CISCO

CCIE
Collaboration
Quick Reference

Akhil Behl

Cisco Press

CCIE Collaboration Quick Reference

Akhil Behl, CCIE No. 19564

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

CCIE Collaboration Quick Reference

Akhil Behl, CCIE No. 19564 (Voice and Security)

Copyright© 2014 Pearson Education, Inc.

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Warning and Disclaimer

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Editor-in-Chief: David Dusthimer

Business Operation Manager, Cisco Press: Jan Cornelssen

Executive Editor: Brett Bartow

Managing Editor: Sandra Schroeder

Development Editor: Marianne Bartow

Senior Project Editor: Tonya Simpson

Copy Editor: Bill McManus

Technical Editor: Paulo Lopes

Editorial Assistant: Vanessa Evans

Designer: Mark Shirar

Composition: Jake McFarland

About the Author

Akhil Behl, CCIE No. 19564, is a solutions architect with Cisco Advanced Services, focusing on Cisco Collaboration and Security architectures. He leads Collaboration and Security projects and service delivery worldwide for Cisco Services and the Collaborative Professional Services (CPS) portfolio. He has played a major role in service conception and creation for various services within Cisco Advanced Services. Akhil has a wide range of experience, from presales to sales to professional services to delivery to post sales, with expertise in consulting, advisory, and guidance services. Prior to his current role, Akhil spent 10+ years working in various roles at Linksys as a technical support lead, as an escalation engineer at the Cisco Technical Assistance Center (TAC), and as a network consulting engineer in Cisco Advanced Services.

Akhil has a bachelor of technology degree in electronics and telecommunications from IP University and a master's degree in business administration from Symbiosis Institute. He is a dual Cisco Certified Internetwork Expert in Voice and Security. He also holds many other industry certifications, such as PMP, ITIL, VCP, CCNA, CCSP, CCVP, ISO/IEC 27002, TOGAF, and CEH.

Over the course of his career, Akhil has presented and contributed at various industry forums such as Enterprise Connect, Cloud Connect, Cloud Summit, Interop, Cisco Networkers, and SecCon. He has several research papers published in various national and international journals, including IEEE journals, and is the author of the Cisco Press title *Securing Cisco IP Telephony Networks*.

About the Technical Reviewer

Paulo Lopes is a network consulting engineer at the Advanced Services Center of Excellence of Cisco Unified Communications for Cisco. He has been working at Cisco supporting and deploying Cisco Unified Communications solutions for more than 10 years. Paulo is currently the tech lead of the Unified Communications virtual team for the Americas.

Dedication

This book is dedicated first to my family, my dear wife Kanika and my lovely sons Shivansh and Shaurya, for without their support, encouragement, and patience, it would not exist. Secondly, to my parents, Vijay Behl and Ravi Behl, and my brothers, Nikhil Behl and Ankit Behl, who have always been there to support me and guide me in all my endeavors.

Acknowledgments

I would like to thank the following amazing people and teams for helping me create this book:

My wife, Kanika, and my kids, Shivansh and Shaurya, for sacrificing many days and weekends over the past year so that I could work on this book. Without their patience and support, this book would not have been possible.

The technical reviewer, Paulo Lopes, for his invaluable feedback and for providing exceptional technical coverage.

The Cisco Press editorial team: Brett Bartow, the executive editor, for seeing the value and vision in the proposed title and providing me the opportunity to build this title; and Marianne Bartow, development editor, and Christopher Cleveland, senior development editor, for their support and guidance all throughout. It is my sincere hope to work again with them in the near future.

Everyone else in the Cisco Press production team, for their support and commitment.

Contents at a Glance

Contents

Icons Used in This Book

Communication Server	PC	PC with Software	Sun Workstation	Macintosh	Access Server	ISDN/Frame Relay Switch
Token Ring	Terminal	File Server	Web Server	Ciscoworks Workstation	ATM Switch	Modem
Printer	Laptop	IBM Mainframe	Front End Processor	Cluster Controller		Multilayer Switch
Gateway	Router	Bridge	Hub	DSU/CSU	FDDI	Catalyst Switch
Network Cloud	Line: Ethernet	Line: Serial	Line: Switched Serial			Cisco ASA

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).

- *Italics* indicate arguments for which you supply actual values.

- Vertical bars (|) separate alternative, mutually exclusive elements.

- Square brackets ([ ]) indicate optional elements.

- Braces ({ }) indicate a required choice.

- Braces within brackets ([{ }]) indicate a required choice within an optional element.

This page intentionally left blank

Cisco Unified Communications Security

As discussed in the previous chapters, a Cisco Collaboration solution has many elements, including infrastructure, endpoints, applications, gateways, and so on. While all of these work together to deliver a seamless user experience, they need to be secured to ensure that business continuity is maintained and the communication channels are operational. The objective of securing a Cisco Collaboration solution is to secure a converged communications network to protect its availability, the confidentiality of data that it carries, and the integrity of this data.

Security Policy

The fundamental step to achieve a robust and secure converged network is to develop a security policy that specifies an appropriate security plan, design, implementation, and operations policy. A security policy gives direction to the efforts to deploy security controls at the various layers of the OSI model, starting at the physical layer, Layer 1, up through the application layer, Layer 7. At a high level, a security policy should at least address the following from a Cisco Collaboration network perspective:

- Acceptable usage and conduct pertinent to Cisco Collaboration network resources

- Physical layer security

- Network infrastructure security

- Perimeter security

- Server hardening

- User endpoint security

- Wireless infrastructure security

- Backup and restore (including disaster recovery) security

- Provision for lawful interception of calls

Threats to Cisco Collaboration Networks

The first step toward securing a Cisco Collaboration solution is to understand the possible threats to infrastructure, endpoints, devices, and applications. Security threats pertinent to Cisco Collaboration networks can be broadly categorized as listed in Table 5-1.

Table 5-1   *Threats to a Cisco Collaboration (Unified IP) Network*

Threat Category	Description
Eavesdropping/ interception attacks	Aimed at voice and signaling sessions, leading to loss of confidentiality or integrity, or both.
Identity theft/ impersonation attacks	Used to exploit information in voice and video streams, leading to loss of confidentiality.
Toll fraud	Occurs by means of unauthorized or fraudulent use of telephony equipment or services.
Denial-of-service (DoS) attacks	Leads to degradation of voice and video services.
Intrusion attacks	Targeted at services associated with or enabled by the telephony implementation, such as servers in the same zone as UC servers.

There's no single security control or tool/mechanism to thwart all the attack types listed in Table 5-1. Defense-in-Depth, also known as a layered security approach, is required to mitigate these threats. The following sections give insight into security measures at the various layers of the OSI model.

Layer 1 Security

Physical security entails securing Cisco Collaboration assets from physical access by an intruder and from potential damage by surrounding environmental factors. The major physical security controls include

- Guards at data center or facility periphery

- Badged access to data center/facilities

- CCTV, alarms, and sensors at data center/facility entry and exits

- Cisco Collaboration equipment secured in racks in data center and in closets at user access level

- Uninterruptible power supply (UPS) for servers and network devices

Layer 2 Security

Layer 2 security can be deployed at the switching layer to prevent attacks originating from the user access layer such as:

- MAC address spoofing
- DHCP spoofing
- Spanning Tree Protocol (STP) manipulation
- ARP poisoning
- Identity spoofing

Port Security

Cisco Catalyst switches have a feature called port security that helps to reduce spoofing and other attacks. Port security restricts the input to an interface by limiting and identifying MAC addresses of end devices. The port security feature can leverage MAC address learning in the following ways:

- **Static secure MAC address:** Manually limits the MAC addresses to be allowed on a switch port by statically configuring the MAC addresses on a per-port basis. This feature allows MAC addresses learned to be saved in Content Addressable Memory (CAM) table and running configuration.

- **Sticky secure MAC address:** The switch port dynamically learns the MAC addresses of connected devices (sticky) configured for sticky secure MAC addresses and stores these in the CAM table and running configuration.

- **Dynamic secure MAC address:** The MAC addresses learned from the switch port set up for dynamic secure MAC addresses are stored only in a switch's CAM table and not in the running configuration.

Upon violation of the number of MAC addresses per port, you can configure violation rules in one of following three ways:

- **Protect:** When the switch port reaches its configured maximum number of secure MAC addresses, it starts dropping frames with an unknown source MAC address.

- **Restrict:** Similar to the protect option, the major difference being that the restrict option can send an SNMP trap and a syslog message. It increments the violation counter when a port security violation occurs.

- **Shutdown:** After a port security violation occurs, the port is shut down and put in err-disable state. This option also allows generation of the SNMP and syslog notifications, identical to the restrict option, and it will also increment a violation counter.

Example 5-1 illustrates enabling port security on a Cisco Catalyst switch for interface FastEthernet 0/10 where the maximum number of MAC addresses is set to 3 on this particular interface, and the port, upon exceeding the maximum count, will be put in err-disable mode (shut down). The **mac-address** command is used to set a static MAC and remember the MAC addresses connected to it (sticky).

Example 5-1   *Cisco Catalyst Switch Port Security Configuration*

```
UCSWITCH(config)# interface FastEthernet 0/10
UCSWITCH(config-if)# switchport port-security
UCSWITCH(config-if)# switchport port-security maximum 3
UCSWITCH(config-if)# switchport port-security violation shutdown
UCSWITCH(config-if)# switchport port-security mac-address 10BD.18DC.97F5
UCSWITCH(config-if)# switchport port-security mac-address sticky
```

DHCP Snooping

DHCP spoofing is used to launch Man-In-The-Middle (MITM), reconnaissance, and DoS attacks. In the DHCP spoofing attack, the attacker enables a rogue DHCP server on a network. When an endpoint (Cisco Unified IP Phone or softphone) sends a broadcast request for the DHCP configuration information, the rogue DHCP server responds before the original DHCP, thereby assigning the attacker-defined IP configuration information. DHCP snooping is a Cisco Catalyst switch feature that helps prevent DHCP spoofing attacks by enabling the switch ports to be set as either trusted (DHCP server-facing interface) or untrusted (user facing). Trusted switch ports can send DHCP requests and acknowledgements, whereas untrusted ports can only forward DHCP requests. DHCP snooping enables the switch to build a DHCP binding table that maps a client MAC address, IP address, VLAN, and port ID. Example 5-2 outlines DHCP snooping configuration where FastEthernet 0/10 is set to trusted and FastEthernet 0/20 is set to untrusted.

Example 5-2   *DHCP Snooping Configuration*

```
UCSWITCH(config)# ip dhcp snooping VLAN 200 201
UCSWITCH(config)# no ip dhcp snooping information option
UCSWITCH(config)# ip dhcp snooping
!
UCSWITCH(config)# interface FastEthernet 0/10
UCSWITCH(config-if)# ip dhcp snooping trust
!
UCSWITCH(config)# interface FastEthernet 0/20
UCSWITCH(config-if)# no ip dhcp snooping trust
UCSWITCH(config-if)# ip dhcp snooping limit
```

DHCP snooping is also used for Dynamic ARP Inspection (DAI), as discussed later in this chapter.

Root Guard and BPDU Guard

When a Cisco switch boots up, Spanning Tree Protocol (STP) identifies one switch as a root bridge. STP uses bridge protocol data units (BPDU) to maintain a loop-free topology by blocking redundant paths between switches. An attacker can send spoofed BPDU packets to imitate a root bridge, thereby causing a reconvergence of the network traffic. The attacker can capture traffic, launch DoS attacks, or initiate MITM attacks. BPDU guard and Root Guard help prevent the DoS or MITM attacks originating as a result of STP manipulation. BPDU Guard helps stop STP manipulation by enabling port(s) that don't accept any BPDUs. Root Guard ensures that when the root (or root bridge) is elected, a new BPDU on a designated port isn't entertained.

The following is a configuration of BPDU Guard and Root Guard for thwarting STP manipulation:

```
UCSWITCH(config)# spanning-tree portfast bpduguard
UCSWITCH(config)# spanning-tree guard root
```

Dynamic ARP Inspection

An attacker can poison the Address Resolution Protocol (ARP) table. The intent is to conceal the identity so that the attacker's switch/PC becomes the default gateway for the telephony subnet. ARP poisoning can be implemented by replying to and poisoning the network so that the attacker's MAC address seems to be mapped to the default gateway IP address of the endpoints. An ARP attack can be mitigated by implementing Dynamic ARP Inspection (DAI), wherein the switch checks the IP/MAC mappings in the DHCP snooping binding table, thereby establishing the authenticity of packets before forwarding the packets to the destination. DAI drops all ARP packets that do not pass the inspection process. Example 5-3 outlines the process to enable DAI on a global and per-interface basis.

Example 5-3 *DAI Interface-Specific and Global Setup*

```
UCSWITCH(config)# ip arp inspection vlan 300
!
UCSWITCH(config)# interface FastEthernet 0/1
UCSWITCH(config-if)# ip arp inspection trust
```

802.1x

802.1x is a standard set by the IEEE 802.1 working group. It's a framework designed to address and provide port-based access control using authentication, primarily using Extensible Authentication Protocol (EAP) as the key protocol. 802.1x is a Layer 2 protocol for transporting authentication messages (EAP) between a supplicant (user/endpoint/PC) and an authenticator (switch or access point) with an (optional) authentication server

(RADIUS) at the back end to authenticate the supplicant. For wired supplicants, EAP over LAN (EAPoL) is used, and for wireless supplicants, EAP over Wireless (EAPoW) is used. Figure 5-1 shows 802.1x via EAPoL and EAPoW for wired and wireless supplicants, respectively, to a RADIUS (Cisco TACACS+) server.
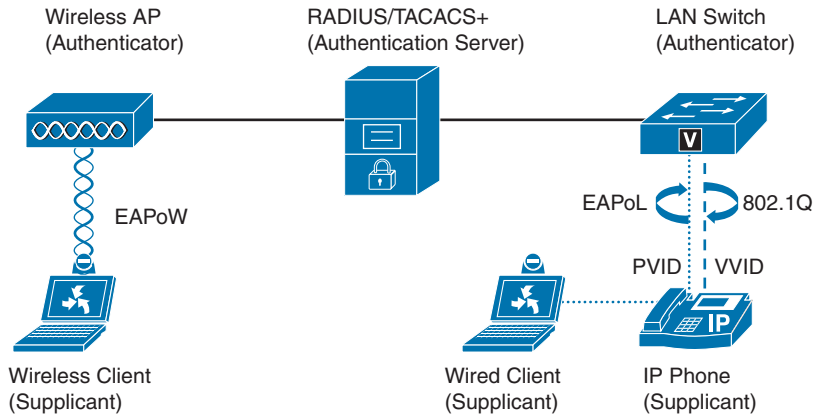
Figure 5-1 *802.1x in Cisco Collaboration Networks*

Multidomain Authentication (MDA) helps define two domains on the same physical switch port: Voice VLAN Identifier (VVID) and Port VLAN Identifier (PVID). The 802.1x process for voice using an EAPoL and MDA approach is shown in the following steps:

Step 1.   A Cisco Unified IP Phone learns VVID from Cisco Discovery Protocol (CDP). Third-party phones use Link Layer Discovery Protocol (LLDP). 802.1x times out.

Step 2.   The switch initiates MAC Authentication Bypass (MAB).

Step 3.   Cisco TACACS+ (RADIUS server) returns Access-Accept with the IP Phone's vendor-specific attribute (VSA).

Step 4.   IP Phone traffic is initially allowed on either VLAN until it sends an 802.1Q tagged packet. Then only voice VLAN is allowed for the IP Phone.

Step 5.   The daisy-chained PC (connected to the PC port on the IP Phone) authenticates using 802.1x or MAB. PC traffic is allowed on the data VLAN only.

Example 5-4 demonstrates the switch configuration for MDA.

Example 5-4 *MDA Setup*

```
UCSWITCH(config)# interface FastEthernet 1/1
UCSWITCH(config-if)# switchport mode access
UCSWITCH(config-if)# switchport access vlan 100
UCSWITCH(config-if)# switchport voice vlan 200
UCSWITCH(config-if)# spanning-tree portfast
UCSWITCH(config-if)# authentication event fail action next-method
```

```
UCSWITCH(config-if)# authentication host-mode multi-domain
UCSWITCH(config-if)# authentication order dot1x mab
UCSWITCH(config-if)# dot1x pae authenticator
UCSWITCH(config-if)# authentication port-control auto
UCSWITCH(config-if)# dot1x timeout tx-period 10
UCSWITCH(config-if)# dot1x max-req 2
UCSWITCH(config-if)# mab
```

Layer 3 Security

At Layer 3 of the OSI model, the following security mechanisms help restrain attacks from within and outside of a network:

■ Deploying RFC 2827 filtering, uRPF, and IP source guard (prevents IP spoofing)

■ Using routing protocol authentication

■ Disabling unnecessary Cisco IOS services (hardening)

RFC 2827 Filtering

To prevent IP spoofing attacks emerging from outside your network, RFC 1918 addresses should be filtered using IP access control lists (ACL). These addresses include the following:

■ 10.0.0.0/8

■ 172.16.0.0/12

■ 192.168.0.0/16

■ 0.0.0.0/8

■ 127.0.0.0/8

■ 169.254.0.0

In addition to these addresses, the multicast range of 224.0.0.0/4, 239.0.0.0/8, and 240.0.0.0/5 and the broadcast address of 255.255.255.255 should be blocked.

IP Source Guard

The IP source guard feature can be enabled on untrusted switch ports. This feature blocks all IP traffic initially, except for DHCP packets captured by the DHCP snooping process. When a client receives a valid IP address from the trusted DHCP server, a port ACL (PACL) is applied to the port. This restricts the traffic only from known client source IP addresses configured in the binding, disregarding any other IP traffic. The following configuration enables IP source guard on the FastEthernet 0/10 interface of a Cisco Catalyst switch:

```
UCSwitch(config)# interface FastEthernet 0/10
UCSwitch(config-if)# ip verify source
```

Unicast Reverse Path Forwarding

Unicast Reverse Path Forwarding (uRPF) is a Cisco IOS feature that can be employed on Cisco IOS routers to prevent attempts to send packets with spoofed source IP addresses. The uRPF feature looks for the source IP address of a packet arriving on the inbound interface of a router in its routing table. If the source IP address exists in the network behind the router, and the routing table contains an entry for the same, the packet is allowed. uRPF requires Cisco Express Forwarding (CEF) to be enabled. The following snippet outlines the configuration of uRPF on FastEthernet 1/1 of a Cisco IOS router:

```
UCRouter(config)# interface FastEthernet 1/1
UCRouter(config-if)# ip verify unicast reverse-path
```

Routing Protocols Security

An attacker can attempt to manipulate the routing tables of routers by injecting his own malicious routes, thereby causing the router to send all voice and data network traffic to his own PC/router or drop the traffic altogether. To protect against such an attack, routing protocols should be secured by using authentication via plain-text authentication or MD5. MD5-based authentication creates a hash value from the key and sends it to the neighbors, where the neighboring router recalculates the hash value with the configured key to verify the integrity of the message. MD5 authentication is supported with the following routing protocols:

- RIPv2
- EIGRP
- OSPF
- BGP4

Router Hardening

Cisco IOS routers can be hardened by disabling services such as finger, TCP and UDP small servers, BootP, and Proxy ARP.

(Firewall) Security for Layers 4 Through 7

Firewalls such as Cisco Adaptive Security Appliance (ASA) enable protection of a Cisco Collaboration network by filtering traffic at Layer 3, Layer 4, and higher layers. In an ideal design, the firewall intercepts the traffic coming from or going to remote sites and the Internet to or from the internal network (data center) and consequently filters based on certain criteria such as source/destination based on subnet, inspection, or ports.

Cisco ASA works in routed mode, transparent mode, or multiple-context mode. In routed mode Cisco ASA appears as a hop in the network—that is, it works at Layer 3. Routed mode supports multiple interfaces and practically all Cisco Collaboration services/applications. For Cisco Collaboration network deployments, Cisco ASA should be configured in a single (default) context as a routed firewall.

Cisco ASA, on the other hand, also works in transparent mode where it is a Layer 2 firewall that acts like a bump in the wire. In transparent mode, Cisco ASA has some limitations pertinent to voice and video traffic:

■ Limited to the use of two traffic forwarding interfaces

■ Lack of support for QoS or Network Address Translation (NAT)

■ Lack of support for multicast routing

■ No site-to-site VPN (except for management of the firewall itself)

Cisco ASA also supports multiple-context mode, also known as *multimode*. In multiple-context mode, the firewall is regarded as multiple separate virtual firewalls on the same physical hardware. However, multiple-mode also has some feature limitations (in addition to those defined for transparent firewall):

■ Lack of support for VPN remote-access services

■ Lack of support for Phone Proxy

■ Lack of support for dynamic routing

Firewall Traversal Mechanisms

Any firewall, including Cisco ASA or an application layer gateway (ALG), is expected to provide certain mechanisms so that voice and video traffic can traverse through the firewall/ALG to reach the destination. Firewall traversal is provided in multiple ways, including NAT traversal, IPsec tunnels, IP ACLs, or port-based ACLs.

NAT Traversal

Almost every firewall (including Cisco ASA) provides NAT services to enable manipulating the IP address or port number, or both, for traffic going out or coming into a network. To ensure that voice traffic is unaltered by NAT, either it should be exempted from NAT or appropriate inspection mechanisms should be applied to enable the firewall to look at the contents of the packets. NAT control can be turned off on Cisco ASA, thereby allowing packets to traverse Cisco ASA unaltered. Also, use of RFC 1918 addresses on internal servers is recommended, where possible, such that globally routable (public) network addresses do not pass through the firewall using a NAT mechanism. NAT/ALG firewalls/devices can inspect signaling in normal mode (that is, TCP/UDP-based

signaling), but with encrypted signaling leveraging Transport Layer Security (TLS), a NAT/ALG-aware firewall is unable to look into the content of packets.

IPsec Tunnels

Site-to-site or remote-access VPN IPsec tunnels can be used to enable NAT exemption. Moreover, if the VPN gateway is placed behind a firewall, the firewall is unable to inspect or modify the contents of the packet within the tunnel. This is an ideal solution when a corporate firewall is required to filter all traffic except voice/video traffic.

IP-Based ACLs

Traffic from the Internet, remote sites, telecommuters, and remote workers can be filtered based on IP ACLs. This allows a modest degree of control on the traffic that traverses through the firewall. In such cases, inspections may still be required to handle voice and video signaling and media traffic.

Port-Based ACLs

Synonymous to IP-based ACLs, port-based ACLs can be used for filtering traffic from/ to an external network to the data center. Port-based ACLs give an administrator or a security engineer a greater degree of control and allow for the least permissive policy. However, port-based ACLs are also the most tedious to configure because every port for a Cisco Collaboration protocol or service needs to be looked at and allowed or denied as per the organization's policy.

In case of voice and video signaling and media traffic, quite a few protocols and ports must be permitted to ensure that the Collaboration services operate appropriately. As discussed in Chapter 3, "Telephony Standards and Protocols," the most commonly used voice and video protocols include SCCP, MGCP, H.323, SIP, RTP, and RTCP.

Moreover, there are other protocols that are used for administration and integration of voice services, such as SSH, TAPI/JTAPI, HTTP, HTTPS, TFTP, DNS, and LDAP.

For a complete list of TCP/UDP ports that are required for firewall traversal for CUCM, refer to "Cisco Unified Communications Manager TCP and UDP Port Usage" at www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/port/9_1_1/CUCM_BK_T2CA6EDE_00_tcp-port-usage-guide-91/CUCM_BK_T2CA6EDE_00_tcp-port-usage-guide-91_chapter_01.html.

For video communications, Cisco Video Communications Server (VCS) can be deployed as Cisco TelePresence VCS Control for use within an enterprise and as the Cisco VCS Expressway for communication with external entities. VCS Expressway enables business-to-business (B2B) communications and includes the features of the Cisco VCS Control with highly secure firewall traversal capability. VCS Expressway can be implemented either on the inside (secure zone) or in the demilitarized zone (DMZ). VCS Expressway firewall traversal is shown in Figure 5-2.
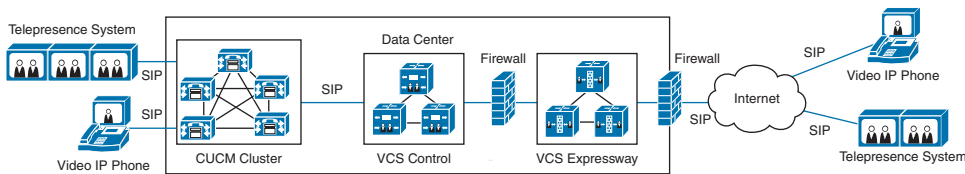
Figure 5-2 *VCS Expressway Firewall Traversal*

It's important to note that SIP and H.323 protocol inspection on the firewall must be disabled. Instead, the firewall should be configured for traversal leveraging requisite ports. For details on the ports that are required for firewall traversal, refer to the deployment guide *Cisco VCS IP Port Usage for Firewall Traversal* (PDF file) at www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X8-1.pdf.

Cisco ASA Proxy Features

Cisco ASA Firewall allows signaling traffic decryption and re-encryption by virtue of the TLS Proxy feature, which enables the inspection engine to look into the packet contents. This alleviates the issue of NAT/ALG-aware firewalls not being able to look into the encrypted (SRTP/TLS) voice and video streams. Cisco ASA supports two major proxy modes:

- **TLS Proxy:** Enables Cisco ASA to decrypt and inspect encrypted signaling before Cisco ASA re-encrypts the signaling to the destination, thereby ensuring that all traffic passing through the firewall is compliant with the organization's security policy. TLS Proxy requires encrypted endpoints on the outside and inside of an ASA-brokered network, which implies that the CUCM cluster within the organization is in mixed mode (a mixed-mode cluster is in secure mode, as explained later in this chapter).

- **Phone Proxy:** Secures remote access for encrypted Cisco Unified IP Phone endpoints and VLAN traversal for Cisco softphones. It enables a remote user to plug in an IP Phone directly to a hotel/home network and make secure calls through the centralized CUCM cluster via the Internet. Moreover, unlike TLS Proxy, Phone Proxy doesn't require internal endpoints to be encrypted; hence, the CUCM cluster within an organization's data center can be in unsecure mode or mixed mode.

Cisco ASA Phone Proxy and TLS Proxy services are not supported with CUCM version 9.x. Instead, Cisco VPN Phone is recommended for secure remote endpoint connection and traversal at the enterprise-edge firewall. Also, as an alternative to the ASA Phone Proxy feature, Cisco Unified Border Element (CUBE) supports Phone Proxy with B2BUA line-side support for CUCM. Phone Proxy is supported with Cisco IOS version 15.3(3) M1 and later on the Cisco Integrated Services Routers Generation 2 (ISR G2) platform. It allows organizations to have phones on the Internet connected to a CUBE at the edge of the enterprise and securely set up signaling/media with phones in the enterprise premises.

Cisco VPN Phone

Cisco VPN Phone is a Cisco Unified IP Phone–based VPN solution that extends the reach of your Cisco Collaboration solution to outside the logical perimeter of your organization. It enables telecommuters, remote workers, and branch office workers to leverage corporate voice and video resources via a phone-based Secure Sockets Layer (SSL) VPN client. Cisco VPN Phone enables remote connectivity with a CUCM cluster for signaling via SSL on the Internet and RTP with an IP Phone within the enterprise premises without extra hardware, as shown in Figure 5-3.
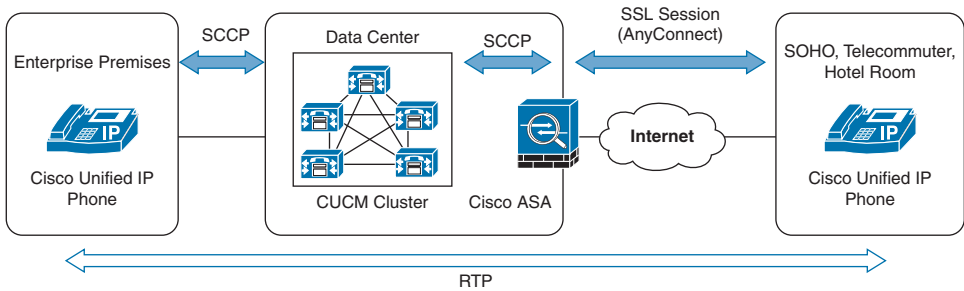
Figure 5-3 *Cisco VPN Phone*

Cisco VPN Phone is supported on 7942G, 7945G, 7962G, 7965G, 7975G, and 99xx series as well as 89xx series Cisco Unified IP Phones. For a complete list of supported IP Phones in a certain CUCM version, go to Cisco Unified CM Administration and choose **Cisco Unified Reporting > System Reports > Unified CM Phone Feature List > Generate a New Report > Feature: Virtual Private Network Client.**

The minimum requirements for implementing Cisco VPN Phone are as follows:

- IP Phone SCCP firmware version 9.0(2)SR1S or later

- CUCM 8.0.1 or later

- Cisco ASA IOS 8.0.4 or later

- AnyConnect VPN Pkg 2.4.1012

- AnyConnect premium license and AnyConnect for Cisco VPN Phone license required for Cisco ASA

Example 5-5 outlines the configuration on Cisco ASA to support Cisco VPN Phone.

Example 5-5 *Cisco ASA VPN Phone Configuration*

```
UCASA(config)# group-policy GroupPolicy1 attributes
UCASA(config-group-policy)# vpn-tunnel-protocol WebVPN
!
UCASA(config)# ip local pool VPN-Phone 10.10.1.200-10.10.1.254 mask 255.255.255.0
!
```

```
UCASA(config)# tunnel-group VPNPhone type remote-access
!
UCASA(config)# tunnel-group VPNPhone webvpn-attributes
UCASA(config-tunnel-webvpn)# group-url https://UCASA.org.corp/PhoneVPN enable
!
UCASA(config)# tunnel-group VPNPhone general-attributes
UCASA(config-tunnel-general)# address-pool VPN-Phone
UCASA(config-tunnel-general)# default-group-policy GroupPolicy1
!
UCASA(config)# webvpn
UCASA(config-webvpn)# enable outside
UCASA(config-webvpn)# anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1
UCASA(config-webvpn)# anyconnect enable
UCASA(config-webvpn)# tunnel-group-list enable
```

The following steps summarize the configuration required on CUCM to support the Cisco VPN Phone feature:

Step 1.   Upload VPN certificates from Cisco ASA to CUCM by going to Cisco Unified CM Operating System Administration and choosing **Security > Certificate Management**. Upload the Cisco ASA self-signed certificate as **Phone-VPN-Trust certificate**.

Step 2.   Configure the VPN gateway by browsing to Cisco Unified CM Administrator and choosing **Advanced Features > VPN > VPN Gateway**.

Step 3.   Create a VPN group under **Advanced Features > VPN > VPN Group**.

Step 4.   Configure the VPN Profile under **Advanced Features > VPN > VPN Profile**.

Step 5.   Assign the VPN group and profile to the Common Phone Profile by going to **Device > Device Settings > Common Phone Profile**.

Step 6.   Configure the Cisco Unified IP Phone with a TFTP server manually and register the IP Phone internally to test and ensure that VPN works, before you give it to a user.

Step 7.   On the Cisco Unified IP Phone, go to **Settings > Security Configuration > VPN Configuration**. Enable **VPN** and use your credentials/certificate to establish a VPN connection.

Application Layer Security

The application layer is the layer at which Cisco Collaboration applications interact with the network, other applications, and endpoints. CUCM, Cisco Unity Connection, and Cisco Unified IM Presence are examples of applications that leverage the OSI model's application layer's services. The following sections address the security mechanisms offered by Cisco Unified CM.

CUCM Security By Default

Cisco has introduced the concept of Security By Default (SBD) from CUCM version 8.0 onward. SBD mandates that every endpoint obtain an Identity Trust List (ITL) file, which is a leaner version of a Certificate Trust List (CTL) file.

Trust Verification Service (TVS) is the core component of the SBD feature. TVS runs on all CUCM servers in the cluster and authenticates certificates on behalf of Cisco Unified IP Phones. TVS certificates, along with a few other key certificates, are bundled in the ITL file. Security By Default provides three basic functions for supported Cisco Unified IP Phones:

- Default authentication of the TFTP downloaded files (configuration, locale, and so on)
- Optional encryption of the TFTP configuration files
- Certificate verification for the phone-initiated HTTPS connections using a remote certificate trust store on CUCM and TVS

ITL is similar to CTL, but ITL does not need any security feature to be enabled explicitly. Moreover, ITL is not a replacement for CTL; it is for initial security so that endpoints can trust the CUCM. To encrypt signaling or media, CTL is still required. The ITL file is created automatically when the cluster is installed. The CUCM TFTP server's private key is used to sign the ITL file. When a CUCM server/cluster is in non-secure mode, the ITL file is downloaded on every supported Cisco Unified IP Phone; however, when a CUCM server/cluster is in mixed mode, the CTL file is downloaded followed by the ITL file. The contents of an ITL file can be viewed by using the CUCM OS CLI command **admin: show itl**.

CUCM Security Modes

CUCM provides two security modes:

- Non-secure mode (default mode)
- Mixed mode (secure mode)

Non-secure mode is the default mode when a CUCM cluster (or server) is installed fresh. In this mode, CUCM cannot provide secure signaling or media services. To enable secure mode on a CUCM server/cluster, the Certificate Authority Proxy Function (CAPF) service must be enabled on the publisher and the Certificate Trust List (CTL) service must be enabled on the publisher and subscribers. Then the cluster can be changed from non-secure mode to mixed mode. The reason it is known as *mixed mode* is that in this mode CUCM can support both secured and non-secured endpoints. For endpoint security, Transport Layer Security (TLS) is used for signaling and Secure RTP (SRTP) is used for media.

To convert a CUCM cluster into mixed mode, follow these steps:

Step 1.   In Cisco Unified CM Administration, choose **Serviceability > Tools > Control Center - Feature Services** and enable CAPF and CTL services on the CUCM publisher and CTL service on all CUCM subscribers.

Step 2.   Restart CCM and TFTP services on every node where these services are enabled.

Step 3.   Return to CUCM Administration and choose **Application > Plugins** to download and install the CTL Client plug-in for Windows.

Step 4.   After the CTL client is installed, log in with the IP address of the publisher and the CUCMAdministrator credentials. Follow the installation prompts.

Step 5.   Click the **Set Cisco Unified CallManager Cluster to Mixed Mode** radio button.

Step 6.   Insert the USB eToken when prompted by the CTL client wizard, and click **OK**.

Step 7.   The CTL client wizard prompts for a second eToken, removes the first eToken, and inserts the second USB eToken. Click **OK**. Click **Finish**. When prompted for the password for the eToken, enter the default password **Cisco123**.

Step 8.   After the CTL client wizard completes signing certificates on each server in the cluster, it reminds you to restart the CCM and TFTP services on whichever servers they are configured. Click **Done**. Restart the CCM and TFTP services on all servers where they are enabled and activated.

You can verify the cluster's conversion to mixed mode by going to **System > Enterprise Parameters**. The parameter Cluster Security Mode should be 1, which indicates that the cluster is running in mixed mode.

CTL Client and CTL File

The CTL client, as discussed earlier, is a plug-in that can be downloaded from the CUCM Administration GUI and that runs on a Windows PC to convert a CUCM cluster from non-secure mode to mixed mode. A CTL client signs various certificates. A CTL file contains the following:

- Server Certificate
- Public Key
- Serial Number
- Signature
- Issuer Name
- Subject Name
- Server Function

- DNS name

- IP address for each server

A CTL file (downloaded to Cisco Unified IP Phones and softclients) consists of the following entries (server entries or security tokens):

- CUCM

- Cisco TFTP

- Alternate Cisco TFTP Server (if any)

- CAPF

- System Administrator Security Token (SAST)

- Cisco ASA Firewall

Figure 5-4 shows the contents of a typical CTL file.
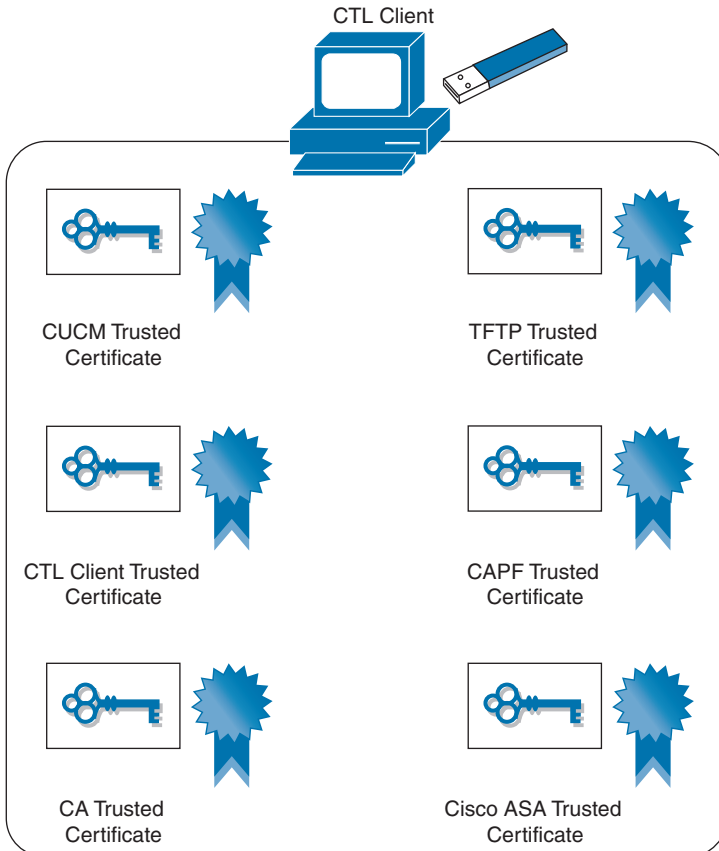
Figure 5-4   *CTL File Contents*

The contents of a CTL file can be viewed by issuing the CUCM OS CLI command **admin: show ctl.**

Cisco Unified IP Phone Certificates

Cisco Unified IP Phone certificates come in two flavors:

- Manufacturer Installed Certificate (MIC)
- Locally Significant Certificate (LSC)

Cisco manufacturing is the source for the MIC. Cisco installs the MIC in nonerasable, nonvolatile memory on a Cisco Unified IP Phone. It is available in all new phone models, and the root Certificate Authority (CA) is Cisco Certificate Authority. On the other hand, the CAPF service is the source (root) of the LSC, which must be installed by the UC administrator in erasable phone memory. The LSC can be signed by an organization's internal CA or an external trusted CA. Figure 5-5 depicts the difference between the MIC and the LSC.
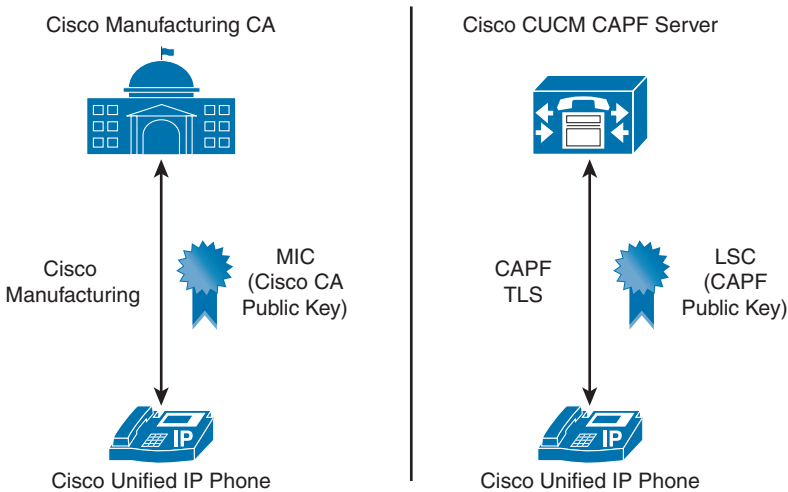
Figure 5-5 *Cisco MIC vs. LSC*

SRTP and TLS

After the endpoints (IP Phones) are secure, CUCM can establish TLS with the endpoints, and the endpoints can negotiate SRTP among themselves. Cisco voice gateways also support encryption as follows:

- MGCP gateway with SRTP package and IPsec tunnel to CUCM (or default gateway device for CUCM). IPsec is for protection of signaling, which in the case of MGCP is in clear text by default.

- H.323 gateway with certificates exchanged with CUCM for SRTP and IPsec for protecting signaling.

- SIP gateway with secure SIP trunk leveraging TLS to protect signaling.

Figure 5-6 gives insight to TLS signaling and SRTP media flow among CUCM, endpoints, and gateways.
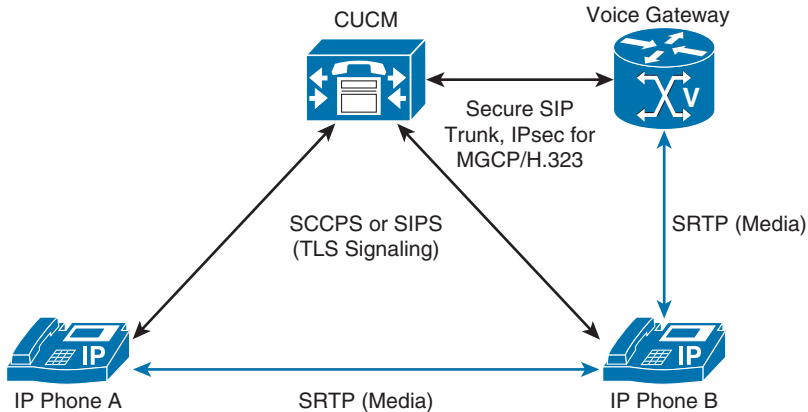
Figure 5-6   *TLS and SRTP Call Flow Between CUCM, Endpoints, and Gateways*

Preventing Toll Fraud

Toll fraud is a chronic issue that has impacted the PSTN and IP worlds alike. Toll fraud can be summarized as the illicit use of a telephony system to make long-distance (international) calls without any accountability. To prevent toll fraud in a Cisco Collaboration network, you can employ various tools:

- CUCM class of service (CoS)

- Voice gateway toll fraud prevention application

- Voice gateway class of restriction (CoR)

- Cisco Unity Connection restriction rules

CUCM Class of Service

CUCM CoS can be enabled via multiple tools, listed and described in Table 5-2.

Table 5-2 *CUCM CoS Components*

CUCM CoS Component	Description
Partitions and calling search spaces (CSS)	Provide segmentation and control to the number that can be called, or vice versa. As a leading practice recommendation, either disable Call Forward All or limit it to an extension within your Collaboration network. Call Forward Busy and Call Forward No Answer should also be limited to internal partitions only. For phones with extension mobility, a logged-out CSS should be restricted to internal and emergency partitions only.
Time-of-Day routing	Allows certain partitions to be active during a preset time period during a day and after this period; these partitions become inactive automatically. Helps restrain calls made to national and international numbers after business hours. See Chapter 4 for more details.
Forced Authorization Code (FAC) and Client Matter Code (CMC)	Used to control the access to international and long distance calls. FAC/CMC forces a user to enter a predetermined code to proceed with a call hitting a route pattern that has FAC enabled. Both FAC- and CMC-processed calls are logged to CUCM Call Detail Records (CDR).
Block off-net to off-net transfers	Allows/disallows off-net to off-net transfers based on a clusterwide service parameter Block OffNet to OffNet Transfer. When enabled, CUCM blocks any off-net to off-net call transfers from endpoints, thereby minimizing the risk of anyone misusing the feature for transferring local PSTN calls to international destinations.
Ad hoc conference restriction	Ad hoc conference calls can be dropped when the originator hangs up. This is achieved by setting the Drop Ad Hoc Conference service parameter to **When Conference Controller Leaves** under **Clusterwide Parameters > Feature > Conference**. This ensures that the other parties (such as external users) cannot initiate a call to another external number.
Route filters	Can be deployed to filter any unwanted area codes as well as calls to known paid/premium numbers.

Cisco Voice Gateway Toll-Fraud Prevention Application

Cisco IOS voice gateways with Cisco IOS 15.1(2)T and later come (by default) enabled with an application that helps stops toll-fraud attempts. This new feature is known as *Call Source Authentication*, which is the default behavior of a toll-fraud prevention feature.

By virtue of this feature, the router automatically adds the destination IP address(es) defined as an IPv4 target in a VoIP dial peer to the trusted source list. This feature is configurable via the global **voice service voip** command:

```
UCRouter(config)# voice service voip
UCRouter(conf-voi-serv)# ip address trusted authenticate
```

Voice Gateway Class of Restriction

Class of restriction (CoR) is analogous to CUCM partitions and CSSs. CoR is implemented at either dialpeers or ephone-dns on a voice gateway. The **dial-peer cor custom** command is equivalent to creating a CUCM partition, whereas **dial-peer cor list** is equivalent to creating a CUCM CSS. CoR can be implemented on SIP and H.323 gateways and while a gateway is in SRST mode. Example 5-6 illustrates CoR configuration on a Cisco IOS gateway.

Example 5-6   *Cisco IOS Gateway CoR Configuration*

```
UCRouter(config)# dial-peer cor custom
UCRouter(config-dp-cor)# name emergency
UCRouter(config-dp-cor)# name local
UCRouter(config-dp-cor)# name national
!
UCRouter(config)# dial-peer cor list emergency
UCRouter(config-dp-corlist)# member emergency
!
UCRouter(config)# dial-peer cor list local
UCRouter(config-dp-corlist)# member emergency
UCRouter(config-dp-corlist)# member local
!
UCRouter(config)# dial-peer cor list national
UCRouter(config-dp-corlist)# member emergency
UCRouter(config-dp-corlist)# member local
UCRouter(config-dp-corlist)# member national
!
UCRouter(config)# dial-peer voice 911 pots
UCRouter(config-dial-peer)# corlist outgoing emergency
<output-omitted for brevity>
!
UCRouter(config)# dial-peer voice 7 pots
UCRouter(config-dial-peer)# corlist outgoing local
<output-omitted for brevity>
!
```

```
UCRouter(config)# dial-peer voice 11 pots
UCRouter(config-dial-peer)# corlist outgoing national
<output-omitted for brevity>
```

Cisco Unity Connection Restriction Rules

Cisco Unity Connection can transfer calls from voice mail to the PSTN. This feature can be exploited for conducting toll fraud. To ensure that your Cisco Unity Connection system denies outgoing calls and/or transfers, configuring the following restriction rules is recommended:

- Create a non-default call-restriction rule for calls and call transfers that denies everything starting with the outside (PSTN) access code; for example, deny 9* transfers from Cisco Unity Connection to PSTN in the United States and 0* in Europe.

- Add restriction table patterns to match appropriate trunk access codes for all phone system integrations.

- Restrict the numbers that can be used for system transfers and for Audio Messaging Interchange Specification (AMIS) message delivery.