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.

H.323 Video Integration 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

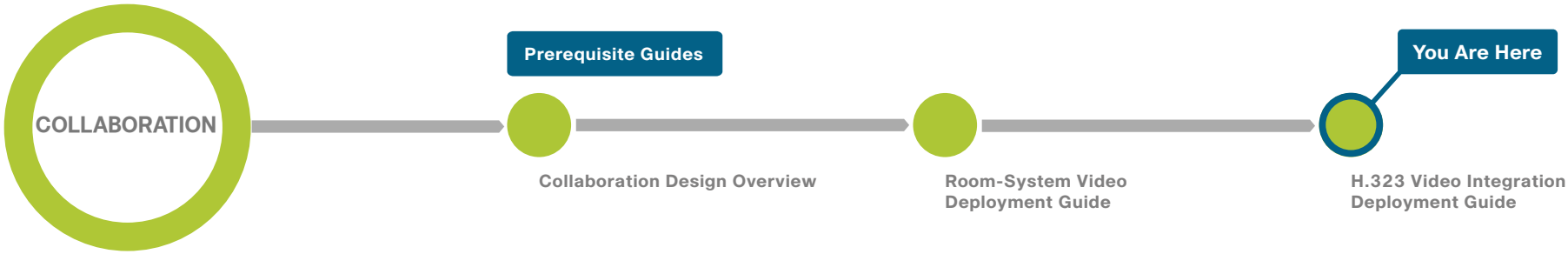
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **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

Organizations have been implementing video conferencing solutions for many years. They moved from ISDN systems to H.323 to take advantage of the excess bandwidth available on their internal IP networks and to save money on escalating ISDN charges. When Session Initiation Protocol (SIP) began to gain popularity in the video marketplace, organizations struggled with the idea of changing signaling protocols just for the sake of changing. As the industry has continued to evolve, SIP has become popular for its ease of use and ability to integrate with other aspects of the business. However, the sheer volume of H.323 systems in use today creates a challenge for organizations faced with installing new systems based on the SIP protocol.

Organizations have expertise within their staff on existing H.323 systems, and the cost to implement is reduced based on familiarity. As technology continues to advance, the end-user community wants to deploy the latest and greatest video equipment. If an organization waits for the perfect moment, they risk missing out on the early advantages of adopting new technology, and then the cycle begins again. Organizations need to perform a balancing act that weighs the benefits of installing new equipment against the associated capital and operational costs on an ongoing basis.

Here are some of the issues faced by organizations when choosing between disparate video solutions:

- They have invested a significant amount of time and money in H.323 endpoints and infrastructure.
- The advantages of deploying SIP solutions are growing.
- Calls do not work natively between H.323 and SIP solutions.
- Updating existing systems to support SIP is time-consuming and costly.

Although SIP adoption is on the rise, H.323 is still the most widely deployed protocol for video conferencing endpoints due to its longevity in the field. Organizations have spent a lot of effort and money deploying H.323, so they understand how it fits into their environment. SIP is easier to implement, but doesn't include all the functionality found in H.323 endpoints. Organizations are driven by their user base to purchase new equipment and the promise of an easier integration into other aspects of the business makes SIP endpoints an attractive part of an overall video architecture. Unfortunately, the existing H.323 systems are not able to communicate directly with SIP systems, and upgrades are often prohibitively expensive.

Depending on when they were purchased, older systems may need software updates to run SIP. The devices may need additional memory or a hardware update to run the latest software. Even without the additional hardware cost, the manpower it takes to upgrade video endpoints and infrastructure equipment will cost an organization a great deal of time and money.

Technology Overview

H.323 systems use gatekeepers for call control, and SIP endpoints use SIP proxy servers. A multipoint control unit (MCU) will typically register with both call control agents to allow devices from each protocol to easily join the same conference. A dual-registration MCU answers some of the protocol interoperability issues, but the question of separate bandwidth control is still not resolved. The details in this guide allow an organization to continue using their existing H.323 systems while migrating to SIP endpoints. Bandwidth control is consolidated into a single device, simplifying the overall configuration.

Cisco® TelePresence Video Communication Server (Cisco VCS) supports SIP and H.323 to allow the different types of endpoints to communicate using one call control agent. However, to correctly handle the interaction between the two protocols, Cisco VCS must remain in the call for the duration. This means that traversal calls between two devices at the same remote site use twice the WAN bandwidth to the Cisco VCS site. Because of this caveat, Cisco does not recommend deploying SIP and H.323 endpoints at the same remote site.

When the two protocols are interworked, organizations gain the following benefits:

- Investment in existing H.323 hardware is preserved.
- SIP endpoints can be deployed when and where they are needed.
- Calls can be made between H.323 and SIP endpoints.
- Upgrades to new software are minimized, preserving capital for new equipment.

When Cisco VCS is deployed in place of an existing H.323 gatekeeper or SIP proxy, endpoint upgrades are not required. The most important aspect of a video solution is the ability to support user-defined features, rather than what protocol is used. If a particular group of endpoints need a feature that is not supported with SIP, they can use H.323 and still have the ability to call the other endpoints within the organization. As more endpoints are purchased, the older ones can be retired and the infrastructure will continue to work as originally designed. Functionality between common sets of solutions is maintained for longer while new equipment is deployed within the organization, which allows for greater return on investment.

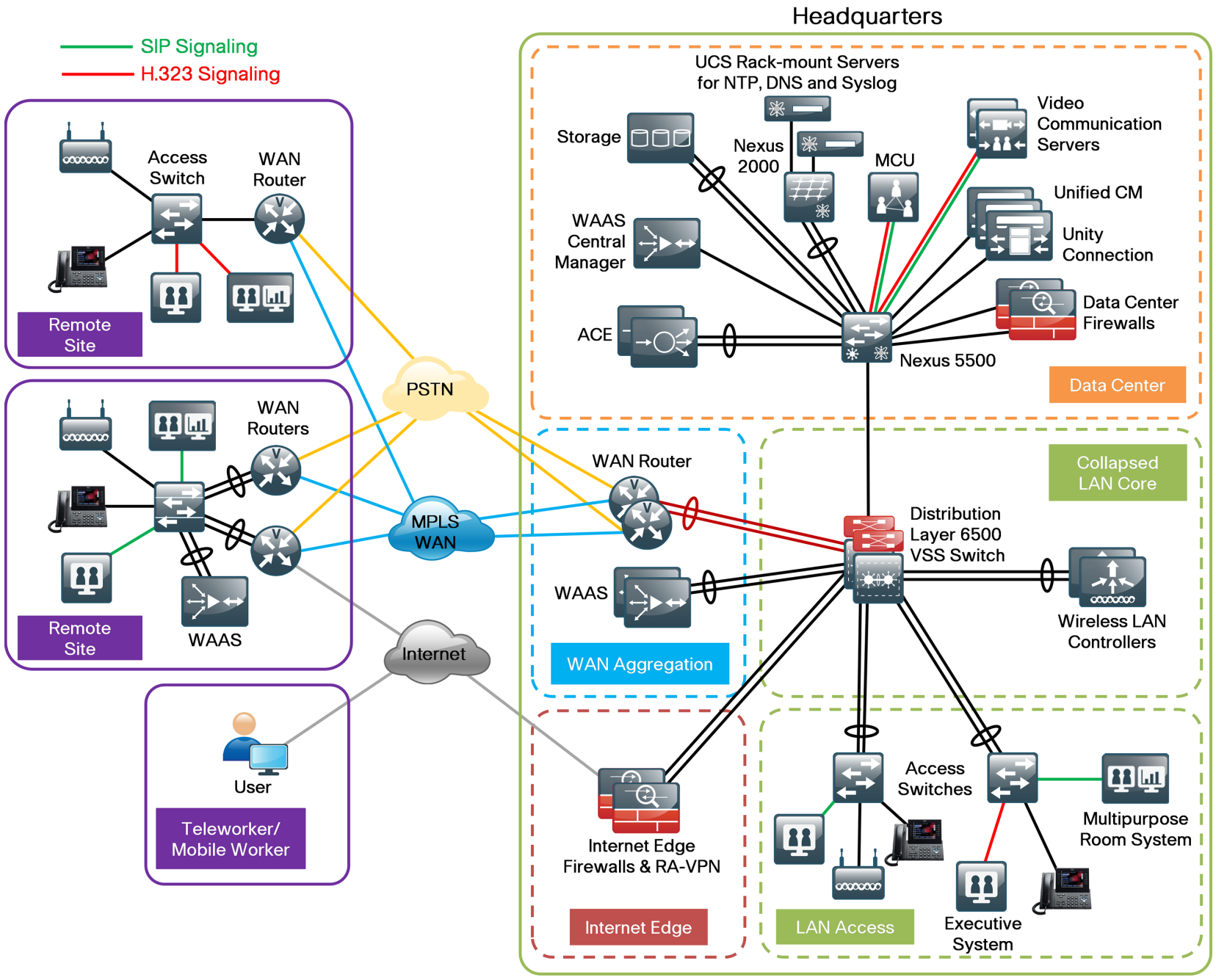
Solution Details

The solution includes the following components shown in the diagram below:

- Cisco VCS for call control, allowing SIP and H.323 interworking
- Personal, executive, and multi-purpose room systems
- Network Time Protocol (NTP) server for logging consistency
- Domain Name System (DNS) for name-to-IP resolution
- Syslog server for logging events (optional)

Notes

Figure 1 - SIP and H.323 video room systems in the Cisco SBA foundation



The endpoints use an eight-digit phone number in the name portion of the URI and an H.323 alias for dialing, which preserves the capability to receive calls from devices that only support numeric dialing. The endpoints in this guide use the *8XXX46XX, 8XXX47XX,* and *8XXX48XX* range of extensions and a domain name of *cisco.local*. The signaling protocols are converted to a common format of dialed digits combined with the domain name, and searches are allowed using numeric-only IDs or numeric-plus-domain-name IDs.

The solution is tested over the Cisco Smart Business Architecture (SBA) Borderless Networks Foundation network, and it uses the medianet quality of service (QoS) and bandwidth control settings recommended by Cisco. Video conferencing traffic is marked as assured forwarding 41 (AF41), and the call signaling is marked as class selector 3 (CS3). The bandwidth for calls between locations is controlled by Cisco VCS.

The bandwidth for calls within a location is handled by the default call settings within the endpoints themselves. The Borderless Networks Foundation deployment is configured to allow 23 percent of the available WAN bandwidth for video calls. The remote sites have 6 Mbps of bandwidth into the Multiprotocol Label Switching (MPLS) cloud, and the headquarters site has 10 Mbps.

Per the medianet guidelines, the call control agent is centralized in the data center. The access, WAN, and campus networks are medianet-enabled, using highly available designs and localized services in the remote sites whenever possible. The video-monitoring capabilities are used to troubleshoot problems when they arise. 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.

Notes

Deployment Details

The process for configuring, registering, and providing bandwidth control for SIP devices has been documented in the *Cisco SBA—Collaboration Room-System Video Deployment Guide*, so it will not be covered again in this guide.

Process

Configuring Cisco VCS for Call Control Between SIP and H.323

1. Create a transform for call routing
2. Create search rules

Cisco VCS is used for call control. Cisco VCS performs signal interworking to allow video devices using SIP and H.323 to seamlessly communicate with each other. The MCU is already configured for H.323 and SIP, so it will use the matching protocol to talk to the registered Cisco VCS endpoints. Bandwidth control will work the same for the H.323 endpoints as it does for SIP endpoints, so no additional configuration is needed.

If you have existing video endpoints and infrastructure components, continue to use H.323 for the highest level of interoperability between them. Cisco VCS supports interworking functionality that enables calls initiated from one signaling protocol to be made to destinations that use the other signaling protocol (that is, from a SIP registered endpoint to an H.323 registered endpoint and vice versa).

Procedure 1 Create a transform for call routing

This procedure describes how to configure Cisco VCS call routing to perform the proper checking to allow calls between H.323 and SIP. After you complete these steps, Cisco VCS will check whether the dialed digits contain the "at" sign (@). If they do not, the @ and SIP domain name are appended to the dialed digits.

For example, if the called address is 85114610, the transform will automatically append the configured domain name to the called address (*85114610@cisco.local*) before attempting to set up the call.

The purpose of appending the valid SIP domain is to standardize called addresses originating from both H.323 and SIP devices.

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

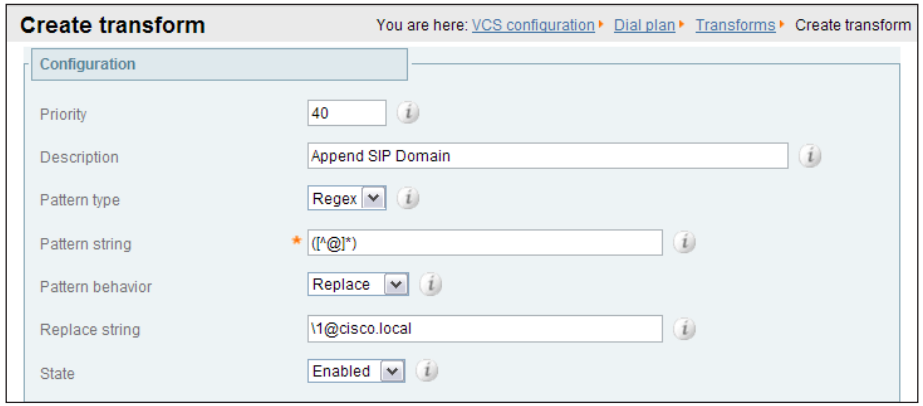
Step 2: Click **Administrator login**, type the following values, and then click **Login**:

- Username—admin
- Password—[password]

Step 3: Navigate to **VCS configuration** > **Dial Plans** > **Transforms**, and then click **New**.

Step 4: Type the following values, and then click **Create transform**:

- Priority—40
- Description—Append SIP Domain
- Pattern type—Regex
- Pattern string—([^@]*)
- Pattern behavior—Replace
- Replace string—\1@cisco.local
- State—Enabled



Procedure 2 Create search rules

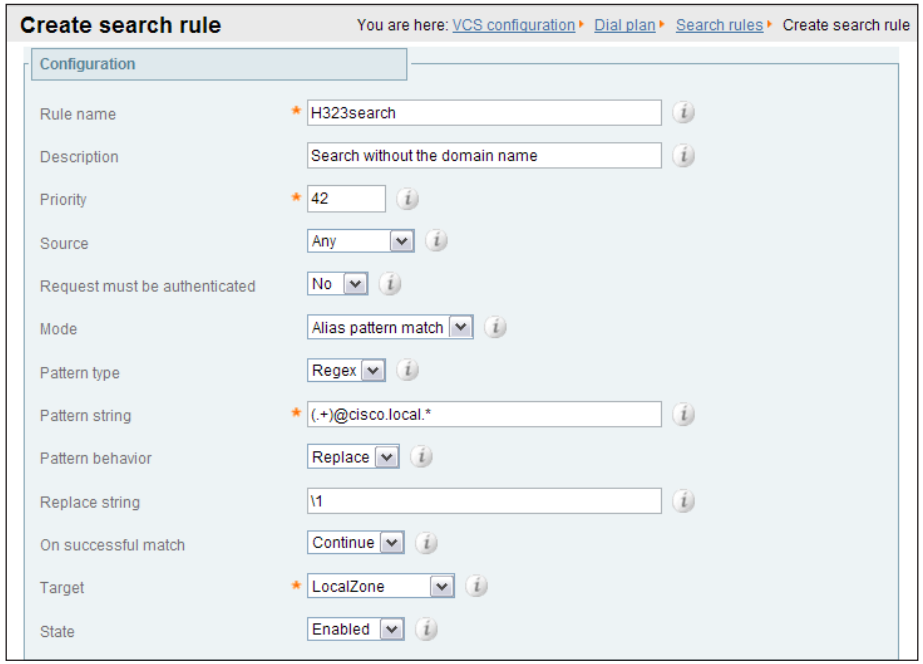
In this procedure, you create two search rules to allow calls between the SIP and H.323 protocols. The rules perform the following checks:

- Strip off the SIP domain portion of the called address, and attempt to find a locally registered H.323 device.
- If no device is located, attempt a second search (without stripping off the SIP domain portion of the called address) to attempt to find a locally registered SIP device.

Step 1: Navigate to **VCS configuration > Dial plan > Search rules**, and then click **New**.

Step 2: Type the following values, and then click **Create search rule**:

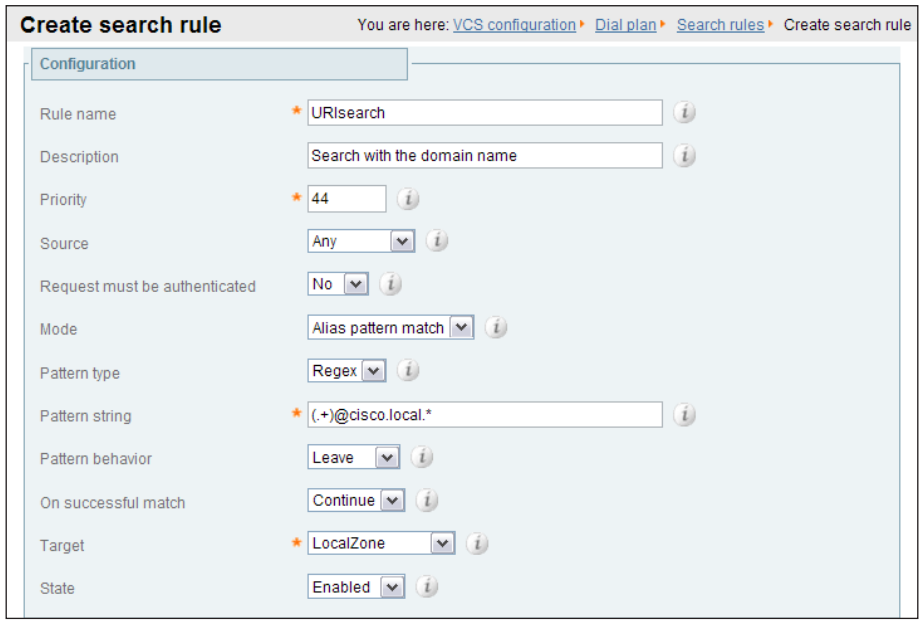
- Rule name—H323search
- Description—Search without the domain name
- Priority—42
- Source—Any
- Request must be authenticated—No
- Mode—Alias pattern match
- Pattern type—Regex
- Pattern string—(.+)@cisco.local.*
- Pattern behavior—Replace
- Replace string—\1
- On successful match—Continue
- Target—LocalZone
- State—Enabled



Step 3: Navigate to **VCS configuration > Dial plan > Search rules**, and then click **New**.

Step 4: Type the following values, and then click **Create search rule**:

- Rule name—URIsearch
- Description—Search with the domain name
- Priority—44
- Source—Any
- Request must be authenticated—No
- Mode—Alias pattern match
- Pattern type—Regex
- Pattern string—(.+)@cisco.local.*
- Pattern behavior—Leave
- On successful match—Continue
- Target zone—LocalZone
- State—Enabled



Tech Tip

After you complete these procedures, you enable the following types of calls between devices registered to Cisco VCS:

An H.323 device registered as H.323id = 85114610 is able to call a SIP device registered as SIP URI = 85104600@cisco.local by dialing *85104600* from the H.323 endpoint.

A SIP device registered as SIP URI = 85104600@cisco.local can call an H.323 device registered with an H.323id of 85114610 by calling *85114610@cisco.local* from the SIP endpoint.

A SIP device registered as SIP URI = 85104600@cisco.local can call an H.323 device registered with an E.164 of 85114610 by dialing *85114610* from the SIP endpoint.

Step 5: Click **Logout**.

The SIP and H.323 advanced configuration of Cisco VCS is complete.

Process

Configuring Cisco TelePresence EX Series for H.323

1. Configure connectivity to the LAN
2. Prepare the H.323 endpoint
3. Configure the H.323 endpoint

Cisco TelePresence EX Series endpoints are executive personal video systems that can be configured using SIP or H.323. Perform these procedures for each H.323 endpoint that you have to register for Cisco VCS. Before getting started, you will need the EX Series information in the following table.

Table 1 - EX Series information for Cisco VCS

Item	Cisco SBA configuration	Your site-specific information
System Name	85114610@cisco.local	
DNS Server Address	10.4.48.10	
DNS Domain Name	cisco.local	
SNMP Community Name	public	
NTP Server Address	10.4.48.17	
Time Zone	GMT -8 (Pacific)	
H.323 Alias	85114610@cisco.local	
H.323 E.164 Number	85114610	
H.323 Gatekeeper Address	10.4.48.130	

Procedure 1 Configure 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 GigabitEthernet1/0/21
```

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

```
interface GigabitEthernet1/0/21
 description EX 90
 switchport access vlan 64
 switchport host
 macro apply EgressQoS
```

Procedure 2 Prepare the H.323 endpoint

By default, the endpoint will use Dynamic Host Configuration Protocol (DHCP) to automatically obtain its IP address from the network layer of the Cisco SBA platform. In this procedure, you verify that the endpoint is getting the correct IP information from the server. You also set the date and time for the endpoints, and use a PC to configure passwords for the admin and root accounts.

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

Step 2: If there is no menu on the screen, tap the touch-screen interface.

Step 3: From the touch screen, navigate to **More** > **Settings** > **System Information**.

Step 4: Record the IP address that will be used in subsequent steps—10.5.3.40.

Step 5: From the touch screen, navigate to **More** > **Settings** > **Administrator Settings** > **Date, Time & Location**, enter the following values, and then select **Save:**

- Time format—12h
- Date Format—mm.dd.yy
- Time Zone—GMT -8:00
- Date and Time—Manual
- Hour—[current hour]
- Minute—[current minute]
- Year—[current year]
- Month—[current month]
- Day—[current day]

Tech Tip

After you set the date manually, you change Date and Time to Auto. This 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 one or two minutes.

Step 6: From the **Date and Time** screen, type the following values, and then click **Save:**

- Date & Time Mode—Auto
- NTP Mode—Manual
- NTP Server—10.4.48.17

Step 7: Using terminal emulation software such as PuTTY, use the IP address from Step 4 to log into the endpoint from a PC via Secure Shell (SSH) Protocol.

Step 8: Log in with the username—admin. **You will not be prompted for a password.**

Step 9: Set the admin password.

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

Step 10: Set the root password.

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

Step 11: Exit from the SSH session.

```
bye
```

Step 12: Close the SSH software on your PC.

The basic preparation of the Cisco EX Series endpoint is complete.

Procedure 3 Configure the H.323 endpoint

In this procedure, you use a web browser to finish the configuration of the H.323 endpoint. When you are done, the endpoint registers to the Cisco VCS server acting as an H.323 gatekeeper for call control. In a clustered environment, H.323 endpoints use a feature called Alternate Gatekeeper to keep track of additional gatekeepers.

When registering with Cisco VCS, the endpoint will respond with the H.323 alternate gatekeepers list containing the cluster peer members. The endpoint will continue to use the first server for re-registrations and for calls. If it loses connection to that server, then it will select an alternate gatekeeper from the supplied list.

Step 1: Type the IP address of the endpoint into your web browser—10.5.3.40

Step 2: From the **Please Sign In** screen, type the following values, and then click **Sign In**:

- Username—admin
- Enter the Password—[password]

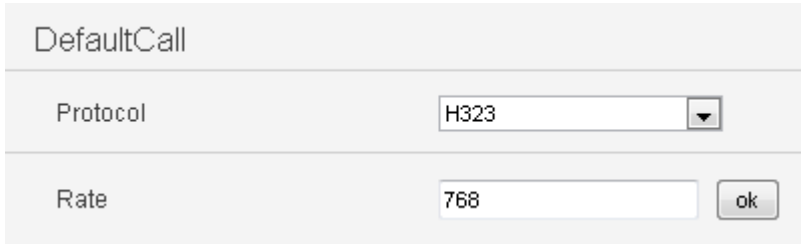
Step 3: From the menu at the top of the page, navigate to **Configuration > Advanced Configuration**.

Tech Tip

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

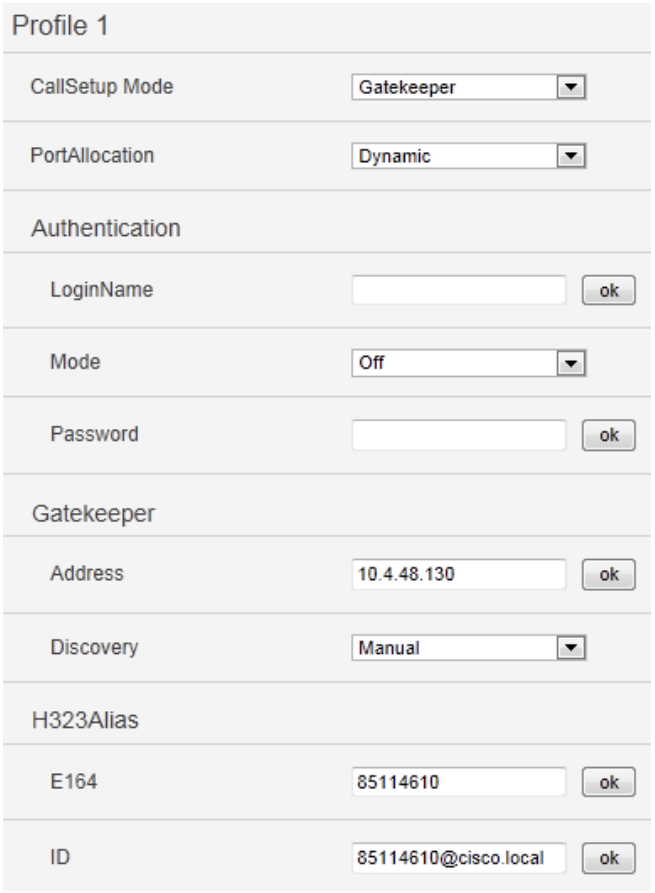
Step 4: Navigate to **Conference 1**, enter the following values, and then click **OK**:

- DefaultCall > Protocol—**H323**
- DefaultCall > Rate—**768**



Step 5: Navigate to **H323**, enter the following values, and then after each entry, click **OK**:

- Profile 1 > CallSetup Mode—**Gatekeeper**
- Profile 1 > PortAllocation—**Dynamic**
- Gatekeeper > Address—**10.4.48.130** (Primary Cisco VCS)
- Gatekeeper > Discovery—**Manual**
- H323Alias > E164—**85114610**
- H323Alias > ID—**85114610@cisco.local**



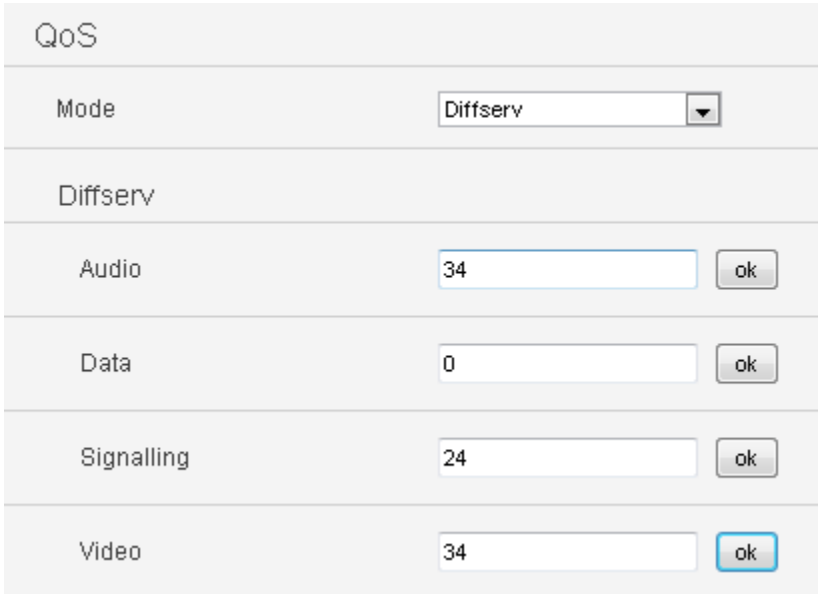
Tech Tip

QoS settings 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*. This will give the video packets a higher priority over non–real-time traffic in the data queues.

The differentiated services code point (DSCP) markings match the medianet-recommended settings for interactive video traffic in Cisco SBA.

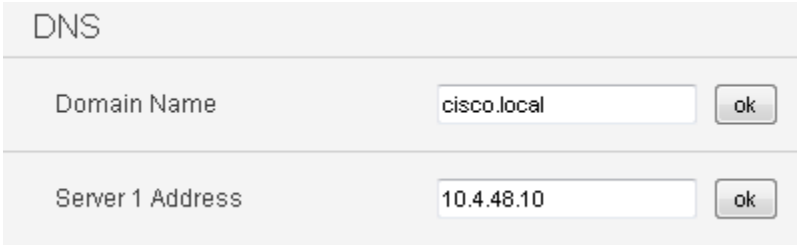
Step 6: Navigate to **Network1** on the endpoint, enter the following values, and then after each entry, click **OK:**

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



Step 7: Navigate to **Network1**, enter the following values, and then after each entry click **OK**:

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

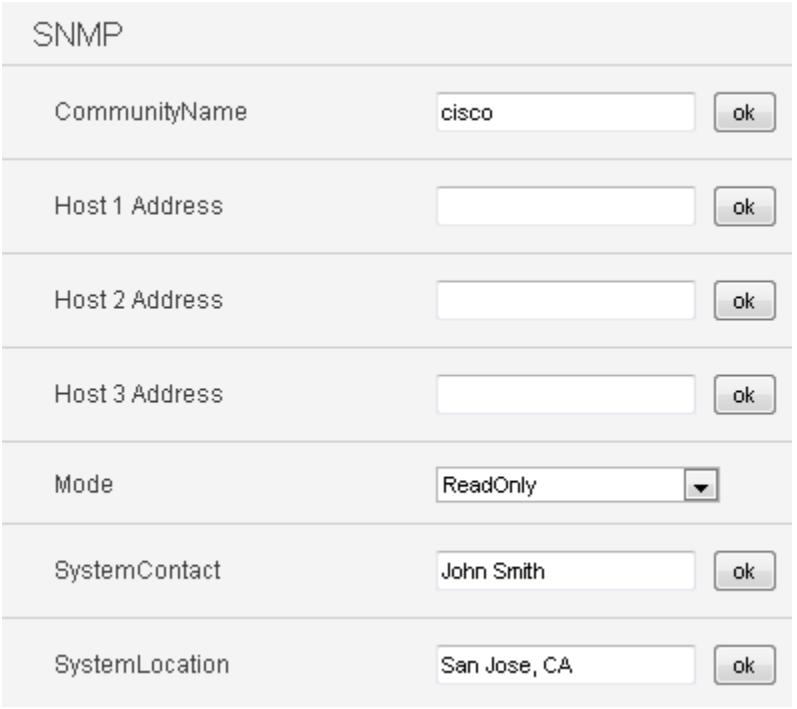


Step 8: Navigate to **NetworkServices**, and enter the following values:

- H323 Mode—**On**
- SIP Mode—**Off**

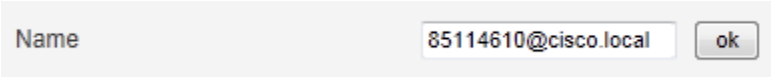
Step 9: Navigate **to NetworkServices**, enter the following values, and then after each entry, click **OK**:

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

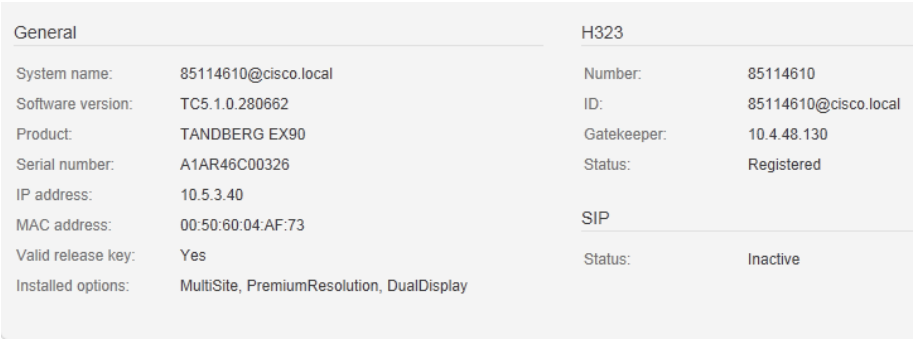


Step 10: Navigate to **SystemUnit**, enter the following value, and then click **OK**:

- Name—85114610@cisco.local



Step 11: Navigate to **Diagnostics > System Information**. Confirm that the system information is correct and the endpoint is registered to Cisco VCS.



Step 12: At the top of the screen, click the arrow next to the **User: admin** prompt, and from the drop-down menu, choose **Sign Out**.

Step 13: Repeat the preceding three procedures for all H.323 endpoints that have to be registered to Cisco VCS.

Process

Testing Point-to-Point Video Calling

1. Dial from SIP to an H.323 alias
2. Dial from SIP to an H.323 E.164 number
3. Dial from H.323 to SIP

After the H.323 endpoints have been configured and registered, it is time to test the calling patterns between the different device types. You start with one of the existing SIP endpoints using the remote control and then move to the H.323 endpoint using the touch screen. Calls will be placed between the two types of endpoints using the transforms and the search rules created in Procedure 1 and Procedure 2 in "Configuring Cisco VCS for Call Control Between SIP and H.323."

Procedure 1 Dial from SIP to an H.323 alias

This procedure calls from SIP to H.323 using the H.323 ID alias to dial. The alias is the fully qualified name of the endpoint that is registered with the gatekeeper function of Cisco VCS.

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

Step 2: Enter 85114610@cisco.local (the alias of an H.323 endpoint)

Step 3: Press the **Green** call button.

The call is connected.

Step 4: To hang up the call, press the **Red** end call button on the remote and select **Disconnect 85114610**.

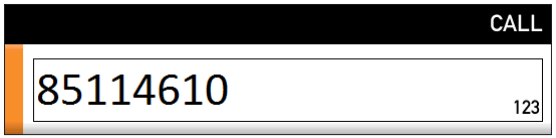
Procedure 2 Dial from SIP to an H.323 E.164 number

This procedure uses the H.323 E.164 number to dial. The number is registered with the gatekeeper that allows numeric-only dialing devices to call the endpoint.

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

Step 2: Enter 85114610 (the E.164 number of an H.323 endpoint).

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



The call is connected.

Step 4: To hang up the call, press the **Red** end call button on the remote and select **Disconnect 85114610**.

The SIP to H.323 point-to-point calling is complete.

Procedure 3 Dial from H.323 to SIP

The next call will be made from the H.323 endpoint using the touch-screen interface.

Step 1: If the touch screen is blank, touch the surface to wake up the unit.

Step 2: Press the **Call** button and from the virtual keyboard, enter 85104600 (the extension of a SIP endpoint), and then press **Start**.

Step 3: After the call is connected, press the red **END** button to hang up the call.

The H.323 to SIP point-to-point 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
	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	
	Software Image for VCS W/ Encrypt Latest Version	SW-VCS-BASE-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 System License Key Software Encrypted	LIC-S52000-TC5.XK9	
	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	
Multipurpose Room System	Cisco TelePresence Profile 42 in w C40 - PHD 1080p 12x Cam, NPP, Touch, 2 Mics	CTS-P42C40-K9	TC5.1.0
	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 Profile 42, 52 and 55 in single screen Wheel Base Mount Kit	CTS-P4252S-WBK	
	Cisco TelePresence Monitor Assembly 42	CTS-P42MONITOR	
	Cisco TelePresence Precision HD 1080p 12X Unit - Silver, + indicates auto expand	CTS-PHD-1080P12XS+	
	Cisco TelePresence Profile Series NPP option	LIC-PCXX-NPP	
	Cisco TelePresence Remote Control TRC 5	CTS-RMT-TRC5	
	Cisco TelePresence Profile 42 C40 Product ID	LIC-P42SC40	
	Software 5.x Encryption	SW-S52000-TC5.XK9	

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 Cisco VCS server.
- We added detailed instructions for configuring the switch ports where the video endpoints are connect to the Catalyst switches
- 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

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

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

© 2012 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

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

B-0000410-1 8/12