, and then click **Save:**

- QoS mode—DiffServ
- Tag value—34 (AF41)

By default, the system log level is set to level 1. This setting configures Cisco VCS to output high-level (easily readable) events in system log and syslog messages. The system logs are stored on a Solarwinds server at the IP address listed below. Administrators can use the information when trouble-shooting problems with the device.

Step 8: Navigate to **System > Logging**, enter the following values, and then click **Save**:

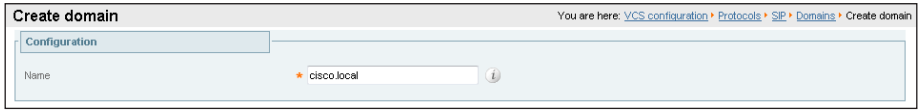
- Log level—1
- Address 1—10.4.48.13



Tech Tip

After the domain name has been configured, SIP endpoints can register using the name. For example, a VCS configured with the domain name of cisco.local will accept registrations from an endpoint with a SIP URI of 4600@cisco.local.

Step 9: Navigate to **VCS configuration > Protocols > SIP > Domains**, and then click **New**.



Step 10: In the **Name** box, enter cisco.local, and then click **Create domain**.

Next, you restart the system. This allows the SNMP and QoS settings to take effect.

Step 11: Navigate to **Maintenance > Restart**, and then click **Restart system**.

Step 12: In the Confirm window, click **OK**. After approximately 2 minutes, the system restarts.

Step 13: Click **Administrator login**, enter the following values, and then click **Login**:

- Username—admin
- Password—[password]

Step 14: If there are any configuration warnings, navigate to **Status > Alarms** and read them to determine if any of them require action on your part. Follow the instructions as required.

Step 15: If they do not require action, click **Select all,** and then click **Acknowledge**.

Procedure 4 Configure a VCS cluster master peer

(Optional)

Cisco VCS uses clustering for redundancy and to add capacity to the video call agent. If your organization has more than 2500 connected users, Cisco recommends a cluster of VCS peers to manage your video endpoints. If your organization does not require a cluster at this time, you can skip this procedure and the next procedure.

This procedure sets up the first (master) peer of a new cluster. Additional peers are added in Procedure 5, "Configure a VCS cluster non–master peer."

Tech Tip

All VCS peers in a cluster must be running the same version of software. The software versions in this guide are documented in Appendix A.

The master VCS will be the source of the configuration information for all VCS peers in the cluster. Non-master VCS peers will have the majority of their configuration deleted and replaced with information from the master.

Step 1: Navigate to **VCS configuration** > **Calls**, in the Call routed mode list choose **Optimal**, and then click **Save**.

Step 2: If the VCS is already in use, enable maintenance mode to take it out of service. Use PuTTY software from your PC to log in to the device via Secure Shell (SSH) Protocol with the username **admin** and password that you configured in Procedure 1.

Step 3: Enable maintenance mode.

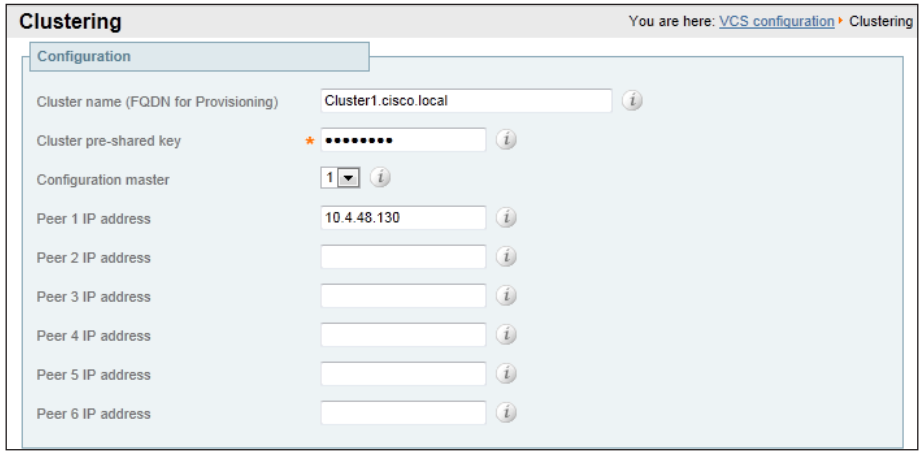
```
xConfiguration SystemUnit Maintenance Mode: On
bye
```

Step 4: If devices are still registered, navigate to **Status** > **Registrations** > **By device**, click **Select all**, and then click **Unregister**.

Step 5: On the Confirm screen, click **Yes**.

Step 6: Navigate to **VCS configuration** > **Clustering**, enter the following values, and then click **Save**:

- Cluster name—**Cluster1.cisco.local**
- Cluster pre-shared key—**[pre-shared key]**
- Configuration master—**1**
- Peer 1 IP address—**10.4.48.130** (master)



Step 7: Read the **Confirm** screen, and then click **Yes.**

Step 8: Navigate to **Maintenance** > **Restart**, click **Restart system**, and then in the **Confirm** screen, click **Yes**. After approximately 2 minutes, the system restarts.

Step 9: Click **Administrator login**, enter the following values, and then click **Login**:

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

Step 10: If there are any configuration warnings, navigate to **Status** > **Alarms** and read them to determine if any of them require action on your part.

Step 11: If they do not require action, click **Select all**, and then click **Acknowledge**.

Step 12: The master peer is now configured. Follow the steps in the next procedure to configure the non–master peers in your cluster.

Procedure 5 Prepare a VCS cluster non–master platform

(Optional)

The following procedure is needed if you plan to use more than one VCS in your environment. If you only have one VCS, please skip ahead to Procedure 7 "Configure VCS subzones".

Before you configure the non–master peer, you need to collect certain information specific to your site. Only one peer can be added at a time, so the steps in this procedure will have to be repeated for each one.

Table 2 - Information you need before configuring the non-master Cisco VCS peers

Item	Cisco SBA configuration	Site-specific details
IPV4 address	10.4.48.131	
IPV4 subnet	255.255.255.0	
IPV4 default gateway	10.4.48.1	
System name	VCSc2	
DNS server address	10.4.48.10	
DNS local host name	VCSc2	
DNS domain name	cisco.local	
Cluster name	Cluster1@cisco.local	
Cluster pre-shared key	[pre-shared key]	
Peer 1 IP address	10.4.48.130	

The VCS can be connected to a Nexus switch in the Data Center or a Catalyst switch in the Server Room. In both cases, QoS policies are added to the ports to maintain video quality during conferences. Please choose the option that is appropriate for your environment.

Option 1. Connect the VCS to a Nexus 2248UP

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

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

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

```
interface Ethernet107/1/2
 description VCS2
 switchport access vlan 148
 spanning-tree port type edge
 service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

Tech Tip

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

Option 2. Connect the VCS to a Catalyst 3750-X

To ensure that video traffic is prioritized appropriately, you must configure the Catalyst access switch port where the VCS is connected to trust the DSCP markings. The easiest way to do this is to clear the interface of any previous configuration and then, apply the egress QoS macro that was defined in the access-switch platform configuration of the *SBA—LAN Deployment Guide*.

Step 1: Login to the 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 VCS is connected.

```
default interface GigabitEthernet1/0/10
```

Step 3: Configure the port as an access port on the same VLAN as the master VCS and apply the Egress QoS policy.

```
interface GigabitEthernet1/0/10
 description VCS2
 switchport access vlan 148
 switchport host
 macro apply EgressQoS
```

In the following steps, set the initial configuration by using a PC connected to the Cisco VCS DATA port via a serial cable.

Step 4: Connect the Ethernet LAN cable from the LAN1 port on the front of the unit to your network.

Step 5: Connect the supplied serial cable from the DATA port on the front of the unit to the serial port on a PC.

Step 6: Use terminal emulation software such as PuTTY and configure the serial port on the PC as follows:

- Baud rate—115200
- Data bits—8
- Parity—none
- Stop bits—1
- Flow control—none

Step 7: Turn on the power switch on the back right of the unit (adjacent to the power cable).

Step 8: Press the soft power button on the back left of the unit. Wait until:

- The green PWR LED on the front of the unit is a steady green color (it may flash briefly during power-up).
- The red ALM LED on the front of the unit has gone out.
- The default IP address (192.168.0.100) is showing in the display panel on the front of the unit.

The terminal emulator program on the PC displays the VCS's startup information. After approximately 4 minutes, you will see the login prompt.

Step 9: Enter the username admin

Step 10: Enter the default password TANDBERG

Step 11: At the prompt, run the install wizard.

```
Run install wizard [n]: y
```

Tech Tip

For security reasons, you are advised to change the admin password from the default of TANDBERG when using the install wizard.

Step 12: Follow the prompts to specify the settings.

```
Do you wish to change the system password? [n]: y
Password for your admin account: [password]
Type the password again: [password]
Whether you want to use IPv4, IPv6 or Both: IPV4
The LAN 1 IP address: 10.4.48.131
The LAN 1 IPv4 subnet mask: 255.255.255.0
The IP default gateway: 10.4.48.1
The Ethernet speed: auto
Whether you want to use SSH: y
Whether you want to use Telnet: n
```

After the install wizard is finished, you are prompted to log in again.

Step 13: Log in with the username admin and the new [password].

Step 14: When you see the install wizard prompt again, enter n to skip the wizard.

Step 15: Restart the system in order for the new settings take effect (required).

```
xCommand restart
```

Tech Tip

For security reasons, you are advised to change the root password from the default of TANDBERG.

After the system restarts, log in as **root** to change the password for the root account.

Step 16: Log in again with the username **root**

Step 17: Enter the default root password **TANDBERG**

Step 18: After logging in, type the **passwd** command.

Step 19: Enter the new password **[password]**

Step 20: When prompted, retype the password **[password]**

Step 21: Type the **exit** command. This logs you out of the root account.

Step 22: Disconnect the serial cable and store it in a safe place.

Procedure 6 Configure a VCS cluster non–master peer

(Optional)

The following procedure is needed if you plan to use more than one VCS in your environment. If you only have one VCS, please skip ahead to Procedure 7 “Configure VCS subzones”.

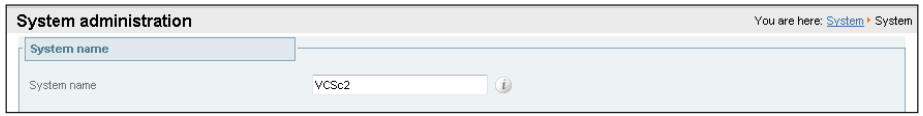
The rest of the configuration of the Cisco VCS is done using a standard web browser. You use the information collected in Table 2 at the beginning of Procedure 5 “Prepare a VCS cluster non-master platform” to fill in the fields.

Step 1: Open a browser window, and enter the IP address of the non–master Cisco VCS: **10.10.48.131**

Step 2: Select **Administrator login**, enter the following values, and then click **Login**:

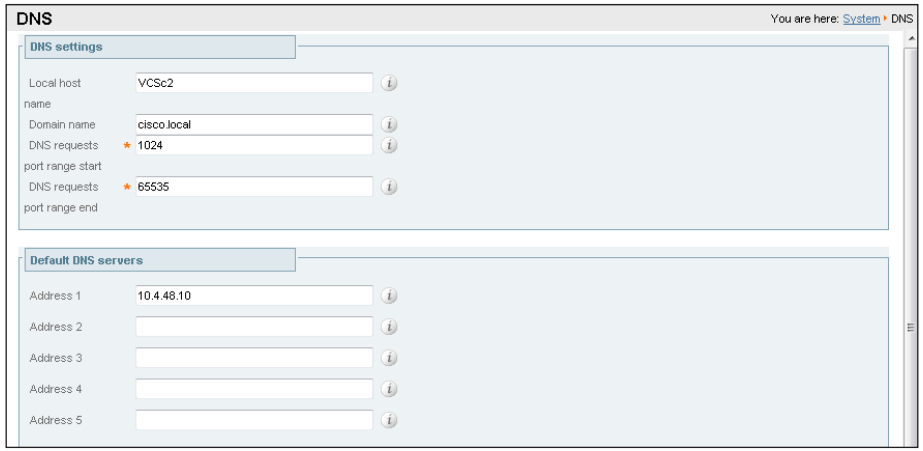
- Username—**admin**
- Password—**[password]**

Step 3: Navigate to **System** > **System**, and in the **System name** box, enter **VCSc2**, and then click **Save**.



Step 4: Navigate to **System** > **DNS,** enter the following values, and then click **Save**:

- Local host name—**VCSc2**
- Domain name—**cisco.local**
- DNS requests port range start—**1024**
- DNS requests port range end—**65535**
- Address 1—**10.4.48.10**



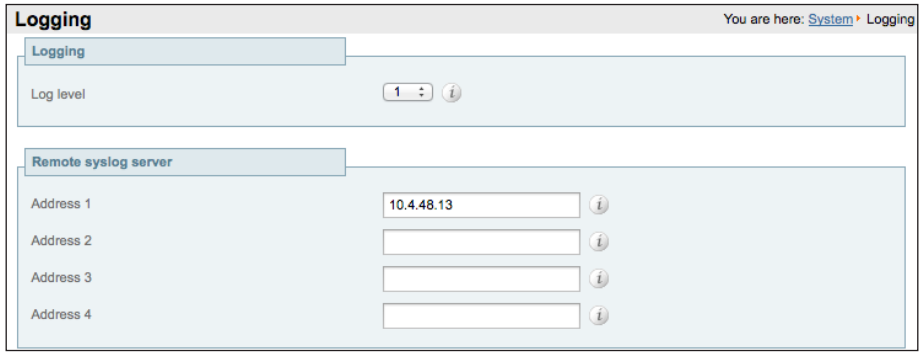
Tech Tip

The QOS settings are copied from the master VCS, so they are not entered in the non-master.

By default, the system log level is set to level 1. This setting configures Cisco VCS to output high-level (easily readable) events in system log and syslog messages. The system logs are stored on a Solarwinds server at the IP address listed below. Administrators can use the information when trouble-shooting problems with the device.

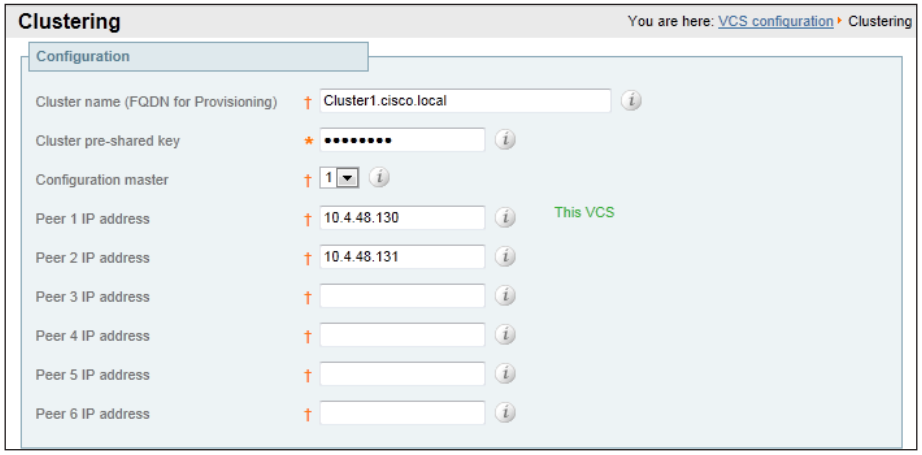
Step 5: Navigate to **System** > **Logging**, enter the following values, and then click **Save** :

- Log level—1
- Address 1—10.4.48.13



Step 6: On the master VCS, navigate to **VCS configuration** > **Clustering**, enter the following value, and then click **Save**.

- Peer 2 IP address—10.4.48.131 (non-master)



Tech Tip

A cluster communication failure alarm is raised on the master and on other non–master peers already in the cluster advising that this new VCS peer is not communicating. This alarm will be cleared later.

Cluster configuration replication is suspended at this point until the new VCS peer is added. Any changes made to the configuration of the cluster will not be replicated until this VCS has been added.

Step 7: Using PuTTY terminal emulation software, use IP address 10.4.48.131 to log in to the non–master VCS from a PC via SSH Protocol. Use the following credentials:

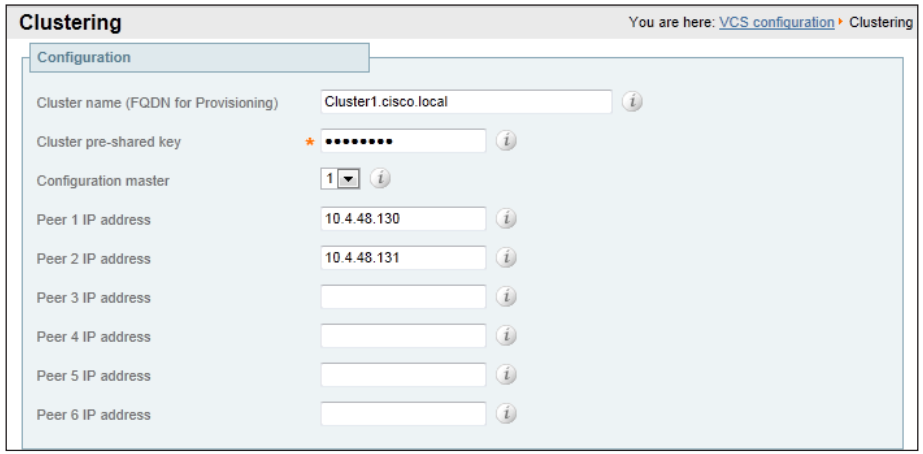
- Login as—admin
- Password—[password]

Step 8: From the command line, set the default level to 2 and add the links by entering the following commands.

```
xcommand DefaultValuesSet Level: 2
xcommand DefaultLinksAdd
bye
```

Step 9: On the non-master VCS, navigate to **VCS configuration** > **Clustering**, enter the following values, and then click **Save**:

- Cluster name—**Cluster1.cisco.local** (same as master)
- Cluster pre-shared key—**[pre-shared key]** (same as master)
- Configuration master—**1** (master is at the Peer 1 IP Address)
- Peer 1 IP address—**10.4.48.130** (master IP address)
- Peer 2 IP address—**10.4.48.131** (this VCS)



Step 10: Read the Confirm screen, and then click **Yes.**

Step 11: Navigate to **Maintenance** > **Restart**, click **Restart** system, and then in the Confirm screen, click **Yes**. After approximately 2 minutes, the system restarts.

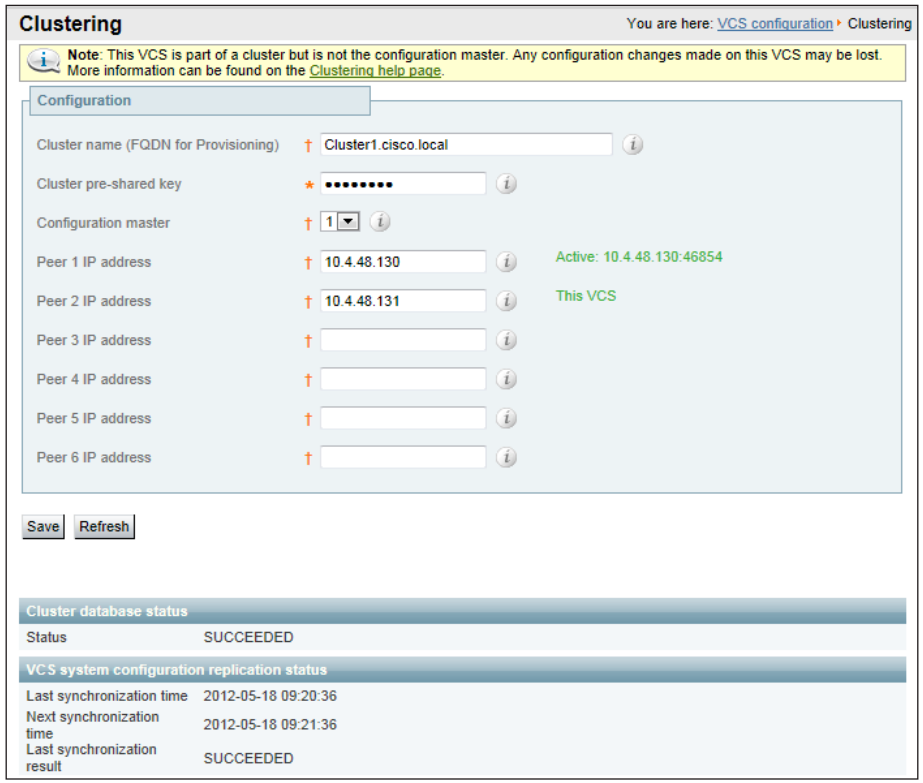
Step 12: Click **Administrator login**, enter the following values, and then click **Login**:

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

Step 13: If there are any configuration warnings, navigate to **Status** > **Alarms** and read them to determine if any of them require action on your part.

Step 14: If they do not require action, click **Select all,** and then click **Acknowledge**.

Step 15: Navigate to **VCS Configuration** > **Clustering** to confirm the master VCS is active and the VCS system configuration replication status is listed as SUCCEEDED.



The non-master peer is now configured.

Tech Tip

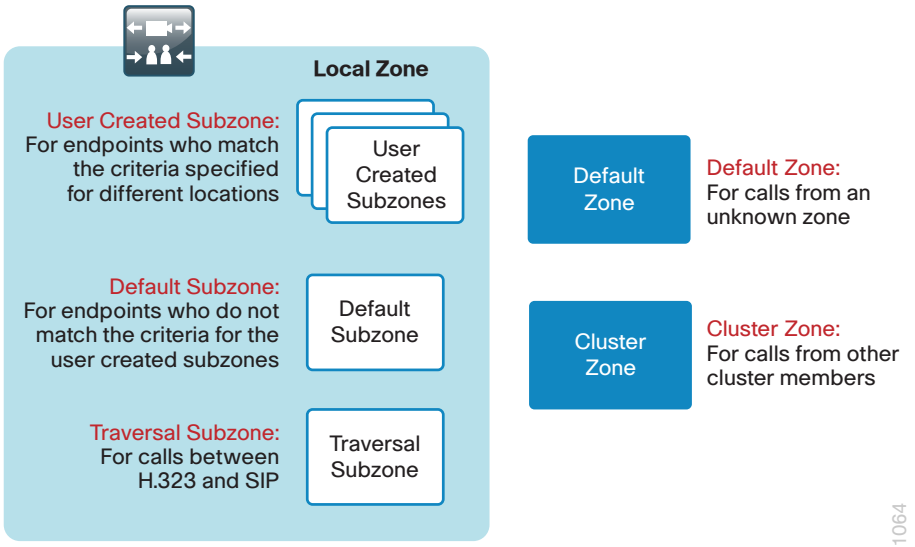
In a VCS cluster environment, the rest of the configuration is completed on the first (master) VCS. The information entered on the master is replicated to the non–master peers every minute.

Procedure 7 Configure VCS subzones

Cisco VCS uses the concept of zones and subzones to define where devices are registered on the network. The proper location of devices is important to allow Cisco VCS to protect the expensive WAN resources in the underlying network. After the location of devices is defined, additional settings called *links* and *pipes* are used to control the number of calls allowed between sites.

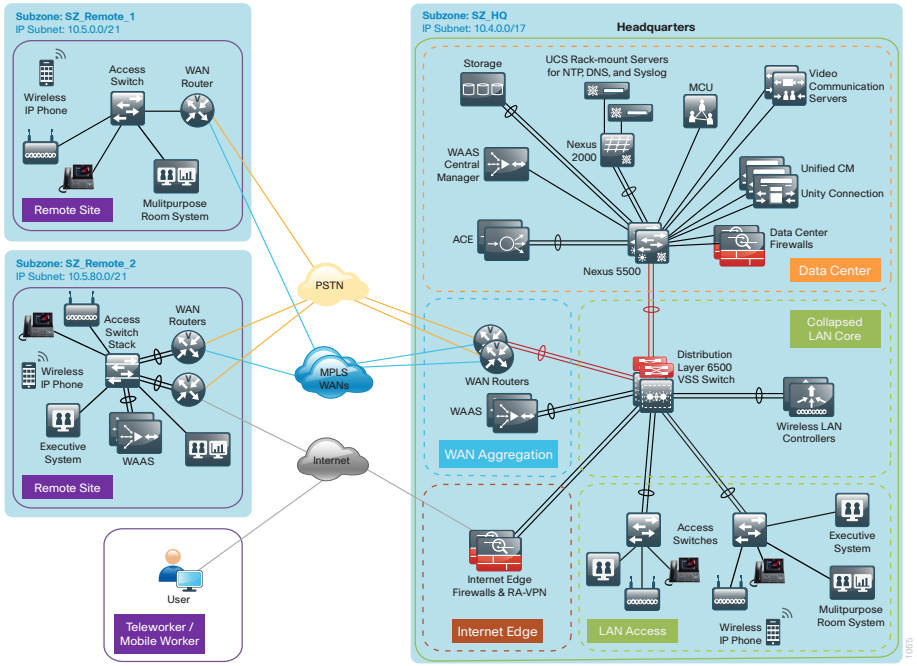
The local zone is a container of subzones local to Cisco VCS. VCS automatically creates a cluster zone, default zone, default subzone, and traversal subzone. Additional subzones are created to segment the video endpoints into their respective locations. Figure 2 below shows the relationship between the zones and subzones.

Figure 2 - Relationship between zones and subzones in Cisco VCS



A subzone is created for the HQ location, as well as one for each remote site location. Figure 3 shows the subzones and IP address ranges in blue as they are defined in the foundation architecture.

Figure 3 - Subzones in foundation architecture

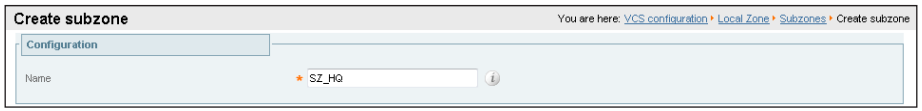


The default subzone is not used, and any rogue endpoints registered to it cannot make calls to the authorized endpoints in the user-created subzones. Bandwidth control among sites is done using links and pipes as outlined below, so you will not utilize the subzone bandwidth settings.

Create one subzone for each location that has video endpoints.

Step 1: From the master VCS, navigate to **VCS configuration** > **Local Zone** > **Subzones**, and then click **New**.

Step 2: On the Create subzone page, in the **Name** box, enter SZ_HQ, and then click **Create subzone.**



Step 3: Create the rest of the subzones that your organization needs by repeating Step 1 and Step 2.

Subzone membership rules are used to assign endpoints to the correct subzones. The easiest way to match the endpoints is IP address subnet ranges. Two membership rules are created for the HQ site to account for the endpoints in the access subnet at 10.4.0.0/24 and Cisco MCU in the server room subnet at 10.4.48.0/24.

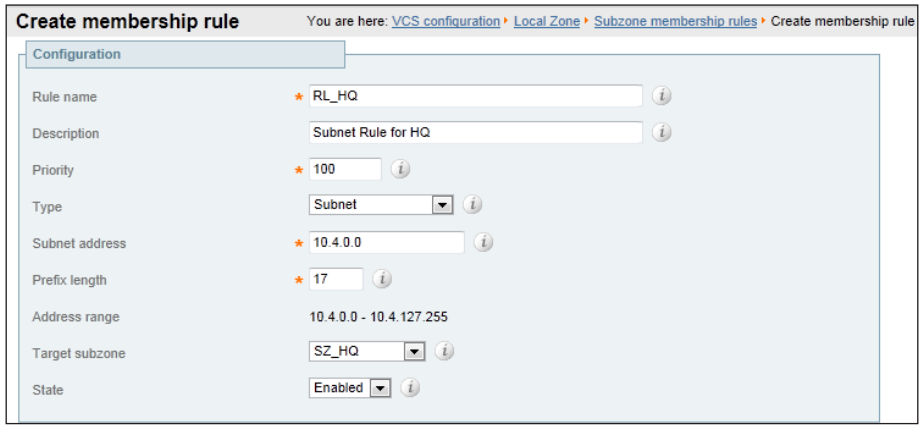
Tech Tip

The address range for the membership rules must correspond with the specified site.

Step 4: Navigate to **VCS configuration** > **Local Zone** > **Subzone membership rules**, and then click **New.**

Step 5: On the **Create membership rule** page, enter the following values, and then click **Create rule**:

- Rule name—RL_HQ
- Description—Subnet Rule for HQ
- Priority—100 (default)
- Type—Subnet
- Subnet address—10.4.0.0
- Prefix length—17
- Target subzone—SZ_HQ
- State—Enabled



Step 6: Create the rest of the membership rules for your organization by repeating Step 4 and Step 5 using the appropriate information for each subnet.

Procedure 8 Configure VCS default bandwidth

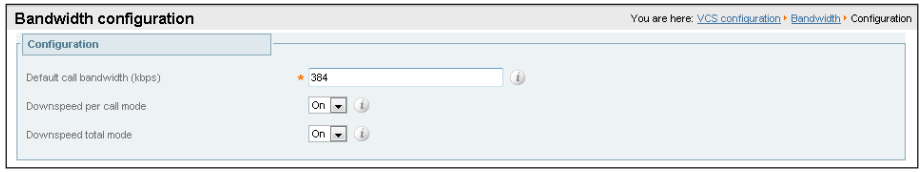
Cisco VCS uses the concept of pipes and links to control the bandwidth between locations. The bandwidth settings for calls within a single subzone are controlled by the default call settings configured in the endpoints.

Tech Tip

The VCS bandwidth configuration page allows you to define a default call bandwidth for endpoints that do not specify an amount in their call signaling.

Step 1: Navigate to **VCS configuration** > **Bandwidth** > **Configuration**, enter the following values, and then click **Save**:

- Default call bandwidth—384
- Downspeed per call mode—On
- Downspeed total mode—On



Process

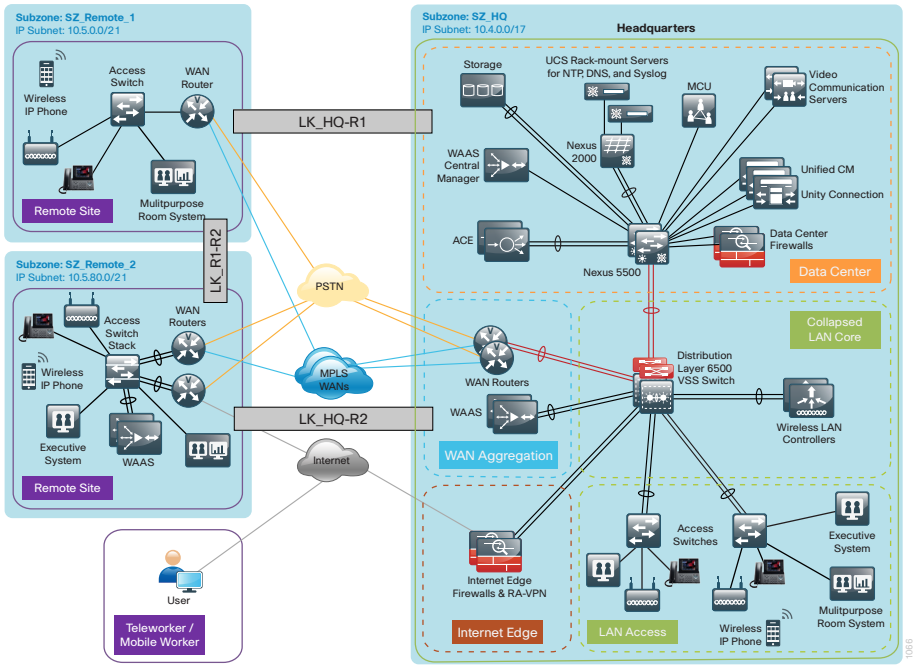
Creating Pipes and Links

1. Create pipes
2. Create links

Pipes and links allow you to manage the number of video calls placed over your WAN. They also allow you to specify the amount of bandwidth per call.

Each location needs a link to all other locations and a single pipe to define the total amount of bandwidth allowed in and out of the subzone.

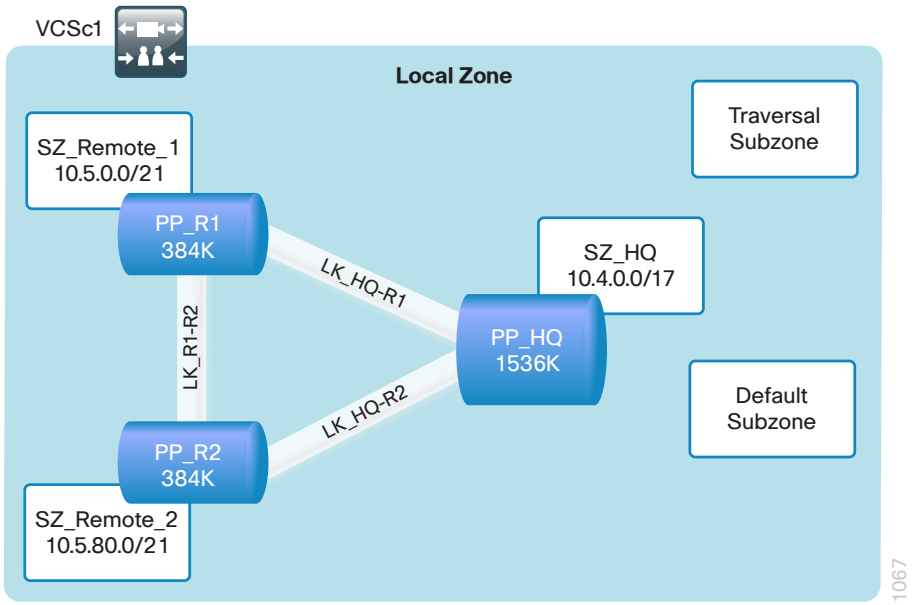
Figure 4 - Links in foundation architecture



The pipes have to be created first because they are needed to configure the new links. Pipes define the amount of bandwidth per call and the total bandwidth in and out of one end of a given link for the subzone. Pipes protect the underlying architecture by restricting the amount of bandwidth entering the low-latency queues defined in the WAN routers. If the queues in a WAN router are overrun by high-priority traffic, all of the calls are degraded. When the Cisco VCS pipe feature determines there is not enough bandwidth for a given call, the endpoint receives a "resources unavailable" message from Cisco VCS.

The bandwidth for the pipes is defined as 1536 kbps for the HQ site and 384 kbps for each remote location. This bandwidth allows four calls into the HQ location and one call to each remote site. In the Borderless Networks Foundation, the low-latency bandwidth for video has been set to 23 percent of the defined bandwidth of a given connection. The specified configuration works with a minimum of a 2-Mbps connection at the remote sites and an 8-Mbps connection at the HQ site. If more calls are needed at a location, you need additional bandwidth for the pipe in that location.

Figure 5 - Relationship between pipes, links, and subzones in Cisco VCS

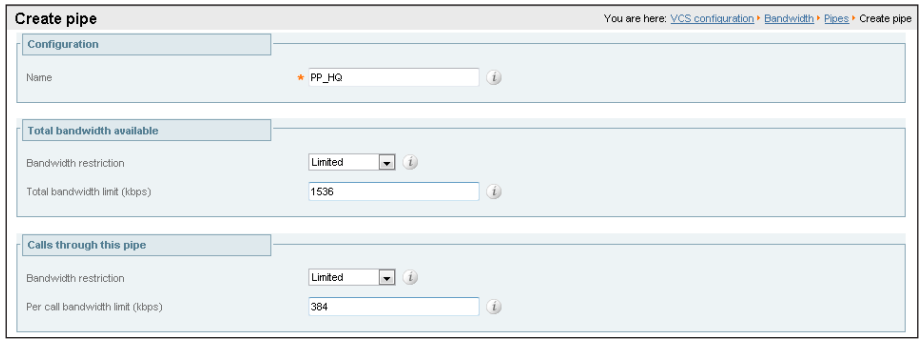


Procedure 1 Create pipes

Step 1: Navigate to **VCS configuration > Bandwidth > Pipes**, and then click **New**.

Step 2: On the Create pipe page, enter the following values, and then click **Create pipe**:

- Name—PP_HQ
- Bandwidth restriction—Limited
- Total bandwidth limit—1536 (four calls in and out of HQ)
- Bandwidth restriction—Limited
- Per call bandwidth—384



Step 3: On the Pipes page, click **New**.

Step 4: On the Create pipe page, enter the following values, and then click **Create pipe**:

- Name—PP_R1
- Bandwidth restriction—Limited
- Total bandwidth limit—384 (one call in and out of remote sites).
- Bandwidth restriction—Limited
- Per call bandwidth—384

Step 5: Create the rest of the pipes that your organization needs by repeating Step 3 and Step 4 using the appropriate information for each site.

Procedure 2 Create links

Cisco VCS creates a number of default links when new subzones are created. Before you create the new links, you must delete the subzone default links. Do not delete the default link that was automatically created between the traversal subzone and the default zone.

Step 1: Navigate to **VCS configuration > Bandwidth > Links**, select the check boxes next to the automatically created subzone links, and then click **Delete.**

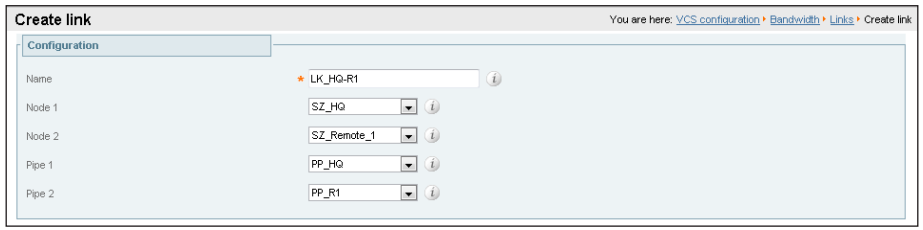
Step 2: On the Confirm page, click **Yes**.

Now that the subzone default links are gone, you can create the new links and assign pipes to them.

Step 3: On the Links page, click **New**.

Step 4: On the Create link page, enter the following values, and then click **Create Link**:

- Name—LK_HQ-R1
- Node 1—the subzone SZ_HQ
- Node 2—the subzone SZ_Remote_1
- Pipe 1—PP_HQ
- Pipe 2—PP_R1



Step 5: Create the rest of the subzone links that your organization needs by repeating Step 3 and Step 4 above, using the appropriate pipes created in Procedure 1

Next, you create a final link between the HQ site and the traversal subzone. This allows reservationless calls to be completed to the MCU by using the H.323 prefix. You do not need to configure pipes on this link because the bandwidth is already being calculated on the links between the sites.

Step 6: On the Links page, click **New**.

Step 7: On the Create link page, enter the following values, and then click **Create Link**:

- Name—LK_HQ-Traversal_SZ
- Node 1—the subzone SZ_HQ
- Node 2—the subzone TraversalSubZone
- Pipe 1—leave the **Pipe 1** field blank
- Pipe 2—leave the **Pipe 2** field blank

Step 8: At the top of the page on the right side, click **Logout**.

The platform configuration of Cisco VCS is complete.

Process

Configuring Cisco TelePresence Multipoint Control Unit

1. Configure MCU connectivity to the LAN
2. Prepare the Cisco MCU platform
3. Configure the Cisco MCU
4. Register MCU with H.323 and SIP

The Cisco TelePresence Multipoint Control Unit (MCU) is used for reservationless and scheduled conferences between the video endpoints. Cisco has several MCUs with different capacities. Depending on how many endpoints you need in concurrent calls, you can choose the MCU that scales to your needs.

Cisco TelePresence MCU	High-definition participants	Standard-definition endpoints
CTI-4501	6	12
CTI-4505	12 at 720p30 6 at 1080p30 6 at 720p60	24
CTI-4510	20 at 720p30 10 at 1080p30 10 at 720p60	40
CTI-4515	30 at 720p30 15 at 1080p30 15 at 720p60	60
CTI-4520	40 at 720p30 20 at 1080p30 20 at 720p60	80

If your organization plans to make extensive use of reservationless conferences, Cisco recommends separating the two conference types onto two MCUs. Separating the two conference types prevents reservationless conferences from using all of the resources on the MCU that supports scheduled conferences.

Scheduled conference calls are created on Cisco MCU for call-in and call-out types of meetings. Before getting started, you need to collect certain information specific to your site. You can fill in the following table.

Table 3 - Information you need before configuring Cisco MCU

Item	Cisco SBA configuration	Site-specific details
IPV4 address	10.4.48.135	
IPV4 subnet	255.255.255.0	
IPV4 default gateway	10.4.48.1	
Host name	MCU	
DNS server address	10.4.48.10	
DNS local host name	MCU	
DNS domain name	cisco.local	
NTP server address	10.4.48.17	
Time zone	Pacific -8	
SNMP read-only community	cisco	
SNMP read/write community	cisco123	
SNMP trap community	cisco	
Remote syslog server	10.4.48.13	

Procedure 1 Configure MCU connectivity to the LAN

The MCU can be connected to a Nexus switch in the Data Center or a Catalyst switch in the Server Room. In both cases, QoS policies are added to the ports to maintain video quality during conferences. Please choose the option that is appropriate for your environment.

Option 1. Connect the MCU to a Nexus 2248UP

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

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

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

```
interface Ethernet107/1/3
 description Codian MCU
 switchport access vlan 148
 spanning-tree port type edge
 service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

Tech Tip

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

Option 2. Connect the MCU to a Catalyst 3750-X

To ensure that video traffic is prioritized appropriately, you must configure the Catalyst access switch port where the MCU is connected to trust the DSCP markings. The easiest way to do this is to clear the interface of any previous configuration and then, apply the egress QoS macro that was defined in the access-switch platform configuration of the *SBA—LAN Deployment Guide*.

Step 1: Login to the 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 VCS is connected.

```
default interface GigabitEthernet1/0/11
```

Step 3: Configure the port as an access port on the same VLAN as the VCS and apply the Egress QoS policy.

```
interface GigabitEthernet1/0/11
 description Codian MCU
 switchport access vlan 148
 switchport host
 macro apply EgressQoS
```

Procedure 2 Prepare the Cisco MCU platform

In the following steps, set the initial configuration by using a PC connected to the console port with a serial cable.

Step 1: Ensure power is connected to Cisco MCU and the Status LED is green.

Step 2: Connect the Ethernet LAN cable from the Ethernet A port on the front of the unit to your network.

Step 3: Connect the console port of Cisco MCU to the serial port of your PC using the blue RJ45 to DB9 cable supplied.

Step 4: Use terminal emulation software such as PuTTY and configure the serial port on the PC as follows:

- Baud rate—38400
- Data bits—8
- Parity—none
- Stop bits—1
- Flow control—none

Step 5: Press **Enter.** The MCU command prompt appears on the terminal.

Step 6: Configure Ethernet Port A for auto-sensing.

```
ethertype auto
```

Step 7: Assign a static IP address.

```
static 10.4.48.135 255.255.255.0 10.4.48.1 10.4.48.10
```

Step 8: Disconnect the serial cable and store it in a safe place.

Procedure 3 Configure the Cisco MCU

The rest of the configuration of the Cisco MCU is done using a standard web browser. You use the information collected in Table 3 at the beginning of this Cisco MCU configuration process to fill in the fields.

Step 1: Open a browser window, and enter the IP address of the Cisco MCU: 10.4.48.135

Step 2: Click **Log in**, enter the following values, and then click **OK**:

- Username—admin
- Password—(leave the **password** field blank)

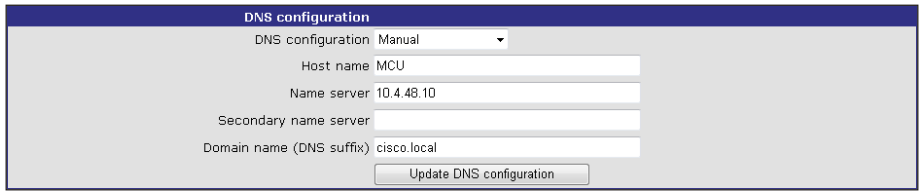
Step 3: On the Login information screen, click **Change password**.

Step 4: On the Change password screen, enter the following values, and then click **OK**.

- Old password—(leave the **Old password** field blank)
- New password—[password]
- Re-enter password—[password]

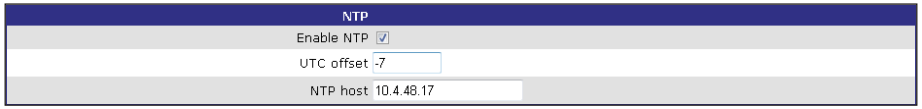
Step 5: Navigate to **Network** > **DNS**, enter the following values, and then click **Update DNS configuration**:

- DNS configuration—Manual
- Host name—MCU
- Name server—10.4.48.10
- Domain name (DNS suffix)—cisco.local



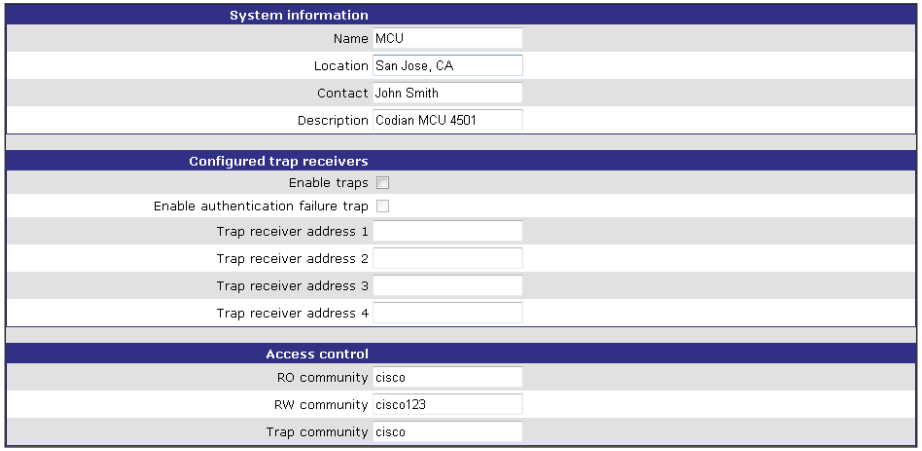
Step 6: Navigate to **Settings** > **Time**, select **Enable NTP**, enter the following values, and then click **Update NTP settings**:

- UTC offset— -7
- NTP host IP address—10.4.48.17



Step 7: Navigate to **Network** > **SNMP**, enter the following values, and then click **Update SNMP settings**:

- Name—MCU
- Location—San Jose, CA (optional)
- Contact—John Smith (optional)
- RO community—cisco
- RW community—cisco123
- Trap community—cisco



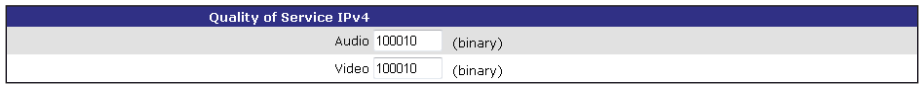
Tech Tip

QoS is needed to put the media and signaling traffic into the low-latency queues defined in the *LAN Deployment Guide*. The QoS setting gives the video packets a higher priority over non–real-time traffic in the data queues.

The Differentiated Service markings match the medianet-recommended settings for interactive video traffic in Cisco SBA.

Step 8: Navigate to **Network > QoS**, enter the following values under Quality of Service IPv4, and then click **Update QoS settings**:

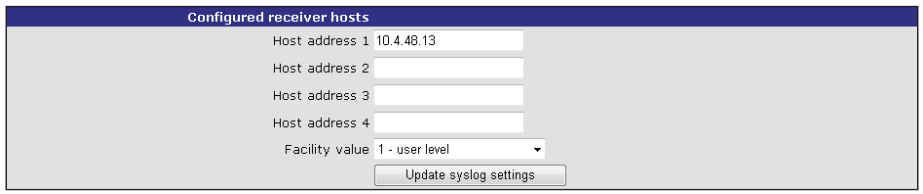
- Audio—**100010** (AF41)
- Video—**100010** (AF41)



By default, the system log level is set to level 1. This setting configures Cisco MCU to output high-level (easily readable) events in system log and syslog messages. The system logs are stored on a Solarwinds server at the IP address listed below. Administrators can use the information when troubleshooting problems with the device.

Step 9: Navigate to **Logs > Syslog**.

Step 10: In the **Host address 1** box, enter **10.4.48.13** (syslog IP address), and then click **Update syslog settings**.



Procedure 4 Register MCU with H.323 and SIP

Registering Cisco MCU with the H.323 gatekeeper on Cisco VCS allows the MCU to accept a reservationless call that was made using the service prefix parameters. This is a simple method for allowing SIP endpoints to dial a common phone number and be connected directly into the conference bridge without pausing at the Auto Attendant.

You will also register Cisco MCU by using SIP, so it can communicate directly with the SIP endpoints without going through the traversal subzone on Cisco VCS.

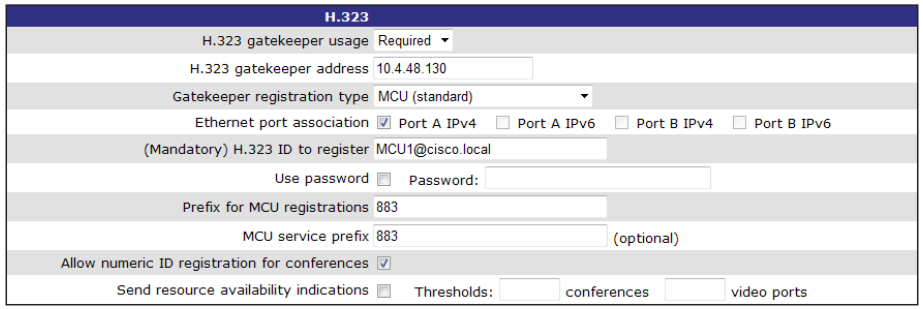
Tech Tip

The gatekeeper registration type is set to MCU (standard) to ensure calls to the same conference ID get routed to the correct device when additional MCUs are added in the future.

When you use the prefix for MCU registrations and the Cisco MCU service prefix, Cisco recommends that you set both prefixes to the same number.

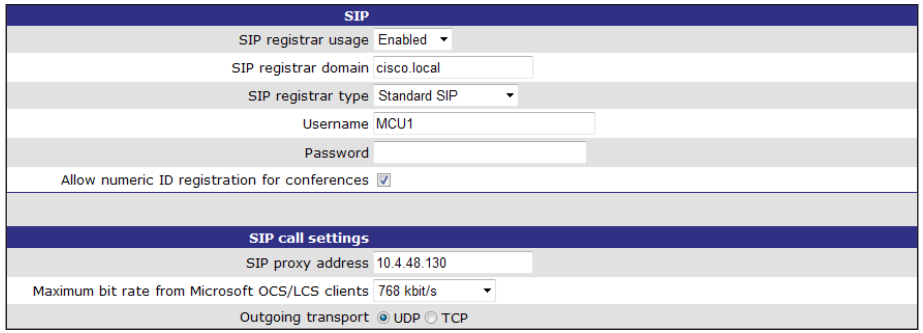
Step 1: Navigate to **Settings** > **H.323**, enter the following values, and then click **Apply changes**:

- H.323 gatekeeper usage—**Required**
- H.323 gatekeeper address—**10.4.48.130**
- Gatekeeper registration type—**MCU (standard)**
- Ethernet port association—**Port A IPv4**
- (Mandatory) H.323 ID to register—**MCU1@cisco.local**
- Prefix for MCU registrations—**883**
- MCU service prefix—**883**
- Select **Allow numeric ID registration for conferences**



Step 2: Navigate to **Settings** > **SIP**, enter the following values, and then click **Apply changes**:

- SIP registrar usage—**Enabled**
- SIP registrar domain—**cisco.local**
- SIP registrar type—**Standard SIP**
- Username—**MCU1**
- Select—**Allow numeric ID registration for conferences**
- SIP proxy address—**10.4.48.130**



Step 3: At the top of the page on the right side, click **Log out.**

The platform configuration of the Cisco MCU is complete.

Process

Configuring Cisco TelePresence System Profile Series

1. Configure Profile connectivity to the LAN
2. Configure the Profile series platform
3. Test point-to-point video calling
4. Block video traffic on backup links

The recommended Cisco TelePresence System Profile Series endpoints are multipurpose room systems that you can configure using SIP. The configuration steps for this platform are the same as they are for any of the Cisco TelePresence System Codec C-Series endpoints. Before getting started, you need to collect certain information specific to your site. You can fill in the following table.

Table 4 - Information you need before configuring SIP endpoints

Item	Cisco SBA configuration	Site-specific details
System name	85104600@cisco.local	
DNS server address	10.4.48.10	
DNS domain name	cisco.local	
SNMP community name	cisco	
NTP server address	10.4.48.17	
Time zone	GMT -8 (Pacific)	
SIP URI	85104600@cisco.local	
SIP Proxy 1 address	10.4.48.130	
SIP Proxy 2 address	10.4.48.131	

Procedure 1 Configure Profile connectivity to the LAN

To ensure that video traffic is prioritized appropriately, you must configure the Catalyst access switch port where the video endpoint is connected to trust the DSCP markings. The easiest way to do this is to clear the interface of any previous configuration and then, apply the egress QoS macro that was defined in the access-switch platform configuration of the *SBA—LAN Deployment Guide*.

Step 1: Login to the 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 video endpoint is connected.

```
default interface GigabitEthernet1/0/23
```

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

```
interface GigabitEthernet1/0/23
 description Profile 42
 switchport access vlan 64
 switchport host
 macro apply EgressQoS
```

Procedure 2 Configure the Profile series platform

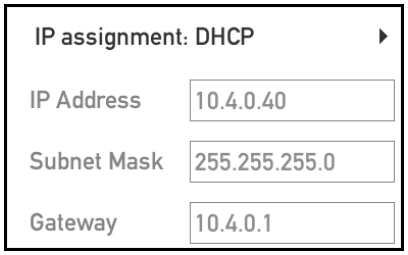
The endpoint uses the Dynamic Host Configuration Protocol (DHCP) to automatically obtain its IP address from the network services layer of the Cisco SBA platform. The configuration of the SIP endpoint is done with the remote control.

Using the remote control, the following steps allow you to verify the endpoint is getting the correct IP information from the server. You also need to manually set the time to allow the NTP service to take over after it is properly configured.

Step 1: Connect all of the cables as specified in the endpoint installation guide, and turn on the power switch. Wait several minutes for the system to power up.

Step 2: If there is no initial menu on the screen, press the **Home** button on the remote.

Step 3: From the Home screen, navigate to **Settings** > **Administrator Settings** > **IP Settings** > **Configure.**



Step 4: Make note of the IP address for future steps. Example: **10.4.0.40**

Step 5: Press the **Home** button.

Step 6: Navigate to **Settings** > **Date and time**, and enter the following values:

- NTP mode—**Off**
- Day—**[current day]**
- Month—**[current month]**
- Year—**[current year]**
- Time—**[current time]**
- Date format: **Month.Day.Year**
- Enter Time format—**12 hours (am/pm)**

Tech Tip

After you set the date the first time, change the NTP mode to Manual. This setting allows the NTP server to take over and maintain the time automatically based on your time-zone offset.

The NTP server can adjust and maintain time for the endpoint only if the time you originally set is accurate to within 1 or 2 minutes.

Step 7: Navigate to **Settings** > **Date and time** again, and enter the following values:

- NTP mode—**Manual**
- NTP server—**10.4.48.17**
- Time zone—**GMT-08:00**

Tech Tip

The endpoint is shipped with a blank password for the admin and root accounts. For security reasons, please change the passwords as soon as possible.

Step 8: Using terminal emulation software such as PuTTY, use the IP address **10.4.0.40** (from the IP setting > Configure screen) to log in to the endpoint via SSH.

Step 9: Log in with the username **admin**.

You are not prompted for a password.

Step 10: At the OK prompt, set the admin password.

```
xcommand systemunit adminpassword set password: [password]
```

Step 11: Set the root password.

```
systemtools rootsettings on [password]
```

Step 12: Log out of the endpoint.

```
Bye
```

Step 13: Close the SSH session on your PC.

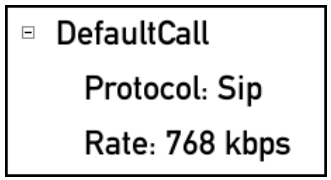
Step 14: From the Home screen, use the remote control to navigate to **Settings > Administrator Settings > Advanced Configuration.**

Tech Tip

The default call rate of 768 kbps is used for calls between endpoints in the same location. Bandwidth for calls between locations is overridden by the Cisco VCS Pipe commands when calling across the WAN.

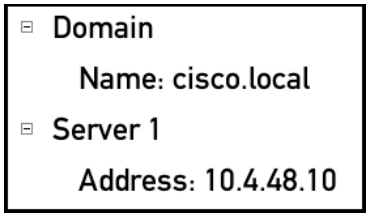
Step 15: From the Advanced Configuration screen, navigate to **Conference 1 > DefaultCall**, and enter the following values:

- Protocol—**Sip**
- Rate—**768 kbps**



Step 16: Navigate to **Network 1 > DNS**, and enter the following values:

- Domain > Name—**cisco.local**
- Server 1 > Address—**10.4.48.10**



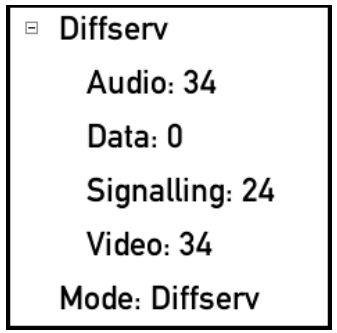
Tech Tip

QoS is needed to put the media traffic into the low-latency queues and the signaling into a class-based weighted fair queue as defined in the *Cisco SBA—LAN Deployment Guide*. The QoS setting gives the video packets a higher priority over non–real-time traffic in the data queues.

The Differentiated Service markings match the medianet-recommended settings for interactive video traffic in Cisco SBA.

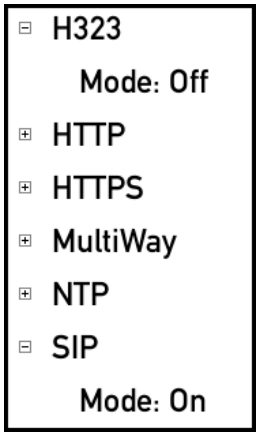
Step 17: Navigate to **Network1 > QoS**, and enter the following values:

- Diffserv > Audio—**34** (AF41)
- Diffserv > Data—**0**
- Diffserv > Signaling—**24** (CS3)
- Diffserv > Video—**34** (AF41)
- Mode—**Diffserv**



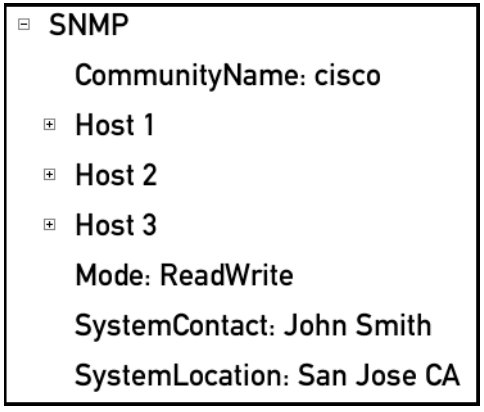
Step 18: Navigate to **NetworkServices**, and enter the following values:

- H323 > Mode—**Off**
- SIP > Mode—**On**



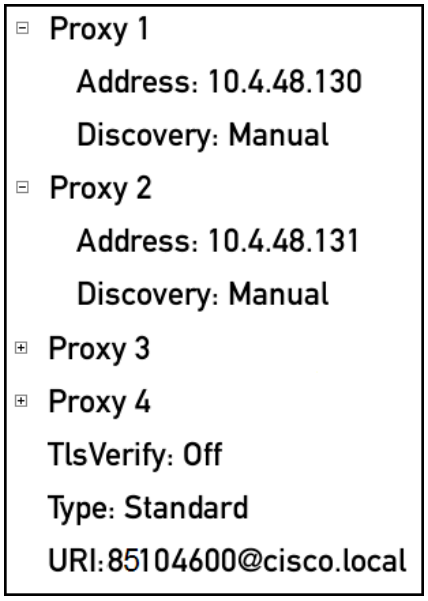
Step 19: Navigate to **NetworkServices > SNMP**, and enter the following values:

- CommunityName—**cisco**
- Mode—**ReadWrite**
- SystemContact—**John Smith** (optional)
- SystemLocation—**San Jose CA** (optional)



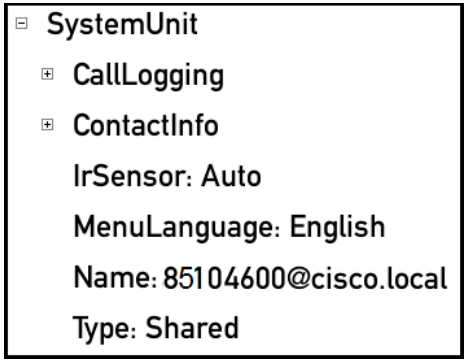
Step 20: Navigate to **SIP > Profile 1**, and enter the following values:

- Proxy 1 > Address—**10.4.48.130**
- Proxy 1 > Discovery—**Manual**
- Proxy 2 > Address—**10.4.48.131**
- Proxy 2 > Discovery—**Manual**
- URI—**85104600@cisco.local**



Step 21: Navigate to **SystemUnit**, and enter the following value:

- Name—**85104600@cisco.local**



Step 22: From the Home screen, navigate to **Settings > System Information.** Confirm the system information is correct and the endpoint is registered with the VCS.

Step 23: If the endpoint does not register with the SIP proxy, return to Step 21 and do the following:

- Remove the Proxy 1 > Address of the VCS server and save it blank.
- Re-enter the IP address and save it.
- Confirm the endpoint is registered with the SIP proxy by following Step 23.

Step 24: Press the **Home** button on the remote.

Step 25: Repeat Step 1 through Step 24 of this procedure for all your SIP endpoints.

After the endpoints have been configured, it is time to test the point-to-point calling.

Procedure 3 Test point-to-point video calling

Step 1: If there is no menu on the screen, press the **Home** button on the remote.

Step 2: Navigate to **Call**, and enter the URI of another SIP endpoint registered to VCS. (Example: **85234730@cisco.local**)

Step 3: On the remote control, press the green **Call** button.

The call is connected.

Step 4: After the call is connected, press the red end-call button on the remote, and then select **Disconnect 85234730**.

The point-to-point calling is complete.

Procedure 4 Block video traffic on backup links

(Optional)

In some cases, you may want to prevent video endpoints from operating when a failover to a backup WAN link occurs. Implementing this blocking avoids transmitting video over a lossy link and lowers the cost of a WAN failure by reducing costly bandwidth usage while maintaining the data connectivity that end users expect.

This configuration will block H.323 and SIP video traffic from passing over the specified interface of a router. It can be applied to the backup router of a dual router design or to the secondary link of a single router design.

Step 1: Login to the router with a username that has the ability to make configuration changes, and enter enable mode.

Step 2: Configure the access list that will block SIP: 5060 (TCP/UDP), Secure SIP: 5061 (TCP/UDP), H.323 Gatekeeper RAS: 1719 (TCP/UDP) H323 Q.931: 1720 (TCP/UDP), standard RTP ports: 16384-32767 (UDP), and allow all other traffic.

```
ip access-list extended ACL-Video-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 1719
 deny udp any any eq 1719
 deny tcp any any eq 1720
 deny udp any any eq 1720
 deny udp any any range 16384 32767
 permit ip any any
```

Step 3: Apply the ACL to the WAN interface you wish to block video traffic.

```
interface Tunnel10
 ip access-group ACL-Video-CONTROL in
```

Process

Configuring Conferences

1. Configure reservationless conferences
2. Configure scheduled conferences

The Cisco TelePresence MCU 4501 is used for reservationless and scheduled conferences. If your organization plans to make extensive use of reservationless conferences, Cisco recommends separating the two conference types onto two MCUs. Separating the two types prevents reservationless conferences from using all of the resources on the MCU that supports scheduled conferences.

You start by configuring reservationless conferences and then move to scheduled conferences. The scheduled conference configuration includes one conference where participants call in and another where Cisco MCU calls each participant at the appointed time.

Procedure 1 Configure reservationless conferences

A reservationless conference is created in real time using a known MCU prefix and a conference ID chosen by the meeting originator. This type of conference is not scheduled ahead of time, so the resources are not reserved on Cisco MCU. For security reasons, the meeting originator may choose a PIN number. The meeting originator sends information about the conference ID and PIN to the remote participants via email, instant message, or text message.

Personal reservationless conference IDs are assigned to an individual user by using the Cisco MCU prefix and the last three or four digits of the user's phone number. For example, an employee with a phone number of 555-555-1234 could have a personal reservationless conference ID of 8831234, with 883 as the prefix and 1234 as the last four digits of the number.

In this example the meeting originator uses the remote control to create the reservationless conference from the SIP endpoint. The endpoint dials the service prefix of 883 along with a conference ID of 1234. The MCU asks if the first caller wants to assign a PIN to the conference. The user presses the pound key (#) or waits for 5 seconds to join the call without assigning a PIN.

The next endpoint dials the same number by using the Cisco web interface and joins the conference already in progress without entering a PIN.

Reader Tip

The following steps are performed from the Cisco TelePresence Profile Series endpoint using the remote control.

Step 1: If there is no menu on the screen, press the **Home** button on the remote, and then select **Call**.

Step 2: Enter 8831234 (the service prefix and conference ID).

Step 3: Press the green **Call** button on the remote.

Step 4: The call is connected to the MCU's Auto Attendant. Because you are the first participant, Cisco MCU asks for a PIN number. If you do not want to use a PIN, press **#.**

Step 5: You are connected to the conference as the only participant.

You perform the next steps from a Cisco TelePresence Executive Series 90 endpoint by using the in-Touch panel interface.

Step 6: From the EX 90 in-Touch panel, select the **Call** button.

Step 7: From the Call screen, enter 8831234, and then press the green **Call** button.

Step 8: Have other endpoints call 8831234 (the reservationless conference ID) as needed.

Step 9: From the EX 90 in-Touch panel, select the red **END** button to hang up the call.

Step 10: On the Profile remote, press the **Red** end call button, and then select **Disconnect 8831234** to hang up the call.

Step 11: Disconnect the other endpoints, as required.

The reservationless conference creation and calling is complete.

Procedure 2 Configure scheduled conferences

Scheduled conferences are created and scheduled on Cisco MCU. The endpoints can call into the conference, or the MCU can dial the endpoints at the start of the meeting. With either method, the MCU registers the conference ID with Cisco VCS for the timeframe of the meeting. A permanent meeting can also be created that reserves the resources of a particular meeting and can be used at any time by the participants.

Scheduled conferences have a prefix of 884. This allows them to be differentiated from the reservationless conferences, which start with 883. In this example, a weekly call-in conference will use the ID of 8841234 and a call-out conference will use 8846789.

If you want Cisco MCU to call the participants at the beginning of the meeting, the endpoint information is entered into the MCU ahead of time. You add an SIP endpoint to the MCU before creating the conferences.

Step 1: Open a browser window, and enter 10.4.48.135 (the IP address of the Cisco MCU).

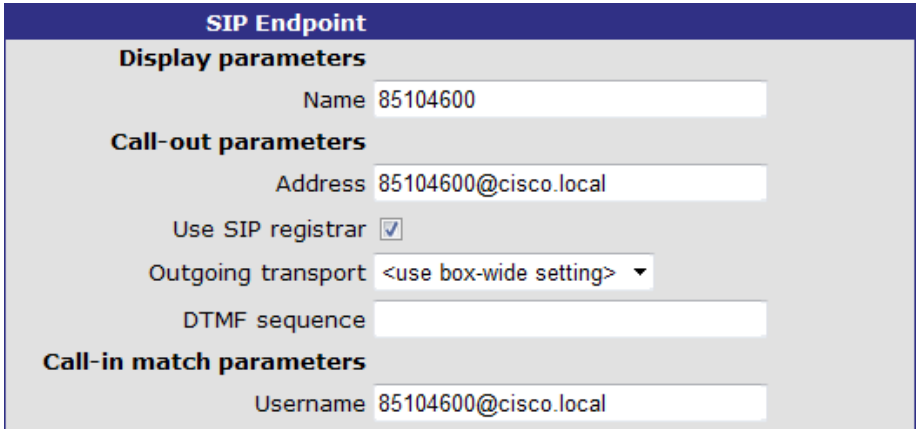
Step 2: Click **Log in**, enter the following values, and then click **OK**.

- Username—admin
- Password—[password]

Step 3: Navigate to **Home** > **Endpoints**, and then click **Add SIP**.

Step 4: On the SIP Endpoint tab, enter the following values, and then click **Add endpoint**:

- Name—85104600
- Call-out parameters > Address—85104600@cisco.local
- Select—Use SIP registrar
- Call-in match parameters > Username—85104600@cisco.local



Step 5: Add as many SIP endpoints as needed by repeating Step 3 and Step 4.

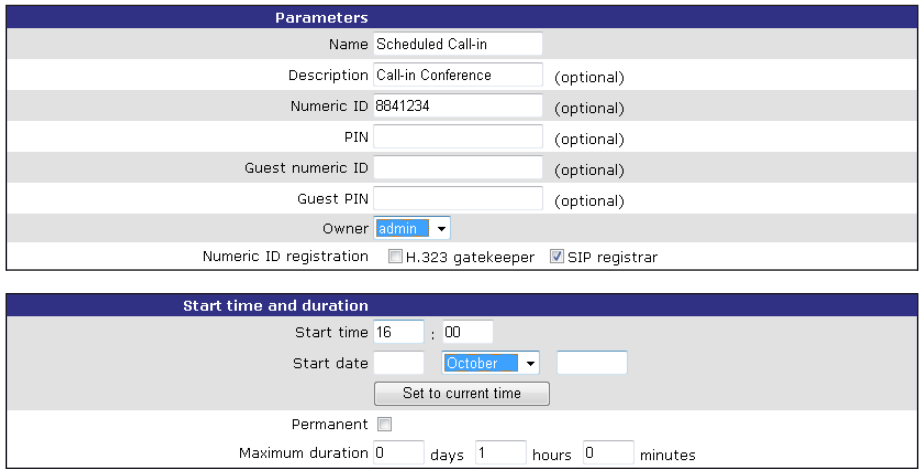
Tech Tip

The next set of steps creates a scheduled conference for call-in participants. Use this type of conference when you are not sure how many people will attend. Just like an audio conference, the resources are reserved on the bridge for the duration of the meeting. If participants do not call in, the ports are not used.

Step 6: Navigate to **Home** > **Conferences** > **Conference List,** and then click **Add new conference.**

Step 7: From the Add conference screen, enter the following values, and then click **Add Conference**:

- Name—Scheduled Call-in
- Description—Call-in Conference
- Numeric ID—8841234
- Numeric ID Registration—SIP registrar
- Start time—[time of meeting]
- Start date—[date of meeting]
- Maximum duration—[length of meeting]



The conference is created for the future date and time.

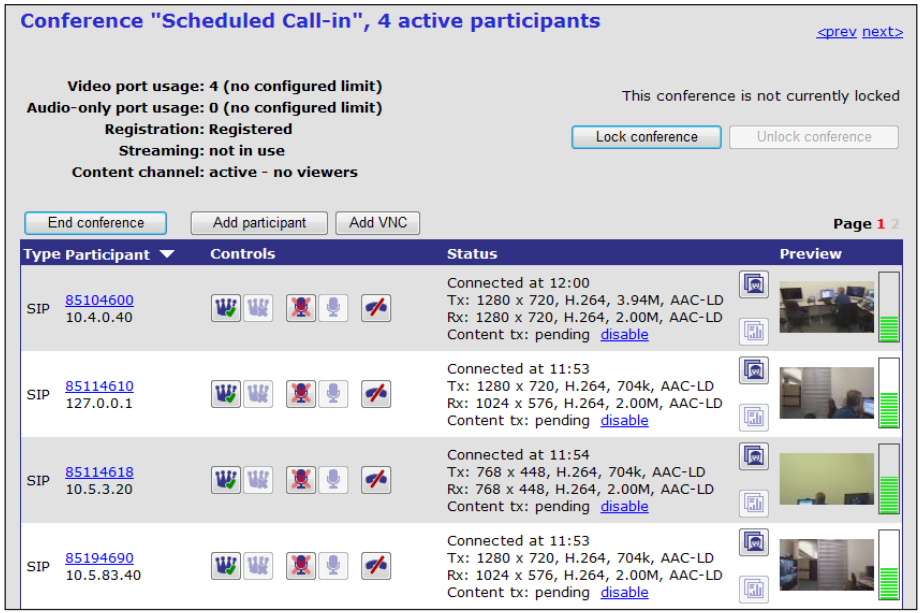
Step 8: When the meeting time arrives, have the participants call in by dialing 8841234@cisco.local from their endpoints.

Reader Tip

Use the next set of steps to manage the conference after the meeting has started.

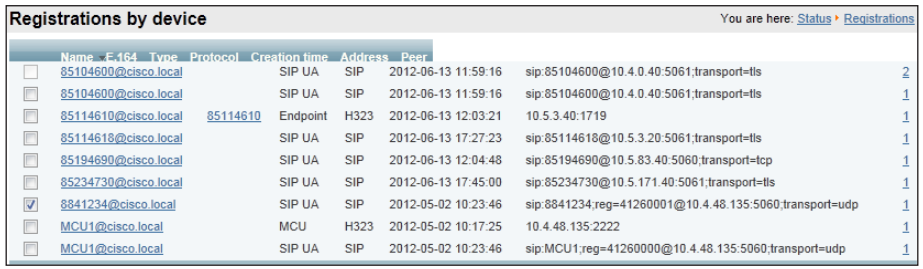
Step 9: After the meeting starts, navigate to **Home > Conferences**, and then click **Scheduled Call in** (the name of the active conference).

Step 10: Manage all aspects of the meeting, as needed.



Step 11: If you want to view the registration, log in to Cisco VCS with the admin account and [password]. The MCU registers the conference ID with VCS when the meeting starts.

Step 12: If you want to view the conference on the VCS, navigate to **Status > Registrations > By device.**



Based on the registration information in Cisco VCS, endpoints can call the conference by using the following IDs: 8841234 or 8841234@cisco.local.

Tech Tip

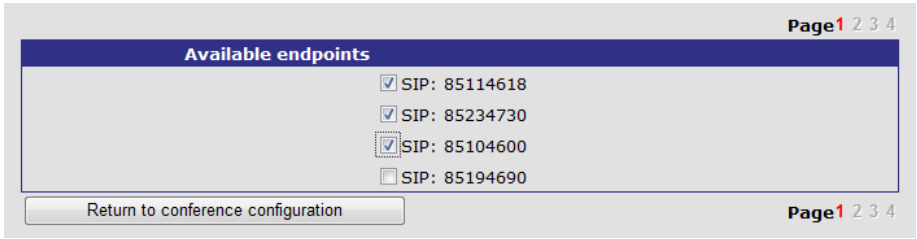
Use this type of conference when the endpoint participants are known ahead of time and they do not want to initiate the call for themselves. This is typically done for executive and boardroom meetings. The resources are reserved on Cisco MCU and all of the ports are active when the call begins.

Step 13: Navigate to **Home > Conferences**, and then click **Add new conference.**

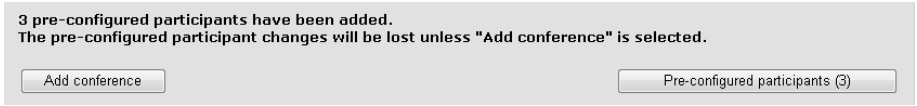
Step 14: On the Add conference screen, enter the following values, and then click **Pre-configured participants:**

- Name—Scheduled Call-out
- Description—Call-out Conference
- Numeric ID—8846789
- Numeric ID Registration—SIP registrar
- Start time—[time of meeting]
- Start date—[date of meeting]
- Maximum duration—[length of meeting]

Step 15: In the Available endpoints list, select the available endpoints for this meeting, and then click **Return to conference configuration**.



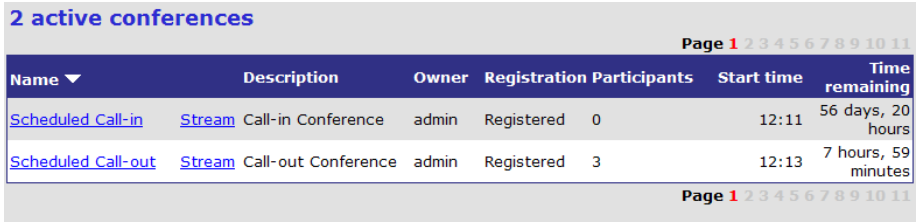
Step 16: On the Add Conference screen, click **Add conference.**



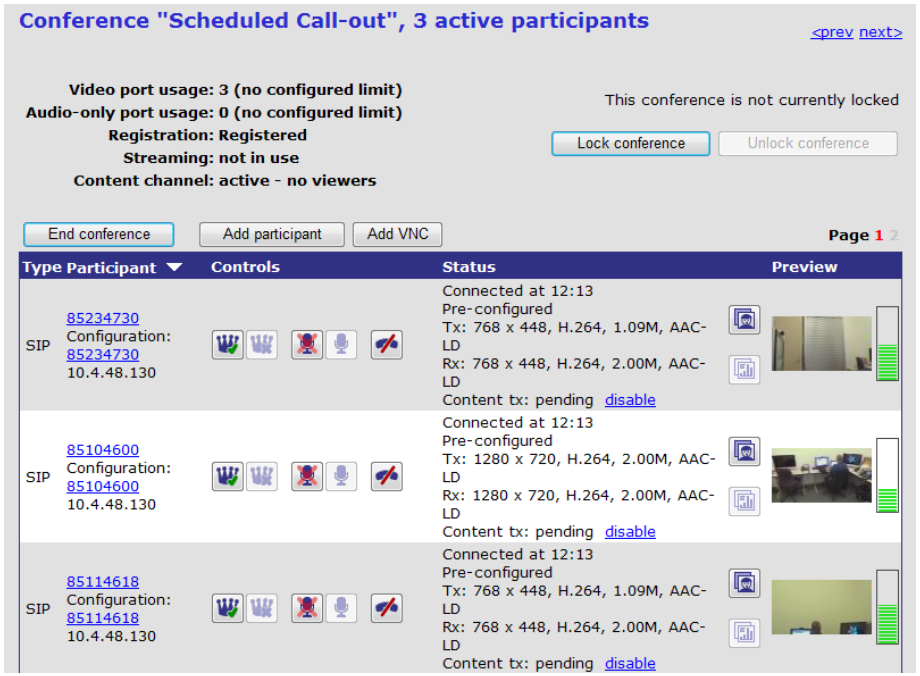
When the date and time arrive, the endpoints are called from Cisco MCU. If auto-answer is enabled on the endpoints, they automatically join the meeting.

The next set of steps manages the conference after the meeting has started and Cisco MCU has called the endpoints.

Step 17: When the meeting starts, navigate to **Home > Conferences > Conference list**, and click **Scheduled Call-out** (the name of the active conference).

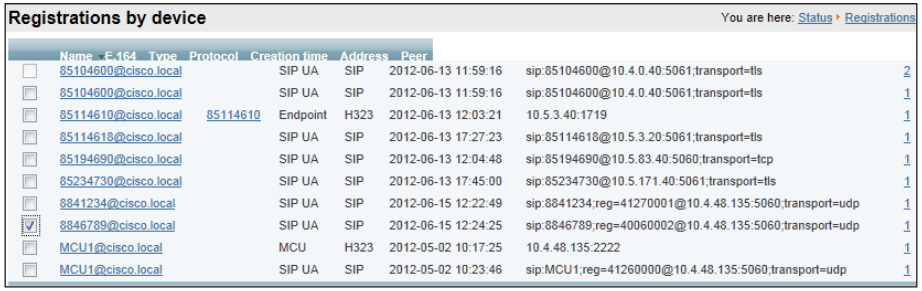


Step 18: Manage all aspects of the meeting, as needed.



Step 19: If you want to view the registration, log in to Cisco VCS with the admin account and [password].The Cisco MCU registers the conference ID with Cisco VCS when the meeting starts.

Step 20: If you want to view the conference on the VCS, navigate to **Status > Registrations > By device.**



Based on the registration information in Cisco VCS, endpoints can also call in to the conference using the following IDs: 8846789 or 8846789@cisco.local.

The scheduled conference creation and calling is complete.

Notes

Appendix A: Product List

Data Center or Server Room

Functional Area	Product Description	Part Numbers	Software
Call Control	Cisco TelePresence Video Communication Server Control	CTI-VCS-BASE-K9	X7.1.0
	Software Image for VCS W/ Encrypt Latest Version	SW-VCS-BASE-K9	
	License Key - VCS K9 Software Image	LIC-VCS-BASE-K9	
	Enable Device Provisioning, Free, VCS Control ONLY	LIC-VCS-DEVPROV	
	Enable GW Feature (H323-SIP)	LIC-VCS-GW	
	100 Traversal Calls for VCS Control only	LIC-VCSE-100	
Multipoint Control Unit	Cisco TelePresence Multipoint Control Unit 4501	CTI-4501-MCU-K9	4.3(2.18)
	Software Image For MCU 4500 Series	SW-4500-MCU-K9	
	License Key For MCU 4501 Software Image; Used During DF	LIC-4501-MCU-K9	
	License Key For Web Conferencing Option, Incl With MCU 4501	LIC-4501-WCO	
	AES and HTTPS Enable Option for MCU 4500 Series	LIC-AESCDN-K9	

Video Endpoints

Functional Area	Product Description	Part Numbers	Software
Executive Room System	Cisco TelePresence System EX90 w NPP, Touch UI	CTS-EX90-K9	TC5.1.0
	Cisco TelePresence Touch 8-inch for EX Series	CTS-CTRL-DV8	
	Software 5.x Encryption	SW-S52000-TC5.XK9	
	Cisco TelePresence Executive 90 Product License Key	LIC-EX90	
	Cisco TelePresence EX Series NPP Option	LIC-ECXX-NPP	
	Cisco TelePresence System License Key Software Encrypted	LIC-S52000-TC5.XK9	
Multipurpose Room System	Cisco TelePresence Profile 42 w PHD 1080p 12x Cam, NPP, Touch, 2 Mics	CTS-P42C40-K9	TC5.1.0
	Cisco TelePresence Monitor Assembly 42	CTS-P42MONITOR	
	Cisco TelePresence Profile 42, 52 and 55 in single screen Wheel Base Mount Kit	CTS-P4252S-WBK	
	Cisco TelePresence Profile 42 C40 Product ID	LIC-P42SC40	
	Codec C40	CTS-C40CODEC-K9-	
	Cisco TelePresence Touch 8-inch for C Series, Profile Series, Quick Set C20	CTS-CTRL-DVC8	
	Cisco TelePresence System DNAM III	CTS-DNAM-III-	
	Cisco TelePresence Precision HD 1080p 12X Unit - Silver, + indicates auto expand	CTS-PHD-1080P12XS+	
	Cisco TelePresence Remote Control TRC 5	CTS-RMT-TRC5	
	Cisco TelePresence Profile Series NPP option	LIC-PCXX-NPP	
	Software 5.x Encryption	SW-S52000-TC5.XK9	

Data Center Core

Functional Area	Product Description	Part Numbers	Software
Core Switch	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5596UP-FA	NX-OS 5.1(3)N1(1a) Layer 3 License
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2	
	Cisco Nexus 5548 up to 48-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5548UP-FA	
	Cisco Nexus 5548 Layer 3 Switching Module	N55-D160L3	
Ethernet Extension	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	—
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	
	Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender	N2K-C2232PP-10GE	

Server Room

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

LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) IP Base
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(1)SE2 LAN Base
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

Appendix B: Changes

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

- We added VCS clustering for customers who need redundancy and the ability to scale beyond the capabilities of a single VCS.
- We added detailed instructions for configuring the switch ports where the VCS, MCU and video endpoints are connected to the Nexus or Catalyst switches.
- We added an optional procedure to block video traffic on a backup link to a remote site.
- We changed the dial plan information, to align it with new video integration guides. This change ensures the video guides use a common set of extension numbers and dialing rules.
- We updated the software on the video infrastructure equipment and the endpoints to the latest shipping versions.

Notes

Feedback

Click here to provide feedback to Cisco SBA.

SMART BUSINESS ARCHITECTURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

B-0000420-1 8/12