H.323 Video Interworking Using VCS

TECHNOLOGY DESIGN GUIDE

August 2013

VALIDATED DESIGN

Table of Contents

Preface

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

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

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

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

How to Read Commands

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

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

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

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

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

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

Comments and Questions

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

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

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

CVD Navigator

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

Use Cases

This guide addresses the following technology use cases:

- **Video Interworking with SIP and H.323**—If organizations have H.323 systems that use call-control gatekeepers and Session Initiation Protocol (SIP) endpoints that use SIP proxy servers, the organizations want a solution that is easy to manage from a central location, without replicating costly components at their remote sites.

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

Scope

This guide covers the following areas of technology and products:

- Video call agent
- Multipurpose room-system video endpoints
- Executive video endpoints
- H.323 and SIP signaling protocols
- Quality of service (QoS) and bandwidth control

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

Proficiency

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

- **CCNA Video**—1 to 3 years configuring voice devices and video single-screen endpoints, supporting telephony and video applications, and troubleshooting

Related CVD Guides

SIP Video Using VCS Technology Design Guide

VCS and UCM Video Integration Technology Design Guide

Video Quality Monitoring Using Medianet Technology Design Guide

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

Introduction

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.

Technology Use Case

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.

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 it 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.

Use Case: Video Interworking with SIP and H.323

Organizations have H.323 systems that use gatekeepers for call control and SIP endpoints that use SIP proxy servers. Organizations have found a dual-registration MCU will answer some of the protocol interoperability issues, but the question of separate bandwidth control is still not resolved. They need a solution that is easy to manage from a central location without replicating costly components at their remote sites.

This design guide enables the following capabilities:

- Single cluster centralized design simplifies deployment and management while saving on infrastructure components.
- Investment in existing H.323 hardware is preserved, and the user community can continue to utilize familiar endpoint functionality.
- SIP endpoints are deployed when and where they are needed to allow the latest technology in locations where it is required.
- Numeric dialing to allow legacy H.323 systems and video-enabled IP phones to participate in calls.
- Calls are made between H.323 and SIP endpoints using dialing rules that are familiar to each type of user.
- Upgrades to new software are minimized, preserving capital for new equipment rather than spending money on older hardware.
- Single point of bandwidth control for SIP and H.323 video endpoints provides the most efficient use of the available WAN resources.

Design Overview

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.

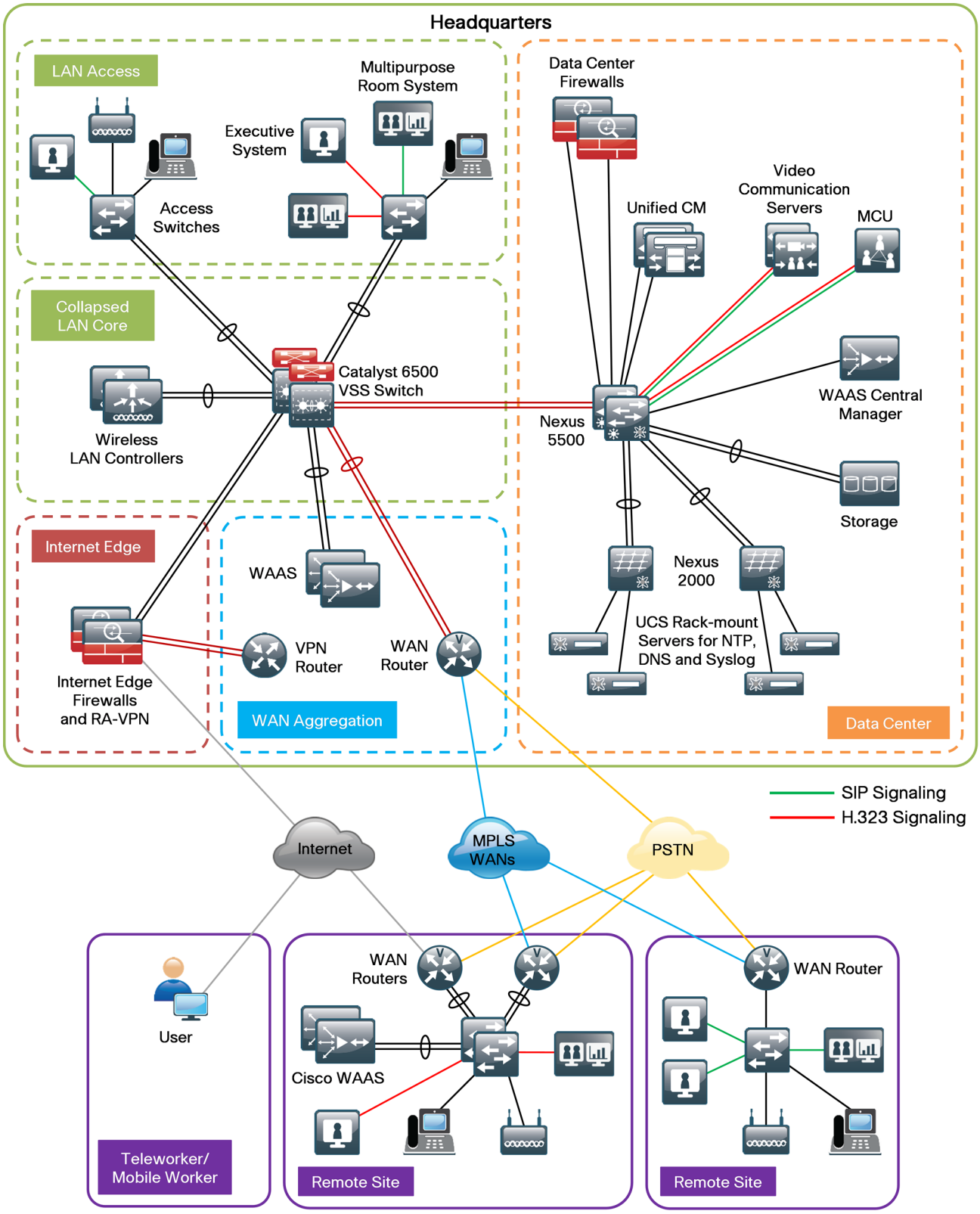
When Cisco TelePresence Video Communication Server (Cisco VCS) is deployed in place of an existing H.323 gatekeeper or SIP proxy, endpoint upgrades are not required. Cisco VCS supports SIP and H.323 in order to allow the different types of endpoints to communicate using one call control agent. However, 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.

Solution Details

The video interworking solution includes the following components (shown in Figure 1):

- 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)

Figure 1 - SIP and H.323 video interworking



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.

QoS and Bandwidth Control

The solution 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 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 media monitoring capabilities are used to troubleshoot problems when they arise.

Deployment Details

The process for configuring, registering, and providing bandwidth control for SIP devices has been documented in the SIP Video Using VCS Design 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 82004610, the transform will automatically append the configured domain name to the called address (*82004610@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**.

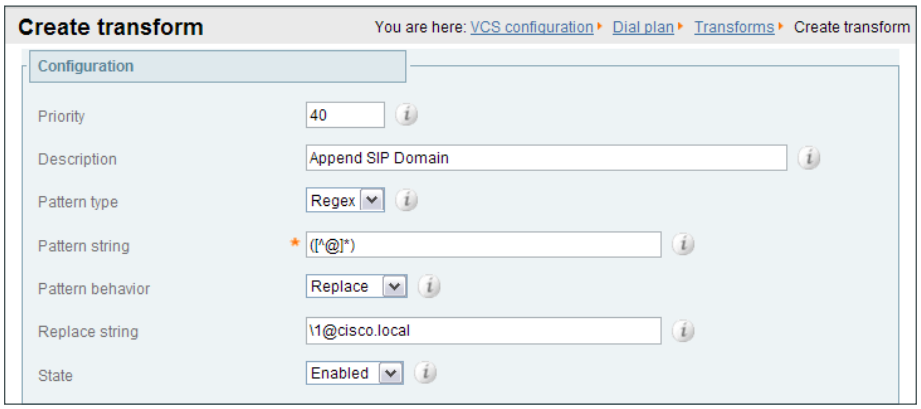
Step 2: Click **Administrator login**, type the following values, and then click **Login**:

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

Step 3: Navigate to **VCS configuration > Dial Plan > 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

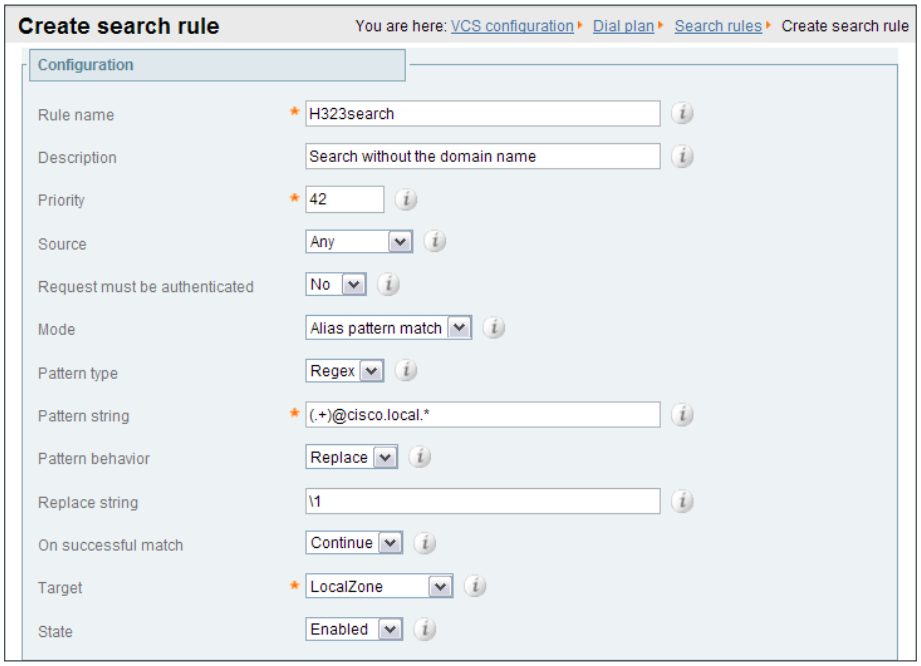
In this procedure, you create two search rules to allow calls between the SIP and H.323 protocols. The rules perform the following checks:

- Strip off the SIP domain portion of the called address, and attempt to find a locally registered H.323 device.
- If no H.323 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**:

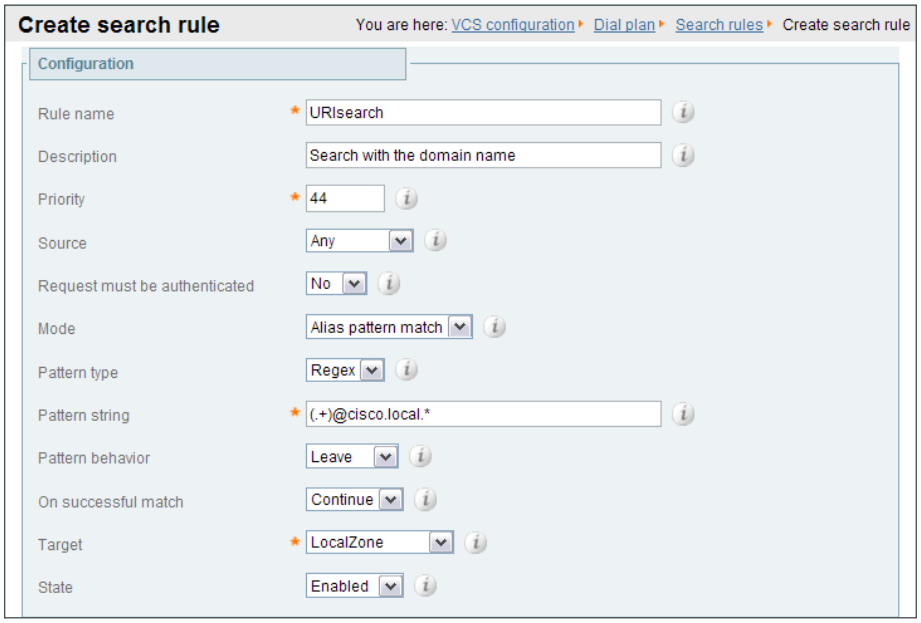
- Rule name–**H323search**
- Description–**Search without the domain name**
- Priority–**42**
- Source–**Any**
- Request must be authenticated–**No**
- Mode–**Alias pattern match**
- Pattern type–**Regex**
- Pattern string–**(.+)@cisco.local.***
- Pattern behavior–**Replace**
- Replace string–**\1**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



Reader 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 = 82004610 is able to call a SIP device registered as SIP URI = 81004600@cisco.local by dialing *81004600* from the H.323 endpoint.

A SIP device registered as SIP URI = 81004600@cisco.local can call an H.323 device registered with an H.323id of 82004610 by calling *82004610@cisco.local* from the SIP endpoint.

A SIP device registered as SIP URI = 81004600@cisco.local can call an H.323 device registered with an E.164 of 82004610 by dialing *82004610* 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 support 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	CVD configuration	Your site-specific information
System Name	82004610@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	82004610@cisco.local	
H.323 E.164 Number	82004610	
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 differentiated services code point (DSCP) markings. The easiest way to do this is to clear the interface of any previous configuration and then apply the egress QoS macro that was defined in the access-switch platform configuration of the Campus Wired LAN Design Guide.

Step 1: 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. 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]**

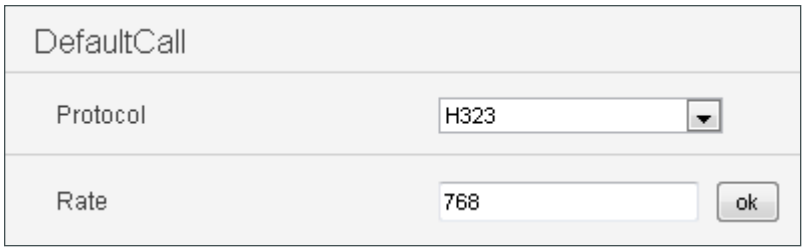
Step 3: From the menu at the top of the page, navigate to **Configuration > Advanced Configuration**.

Tech Tip

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

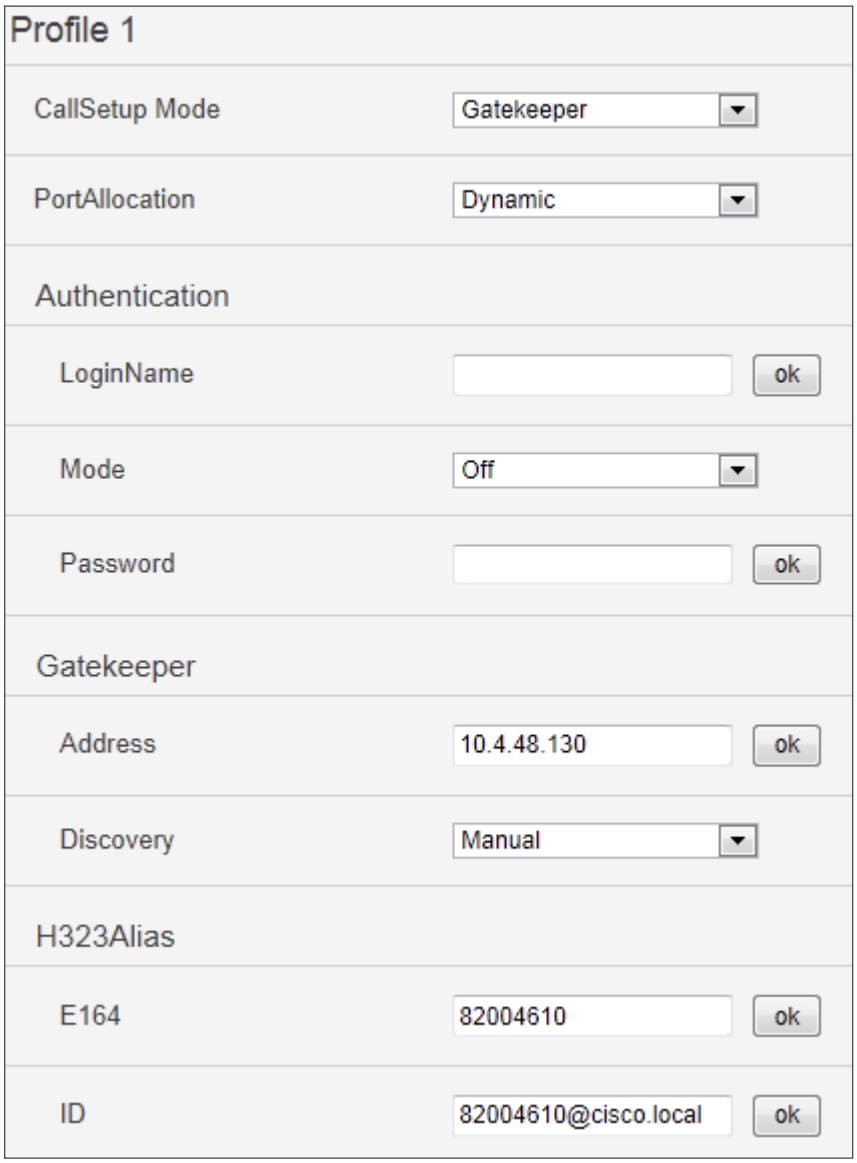
Step 4: Navigate to **Conference 1**, enter the following values, and then click **OK**:

- 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–**82004610**
- H323Alias > ID–**82004610@cisco.local**



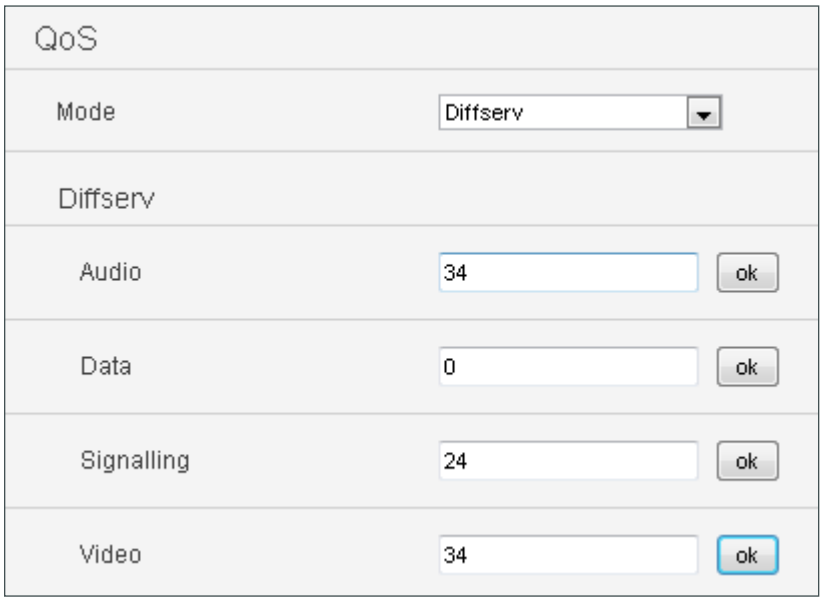
Tech Tip

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 Campus Wired LAN Design 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.

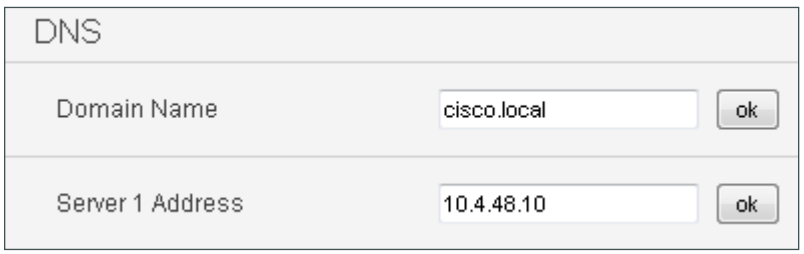
Step 6: Navigate to **Network1** on the endpoint, enter the following values, and then after each entry, click **OK:**

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



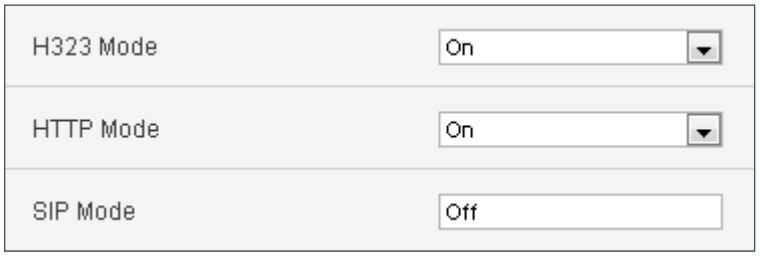
Step 7: Navigate to **Network1**, enter the following values, and then after each entry, click **OK**:

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



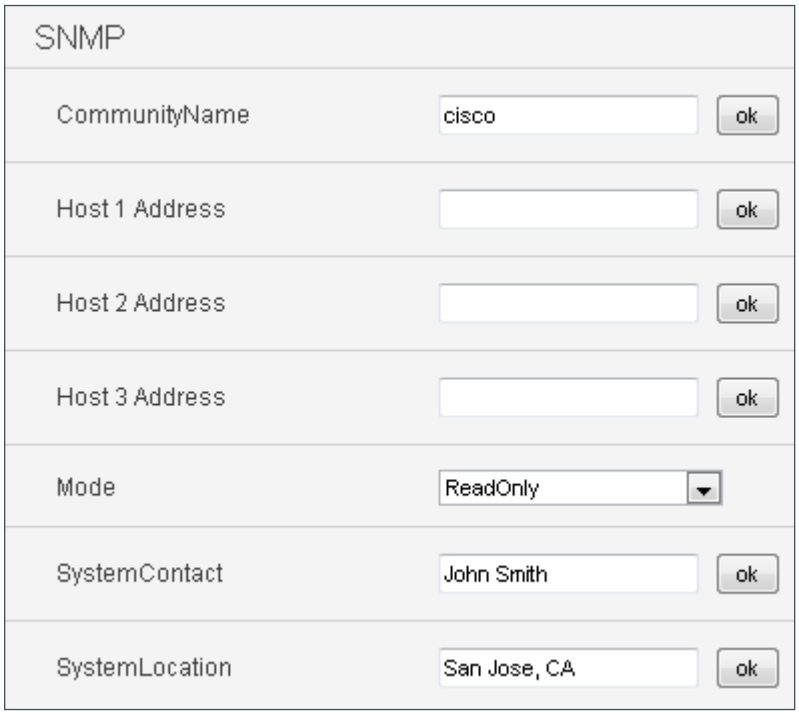
Step 8: Navigate to **NetworkServices**, and enter the following values:

- H323 Mode—**On**
- SIP Mode—**Off**



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

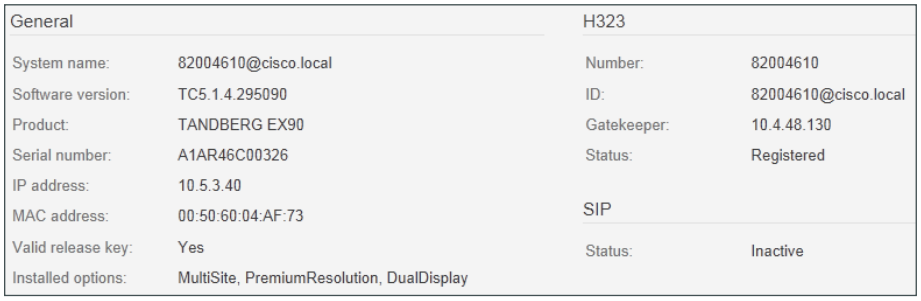
- Mode—**ReadOnly**
- CommunityName—**cisco**
- SystemContact—**John Smith** (optional)
- SystemLocation—**San Jose, CA** (optional)



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

- Name—**82004610@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 by 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 **82004610@cisco.local** (the alias of an H.323 endpoint)

Step 3: Press the green call button.

The call is connected.

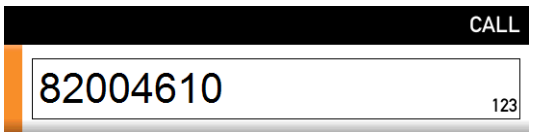
Step 4: To hang up the call, press the red end-call button on the remote, and then select **Disconnect 82004610**.

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 **82004610** (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 then select **Disconnect 82004610**.

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 by 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.

Step 3: From the virtual keyboard, enter **81004600** (the extension of a SIP endpoint), and then press **Start**.

Step 4: 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.

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	X7.2.0
	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	

Video Endpoints

Functional Area	Product Description	Part Numbers	Software
Executive Room System	Cisco TelePresence System EX90 w NPP, Touch UI	CTS-EX90-K9	TC5.1.4
	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	Profile 55 in w C40 NPP PHD 1080p 12x Cam Touch 2 Mics	CTS-P55C40-K9	TC5.1.4
	Cisco TelePresence Monitor Assembly 55	CTS-P55MONITOR	
	Cisco TelePresence Profile 42, 52 and 55 in single screen Wheel Base Mount Kit	CTS-P4252S-WBK	
	Profile 55 C40 Product ID	LIC-P55C40	
	Codec C40	CTS-C40CODEC-K9-	
	InTouch 8 - Control Device- + PID for Service	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	
	XLR Table mic - for auto expand only	CTS-MIC-TABL20XLR+	

LAN Access Layer

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

Feedback

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

B-0000410-1 08/13