Cisco Virtual Office: Secure Voice and Video

The scope of this deployment guide is to provide detailed design and implementation information for deploying highly secure voice and video with Cisco® Virtual Office. Please refer to the Cisco Virtual Office overview for further information about the solution, its architecture, and all the related components.

Contents

1. Introduction

Cisco Virtual Office (CVO) is a highly secure end-to-end solution that brings enterprise-quality voice, video, wireless, and data into the home and remote offices. It is designed to bring unified communications to employees' home offices, increasing their satisfaction and productivity. This deployment guide covers the deployment of highly secure, voice and video in a CVO environment. For a complete list of supported and recommended products and images, please refer to the CVO Datasheet.

2. 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 of ISR G2 and establishing the trust and authorization of the end devices. Network security will be provided using the Cisco ISR G2 sitting behind the ISP-provided broadband modem. The IP Security (IPsec) with Triple Digital Encryption Standard (3DES) or Advanced Encryption Standard (AES) for encryption is used by ISR G2 to make the connection secure.

The CVO uses hierarchical QoS mechanism to provide shaping and Low Latency Queuing (LLQ), allowing for simultaneous use of voice, video and data services without compromising on the quality of services, and allowing for the prioritization of real-time and latency-sensitive traffic such as voice and video. The Network Based Application Recognition (NBAR) is also used to perform deep packet analysis. The NBAR determines the protocol used in the packet such as SIP, SCCP, H.323, etc. By using NBAR and QoS, the Cisco Virtual Office router makes sure that voice and video services are correctly prioritized and external heavy bandwidth applications do not cause degradation of the quality of voice and video.

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

2.1 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 entailed by the use of DMVPN in CVO, the bandwidth on each direction should be at least 128 kbps for G.711 and 80 kbps for G.729. However, to accommodate for data traffic and ISP network congestion, it is recommended to have a minimum of 256kbps in each direction to avoid any voice related problems.

Video calls consume lot more bandwidth than voice calls and require broadband services that can provide high uplink speed. The H263 and H264 are the most popular codecs that are used by video end points. H264 codec is used by default in Cisco supported end points. These codecs require different bandwidth depending on the resolution, size and the Frames per Second (FPS) used by the video end points. For example, a minimum 1Mbps uplink and downlink will be required for VGA 640x480 resolution using 30 fps. Similarly, for High Definition 720P video calls with 1280x720 resolutions and 30 fps will require minimum 2Mbps bandwidth in each direction.

2.2 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 CVO spoke router so that voice, video and other essential traffic gets a higher priority to use the uplink bandwidth. Regular data packets are given a lower priority.

If the CVO 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 CVO spoke router such as 881 or 891 was used to match the traffic using a Cisco IOS Software feature called Network Based Application Recognition (NBAR). NBAR allows the network to provide differentiated services to each application. It ensures performance for mission critical applications. One can provide absolute priority and guaranteed bandwidth to his mission-critical applications and then do the respective packet matching.

```
class-map match-any NBAR_MAP_TP
 match protocol telepresence-media
 match protocol telepresence-control
class-map match-any NBAR_MAP_Tandberg
 match access-group name NBAR_MAP_Tandberg
class-map match-any NBAR_MAP_Video
  match access-group name Movi
  match access-group name CUVA
  match protocol rtp payload-type "97"
  match access-group name NBAR_MAP_Video
class-map match-any NBAR_MAP_VoIP
 match access-group name Cisco_phone_voice_video
 match protocol rtp audio
class-map match-any NBAR_MAP_Signaling
 match protocol skinny
 match protocol sip
class-map match-all NBAR_MAP_Scavenger
 match access-group name NBAR_MAP_Scavenger
policy-map NBAR_SET
class NBAR_MAP_TP
  set ip dscp cs2
class NBAR_MAP_Tandberg
```

```
  set dscp cs4
class NBAR_MAP_Video
  set dscp cs2
class NBAR_MAP_VoIP
  set ip precedence 5
class NBAR_MAP_Signaling
  set ip precedence 3
class NBAR_MAP_Scavenger
  set ip precedence 1
class class-default
  set dscp default
```

2.3 Authentication

Cisco Virtual Office routers can be configured with user/device authentication such as Authentication Proxy (auth-proxy) and IEEE 802.1x. With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecure ACS, or RADIUS, or TACACS+ authentication servers . The 802.1x-based authentication is used to authenticate hosts connecting to the Ethernet switch ports of the CVO router. Deploying this feature in CVO ensures that only authenticated hosts can gain access to the VPN. Unauthenticated hosts can only access the Internet. This is particularly helpful for separating "spouse and kids" computers from employee computers. When 802.1x is enabled, Cisco IP phone can use 802.1x to authenticate. The Cisco Discovery Protocol (CDP) can be used to bypass 802.1x. MAC authentication bypass (MAB) can also be used to bypass 802.1x. For 3rd party phones, MAB can be used to authenticate. When 802.1x is not enabled, CDP can still be used to detect Cisco IP phones and place them on the voice VLAN (separate from the data VLAN).

The following 881 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.

```
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 mac-auth-bypass
 dot1x timeout quiet-period 1
 dot1x timeout tx-period 1
 dot1x max-req 1
 dot1x reauthentication
 dot1x guest-vlan 20
 spanning-tree portfast
```

Note: The same configuration defined in interface F0 should be configured on the rest of the switchports. The command “dot1x mac-auth-bypass” should be configured to enable MAB. In addition, for non-cisco phones, the correct voice vlan should be pushed from the ACS server and ‘device-traffic-class=voice’ av-pair should be configured in ACS as part of the 802.1x MAB authorization.

2.4 Configuration File

When Cisco IP phone or Cisco Unified Personal Communicator (CUPC) 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 option 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 > <netbios-name-server <Corp. NETBIOS servers>
update arp
```

3. 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.

3.1. 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.

3.2. SIP Based Phone Deployment

The SIP IP phone deployment is the same as the SCCP deployment. The Cisco IP phones with SIP support uses tcp and udp port 5060 to communicate with primary and secondary Cisco Unified Communications Manager. Some of the Cisco phones such as 7960G, 8945, 6921 and 6941 supports both skinny and sip images. The port 5060 must be opened in the CVO to register the IP phones to CUCM.

3.3 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.

3.4 SoftPhone Deployment

Cisco Unified Personal 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.

3.5 Video End Points Deployment

3.5.1 Cisco Telepresence E20/EX60/EX90

The CVO supports multiple Tandberg video end points. However, the recommended end points are E20, EX60 and EX90. The IP Video Phone E20 is a business quality personal video conferencing unit that allows for a fully integrated video experience. The CUCM 8.5 and above is required to support native connectivity for E20. A minimum of 1.0Mbps bandwidth is required to make standard video calls using E20. E20 can support a maximum resolution of 768 x 448@30fps (w448p) and requires minimum of 1.5Mbps to support high resolution video calls.

The EX Series provides a high quality HD 1080P 30fps video. The EX series streamlines your desk and your communication with one PC screen, video and phone. The CUCM 8.6 and above is required to provide a native support for EX series. The EX series requires high bandwidth due to its high resolution. A minimum of 3.5 Mbps bandwidth is required for HD 720P calls. For HD 1080p, a minimum bandwidth of 6Mpbs is required for good quality video calls.

Cisco Telepresence call control manager VCS can also be used to provide call control service for voice and video for the above video endpoints. Cisco VCSX 6.1 and above should be used to deploy these endpoints.

Note: The Telepresence software Release TC4.1 and later builds should be used for video points to work with CUCM 8.5 and VCSX 6.1.

The above Telepresence video end points use the multiple ranges of UDP ports that should be matched by the QoS policy. Following QOS policies must be applied on the CVO spoke to provide good quality video.

```
ip access-list extended NBAR_MAP_Tandberg
 permit udp any range 2326 2485 any dscp 35
 permit udp any range 49152 65535 any dscp 35
 permit udp any range 46000 49000 any dscp 35
class-map match-any NBAR_MAP_Tandberg
 match access-group name NBAR_MAP_Tandberg
policy-map NBAR_SET
class NBAR_MAP_Tandberg
  set dscp cs4
class-map match-any QOS_TP_Tandberg
 match ip dscp cs2
 match ip dscp cs4
 match ip precedence 4
policy-map CSM_POLICY_MAP_HR_1
 class class-default
 shape average 6144300 153600 153600
policy-map CSM_POLICY_MAP_1
 class QOS_TP_Tandberg
  bandwidth 4915
  queue-limit 256 packets
  class class-default
  no fair-queue
policy-map CSM_POLICY_MAP_HR_1
 class class-default
   service-policy CSM_POLICY_MAP_1
```

In case Auth Proxy is being enabled, then following ports must be opened in ACL “auth_proxy_inbound_acl”.

```
ip access-list extended auth_proxy_inbound_acl
 permit udp any range 2326 2485 any
 permit udp any range 46000 49000 any
 permit udp any range 49152 65535 any
 permit udp any any range 5060 5061
 permit tcp any range 5060 5061 any (Only one way voice/video if not added)
 permit tcp any any range 5060 5061
 permit udp any range 16384 32784 any
 permit tcp any any eq 6970 (only for Tandberg E20 Series)
!
```

3.5.2 Cisco CP-9971

The Cisco Unified IP Phone 9971 delivers high-quality advanced interactive multimedia communications. The phone has large backlit, vibrant high-resolution 640 x 480 pixel fully-adjustable color display. The phone requires Cisco Unified Video Camera to provide interactive video. The phone has both wireless and Bluetooth and provides high-definition voice (HD voice) to provide greater clarity in communications.

The CP-9971 supports the SIP protocol. Hence, if Auth Proxy is being enabled then both 5060 and 5061 port must be opened in the auth proxy access list to register the phone with the CUCM. The following configurations needed to be added in the Auth Proxy access list to open the relevant ports:

```
permit udp any any range 5060 5061
permit tcp any any range 5060 5061
```

3.5.3 Cisco CP-8945

The Cisco Unified IP Phone 8945 delivers comprehensive multimedia features and capabilities, including real-time video communications and low power consumption. The phone has a built-in, VGA-quality video camera that supports up to 30 frames per second and has a high-resolution 5-inch color display (VGA). The phone supports both SIP and SCCP image. In case the SIP image is used and Auth Proxy is enabled then both 5060 and 5061 port must be opened in the access list to register the phone with the CUCM.. Please refer to access-lists configuration required for CP-9971.

3.5.4 Cisco Movi

Movi offers a cost-effective, easy to use video solution. It allows teleworkers to stay visually connected to colleagues, customers or suppliers. With only an existing computer and a USB Camera, thousands of users in a video-enabled enterprise can connect from public spaces or remote offices whenever they need. Compared with consumer-based PC video solutions, Movi offers unparalleled quality, reliability and ease of use. Movi is a standards-based solution, and it is interoperable with the rest of an enterprise video deployment.

Movi is a SIP based client. If Auth proxy is enabled then some additional ports need to be open in order to make the device register with the CUCM. The following configurations needed to be added in the Auth Proxy access list to open the relevant ports:

```
permit udp any range 2326 2485 any

permit udp any any range 5060 5061

permit tcp any range 5060 5061 any

permit tcp any any range 5060 5061

permit udp any range 16384 32784 any

permit udp any range 14040 14240 any (required for MOVI)
```

3.5.5 Cisco UC Integration for Microsoft Office Communicator (CUCIMOC)

CUCIMOC is a soft phone client integration for Microsoft Office Communicator (MOC). It is used for both voice and video calls. CUCIMOC client can be integrated with both SCCP and SIP phones. The user can make voice and video calls through CUCI MOC soft phone or through desk phone. If Auth proxy is enabled then some additional ports need to be open in order to make the device register with the CUCM. The following configurations needed to be added in the Auth Proxy access list to open the relevant ports:

```
permit udp any range 2326 2485 any

permit udp any any range 5060 5061

permit tcp any range 5060 5061 any

permit tcp any any range 5060 5061

permit udp any range 16384 32784 any
```

3.6 Wireless IP Phone Deployment

The Cisco Unified IP Phone CP-9971 have a built-in 802.11a/b/g Wireless-fidelity (Wi-Fi) radio. The phone can be configured as either wired or wireless mode. An external power should be connected to phone to enable Wi-Fi and configure wireless settings. If the phone is getting power through PoE then the Wi-Fi will not be enabled. This phone supports different wireless authentication such as Wired Equivalent Privacy (WEP), and LEAP, EAP-FAST etc. 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.

4. CVO Voice and Video Traffic Classification

Following traffic classifications must be followed for Video end points.

End Points	NBAR Match	QOS Policies
CIUS	UDP/16384-32784 for Voice (Prec 5) Payload 97 for Video (CS4)	Priority Queue (128K) CBFWQ (384K)
CUVA	UDP/5445; CS4	CBFWQ (384K)
CP-9900 Series CP-8900 Series	UDP/16384-32784 for Voice (Prec. 5) Payload 97 for Video (CS4)	Priority Queue (128K) CBFWQ (384K)
MOVI	UDP/14040-14240 (CS2)	CBFWQ (1Mbps)
Tandberg MXP1700	UDP/46000-49000 DSCP CS2	CBFWQ (1Mbps)
Tandberg E20	UDP/2326 -2485 (CS4) DSCP CS2	CBFWQ (1Mbps)
Tandberg EX Series	UDP/2326-2485 DSCP CS4	CBFWQ (1Mbps)

5. Appendix

5.1 CVO QOS Policies and Configurations

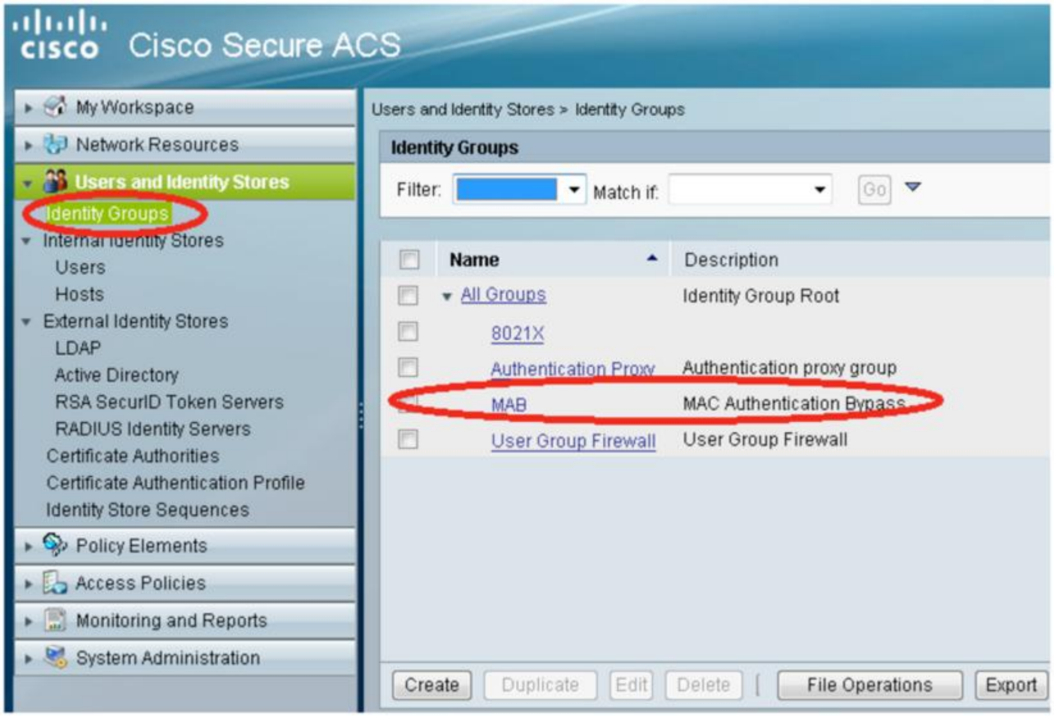
The section lists down the recommended QOS policies for the CVO spoke (ISR G2). These QOS policies must be applied on the CVO spoke (ISR G2) to provide good quality of Telepresence Video and Voice phones.

```
!************************* NBAR::ACL *********************************
ip access-list extended NBAR_MAP_Scavenger
 permit tcp any any eq 16384
ip access-list extended NBAR_MAP_Tandberg
 permit udp any range 2326 2485 any dscp 35
 permit udp any range 49152 65535 any dscp 35
 permit udp any range 46000 49000 any dscp 35
ip access-list extended NBAR_MAP_Video
 permit udp any range 2326 2485 any dscp 33
 permit udp any range 49152 65535 any dscp 33
 permit udp any range 46000 49000 any dscp 33
!************************* NBAR::Class-map ****************************
class-map match-any NBAR_MAP_Tandberg
 match access-group name NBAR_MAP_Tandberg
class-map match-any NBAR_MAP_Video
  match access-group name Movi
  match access-group name CUVA
  match protocol rtp payload-type "97"
  match access-group name NBAR_MAP_Video
class-map match-any NBAR_MAP_VoIP
 match access-group name Cisco_phone_voice_video
 match protocol rtp audio
class-map match-any NBAR_MAP_Signaling
 match protocol skinny
 match protocol sip
class-map match-all NBAR_MAP_Scavenger
 match access-group name NBAR_MAP_Scavenger


!************************* NBAR::Policy-map ****************************
policy-map NBAR_SET
class NBAR_MAP_Tandberg
  set dscp cs4
class NBAR_MAP_Video
  set dscp cs2
class NBAR_MAP_VoIP
  set ip precedence 5
class NBAR_MAP_Signaling
  set ip precedence 3
class NBAR_MAP_Scavenger
  set ip precedence 1
class class-default
  set dscp default
!********************** QoS::ACL ******************************
ip access-list extended CSM_QOS_ACL_1
 permit udp any any eq isakmp

!********************** QoS::Class-map **************************
class-map match-any CSM_CLASS_MAP_1
 match ip dscp cs3
 match ip precedence 3
```

```
class-map match-any CSM_CLASS_MAP_2
 match access-group name CSM_QOS_ACL_1
 match ip precedence 7
 match ip precedence 6
class-map match-any CSM_CLASS_MAP_3
 match ip dscp ef
 match ip precedence 5
class-map match-any QOS_TP_Tandberg
 match ip dscp cs2
 match ip dscp cs4
 match ip precedence 4
!********************** QoS::Policy-map ************************
policy-map CSM_POLICY_MAP_HR_1
 class class-default
 shape average 6144300 153600 153600
policy-map CSM_POLICY_MAP_1
 class CSM_CLASS_MAP_1
   bandwidth 32
   queue-limit 128 packets
 class CSM_CLASS_MAP_2
   bandwidth 32
   queue-limit 128 packets
 class CSM_CLASS_MAP_3
   priority 128
 class QOS_TP_Tandberg
   bandwidth 4915
   queue-limit 256 packets
  class class-default
policy-map CSM_POLICY_MAP_HR_1
 class class-default
    service-policy CSM_POLICY_MAP_1
int Fastethernet4 (Wan Interface)
   service-policy output CSM_POLICY_MAP_HR_1
int vlan10
   service-policy input NBAR_SET
```

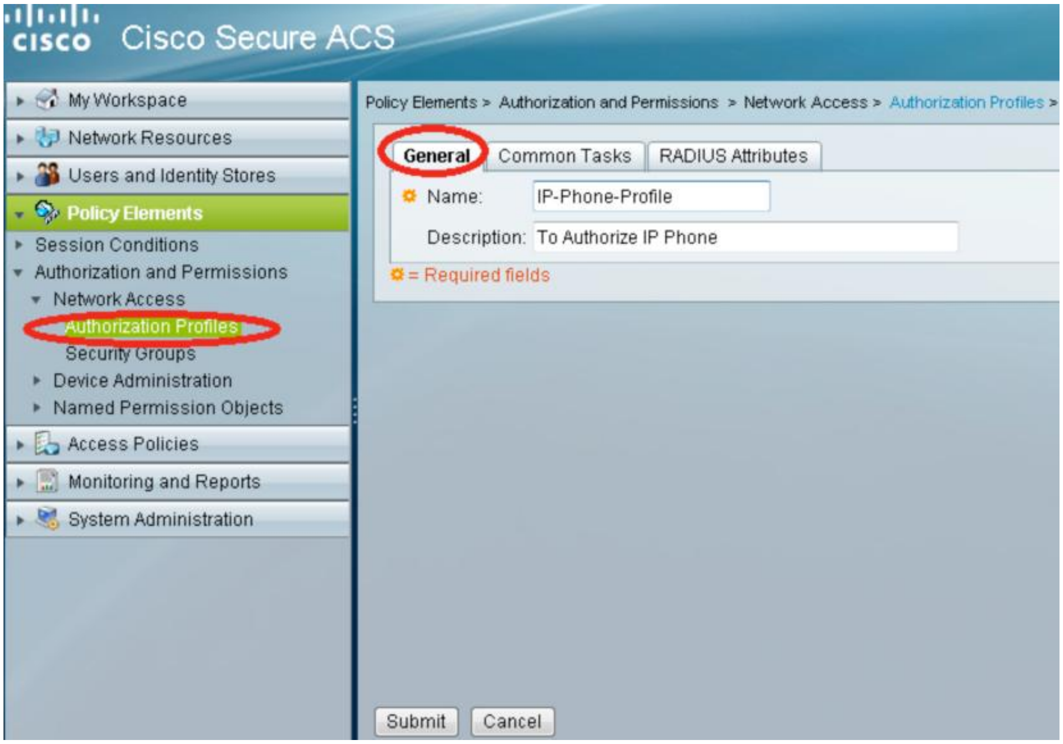
5.2 Creating MAB Authorization Policies in ACS

Create a group MAB under ACS in section Users and identity stores:



	Name	Description
□	All Groups	Identity Group Root
□	8021X	
□	Authentication Proxy	Authentication proxy group
	MAB	MAC Authentication Bypass
□	User Group Firewall	User Group Firewall

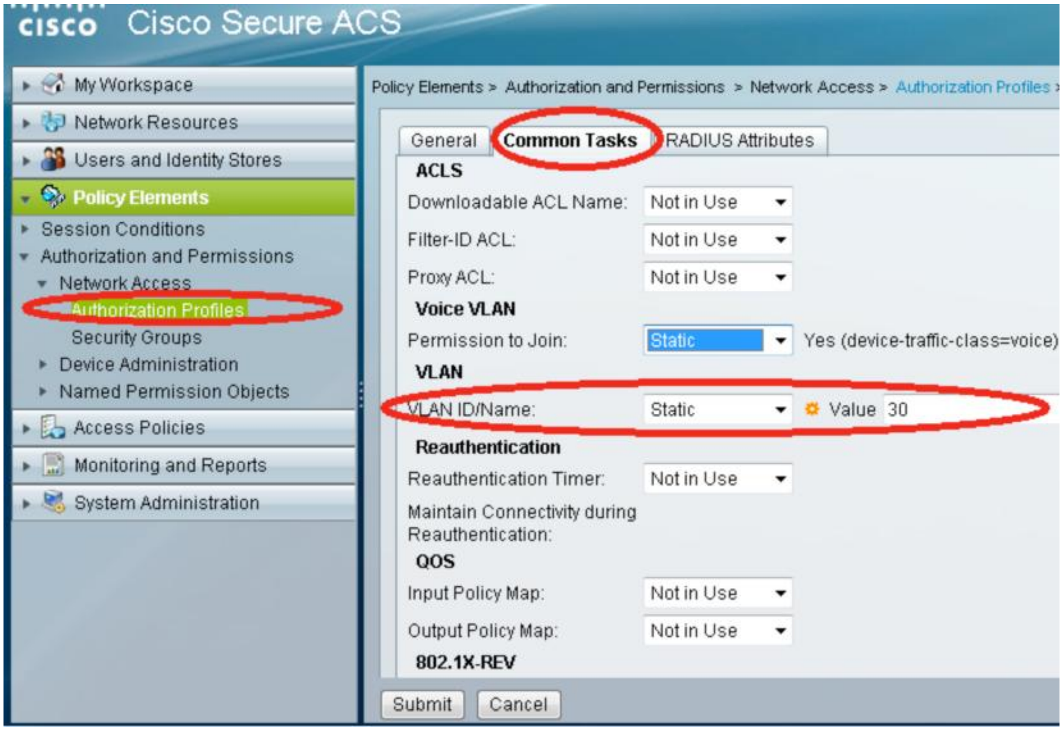
Create a Network Authorization Profile for Voice and Telepresence phones under network Access:



Name: IP-Phone-Profile

Description: To Authorize IP Phone

Under the Tab “Common Tasks”, select Vlan ID as Static and put VLAN value such as 30. Change Voice Vlan to Static.



ACLS

Downloadable ACL Name: Not in Use

Filter-ID ACL: Not in Use

Proxy ACL: Not in Use

Voice VLAN

Permission to Join: Static Yes (device-traffic-class=voice)

VLAN

VLAN ID/Name: Static Value 30

Reauthentication

Reauthentication Timer: Not in Use

Maintain Connectivity during Reauthentication:

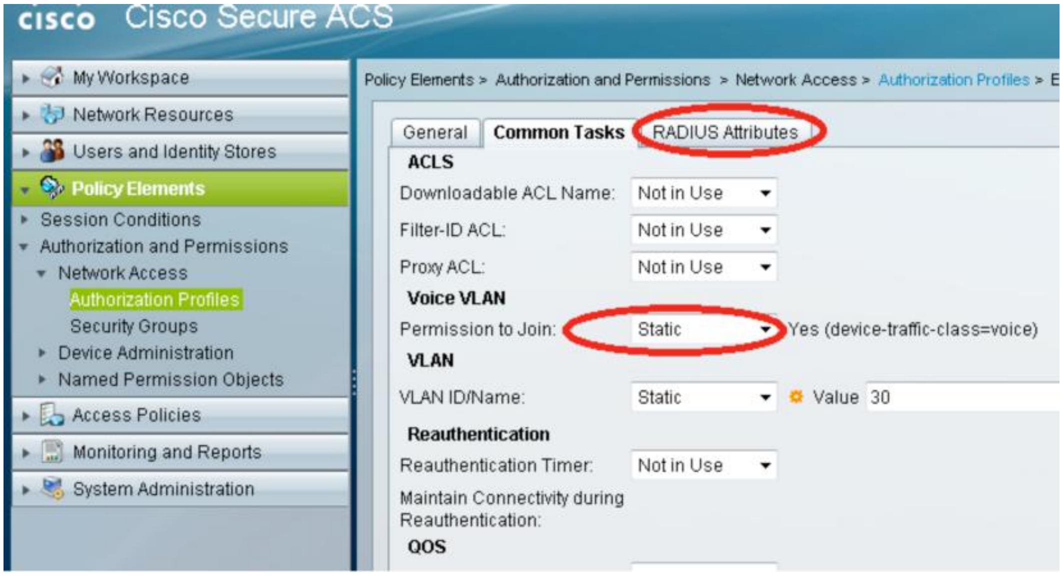
QOS

Input Policy Map: Not in Use

Output Policy Map: Not in Use

802.1X-REV

Under the Tab “Radius Attributes”, select dictionary type as “Radius-Cisco”:



ACLS

Downloadable ACL Name: Not in Use

Filter-ID ACL: Not in Use

Proxy ACL: Not in Use

Voice VLAN

Permission to Join: Static Yes (device-traffic-class=voice)

VLAN

VLAN ID/Name: Static Value 30

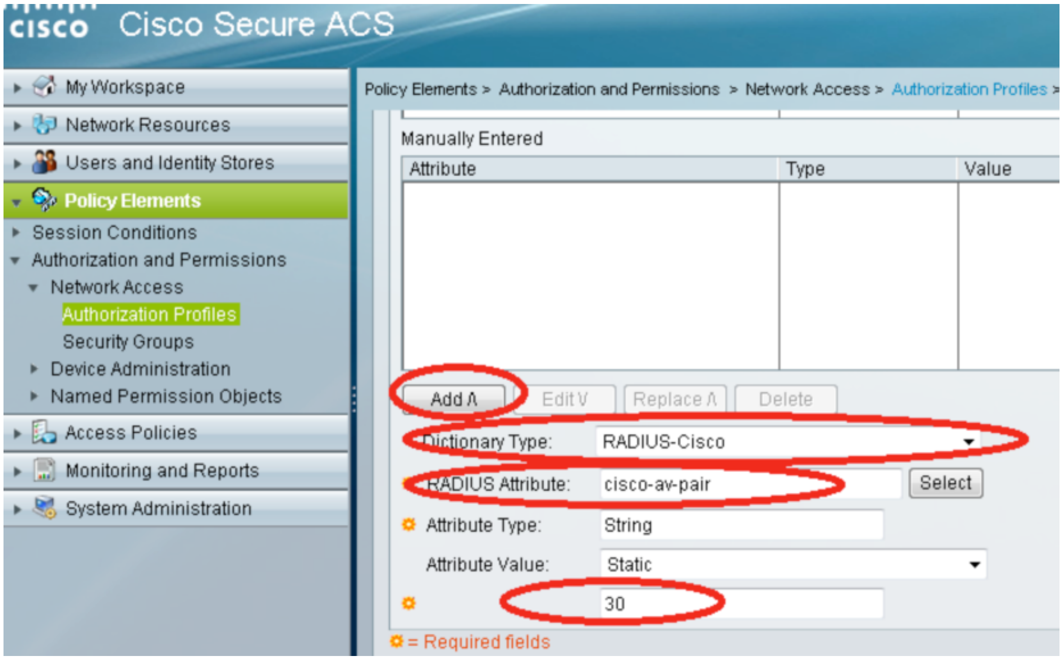
Reauthentication

Reauthentication Timer: Not in Use

Maintain Connectivity during Reauthentication:

QOS

Select Dictionary type “RADIUS-Cisco” and cisco-av-pair under “Radius Attribute”. Assign the value of cisco-av-pair as Vlan ID i.e. 30. Press Add button and then submit.



Manually Entered

Attribute	Type	Value

Dictionary Type: RADIUS-Cisco

RADIUS Attribute: cisco-av-pair

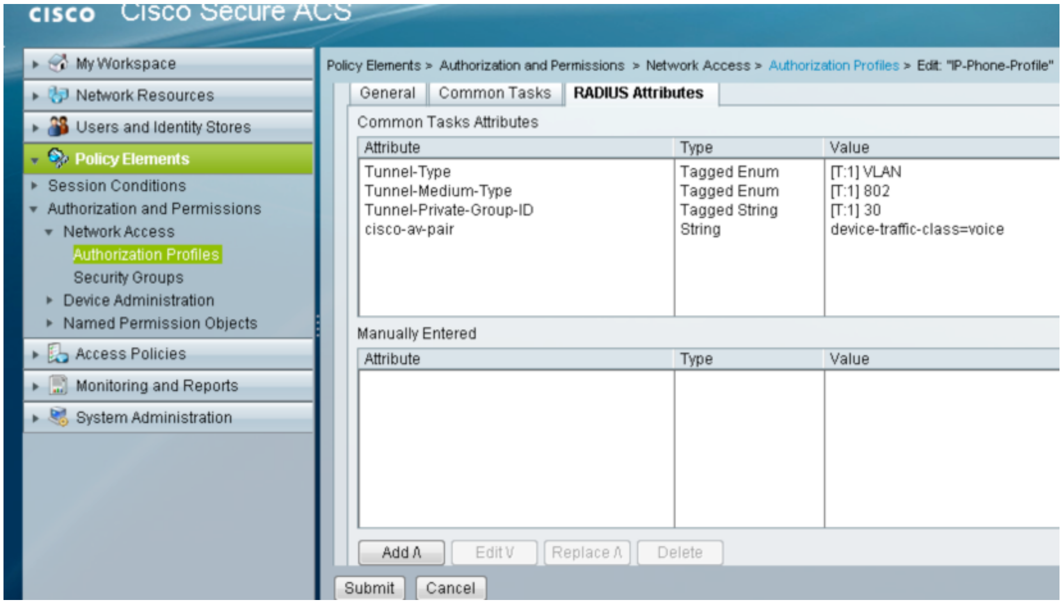
Attribute Type: String

Attribute Value: Static

30

= Required fields

Here is the snapshot of ACS after the profile configuration.



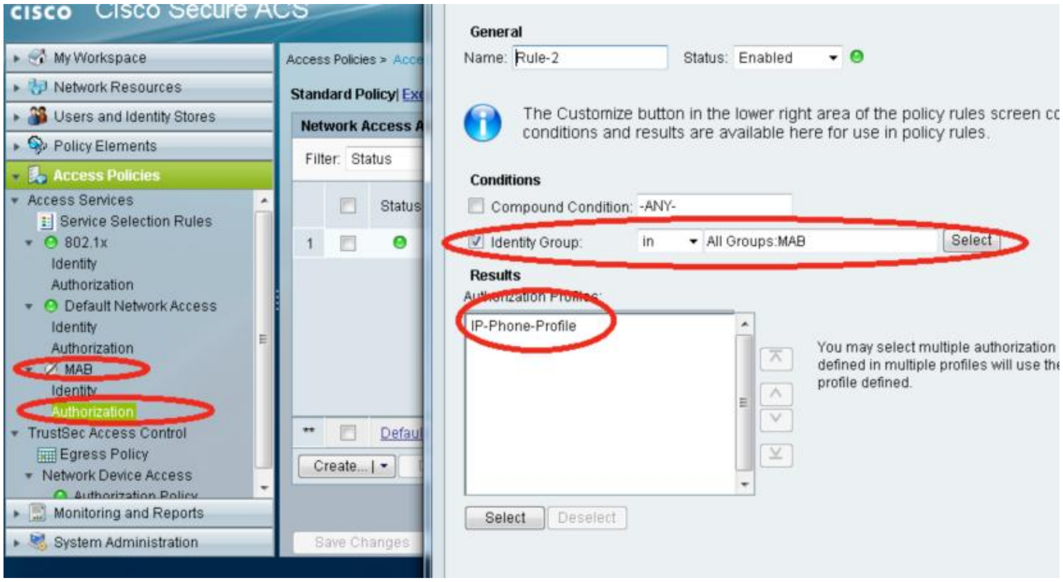
Common Tasks Attributes

Attribute	Type	Value
Tunnel-Type	Tagged Enum	[T:1] VLAN
Tunnel-Medium-Type	Tagged Enum	[T:1] 802
Tunnel-Private-Group-ID	Tagged String	[T:1] 30
cisco-av-pair	String	device-traffic-class=voice

Manually Entered

Attribute	Type	Value

Create a MAB Authorization under Access Services. Create a rule and select IP-Phone-Profile:



General

Name: Rule-2 Status: Enabled

The Customize button in the lower right area of the policy rules screen cc
conditions and results are available here for use in policy rules.

Conditions

☐ Compound Condition: -ANY-

☑ Identity Group: in All Groups:MAB Select

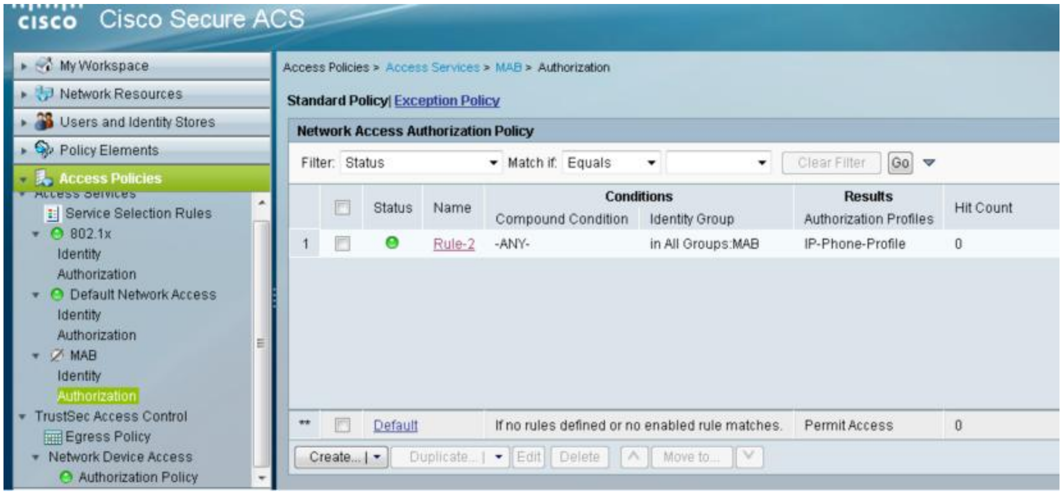
Results

Authorization Profiles:

IP-Phone-Profile

You may select multiple authorization
defined in multiple profiles will use the
profile defined.

The Authorization policy will be as follows after the creation:



Access Policies > Access Services > MAB > Authorization

Standard Policy| Exception Policy

Network Access Authorization Policy

Filter: Status Match if: Equals

		Status	Name	Conditions		Results	Hit Count
				Compound Condition	Identity Group	Authorization Profiles	
1	☐	●	Rule-2	-ANY-	in All Groups:MAB	IP-Phone-Profile	0
**	☐		Default	If no rules defined or no enabled rule matches.		Permit Access	0

6. References

- Cisco 802.1x port based authentication
- Cisco Unified IP Phone 8945
- Cisco Unified IP Phone 9971
- Cisco Tandberg Video End Points
- Cisco Virtual Office Deployment Guide
- Cisco Virutal Office Datasheet
- Cisco Movi

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.**

Printed in USA C11-492810-01 03/12