

Cisco Virtual Office: Secure Voice and Video

This white paper provides detailed design and implementation information for deploying highly secure voice and video with Cisco® Virtual Office. Please refer to the Cisco Virtual Office overview (found at <http://www.cisco.com/go/cvo>) for further information about the solution, its architecture, and all of its components.

Introduction

Cisco Virtual Office provides a highly secure end-to-end solution that brings enterprise-quality services for voice, video, wireless, and data into the home office. It is designed to bring unified communications to employees' home offices, increasing their flexibility and user satisfaction and improving their overall productivity. This guide covers the deployment of highly secure, voice and video. Security can be deployed in two scenarios:

- It can be enabled at the network endpoint, typically a router, providing the flexibility and transparency to plug in multiple voice or wireless devices or applications behind this endpoint. The network endpoint permits the use of other features that help ensure the trust and identity of the end user, and better quality of service (QoS) can be achieved when the proper capabilities are enabled.
- It can be enabled on the end device (such as wired or wireless IP phones), providing highly secure voice and video services. This scenario limits the ability to deploy multiple voice applications because of the lack of security on such devices. Also, the QoS capabilities of an IP phone as an endpoint are usually quite limited, and commonly there is a need to have a front box that provides network access and sharing. This dilutes the effectiveness of the QoS done at the IP phone.

Recommended Platforms and Images

- Spoke: Cisco 870W Access Router, or Cisco 880 Series or 1800 Series Integrated Services Router (ISR)
- Hub: Cisco 2800 or 3800 Series Integrated Services Router, or Cisco 7200 Series Router
- Authentication, authorization, and accounting (AAA) server: Cisco Secure Access Control Server (ACS)
- Image 880: 12.4(20)T and above
- Image on all other platforms: 12.4(15)T and above
- Wireless IP phones: Cisco Unified Wireless IP Phone 7921G
- Dual-mode phones: Nokia E series using Nokia Intellisync Call Connect 1.1 for Cisco

Secure Voice and Video Deployment

The first step in deploying voice and video is to secure the network endpoint by enabling Cisco Virtual Office layered security features on the Cisco IOS® Software router and establishing the trust and authorization of the end devices. Network security will be provided using the router sitting behind the ISP-provided broadband modem.

This section summarizes the integration of network security, voice, and video.

Router Setup

It is important to have QoS defined for the voice-over-IP (VoIP) traffic based on the available uplink bandwidth provided by the ISP. With respect to security and authentication, VoIP traffic needs to be enabled through the layered security deployed in the Cisco Virtual Office network infrastructure. The host-based authentication (for example, IEEE 802.1x) will use Cisco Discovery Protocol to detect VoIP devices connected in the local network behind the router. The user authentication (for example, Authentication Proxy) will need explicit access control lists (ACLs) defined.

Available Bandwidth and Network Quality

Usually the residential broadband connections provide good downlink speed but are not so generous with the uplink speed. During a voice call, traffic gets generated from the talking party to the listener. The bandwidth usage depends on the codec being used. The popular ones are G.729 and G.711. G.729 uses low bandwidth but is more sensitive to jitter and packet loss. G.711 uses higher bandwidth but can tolerate packet loss better. To accommodate generic routing encapsulation (GRE)/IP Security (IPsec) overhead, the bandwidth on each direction should be at least 128 kbps for G.711 and 80 kbps for G.729. However, for end users at least 256kbps is recommended to avoid any voice-related problems, because ISPs are very unstable at times, and moreover multiple applications could be running at the same time.

Quality of Service

The residential broadband connectivity does not usually have any QoS enabled; it is a best effort network. But QoS can be applied on the VPN spoke router so that voice and other essential traffic gets a higher priority to use the uplink bandwidth. Regular data packets are given a low priority.

If the VPN router is sitting behind another broadband termination device (for example, a cable modem), enabling traffic shaping will prevent the router from sending more traffic than the link can carry. For example, if a Cisco 881 ISR is connected behind a cable modem, the modem's uplink will get congested long before the Cisco 881 router's outbound Ethernet interface is congested. If the traffic-shaping value is configured appropriately, the Cisco 881 router will not send more traffic than the modem can forward without dropping packets. In the case of video IP phones, video traffic needs to be prioritized accordingly.

The following configuration on a Cisco 880 router shows how to match the traffic using a Cisco IOS Software feature called Network Based Application Recognition (NBAR) and then do the respective packet matching. Using NBAR for traffic matching is a good solution when the IP phones are not provided by Cisco, when there is no guarantee that the traffic will be marked correctly with differentiated services code point (DSCP) values. Using NBAR, it is possible to do a much better packet analysis and thus match traffic more accurately.

```
class-map match-any call-setup
match ip dscp cs3
match ip precedence 3
class-map match-any internetwork-control
match access-group name isakmp_acl
match ip precedence 6
match ip precedence 7
class-map match-any voice
```

```
match access-group name voice_acl
match ip precedence 5
class-map match-any routing
match protocol eigrp
class-map match-all discover_signaling
match protocol skinny
class-map match-all discover_video
match protocol rtp video
class-map match-all discover_voip
match protocol rtp audio
class-map match-any video
match access-group name video_acl
match ip dscp af41
match ip precedence 4
class-map match-all non_voip
match access-group name non_voip_traffic_acl

    policy-map mark_incoming_traffic
class discover_signaling
set dscp cs3
class discover_video
set dscp af41
class discover_voip
set dscp ef
class non_voip
set dscp default

policy-map voice_and_video
class voice
bandwidth 128
class call-setup
priority percent 5
class internetwork-control
priority percent 5
class routing
priority percent 5
class video
priority 384
class class-default
fair-queue
random-detect
policy-map shaper
class class-default
shape average 750000 7500
service-policy voice_and_video

ip access-list extended isakmp_acl
```

```
permit udp any any eq isakmp

ip access-list extended voice_acl
permit udp any any range 24576 24656

ip access-list extended non_voip_traffic_acl
permit ip any any

ip access-list extended video_acl
permit udp any any eq 5445
permit udp any any range 2326 2373

interface BVI1
ip nbar protocol-discovery
service-policy input mark_incoming_traffic

interface FastEthernet4
service-policy output shaper
```

Security and Authentication

Cisco Virtual Office routers are usually configured with some kind of user/device authentication. They are mainly Authentication Proxy (auth-proxy) and IEEE 802.1x (spouse and kids feature). These authentication mechanisms need clients running on the IP device. Since IP phones do not have support for these clients, they need to be bypassed from the authentication, without compromising the Cisco Virtual Office security architecture. 802.1x provides a way to detect Cisco IP phones from Cisco Discovery Protocol and bypass authentication. Auth-proxy currently does not support the Cisco Discovery Protocol, and VoIP initial setup traffic needs to be bypassed on the ACL. Cisco IOS Firewall or a zone-based firewall will be defined for actual Routing Table Protocol (RTP) traffic flow while the call is in progress. The following configuration shows 802.1x configurations for an IP phone:

```
! Using 802.1x authenticated in an AAA
!
aaa group server radius dot1x
  server-private <aaa> auth-port 1812 acct-port 1813 key 0 <key>
ip radius source-interface Vlan10
!
aaa authentication dot1x default group dot1x
aaa authorization network default group dot1x
!
! Enable dot1x feature globally
dot1x system-auth-control
!
interface Vlan10
  description Data VLAN to used with wireless
  ip address 10.99.229.161 255.255.255.248
```

```
no ip redirects
no ip unreachable
no ip proxy-arp
ip pim sparse-dense-mode
ip nat inside
ip inspect test in
ip virtual-reassembly
ip tcp adjust-mss 1360
no autostate
tms-class
!!
! Adding a voice VLAN. The voice VLAN has an ACL that allows only
skinny
!
interface Vlan11
description Voice VLAN
ip unnumbered Vlan10
ip access-group allow_skinny_acl in
ip inspect voice_fw in
no autostate
!
interface Vlan20
description Guest VLAN
ip address 10.1.1.1 255.255.255.0
ip pim sparse-dense-mode
ip nat inside
ip inspect test in
ip virtual-reassembly
no autostate
!
!
interface FastEthernet0
switchport access vlan 10
switchport voice vlan 11
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication
dot1x guest-vlan 20
spanning-tree portfast
!
interface FastEthernet1
switchport access vlan 10
switchport voice vlan 11
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication
dot1x guest-vlan 20
spanning-tree portfast
```

```
!  
interface FastEthernet2  
  switchport access vlan 10  
  switchport voice vlan 11  
  dot1x pae authenticator  
  dot1x port-control auto  
  dot1x reauthentication  
  dot1x guest-vlan 20  
  spanning-tree portfast  
!  
interface FastEthernet3  
  switchport access vlan 10  
  switchport voice vlan 11  
  dot1x pae authenticator  
  dot1x port-control auto  
  dot1x reauthentication  
  dot1x guest-vlan 20  
  spanning-tree portfast  
!  
  
!! This list allows skinny traffic on Voice VLAN!!  
!  
ip access-list extended allow_skinny_acl  
  permit udp any any range bootps bootpc  
  permit udp any any eq domain  
  permit udp any any eq tftp  
  permit tcp any any eq 2000  
  permit udp any any range 24576 24656  
  permit udp any any eq 5445  
  permit udp any any range 2326 2373  
  deny ip any any log
```

Voice and Video with Network Address Translation

Skiny Client Control Protocol (SCCP) can now be deployed over Network Address Translation (NAT). This is a common situation for remote access VPN deployments in which the small office/home office (SOHO) router connects to the VPN server using Easy VPN in client mode. In this mode of operation, all remote traffic is network address translated. After Cisco IOS Software Release 12.4(11)T2, SCCP is supported over NAT for voice calls. After Cisco IOS Software Release 12.4(15)T, SCCP-based video calls are supported. One example is when a Cisco Unified IP Phone 7970G is used in combination with Cisco Unified Video Advantage. Another common example is the use of video on the Cisco Unified IP Phone 7985G. For Cisco 880 routers, release 12.4(20)T and above is used, whereas for all other platforms release 12.4(15)T and above can be used.

Other Configurations

When the SCCP-based VoIP physical phone or Cisco IP Communicator (Cisco IP SoftPhone) boots up, it downloads a configuration file from a Trivial File Transfer Protocol (TFTP) server. The

IP address of this TFTP server can be statically configured on the IP phone or downloaded as a Dynamic Host Configuration Protocol (DHCP) option 150. Using the DHCP option is more viable from a management perspective.

The following configuration example is based on the Cisco 881 router:

```
ip dhcp pool client
import all
network 10.32.100.0 255.255.255.248
dns-server <corp. DNS server> <ISP DNS server>
default-router 10.32.100.1
domain-name mycorp.com
option 150 ip <TFTP server's address used by Skinny IP phone>
netbios-name-server <Corp. NETBIOS servers>
update arp
```

Voice and Video Deployment Scenarios

The Cisco Virtual Office solution supports both SCCP and Session Initiation Protocol (SIP) based VoIP deployments. The following VoIP deployment cases are supported.

SCCP-Based Phone Deployment

Cisco IP phones with SCCP support use TCP port 2000 to communicate with the primary and secondary Cisco Unified Communications Manager. Support for SCCP or SIP on the IP phones depends upon the firmware being used. The ACL defined on the Cisco Virtual Office router will block anything but the essential traffic needed for VoIP. This would be the traffic to the TFTP server, Cisco Unified Communications Manager, and the service servers.

Physical Phone Deployment

The Cisco 7960G and 7970G IP phones are the flagship VoIP physical phone solutions provided by Cisco. There is no difference between the phones for either of the phones from a secure voice deployment perspective.

Once the Cisco Virtual Office router is configured, as mentioned in the previous section, the IP phone (if already registered and configured on Cisco Unified Communications Manager) is ready to be plugged in behind the router, and it will start working without any changes. The various aspects mentioned in the initial setup need to be configured for good-quality VoIP deployment and also for successful configuration of an IP phone on Cisco Unified Communications Manager. Other Cisco VoIP-based phones, such as the Cisco Unified IP Phone 7975G, can also be used.

SoftPhone Deployment

Cisco IP Communicator is a VoIP Cisco IP SoftPhone and can be configured as an SCCP or SIP client. Cisco Discovery Protocol support is not needed for Cisco IP Communicator to work, and once the PC is authenticated and gets an IP address from the corporate pool, Cisco IP Communicator should work. The auth-proxy bypass configuration used for regular IP phones will also work for Cisco IP Communicator.

Wireless IP Phone Deployment

The Cisco Unified Wireless IP Phone 7920 is a Wi-Fi IP phone and supports only SCCP. This phone supports regular Wired Equivalent Privacy (WEP) and Cisco LEAP for wireless authentication. After the wireless authentication step is completed, the phone will register with Cisco Unified Communications Manager as a regular IP phone would, and will be ready for use.

Video Phone Deployment

The Cisco 7960G and 7970G IP phones are two of the IP phone models that provide support for video VoIP physical phone deployment using Cisco Unified Video Advantage. Cisco Unified Video Advantage is a personal video telephony solution that enables users to make video telephone calls as easy as regular phone calls, instead of requiring the use of complicated room videoconferencing systems or PC-based applications. It comprises the Cisco Unified Video Advantage software application and the Cisco VT Camera, a video telephony Universal Serial Bus (USB) camera. Cisco Unified Communications Manager Release 4.0(1), Service Release 2a or later, is required to support the Cisco Unified Video Advantage solution. For more details on Cisco Unified Video Advantage and its unique advantages, refer to http://www.cisco.com/en/US/docs/video/cuva/1_0/administration/guide/vunder.html.

Before connecting the Cisco VT Camera to the USB port on the PC for the first time, follow the steps to install the Cisco Unified Video Advantage software application on the PC. The application will prompt for the Cisco VT Camera to be connected. Once the installation is complete, the Cisco Unified Video Advantage icon will appear on the screen. When the icon is enabled, click on Start -> Start Video Check; both the local and remote video screen will appear and will display the local video being captured.

Before the video call is established with the other user, make sure the same is enabled at his end. Also make sure that UDP port 5445 is bypassed in the ACL at both ends, as 5445 is the TCP port used by Cisco Unified Video Advantage for video. No additional configuration changes are needed; the router setup section will satisfy the needs for the IP phone to work. When the call is established, the local screen will continue to show the local video, but the remote screen will now display the remote video.

Voice over WLAN (VoWLAN) Dual-Mode Phone Deployment

Nokia E series dual-mode phones give users the option of making calls over a cellular or wireless network. Using the wireless capability of the Cisco 881 router, these dual-mode phones can register with Cisco Unified Communications Manager, thus extending the office extension on the Nokia phones. Using the VPN gateway at the main site, users can make calls securely from public hotspots. In order to use a SCCP client, for example, Nokia Intellisync Call Connect for Cisco, however, a license would be needed from Cisco.

Go to http://www.cisco.com/web/partners/pr46/solutions_plus/mobile_business_solutions.html for a technical overview and purchasing options for these products.

SIP-Based VoIP Solution

Physical Phone Deployment

The Cisco Unified IP Phone 7960G supports both SCCP and SIP images, unlike the Cisco 7970G and 7920 IP phones, which support only SCCP. The SIP IP phone deployment is the same as the SCCP deployment.

Cisco ATA-Based Analog Physical Phone Deployment

Cisco ATA 186 and ATA 188 Analog Telephone Adaptors are handset-to-Ethernet adapters that allow regular analog phones to connect to IP-based telephony networks. The Cisco ATA device needs to register with the SIP server to make SIP calls.

The initial step involves connecting the Cisco ATA device behind the Cisco Virtual Office router, where it will get an IP address assigned dynamically from the intranet pool. 802.1x does not distinguish the Cisco ATA using Cisco Discovery Protocol, so to bypass 802.1x authentication for the device, add the Cisco ATA's Ethernet interface mac-address to the 802.1x authorized device list.

Plug the regular analog phone into line 1, and check for a dial tone. If configured correctly, the tone should be available and the SIP-enabled analog phone is ready for calls.

Linksys Router-Based Analog Physical Phone Deployment

The Linksys RT31P2 is a broadband router that provides both Internet and telephony capabilities. The router has two standard telephone jacks to enable high-quality, feature-rich telephone service through the broadband connection. Each phone jack operates independently, providing having two phone lines. The Linksys router needs to register with the SIP server to make SIP calls.

The initial step involves connecting the Linksys router behind the Cisco Virtual Office router, where it will get an IP address assigned dynamically from the intranet pool after successful authentication. 802.1x does not distinguish the Linksys router using Cisco Discovery Protocol, so bypassing authentication automatically is not possible. Hence, to get an IP address assigned from the intranet pool, add the Linksys router's "Internet: interface mac-address to the 802.1x authorized device list.

Connect to the Linksys router's main menu through the provided administrative username/password. From the main menu, select "Voice" and then Line1. Enter the provided virtual number into the User Id: field and the SIP password into the Authenticate Password: field. Enter the SIP registration server address into Registration/Proxy Server: field. Repeat this step for line 2 if the second line needs to be activated as well.

For the best voice quality, leave the Voice Quality: field at its default (G.711). If you have limited bandwidth, choose G.729. Once the settings are done, click "Save" and then let the Linksys router reboot.

Plug the regular analog phone into line 1, and check for a dial tone. If configured correctly, the tone should be available, and the SIP-enabled analog phone is ready for calls.

Third-Party Wireless Phone Deployment

A third-party Wi-Fi SIP phone can also be enabled on the Cisco Virtual Office network. If the Wi-Fi SIP phone needs to connect to the SIP server, and then it needs to support one of the acceptable wireless authentication methods, namely static WEP or Cisco LEAP. If supported, the device will first authenticate successfully, get the IP address from the intranet pool, and then register to the Cisco SIP registration/proxy server. Once done, the phone is ready to make SIP-based calls.

If a Wi-Fi SIP phone does not support acceptable wireless security, it cannot be part of a Cisco voice VLAN. A separate guest VLAN may be created for this device so that it can access the internet. Access to the Cisco network will not be allowed from this VLAN because it is associated with weak wireless security. In the Cisco Virtual Office deployment scenario, the Wi-Fi SIP phone supports only regular WEP, and hence, using the guest VLAN, it will get Internet access and will

register with a publicly available SIP server or with one of the commercial SIP VoIP service providers. Once done, the phone is ready to make SIP-based calls.

VoWLAN Dual-Mode Phone Deployment Based on the Nokia E Series

Nokia E series dual-mode phones give users the option of making calls over a cellular network or wireless network. Using wireless capability, these dual-mode phones can register with Cisco Unified Communications Manager, thus extending the office extension on the Nokia phones. Using the VPN gateway at the main site, users can make calls securely from public hotspots. The SIP client is native in the Nokia dual-mode phone.

Go to http://www.cisco.com/web/partners/pr46/solutions_plus/mobile_business_solutions.html for a technical overview and purchasing options of these products.

Troubleshooting and Show Commands

- Troubleshooting Cisco Unified Communications Manager: For more information, read the troubleshooting guide at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_troubleshooting_guides_list.html
- show policy map interface: To monitor the results of a service policy created with Cisco Modular QoS command-line interface (CLI) (MQC)

This sample output indicates the packet loss and also shows the number of packets matching each class type. For example, dscp 46 is used for voice, and the output shows that 931,053 voice packets were identified and given a higher priority compared to other packets.

```
show policy-map interface f4
FastEthernet4

Service-policy output: voice

Class-map: voice (match-any)
  931053 packets, 273729582 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: ip dscp ef (46)
  931053 packets, 273729582 bytes
  5 minute rate 0 bps
Match: ip dscp cs5 (40)
  0 packets, 0 bytes
  5 minute rate 0 bps
Match: ip precedence 5
  0 packets, 0 bytes
  5 minute rate 0 bps
Match: access-group name voice_acl
  0 packets, 0 bytes
  5 minute rate 0 bps
Queueing
  Strict Priority
```

```
Output Queue: Conversation 264
Bandwidth 128 (kbps) Burst 3200 (Bytes)
(pkts matched/bytes matched) 22/6468
(total drops/bytes drops) 0/0

Class-map: call-setup (match-any)
45643 packets, 6138247 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: ip dscp af31 (26)
0 packets, 0 bytes
5 minute rate 0 bps
Match: ip dscp af32 (28)
0 packets, 0 bytes
5 minute rate 0 bps
Match: ip dscp cs3 (24)
45643 packets, 6138247 bytes
5 minute rate 0 bps
Match: ip precedence 3
0 packets, 0 bytes
5 minute rate 0 bps
Queueing
Output Queue: Conversation 265
Bandwidth 2 (%)
Bandwidth 2000 (kbps)Max Threshold 64 (packets)
(pkts matched/bytes matched) 2/268
(depth/total drops/no-buffer drops) 0/0/0

Class-map: internetwork-control (match-any)
188544 packets, 27484352 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: ip dscp cs6 (48)
188544 packets, 27484352 bytes
5 minute rate 0 bps
Match: access-group name control_acl
0 packets, 0 bytes
5 minute rate 0 bps
Match: access-group name isakmp_acl
0 packets, 0 bytes
5 minute rate 0 bps
Match: ip precedence 6
0 packets, 0 bytes
5 minute rate 0 bps
Match: ip precedence 7
0 packets, 0 bytes
5 minute rate 0 bps
Queueing
Output Queue: Conversation 266
```

```

Bandwidth 5 (%)
Bandwidth 5000 (kbps)Max Threshold 64 (packets)
(pkts matched/bytes matched) 5709/715022
(depth/total drops/no-buffer drops) 0/0/0

Class-map: class-default (match-any)
 940377 packets, 179331619 bytes
 5 minute offered rate 1000 bps, drop rate 0 bps
Match: any
Queueing
  Flow Based Fair Queueing
  Maximum Number of Hashed Queues 256
  (total queued/total drops/no-buffer drops) 0/0/0
  exponential weight: 9

```

class	Transmitted	Random drop	Tail drop	Minimum
Maximum	Mark			
thresh	pkts/bytes	pkts/bytes	pkts/bytes	thresh
	prob			
0	940376/179331545	0/0	0/0	20
40	1/10			
1	0/0	0/0	0/0	22
40	1/10			
2	0/0	0/0	0/0	24
40	1/10			
3	0/0	0/0	0/0	26
40	1/10			
4	0/0	0/0	0/0	28
40	1/10			
5	0/0	0/0	0/0	30
40	1/10			
6	0/0	0/0	0/0	32
40	1/10			
7	0/0	0/0	0/0	34
40	1/10			
rsvp	0/0	0/0	0/0	36
40	1/10			

References

- Cisco Virtual Office Deployment Guide:
http://www.cisco.com/en/US/tech/tk583/tk372/technologies_white_paper0900aecd801dc5b2.shtml
- IP Telephony/Voice over IP (VoIP):
http://www.cisco.com/en/US/tech/tk652/tk701/tech_protocol_family_home.html
- SCCP: http://www.cisco.com/en/US/tech/tk652/tk701/tk589/tech_protocol_home.html
- SIP: http://www.cisco.com/en/US/tech/tk652/tk701/tk587/tech_protocol_home.html
- Cisco ATA 180 Series Analog Telephone Adaptors:
<http://www.cisco.com/en/US/products/hw/gatecont/ps514/index.html>

- Cisco Unified IP Phones 7900 Series:
<http://www.cisco.com/en/US/products/hw/phones/ps379/index.html>
- Cisco IP Communicator:
<http://www.cisco.com/en/US/products/sw/voicesw/ps5475/index.html>
- Cisco IP SoftPhone: <http://www.cisco.com/en/US/products/sw/voicesw/ps1860/index.html>
- Cisco SIP IP Phone software for the Cisco 7960 IP phone:
<http://www.cisco.com/en/US/products/sw/voicesw/ps2156/index.html>
- Cisco Unified Video Advantage:
<http://www.cisco.com/en/US/products/sw/voicesw/ps5662/index.html>
- Cisco Aironet® 1200 Series Access Point :
<http://www.cisco.com/en/US/products/hw/wireless/ps430/index.html>
- Wi-Fi Protected Access (WPA) configuration overview:
http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example_09186a00801c40b6.shtml



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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0807R)