

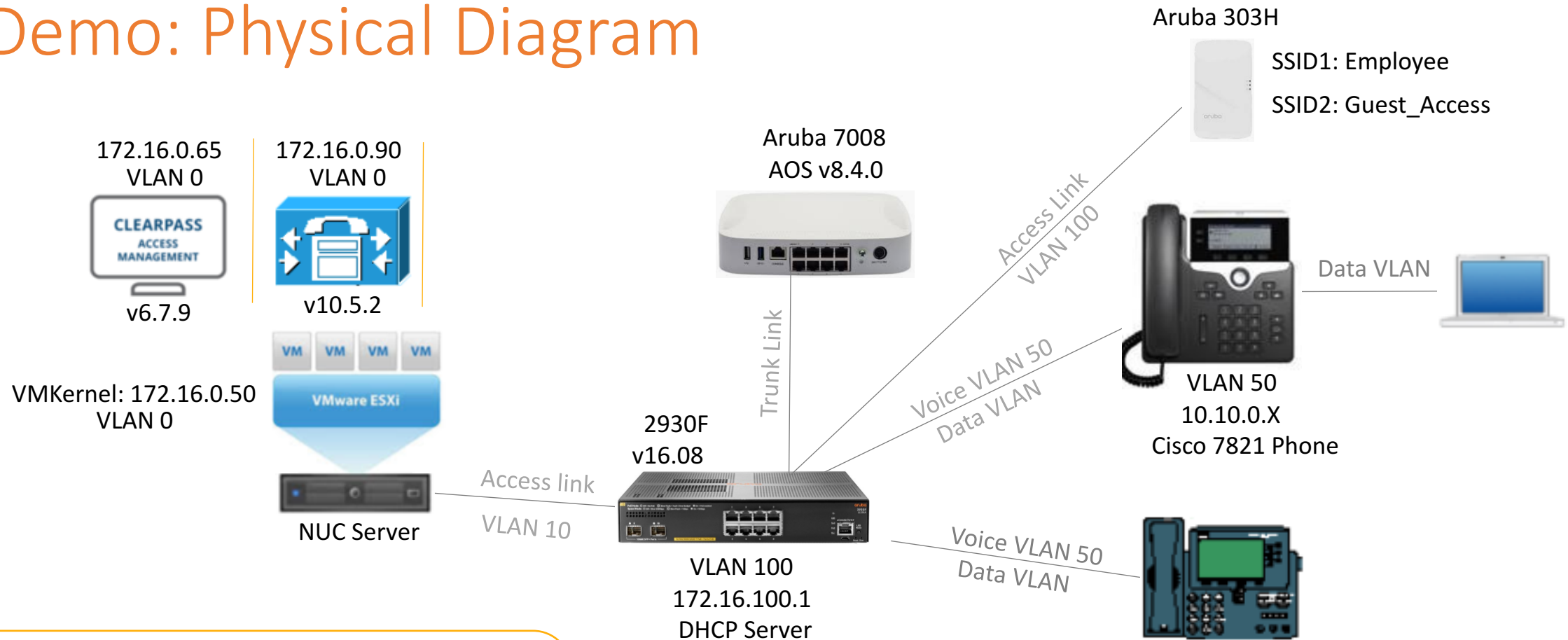


a Hewlett Packard
Enterprise company

Aruba AOS switches- Cisco IP telephony

Adolfo Bolivar
May 2019

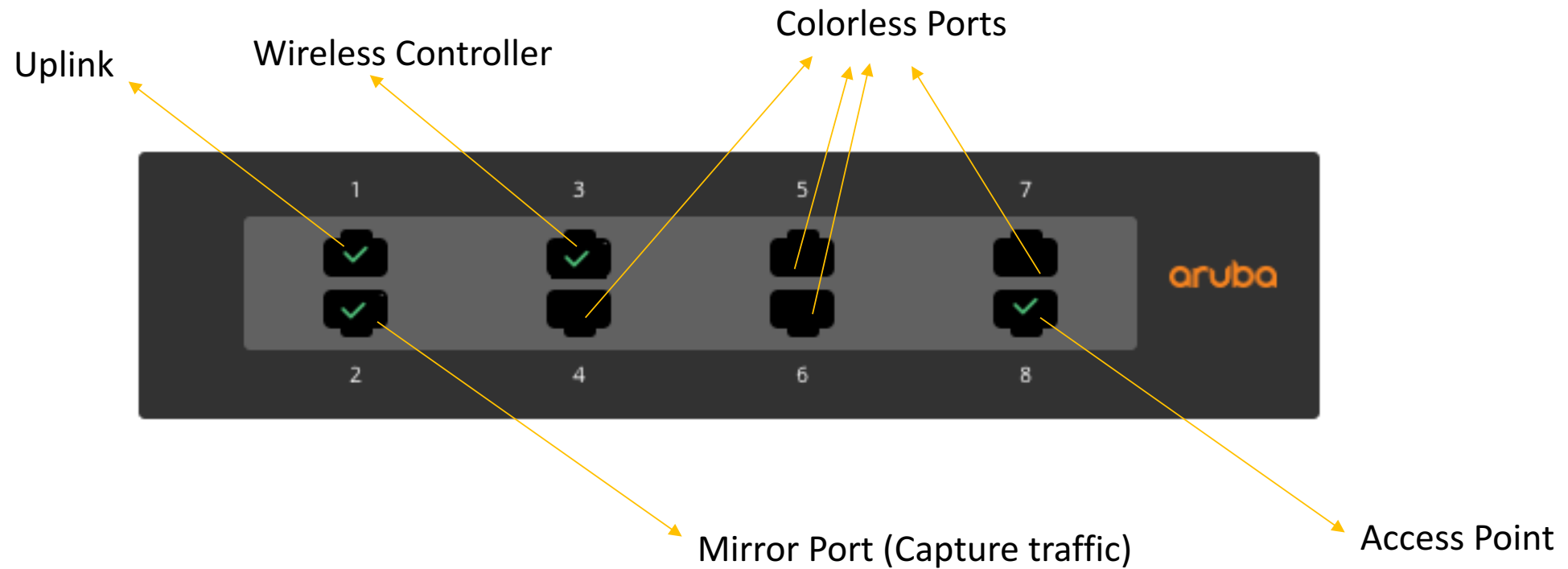
Demo: Physical Diagram



VLAN 10: 172.16.0.0/24 - Datacenter VLAN
VLAN 50: 10.10.0.0/24 - VoIP VLAN
VLAN 80: 192.168.6.0/24 - Guest VLAN
VLAN 90: 192.168.7.0/24 - Employee VLAN
VLAN 100: 172.16.100.0/24 - Management VLAN

2930F - Physical Connections

- Ports 4-7: Connect IP phones or End Users





a Hewlett Packard
Enterprise company

Task: Config 2930F switch to support Cisco IP Phones

Disable Aruba Central

- Disable ArubaOS switches to contact Aruba Activate and Aruba Central:

```
2930F-8(config)# aruba-central disable
2930F-8(config)#
2930F-8(config)# activate software-update disable
2930F-8(config)# activate provision disable
```

```
2930F-8# show activate software-update
```

Configuration and Status - Activate Software Update

Activate Server Address	: device.arubanetworks.com
Activate Server Polling	: Disabled
Installed Software Version	: WC.16.08.0003
Server Software Version	: Not available - polling disabled.
Server Software Image URL	: Not available - polling disabled.

Voice VLAN – DHCP Option 150

- Configuring voice VLANs separates voice traffic from data traffic. You must configure the port as a tagged member of the voice VLAN and a tagged or untagged member of the data VLAN.

```
vlan 50
 name "Voice"
 tagged 1
 ip address 10.10.0.1 255.255.255.0
 voice
 dhcp-server
 exit
```

Port 1 -> Uplink

Voice VLAN definition

- Per Cisco requirements, you may need to enable DHCP Option 150 so that in the DHCP broadcasts, phones see a list of all TFTP (CUCM) servers that are connected to the network.

```
dhcp-server pool "VOICE"
 default-router "10.10.0.1"
 dns-server "8.8.8.8"
 network 10.10.0.0 255.255.255.0
 option 150 ip "172.16.0.90"
 range 10.10.0.5 10.10.0.20
 exit
```

Option 150 definition -> CUCM IP Address

Cisco IP Phone 7940/60

- IP Phone 7960 is a Cisco pre-standard PoE phone and it does not support LLDP, just CDP.

<https://community.cisco.com/t5/switching/cisco-ip-phones-7960-7940-getting-data-vlan-ip/td-p/2172889>

- Aruba switches supports these type of phones by entering two commands:

```
2930F-8(config)#  
2930F-8(config)# power-over-ethernet pre-std-det  
2930F-8(config)#  
2930F-8(config)# cdp mode pre-standard-voice  
2930F-8(config)# end  
2930F-8#
```



a Hewlett Packard
Enterprise company

Task: How to authenticate Cisco Phones?

Cisco 7960 Phone only supports MAC Based Auth

**Cisco IP Phones that do not Support
802.1X**

Cisco IP Phone Model	Support For 802.1X
7902, 7905	No
7910, 7912, 7920	No
7935, 7936	No
7940	No
7960	No

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/IP_Tele/IP_Telephony_DIG.html

Cisco 7821 supports EAP-FAST and EAP-TLS

- Cisco IP phones support authentication via username and password using EAP-MD5 / EAP-FAST methods of authentication. <https://www.cisco.com/c/dam/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-c11-739097.pdf>

Phone Models				
802.1X (Wired)	7900	6900, 8900, 9900	7811, 7821, 7841, 7861	8811, 8821, 8841, 8845, 8851, 8861, 8865
EAP-MD5	Yes	Yes	No (deprecated)	No (deprecated)
EAP-FAST	Yes	Yes	Yes	Yes
EAP-TLS	Yes	Yes	Yes	Yes

EAP-FAST is not secure

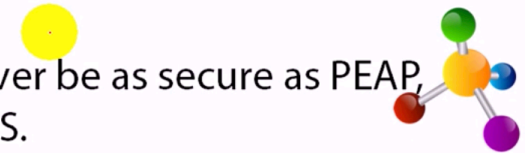
- EAP-FAST method: <https://community.arubanetworks.com/t5/Community-Tribal-Knowledge-Base/Wireless-Security-Myths-and-Realities/ta-p/20430> and <https://www.youtube.com/watch?v=bXtS2FigxGg>

Other things to Avoid...

- **Cisco LEAP (vulnerable to dictionary attacks)**
- **EAP-FAST (doesn't securely provide mutual authentication)**

Issues

- Phase 0
 - MS-CHAPv2 is weak and can be cracked
 - Man in the middle attack
 - Attacker can pose as the A.S
- Still better than LEAP
 - Phase 0 is only done once
 - Attacker must be active, which opens him up for detection
- EAP-FAST can never be as secure as PEAP, EAP-TLS, EAP-TTLS.



EAP-TLS and MIC on Cisco Phones

Manufacturing Installed Certificate (MIC)

- Cisco IP Phones ship from the factory with a unique MIC pre-installed.
- MIC is valid for 10 years.
- No certificate revocation support.

MIC CA certificates included in both the CallManager and CAPF trust stores:

- Cisco_Manufacturing_CA
- Cisco_Root_CA_2048

Not recommended to use MIC for 802.1x: MIC by itself cannot be used to determine if this phone is a corporate asset or a rogue Cisco phone. For that, you need an LSC (Locally Significant Certificate). → Clearpass will check the MIC and a list of valid MAC Addresses in order to discard rogue Cisco Phones.

<https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2013/pdf/BRKUCC-2501.pdf>



a Hewlett Packard
Enterprise company

Task: Configure 802.1X, MAC Authentication & LUR

Radius Server config

```
(config)# radius-server host 172.16.0.65 clearpass
```

Radius server is hosted by ClearPass

```
(config)# ip client-tracker trusted  
(config)# ip source-interface radius vlan 100  
(config)#  
(config)# radius-server host 172.16.0.65 key Aruba123!  
(config)# radius-server host 172.16.0.65 dyn-authorization  
(config)# radius-server host 172.16.0.65 time-window plus-or-minus-time-window 30  
(config)# aaa server-group radius Clearpass host 172.16.0.65
```

Trusted option enables tracking of trusted clients

RADIUS source interface

Configure the RADIUS server, specifying ClearPass's IP address

Enable dynamic authorization for the RADIUS server

Configure replay protection for dynamic authorization messages

Associates a RADIUS server with a server group. Each group can contain up to 3 RADIUS servers

AAA service and Role Based Access

```
2930F-8P(config)# aaa authentication port-access eap-radius server-group Clearpass
2930F-8P(config)# aaa authentication mac-based chap-radius server-group Clearpass
2930F-8P(config)# aaa accounting network start-stop radius server-group Clearpass
2930F-8P(config)# aaa accounting update periodic 5
2930F-8P(config)# aaa authorization user-role enable
Some legacy secure client access functionality is not supported when user roles are enabled.
Please refer to the end user documentation for details.
```

- 802.1X EAP Based Authentication
- MAC Authentication, CHAP is more secure than PAP
- Enable Radius Accounting
- Update interval (minutes)

A user role determines the client network privileges, the frequency of re-authentication, and applicable bandwidth contracts along with other permissions.

Every client is associated with a user role or the client is blocked from access to the network

Port Access config

```
2930F-8(config)# aaa port-access authenticator active
2930F-8(config)# aaa port-access authenticator 4-7 client-limit 10
2930F-8(config)# aaa port-access mac-based 4-7
2930F-8(config)# aaa port-access mac-based 4-7 addr-limit 10
2930F-8(config)# aaa port-access authenticator 4-7
2930F-8(config)# aaa port-access authenticator 4-7 supplicant-timeout 10
2930F-8(config)# aaa port-access authenticator 4-7 tx-period 10
```

Activate 802.1X authenticator

Permit up to 10 active clients per port

Enable MAC authentication on ports 3-8

Permit up to 10 authenticated MACs per port

Configure 802.1X authentication on the switch ports

Supplicant timeout period (seconds)

EAP Request-Identity waiting period (seconds)

Port Access config

```
2930F-8(config)# aaa port-access 4-7 auth-order authenticator mac-based  
2930F-8(config)#
```

Assign an order of Authentication between 802.1X and MAC Authentication.

In the earlier releases, all authentication methods were attempted in parallel. 802.1x had the highest priority, followed by MAC, Web, and local MAC authentication.

```
2930F-8(config)# aaa port-access 4-7 auth-priority authenticator mac-based  
2930F-8(config)#
```

Authentication method with higher priority is used to access a client when both methods are configured to succeed through the Authentication server.

Config Classes

```
2930F-8(config)# class ipv4 "DNS"  
2930F-8(config-class)# 10 match udp any any eq 53  
2930F-8(config-class)# exit
```

→ DNS Protocol

```
2930F-8(config)# class ipv4 "DHCP"  
2930F-8(config-class)# 10 match udp any any eq 67  
2930F-8(config-class)# 20 match udp any any eq 68  
2930F-8(config-class)# exit
```

→ DHCP Protocol

```
2930F-8(config)# class ipv4 "WEB-TRAFFIC"  
2930F-8(config-class)# 10 match tcp any any eq 80  
2930F-8(config-class)# 20 match tcp any any eq 443  
2930F-8(config-class)# exit
```

→ Web Traffic

```
2930F-8(config)# class ipv4 "IP-ANY-ANY"  
2930F-8(config-class)# 10 match ip any any  
2930F-8(config-class)# exit
```

→ Any traffic - Any destination

```
2930F-8(config)# class ipv4 "VOICE"  
2930F-8(config-class)# match ip any 10.10.0.0/24  
2930F-8(config-class)# match ip any host 172.16.0.90  
2930F-8(config-class)# exit
```

→ Allow voice traffic network
Allow traffic to Callmanager

Policy and Local User Role (LUR) for Voice Traffic

User Policy Definition

```
2930F-8(config)# policy user "VOICE-POLICY"  
2930F-8(policy-user)# class ipv4 "DNS" action permit  
2930F-8(policy-user)# class ipv4 "DHCP" action permit  
2930F-8(policy-user)# class ipv4 "VOICE" action permit  
2930F-8(policy-user)# class ipv4 "IP-ANY-ANY" action deny  
2930F-8(policy-user)# exit
```

→ Permit DNS Protocol

→ Permit DHCP Protocol

→ Permit Voice Network (Phones and Callmanager)

→ Deny traffic to Datacenter and Internet

User Role Definition

```
2930F-8(config)# aaa authorization user-role name VOICE-ROLE  
2930F-8(user-role)# policy "VOICE-POLICY"  
2930F-8(user-role)# reauth-period 300  
2930F-8(user-role)# vlan-name-tagged "Voice"  
2930F-8(user-role)# end
```

→ Re-authenticate every 5 minutes
(testing purpose)

Role Based Access for Phones – Voice Role

```
2930F-8# show user-role VOICE-ROLE
```

User Role Information

Name	: VOICE-ROLE
Type	: local
Reauthentication Period (seconds)	: 3000
Cached Reauth Period (seconds)	: 0
Logoff Period (seconds)	: 300
Untagged VLAN	:
Tagged VLAN	: Voice
Captive Portal Profile	:
Policy	: VOICE-POLICY
Tunnelednode Server Redirect	: Disabled
Secondary Role Name	:
Device Attributes	: Disabled

```
2930F-8#
```

Role created on switch

Re authentication

VLAN 50

Policy Applied



a Hewlett Packard
Enterprise company

Task: Configure QoS

Adjust the DSCP – CoS mapping

- Cisco phones mark voice as EF and CoS 5. ArubaOS-switch default for the DSCP EF class is priority 7.

```
2930F-8# show qos dscp-map
```

DSCP Policies

NOTE: The policies shown below are not currently enabled. Use the 'qos type-of-service diff-services' command to apply DSCP policies to inbound traffic.

DSCP CodePoint	DSCP Value	802.1p tag	DSCP Policy name
----------------	------------	------------	------------------

101101	45	5	
101110	46	7	ef
101111	47	5	

```
2930F-8(config)# qos dscp-map 101110 priority 5
2930F-8(config)# qos type-of-service diff-services
```

```
2930F-8# show qos dscp-map
```

DSCP Policies

NOTE: The policies shown below are not currently enabled. Use the 'qos type-of-service diff-services' command to apply DSCP policies to inbound traffic.

DSCP CodePoint	DSCP Value	802.1p tag	DSCP Policy name
----------------	------------	------------	------------------

101101	45	5	
101110	46	5	ef
101111	47	5	

Set the voice traffic a CoS value of 5

- CoS is a 3-bit field that is present in an Ethernet frame header when 802.1Q VLAN tagging is present.

```
2930F-8(config)# vlan 50
2930F-8(vlan-50)# qos priority 5
2930F-8(vlan-50)# exit
2930F-8(config)# exit
```

<https://community.arubanetworks.com/t5/Wired-Intelligent-Edge-Campus/Voice-VLAN-on-Aruba-switches/td-p/417811>



a Hewlett Packard
Enterprise company

Task: Connect Cisco Phone
7960 and 7820 to Aruba switch
2930F

Cisco IP Phone 7960 - boot process

- IP Phone sends CDP messages in order to get the voice vlan:

No.	Time	Source	Destination	Protocol	Length	Info
403	106.873661	HewlettP_8b:e7:7b	CDP/VTP/DTP/Pag...	CDP	258	Device ID: 2930F-8(94f128-8be770) Port ID: 5
478	117.611232	Cisco_84:d9:32	CDP/VTP/DTP/Pag...	CDP	128	Device ID: SEP001BD584D932 Port ID: Port 1
481	117.873455	HewlettP_8b:e7:7b	CDP/VTP/DTP/Pag...	CDP	258	Device ID: 2930F-8(94f128-8be770) Port ID: 5
484	118.611438	Cisco_84:d9:32	CDP/VTP/DTP/Pag...	CDP	128	Device ID: SEP001BD584D932 Port ID: Port 1

▶ Frame 478: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface 0

▶ IEEE 802.3 Ethernet

▶ Logical-Link Control

▼ Cisco Discovery Protocol

Version: 2

TTL: 180 seconds

Checksum: 0x091e [correct]

[Checksum Status: Good]

▶ Device ID: SEP001BD584D932

▶ Port ID: Port 1

▶ Capabilities

▶ Software Version

▼ Platform: Cisco IP Phone 7960

Type: Platform (0x0006)

Length: 23

Platform: Cisco IP Phone 7960

▶ VoIP VLAN Query: 512

▶ Duplex: Full

▼ Power Consumption: 6300 mW

Type: Power consumption (0x0010)

Length: 6

Power Consumption: 6300mW

▶ Type: Unknown (0x001c), length: 7

Cisco IP Phone 7960 - boot process

- Switch uses CDP to inform the Cisco IP Phone which voice should use:

No.	Time	Source	Destination	Protocol	Length	Info
481	117.873455	HewlettP_8b:e7:7b	CDP/VTP/DTP/PAG...	CDP	258	Device ID: 2930F-8(94f128-8be770) Port ID: 5
494	118.611429	Cisco_84:d9:32	CDP/VTP/DTP/PAG...	CDP	128	Device ID: SEP001BD584D932 Port ID: Port 1
498	118.873984	HewlettP_8b:e7:7b	CDP/VTP/DTP/PAG...	CDP	258	Device ID: 2930F-8(94f128-8be770) Port ID: 5

▶ Frame 481: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits) on interface 0
▶ IEEE 802.3 Ethernet
▶ Logical-Link Control
▼ Cisco Discovery Protocol
Version: 2
TTL: 180 seconds
Checksum: 0xd4c2 [correct]
[Checksum Status: Good]
▶ Device ID: 2930F-8(94f128-8be770)
▼ Software Version
Type: Software version (0x0005)
Length: 130
Software version: Revision WC.16.08.0003, ROM WC.16.01.0006 (/ws/swbuildm/rel_yakima_qaoff/code/build/lvm(swbuildm_rel_yakima_qaoff_rel_yakima))
▼ Platform: Aruba2930F-8G-PoE+-
Type: Platform (0x0006)
Length: 23
Platform: Aruba2930F-8G-PoE+-
▶ Addresses
▶ Port ID: 5
▶ Capabilities
▶ Native VLAN: 1
▼ VoIP VLAN Reply: 50
Type: VoIP VLAN Reply (0x000e)
Length: 7
Data: 01
Voice VLAN: 50
▶ Trust Bitmap: 0x00
▶ Untrusted port CoS: 0x00

Cisco IP Phone 7960 - boot process

- IP Phone received the CUCM IP address (TFTP) via DHCP Option 150

[illegible]

Cisco IP Phone 7960 - boot process

- IP Phone requests the CTL<MAC Address>.tlv file and then requests the SEP<MAC Address>.cnf.xml file (config file) via TFTP

No.	Time	Source	Destination	Protocol	Length	Info
438	113.821593	10.10.0.8	172.16.0.90	TFTP	77	Read Request, File: CTLSEP001BD584D932.tlv, Transfer type: octet
439	113.822103	172.16.0.90	10.10.0.8	TFTP	65	Error Code, Code: File not found, Message: File not found
440	113.842458	10.10.0.8	172.16.0.90	TFTP	78	Read Request, File: SEP001BD584D932.cnf.xml, Transfer type: octet
441	113.843531	172.16.0.90	10.10.0.8	TFTP	562	Data Packet, Block: 1

▶ Frame 440: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0

▶ Ethernet II, Src: Cisco_84:d9:32 (00:1b:d5:84:d9:32), Dst: HewlettP_8b:e7:70 (94:f1:28:8b:e7:70)

▶ 802.1Q Virtual LAN, PRI: 5, DEI: 0, ID: 50

▶ Internet Protocol Version 4, Src: 10.10.0.8, Dst: 172.16.0.90

▶ User Datagram Protocol, Src Port: 50128, Dst Port: 69

▼ Trivial File Transfer Protocol

 Opcode: Read Request (1)

 Source File: SEP001BD584D932.cnf.xml

 Type: octet

Cisco IP Phone 7960 - boot process

- IP Phone receives the extension number and settings via Skinny Protocol

No.	Time	Source	Destination	Protocol	Length	Info
591	124.536436	172.16.0.90	10.10.0.8	SKINNY...	82	LineStatV2Res
593	124.561099	10.10.0.8	172.16.0.90	SKINNY...	74	LineStatReq
594	124.561353	172.16.0.90	10.10.0.8	SKINNY...	94	LineStatV2Res
596	124.582603	10.10.0.8	172.16.0.90	SKINNY...	74	SpeedDialStatReq

▶	Frame 594: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
▶	Ethernet II, Src: HewlettP_8b:e7:70 (94:f1:28:8b:e7:70), Dst: Cisco_84:d9:32 (00:1b:d5:84:d9:32)
▶	802.1Q Virtual LAN, PRI: 3, DEI: 0, ID: 50
▶	Internet Protocol Version 4, Src: 172.16.0.90, Dst: 10.10.0.8
▶	Transmission Control Protocol, Src Port: 2000, Dst Port: 49862, Seq: 1757, Ack: 613, Len: 36
▼	Skinny Client Control Protocol
	Data length: 28
	Header version: Basic (0x00000000)
	Message ID: LineStatV2Res (327)
	lineNumber: 1
▶	lineType
	lineDirNumber: 1001
	lineFullyQualifiedDisplayName: 1001
	lineTextLabel: 1001
	[Request In: 593]
	[Response Time: 0.000254000 seconds]

Cisco IP Phone Pre-standard PoE and CDP only supported

```
2930F-8# sh cdp neig detail 5
```

CDP neighbors information for port 5

```
Port : 5
Device ID : SEP001BD584D932
Address Type : IP
Address : 10.10.0.8
Platform : Cisco IP Phone 7960
Capability : Host Phone Two-port Mac Relay
Device Port : Port 1
```

```
2930F-8#
```

```
2930F-8# show power-over-ethernet 5
```

Status and Configuration Information for port 5

Power Enable	: Yes	PoE Port Status	: Delivering
PLC Class/Type	: 0/1	Priority Config	: low
DLC Class/Type	: 0/-	Pre-std Detect	: on
Alloc By Config	: usage	Configured Type	:
Alloc By Actual	: usage	PoE Value Config	: n/a

Cisco IP Phone standard PoE and CDP/LLDP supported

```
2930F-8# sh cdp neig detail 6
```

```
CDP neighbors information for port 6
```

```
Port : 6
Device ID : SEPE0D173E55320
Address Type : IP
Address : 10.10.0.5
Platform : Cisco IP Phone 7821
Capability : Host Phone Two-port Mac Relay
Device Port : Port 1
Version : sip78xx.12-0-1-11.loads
```

```
Port : 6
Device ID : 10.10.0.5
Address Type : IP
Address : 10.10.0.5
Platform : Cisco IP Phone 7821, V1, sip78xx.12-0-1-11.loads
Capability : Switch Phone
Device Port : SW PORT
Version : Cisco IP Phone 7821, V1, sip78xx.12-0-1-11.loads
```

```
2930F-8#
```

```
2930F-8# show power-over-ethernet 6
```

```
Status and Configuration Information for port 6
```

Power Enable	: Yes	PoE Port Status	: Delivering
PLC Class/Type	: 1/1	Priority Config	: low
DLC Class/Type	: 1/2	Pre-std Detect	: on
Alloc By Config	: usage	Configured Type	:
Alloc By Actual	: lldp	PoE Value Config	: n/a

Task done!: Cisco IP SCCP and SIP Phones registered to CUCM

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go
adminapp | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾













Find and List Phones Related Links: Actively Logged In Device Report Go

+ Add New Select All Clear All Delete Selected Reset Selected Apply Config to Selected

Status
4 records found

Phone (1 - 4 of 4) Rows per Page 50

Find Phone where Device Name begins with Find Clear Filter Select item or enter search text

		Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IPv4 Address	Copy	Super Copy
<input type="checkbox"/>		SEP001BD584D932	Auto 1001	Default	SCCP	Registered with 172.16.0.90	10.10.0.8		
<input type="checkbox"/>		SEP006440B58F2D	Auto 1000	Default	SCCP	Unregistered	10.10.0.5		
<input type="checkbox"/>		SEP64168DBB9670	Auto 1003	Default	SCCP	Unregistered	10.10.0.10		
<input type="checkbox"/>		SEPE0D173E55320	Auto 1002	Default	SIP	Registered with 172.16.0.90	10.10.0.9		

Add New Select All Clear All Delete Selected Reset Selected Apply Config to Selected

IP Phone 7960 (SCCP)
IP Phone 7821 (SIP)



a Hewlett Packard
Enterprise company

Task: Test MAC Auth when
Cisco Phone 7960 is connected
to the switch

Debug 2930F

```
2930F-8P# debug security port-access mac-based
2930F-8P# debug security port-access authenticator
2930F-8P# debug security radius-server
2930F-8P# debug destination session
2930F-8P#
```

MAC Authentication

802.1X Authentication

Prints debug messages to terminal

802.1X EAP process start:

```
0000:08:46:52.65 1X m8021xCtrl:Port 5: connection detected.
0000:08:46:52.65 1X m8021xCtrl:Port 5: sent ReqId #1 to 0180c2-000003.
0000:08:46:58.49 1X m8021xCtrl:Port 5: added new client 001bd5-84d932.
```

802.1X EAP process fails, MAC Authentication Bypass starts:

```
0000:08:47:22.20 1X m8021xCtrl:Port 5: There is no EAP response from
client:001bd5-84d932
0000:08:47:22.20 1X m8021xCtrl:Port 5:Auth order: Mac authentication will be
triggered client: 001bd5-84d932 as there is no EAP response.
```

Phone is authenticated, VLAN 50 and VOICE Role are assigned:

```
0000:08:47:22.23 MAC mWebAuth:Port: 5 MAC: 001bd5-84d932 RADIUS Attributes,
tagged vid: 50.
0000:08:47:22.23 MAC mWebAuth:Port: 5 MAC: 001bd5-84d932 [72] client accepted
with role 'VOICE-ROLE'.
```

Access Tracker - Clearpass

aruba ClearPass Policy Manager Menu

Monitoring » Live Monitoring » Access Tracker

Access Tracker May 28, 2019 16:00:43 COT

Auto Refresh

Request Details

Summary Input Output

Login Status:	ACCEPT
Session Identifier:	R00000023-01-5ced9f50
Date and Time:	May 28, 2019 15:51:28 COT
End-Host Identifier:	00-1b-d5-84-d9-32 Open in AirWave
Username:	001bd584d932
Access Device IP/Port:	172.16.100.1:5 (2930F switch / Aruba)
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	2930F MAC Authentication
Authentication Method:	MAC-AUTH
Authentication Source:	Local:localhost
Authorization Source:	[Guest Device Repository]
Roles:	IP-Phone, [User Authenticated]
Enforcement Profiles:	IP Phone Enforcement
Service Monitor Mode:	Disabled

Showing 2 of 1-20 records

[Change Status](#) [Show Configuration](#) [Export](#) [Show Logs](#) [Close](#)

us Request Timestamp

2019/05/28 15:55:32
2019/05/28 15:51:28
2019/05/28 15:26:18
2019/05/28 15:26:12
2019/05/28 15:01:28
2019/05/28 14:37:03
2019/05/28 14:36:18
2019/05/28 14:36:12
2019/05/28 13:47:03

© Copyright 2018 Hewlett Packard Enterprise Development LP May 28, 2019 16:10:57 COT Authentication ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Show command – 2930F

```
2930F-8# sh port-acc client 5
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
5	001bd584d932	001bd5-84d932	10.10.0.8	VOICE-ROLE	MAC	50

```
2930F-8# sh vlan 50
```

Status and Counters - VLAN Information - VLAN 50

VLAN ID : 50
Name : Voice
Status : Port-based
Voice : Yes
Jumbo : No
Private VLAN : none
Associated Primary VID : none
Associated Secondary VIDs : none

Port Information	Mode	Unknown VLAN	Status
------------------	------	--------------	--------

1	Tagged	Learn	Up
5	MACAUTH	Learn	Up



a Hewlett Packard
Enterprise company

Task: Test 802.1X Auth when
Cisco Phone 7821 is connected
to the switch

Debug 2930F

2930F-8P# debug security port-access mac-based	→	MAC Authentication
2930F-8P# debug security port-access authenticator	→	802.1X Authentication
2930F-8P# debug security radius-server		
2930F-8P# debug destination session	→	Prints debug messages to terminal
2930F-8P#		

802.1X EAP process start:

```
0000:09:12:38.29 1X    m8021xCtrl:Port 6: connection detected.
0000:09:12:38.29 1X    m8021xCtrl:Port 6: sent ReqId #1 to 0180c2-000003.
```

802.1X EAP process continues:

```
0000:09:13:04.09 1X    m8021xCtrl:Port 6: received RspId #1 from e0d173-e55320.
0000:09:13:04.09 1X    m8021xCtrl:Port 6: enterAuthState for client
e0d173-e55320, State SM_AUTHENTICATING for CP-7821-SEPE0D173E55320
```

Phone is authenticated, VLAN 50 and VOICE Role are assigned:

```
0000:09:13:06.55 RAD    tRadiusR:ACCESS ACCEPT id: 201 from 172.16.0.65 received.
0000:09:13:06.55 1X    m8021xCtrl:Port 6: Received Auth Success for client
e0d173-e55320, User CP-7821-SEPE0D173E55320.
0000:09:13:06.55 1X    m8021xCtrl:Port: 6 MAC: e0d173-e55320 RADIUS Attributes,
tagged vid: 50.
```

Access Tracker - Clearpass

The screenshot displays the Aruba ClearPass Policy Manager interface. The left sidebar shows the navigation menu with 'Monitoring' selected. The main content area is titled 'Access Tracker' and shows a list of requests. A 'Request Details' modal is open, displaying the following information:

Request Details			
Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00000026-01-5ceda64a		
Date and Time:	May 28, 2019 16:21:17 COT		
End-Host Identifier:	e0-d1-73-e5-53-20 Open in AirWave		
Username:	CP-7821-SEPE0D173E55320		
Access Device IP/Port:	172.16.100.1:6 (2930F switch / Aruba)		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	802.1X EAP-TLS Wired Phone		
Authentication Method:	EAP-TLS		
Authentication Source:	Local:localhost		
Authorization Source:	[Guest Device Repository]		
Roles:	IP-Phone, [User Authenticated]		
Enforcement Profiles:	IP Phone Enforcement		
Service Monitor Mode:	Disabled		

At the bottom of the modal, there is a navigation bar with the following elements:

- Showing 1 of 1-20 records
- Change Status
- Show Configuration
- Export
- Show Logs
- Close

The background interface shows a list of requests with columns for 'Request Timestamp' and 'Request Details'. The timestamp for the selected request is 2019/05/28 16:21:17.

Show command – 2930F

```
2930F-8# sh port-acc client 6
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
6	CP-7821-SE...	e0d173-e55320	10.10.0.5	VOICE-ROLE	8021X	50

```
2930F-8# sh vlan 50
```

Status and Counters – VLAN Information – VLAN 50

VLAN ID : 50
Name : Voice
Status : Port-based
Voice : Yes
Jumbo : No
Private VLAN : none
Associated Primary VID : none
Associated Secondary VIDs : none

Port	Information Mode	Unknown VLAN	Status
1	Tagged	Learn	Up
5	MACAUTH	Learn	Up
6	802.1x	Learn	Up



a Hewlett Packard
Enterprise company

Task: Connect a PC to the Cisco
Phone, authenticate the user
via 802.1X

Debug 2930F

2930F-8P# debug security port-access mac-based	→	MAC Authentication
2930F-8P# debug security port-access authenticator	→	802.1X Authentication
2930F-8P# debug security radius-server	→	
2930F-8P# debug destination session	→	Prints debug messages to terminal
2930F-8P#		

802.1X EAP process start:

```
0000:09:40:57.48 1X    m8021xCtrl:Port 6: added new client 3c18a0-9c2ad6.  
0000:09:41:04.19 1X    m8021xCtrl:Port 6: sent ReqId #83 to 3c18a0-9c2ad6.
```

802.1X EAP process continues:

```
0000:09:41:04.24 1X    m8021xCtrl:Port 6: received RspId #83 from 3c18a0-9c2ad6.  
0000:09:41:04.24 1X    m8021xCtrl:Port 6: enterAuthState for client  
3c18a0-9c2ad6, State SM_AUTHENTICATING for adolfo.bolivar
```

User is authenticated, VLAN 90 and Employee Role are assigned:

```
0000:09:41:04.35 RAD    tRadiusR:ACCESS ACCEPT id: 227 from 172.16.0.65 received.  
0000:09:41:04.35 1X    m8021xCtrl:Port 6: Received Auth Success for client  
3c18a0-9c2ad6, User adolfo.bolivar.  
0000:09:41:04.35 1X    m8021xCtrl:Port: 6 MAC: 3c18a0-9c2ad6 RADIUS Attributes,  
vid: 90.
```

Access Tracker - Clearpass

aruba ClearPass Policy Manager Menu

Monitoring » Live Monitoring » Access Tracker

Access Tracker May 28, 2019 16:56:54 COT Auto Refresh

Request Details

Summary Input Output Accounting

Login Status:	ACCEPT
Session Identifier:	R00000028-01-5cedacda
Date and Time:	May 28, 2019 16:49:15 COT
End-Host Identifier:	3c-18-a0-9c-2a-d6 Open in AirWave
Username:	adolfo.bolivar
Access Device IP/Port:	172.16.100.1:6 (2930F switch / Aruba)
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	Wired_802.1X
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	Local:localhost
Authorization Source:	[Local User Repository]
Roles:	Employee, [User Authenticated]
Enforcement Profiles:	[Allow Access Profile], Wired_Employee Enforcement
Service Monitor Mode:	Disabled

Showing 3 of 1-20 records [Change Status](#) [Show Configuration](#) [Export](#) [Show Logs](#) [Close](#)

© Copyright 2018 Hewlett Packard Enterprise Development LP May 28, 2019 16:58:12 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Show command – 2930F

PC connected to Cisco 7821, EMPLOYEE Role assigned:

Port Access Client Status						
Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
5	001bd584d932	001bd5-84d932	10.10.0.8	VOICE-ROLE	MAC	50
6	adolfo.bol...	3c18a0-9c2ad6	192.168.8.2	EMPLOYEE-ROLE	8021X	90
6	CP-7821-SE...	e0d173-e55320	10.10.0.5	VOICE-ROLE	8021X	50
7	AP303H - 1...	204c03-202290	172.16.100.2	ACCESS_POINT-ROLE	8021X	100

PC connected to Cisco 7960 , EMPLOYEE Role assigned :

Port Access Client Status						
Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
5	adolfo.bol...	3c18a0-9c2ad6	192.168.8.2	EMPLOYEE-ROLE	8021X	90
5	001bd584d932	001bd5-84d932	10.10.0.8	VOICE-ROLE	MAC	50
6	CP-7821-SE...	e0d173-e55320	10.10.0.5	VOICE-ROLE	8021X	50
7	AP303H - 1...	204c03-202290	172.16.100.2	ACCESS_POINT-ROLE	8021X	100

Show command – 2930F

PC connected directly to the switch , EMPLOYEE Role assigned :

```
2930F-8# sh port-acc client
```

Port Access Client Status

Port	Client Name	MAC Address	IP Address	User Role	Type	VLAN
4	adolfo.bol...	3c18a0-9c2ad6	192.168.8.2	EMPLOYEE-ROLE	8021X	90
5	001bd584d932	001bd5-84d932	10.10.0.8	VOICE-ROLE	MAC	50
6	CP-7821-SE...	e0d173-e55320	10.10.0.5	VOICE-ROLE	8021X	50
7	AP303H - 1...	204c03-202290	172.16.100.2	ACCESS_POINT-ROLE	8021X	100

What happens when a PC is disconnected from Cisco Phone?

If the device unplugs from behind the phone, the switch cannot rely on link state to know when to clear the session:

- Proxy EAPoL-Logoff can provide a solution for 802.1X-authenticated data devices. Proxy EAPoL-Logoff enables the phone to transmit an EAPoL-Logoff message on behalf of the data device when the phone detects that an 802.1X device has unplugged from behind the phone.

Debug – 2930F

As soon as PC is disconnected, Cisco Phone sends a EAPOL logoff message, then the switch clears the User authentication session:

```
0000:09:42:28.65 1X    m8021xCtrl:Port 6: received EAPOL Logoff from
    3c18a0-9c2ad6.
0000:09:42:28.65 1X    m8021xCtrl:Port 6: stopping Acct session for client
    3c18a0-9c2ad6, user adolfo.bolivar termination code is 1.
0000:09:42:28.65 1X    m8021xCtrl:Port 6: removed client 3c18a0-9c2ad6 from all
    VLANs.
```

[illegible]



a Hewlett Packard
Enterprise company

Task: Test QoS

CoS and DSCP tags

No.	Time	Source	Destination	Protocol	Length	Info
179	11.586860	10.10.0.5	10.10.0.8	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF2C0B203, Seq=56795, Time=1953080467
180	11.600876	10.10.0.8	10.10.0.5	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x32D984DE, Seq=1535, Time=190496
181	11.606838	10.10.0.5	10.10.0.8	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF2C0B203, Seq=56796, Time=1953080627
182	11.620854	10.10.0.8	10.10.0.5	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x32D984DE, Seq=1536, Time=190656

▶ Frame 179: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface 0
 ▶ Ethernet II, Src: Cisco_e5:53:20 (e0:d1:73:e5:53:20), Dst: Cisco_84:d9:32 (00:1b:d5:84:d9:32)
 ▼ 802.1Q Virtual LAN, PRI: 5, DEI: 0, ID: 50
 101. = Priority: Voice, < 10ms latency and jitter (5)
 ...0 = DEI: Ineligible
 0000 0011 0010 = ID: 50
 Type: IPv4 (0x0800)
 ▼ Internet Protocol Version 4, Src: 10.10.0.5, Dst: 10.10.0.8
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 ▼ Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
 1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
 00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
 Total Length: 200
 Identification: 0x1ee9 (7913)
 ▶ Flags: 0x00
 Fragment offset: 0
 Time to live: 64
 Protocol: UDP (17)
 Header checksum: 0x4664 [validation disabled]
 [Header checksum status: Unverified]
 Source: 10.10.0.5
 Destination: 10.10.0.8
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]
 ▶ User Datagram Protocol, Src Port: 19104, Dst Port: 18162
 ▶ Real-Time Transport Protocol



a Hewlett Packard
Enterprise company

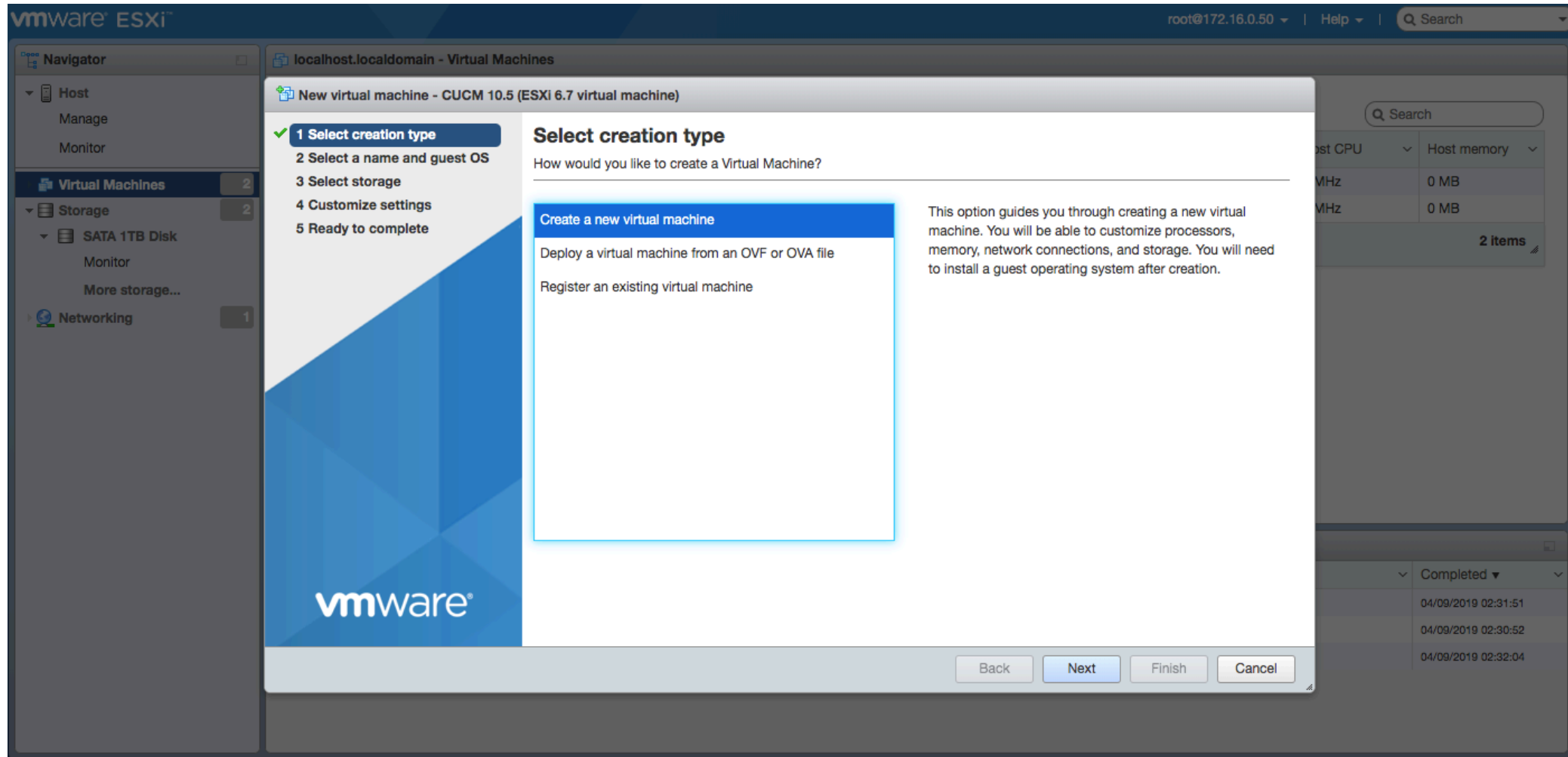
Task: Install CUCM

CUCM VM requirements

Cisco Unified Communications Manager (CUCM) configuration that supports up to 1000 users per node:

- Red Hat Enterprise Linux 6 (64-bit) CPU
- 2 vCPU
- Memory: 4 GB
- Disk: 1 - 80 GB disk

Create a new VM



Name of VM

New virtual machine - CUCM 10.5 (ESXi 6.7 virtual machine)

✓ 1 Select creation type
2 Select a name and guest OS
3 Select storage
4 Customize settings
5 Ready to complete

Select a name and guest OS

Specify a unique name and OS

Name

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility

Guest OS family

Guest OS version

vmware

Back Next Finish Cancel

Assign hardware resources, Select the CUCM - ISO file

New virtual machine - CUCM 10.5 (ESXi 6.7 virtual machine)

- ✓ 1 Select creation type
- ✓ 2 Select a name and guest OS
- ✓ 3 Select storage
- ✓ 4 Customize settings
- 5 Ready to complete

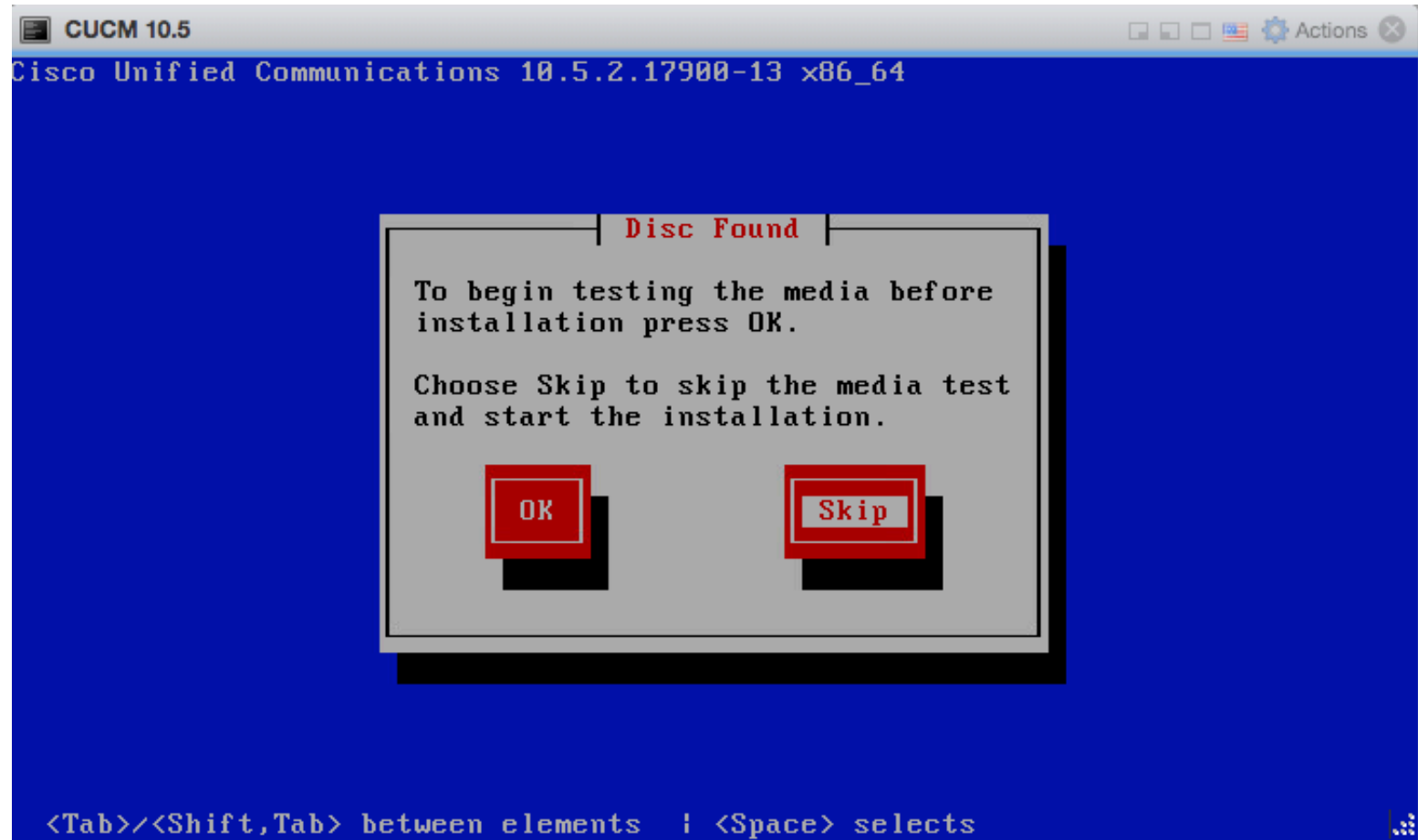
Customize settings

Configure the virtual machine hardware and virtual machine additional options

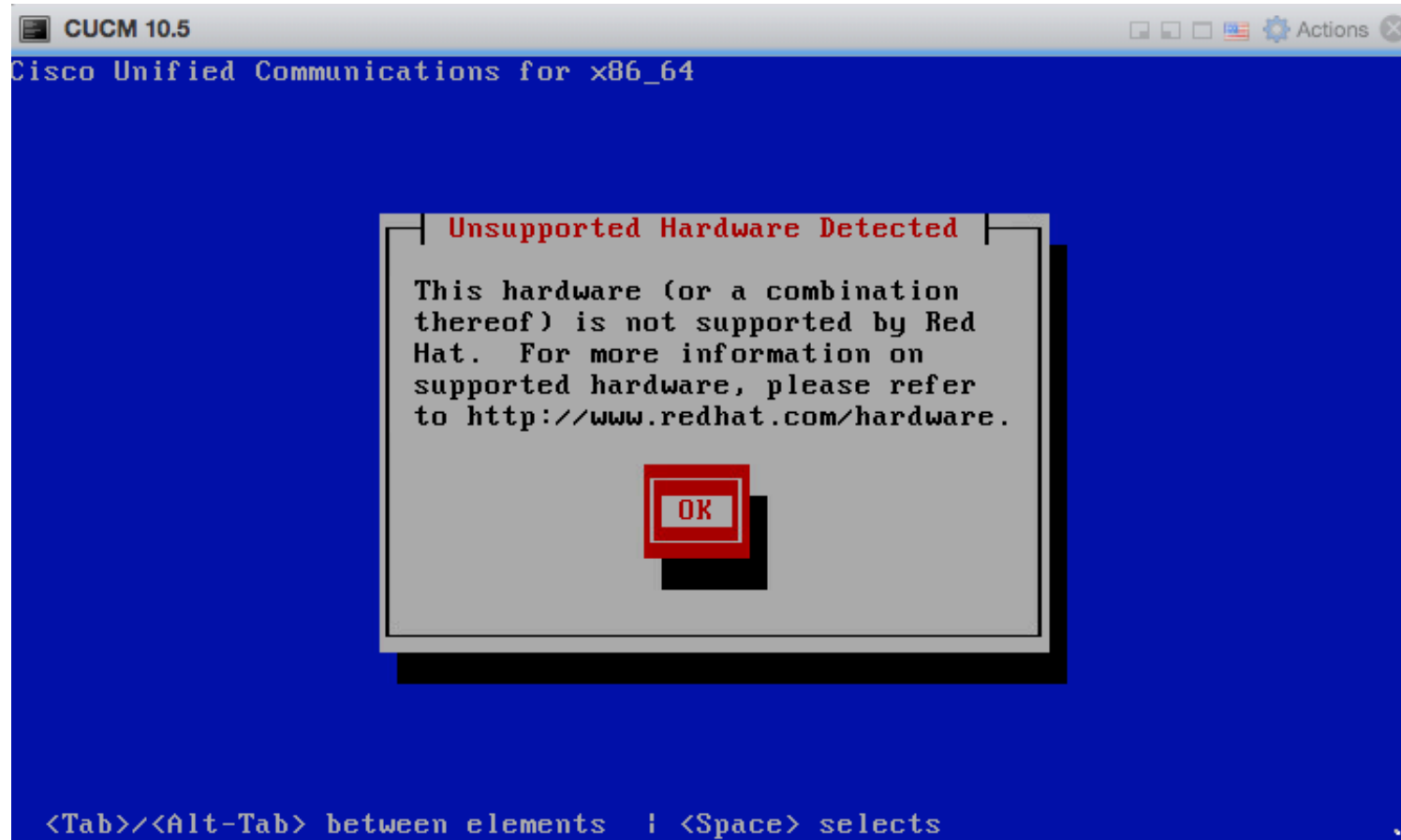
CPU	2		
Memory	4096	MB	
Hard disk 1	80	GB	
SCSI Controller 0	VMware Paravirtual		
SATA Controller 0			
USB controller 1	USB 2.0		
Network Adapter 1	VM Network	<input checked="" type="checkbox"/> Connect	
CD/DVD Drive 1	Datastore ISO file	<input checked="" type="checkbox"/> Connect	
Video Card	Default settings		

Back Next Finish Cancel

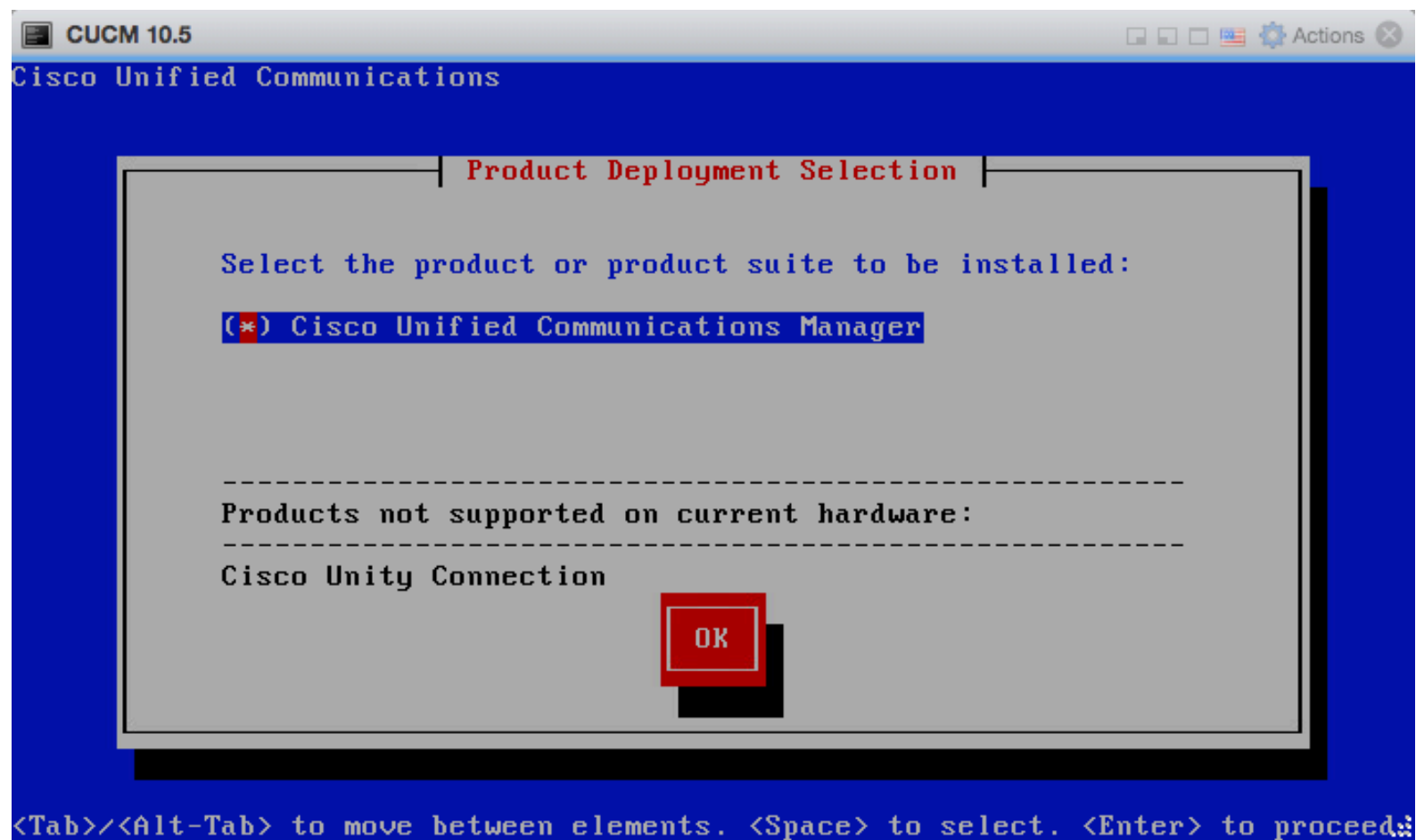
Click on Skip



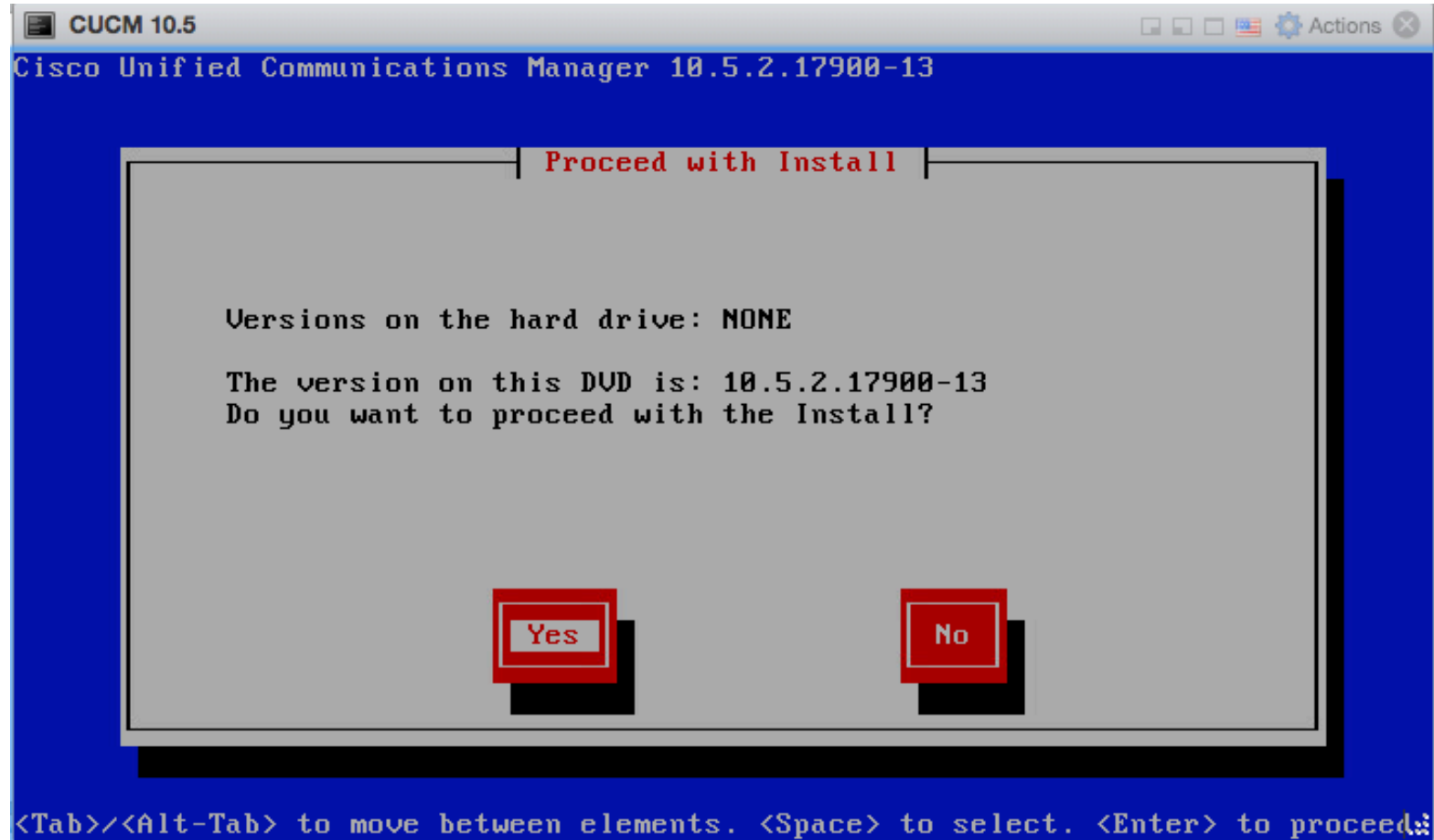
Ignore warning message



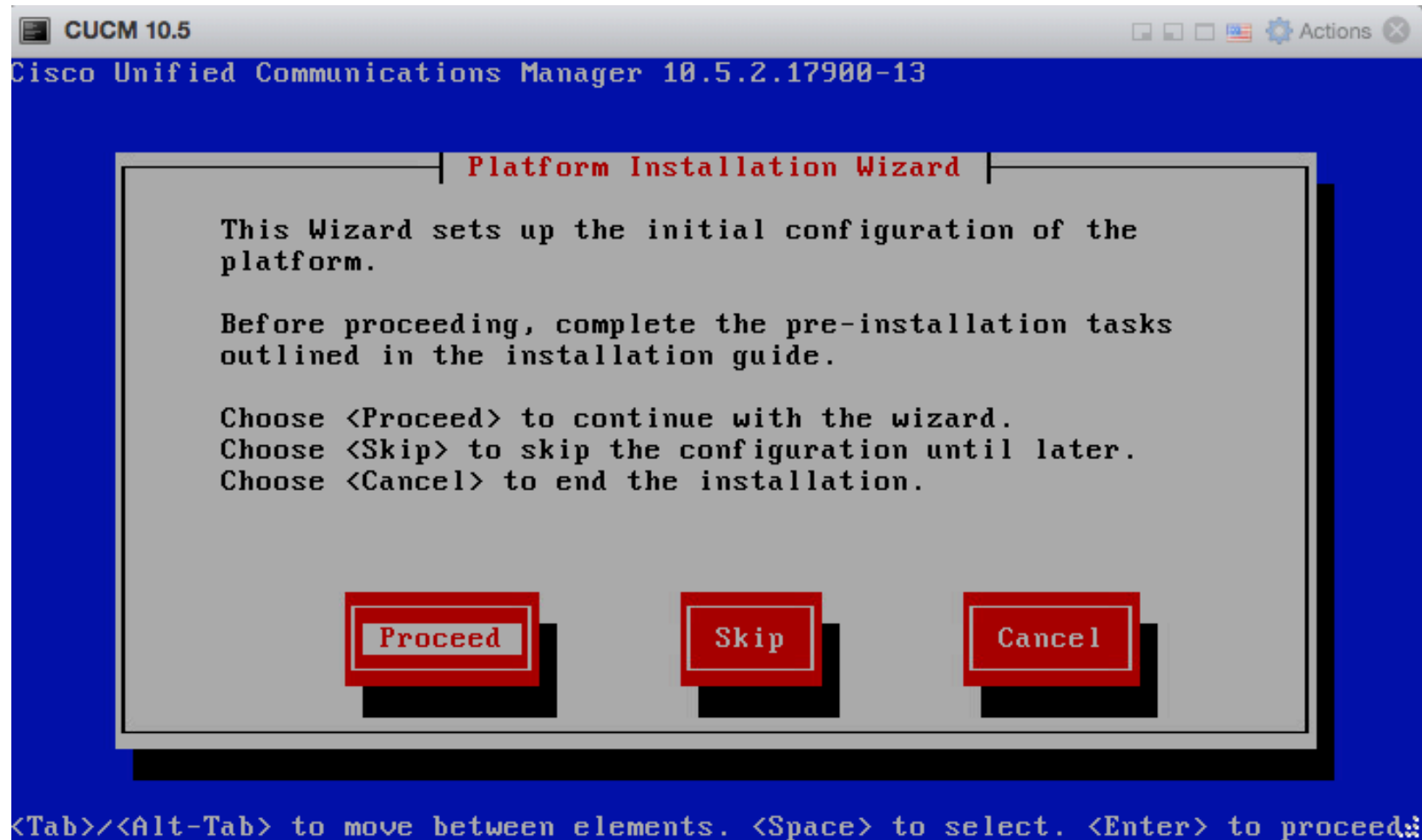
Select CUCM, click ok



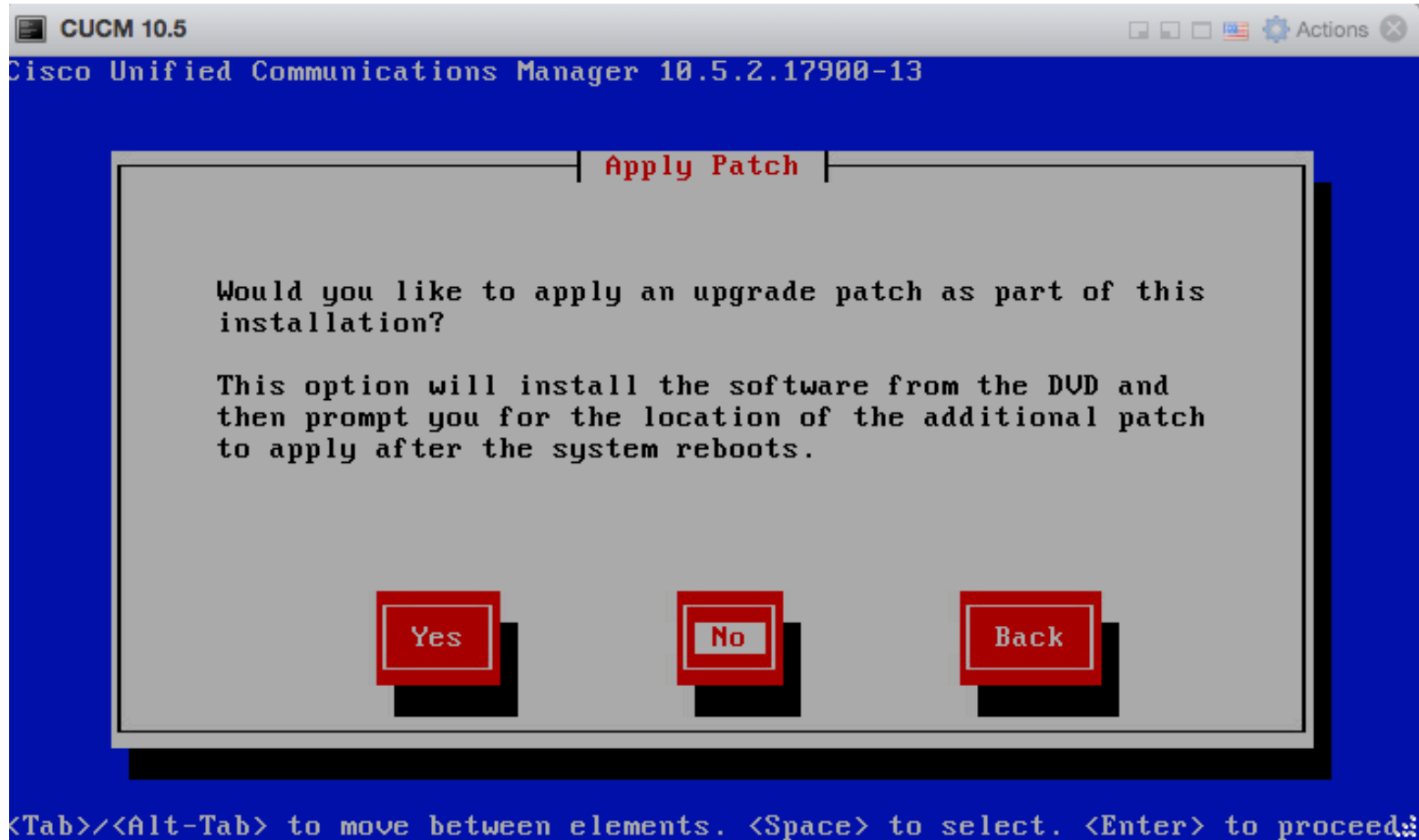
Click yes to install CUCM 10.5.2



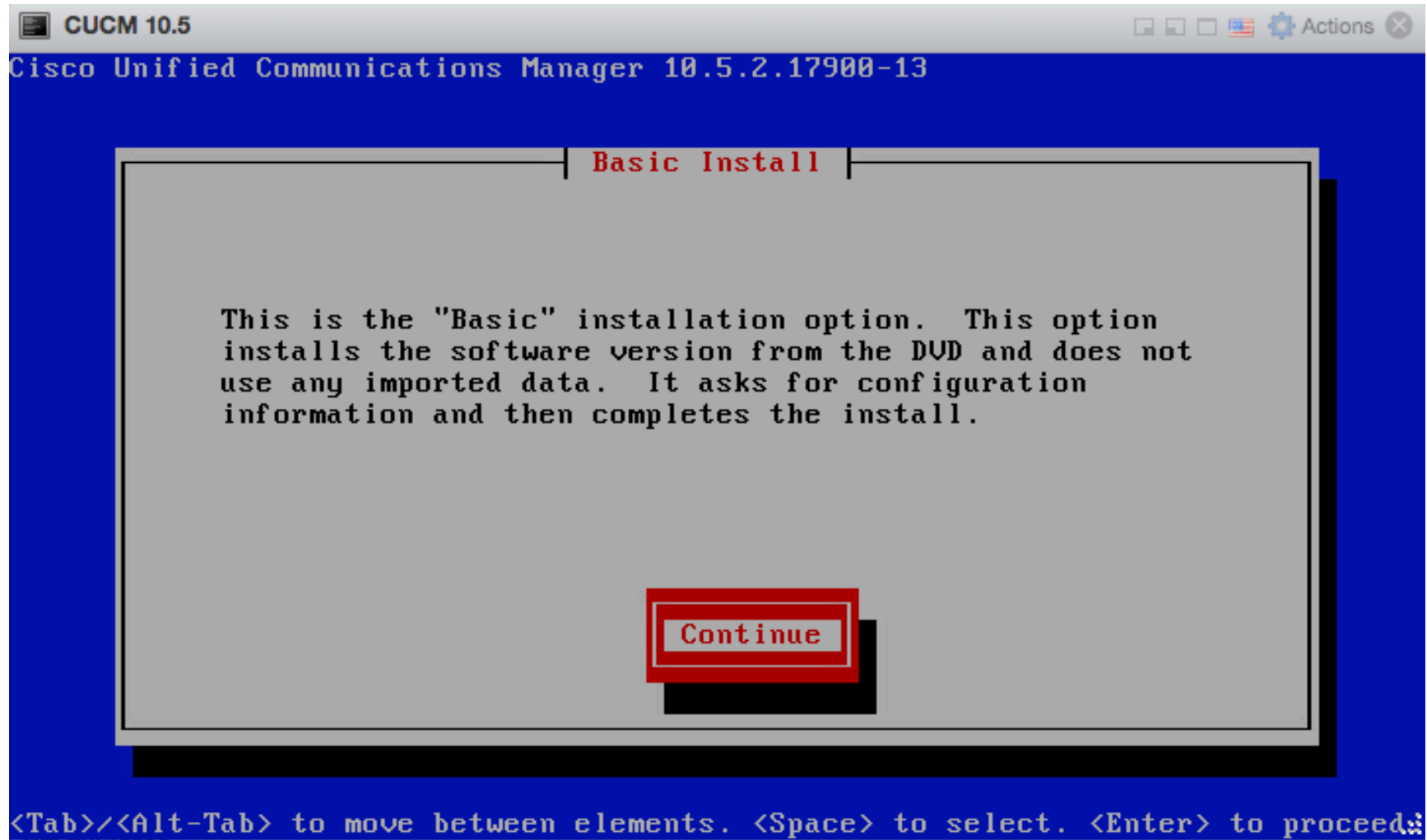
Proceed



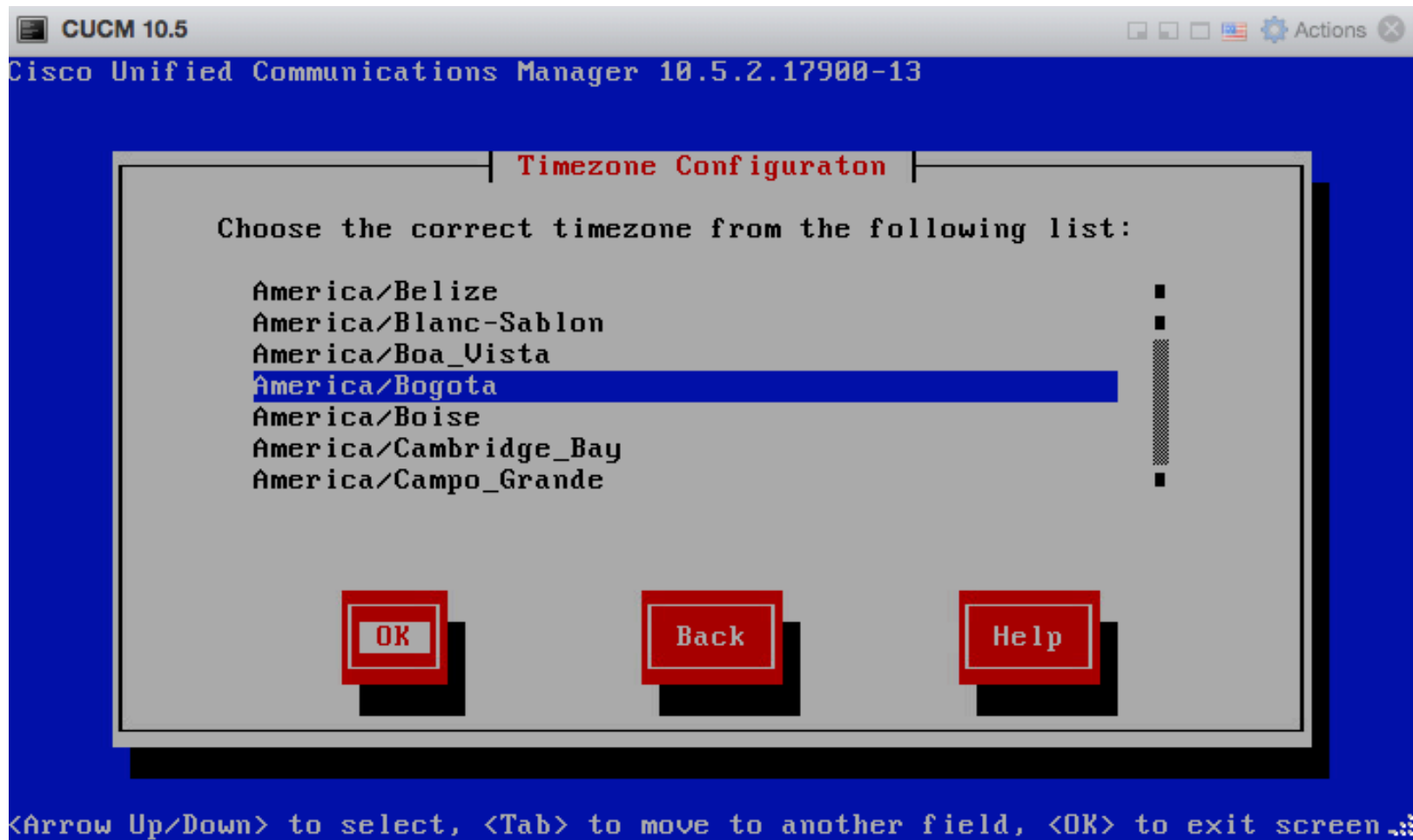
Skip patch file



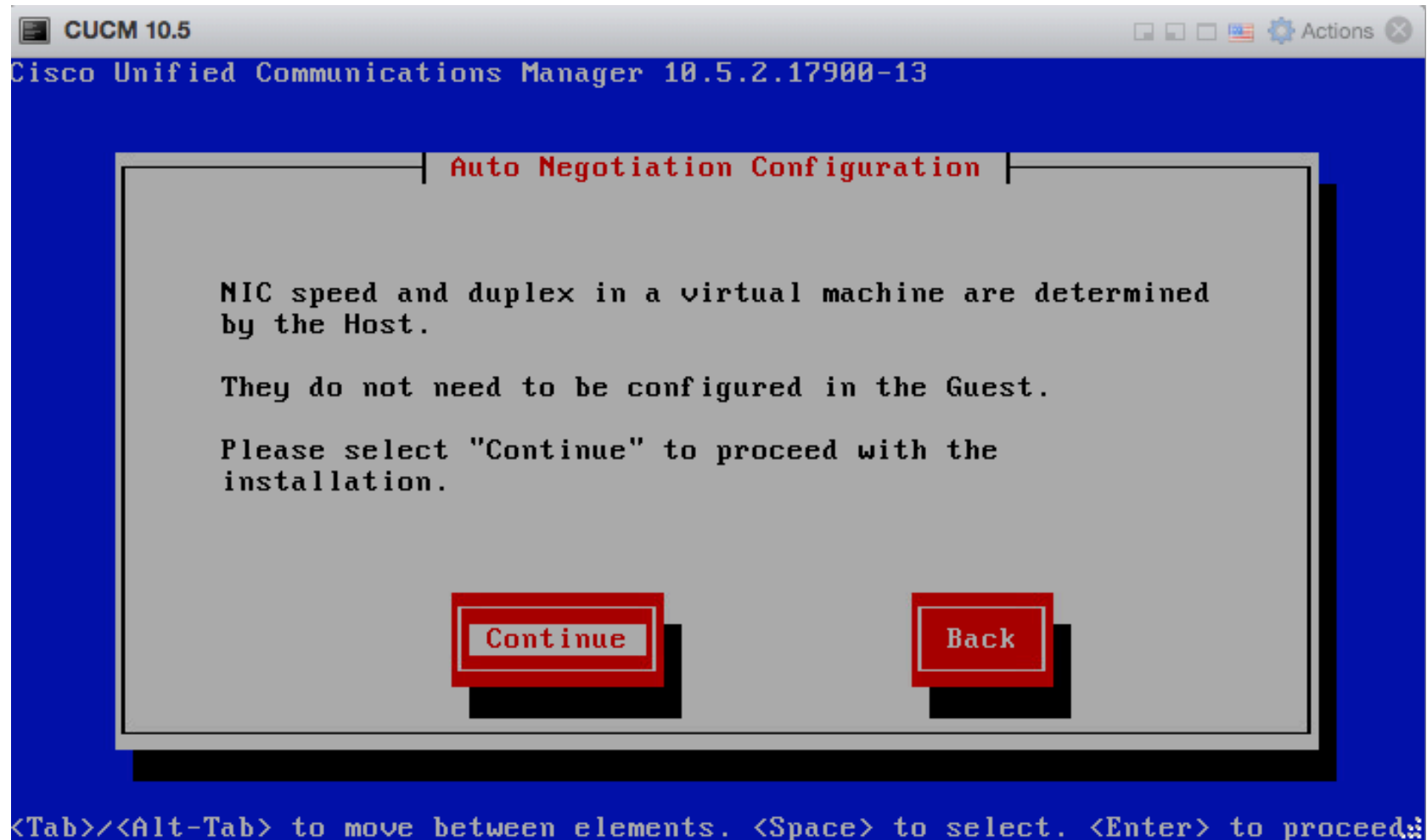
Basic installation option



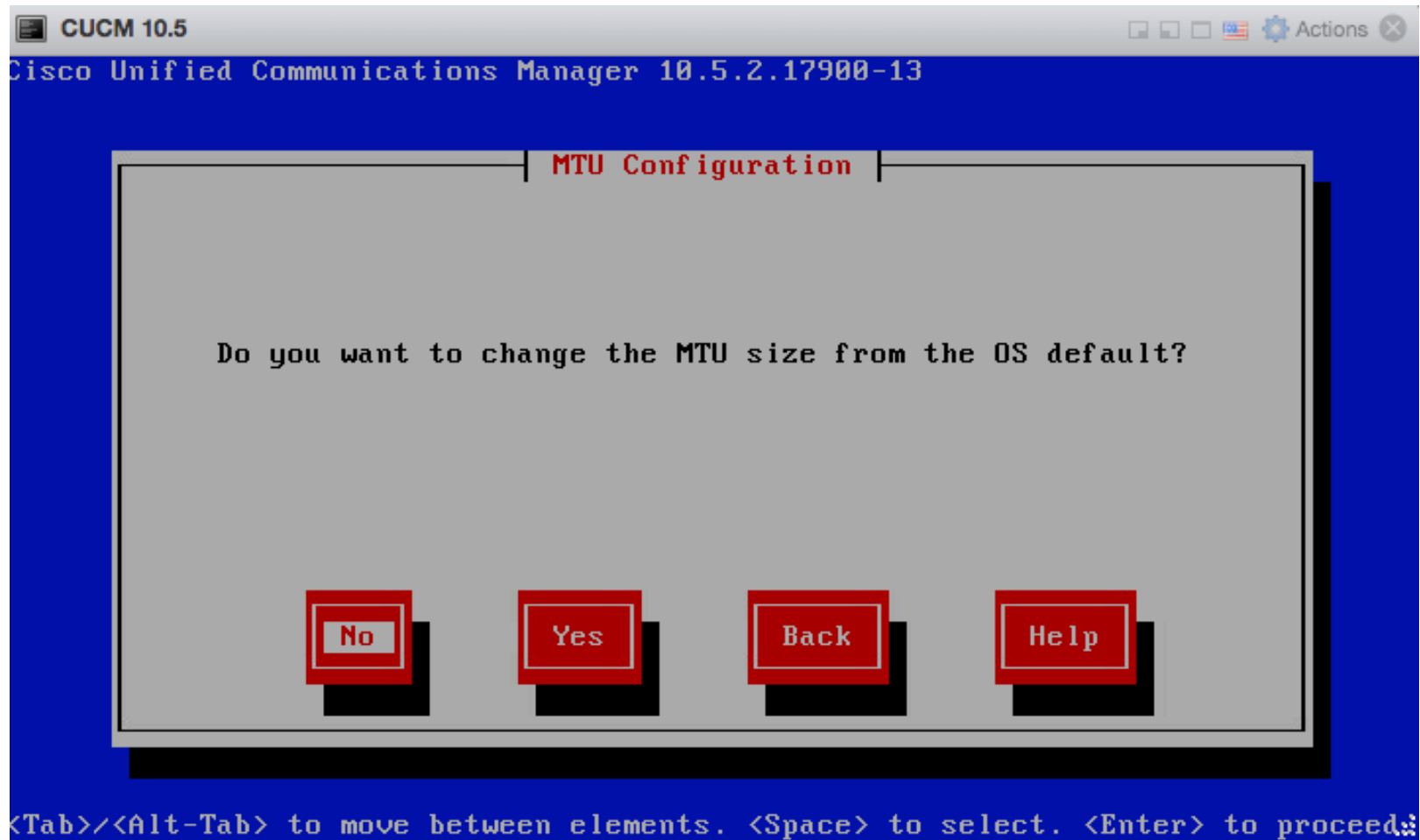
Choose your timezone



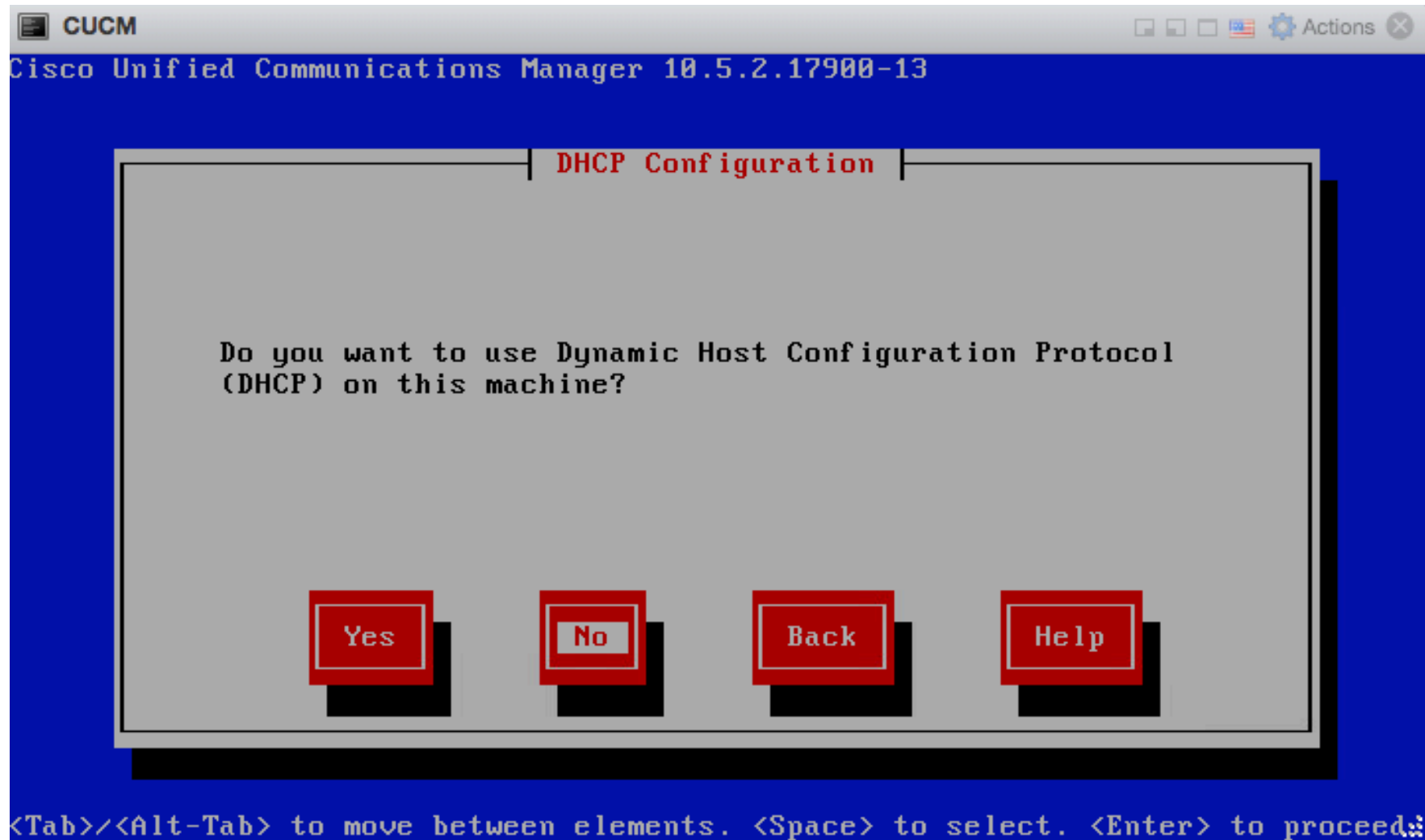
Continue



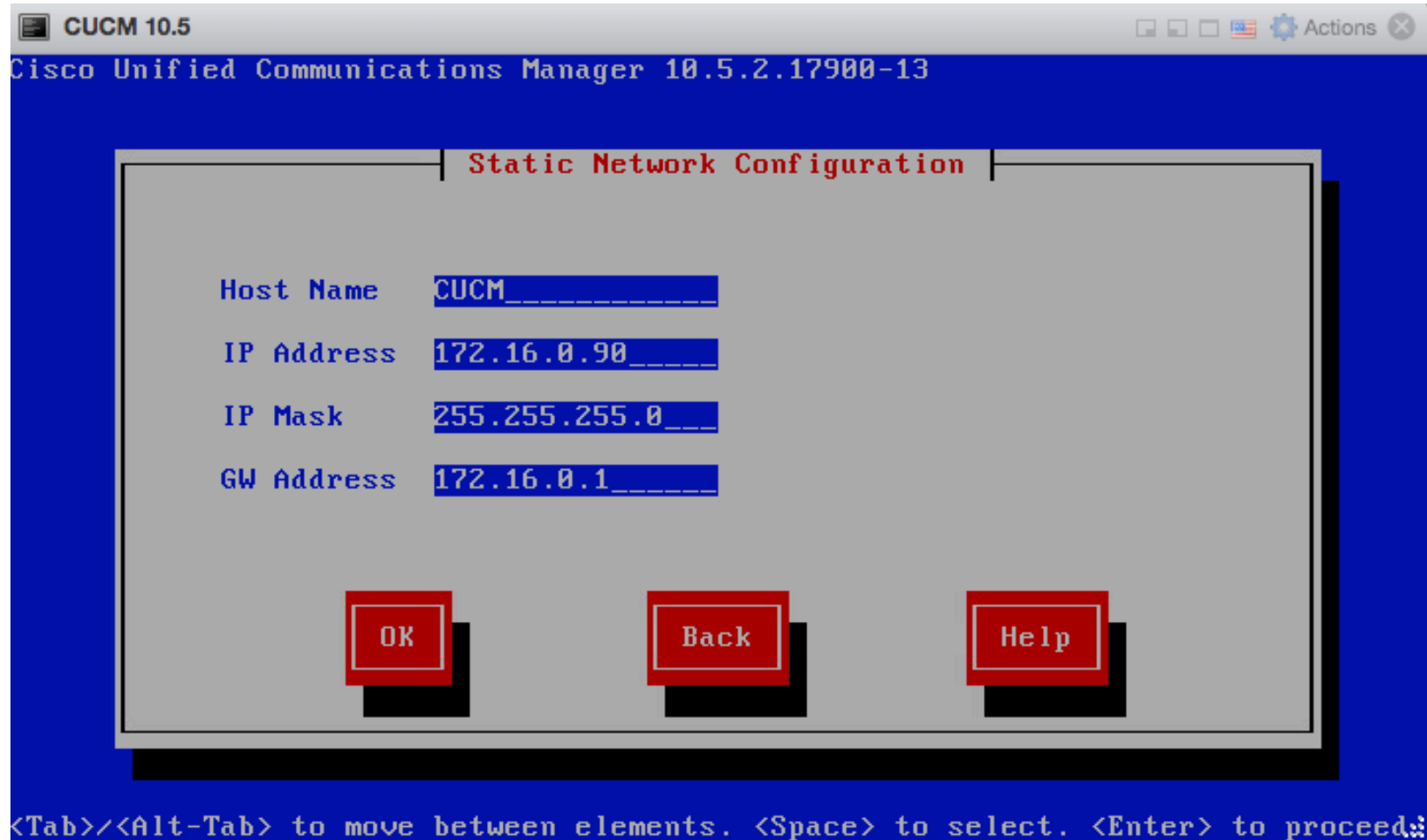
Default MTU size



Not use DHCP



Enter IP address



The screenshot shows a terminal window titled "CUCM 10.5" with a subtitle "Cisco Unified Communications Manager 10.5.2.17900-13". The main content area is titled "Static Network Configuration" and contains four input fields: "Host Name" with the value "CUCM", "IP Address" with the value "172.16.0.90", "IP Mask" with the value "255.255.255.0", and "GW Address" with the value "172.16.0.1". Below these fields are three red buttons labeled "OK", "Back", and "Help". At the bottom of the window, a status bar provides navigation instructions: "<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed".

CUCM 10.5

Cisco Unified Communications Manager 10.5.2.17900-13

Static Network Configuration

Host Name CUCM

IP Address 172.16.0.90

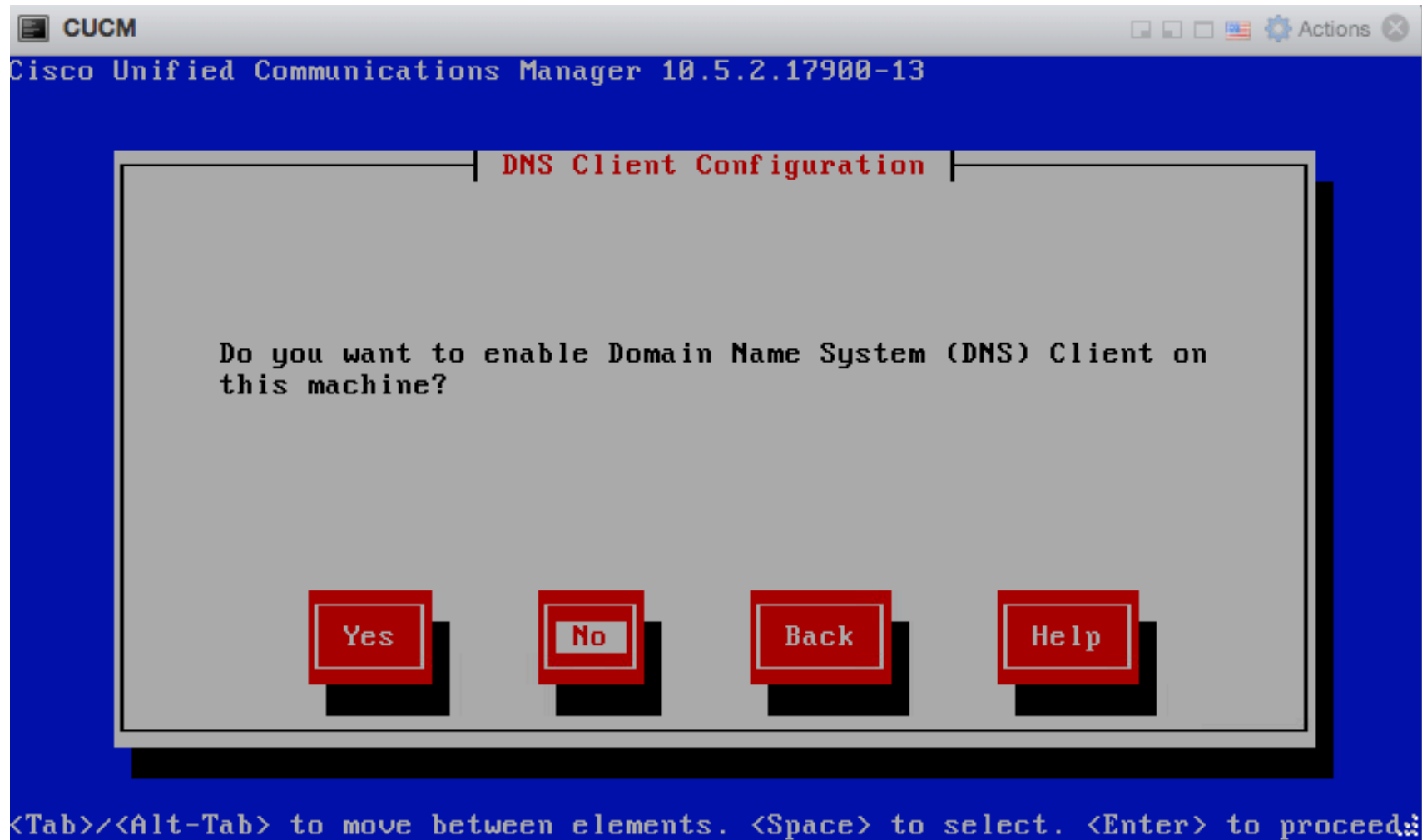
IP Mask 255.255.255.0

GW Address 172.16.0.1

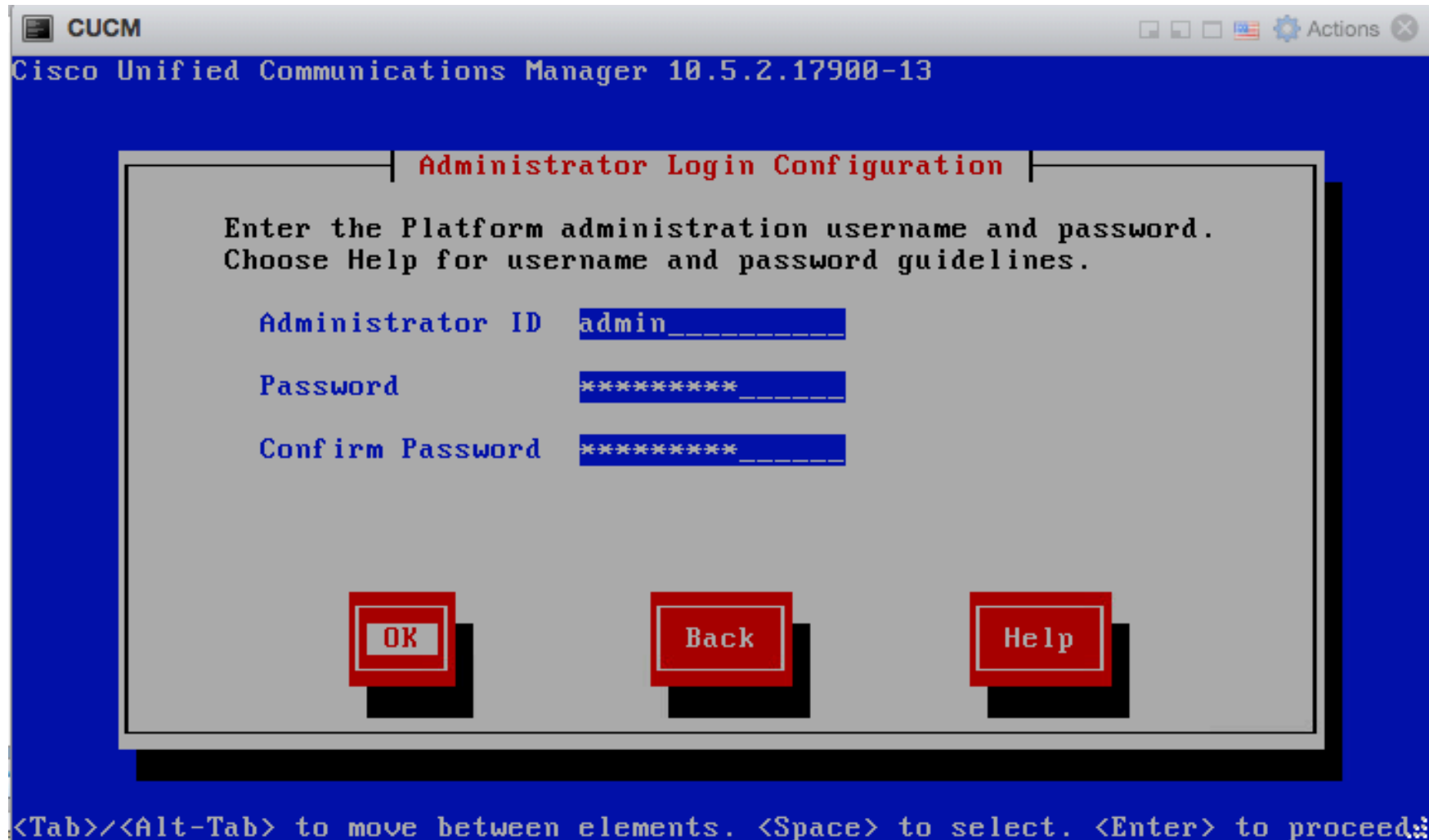
OK Back Help

<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed

Not enable DNS



Enter username and password



The screenshot shows the Cisco Unified Communications Manager (CUCM) Administrator Login Configuration screen. The window title is "CUCM" and the address bar shows "Cisco Unified Communications Manager 10.5.2.17900-13". The main content area is titled "Administrator Login Configuration" and contains the following text:

Enter the Platform administration username and password.
Choose Help for username and password guidelines.

The form has three input fields:

- Administrator ID:
- Password:
- Confirm Password:

At the bottom of the form, there are three buttons: "OK", "Back", and "Help".

At the bottom of the window, there is a status bar with the text: "<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed."

Additional information

CUCM

Cisco Unified Communications Manager 10.5.2.17900-13

Certificate Information

Enter information about your organization. This is used to generate security certificates for this node.

Organization Test-CUCM

Unit Aruba

Location Bogota

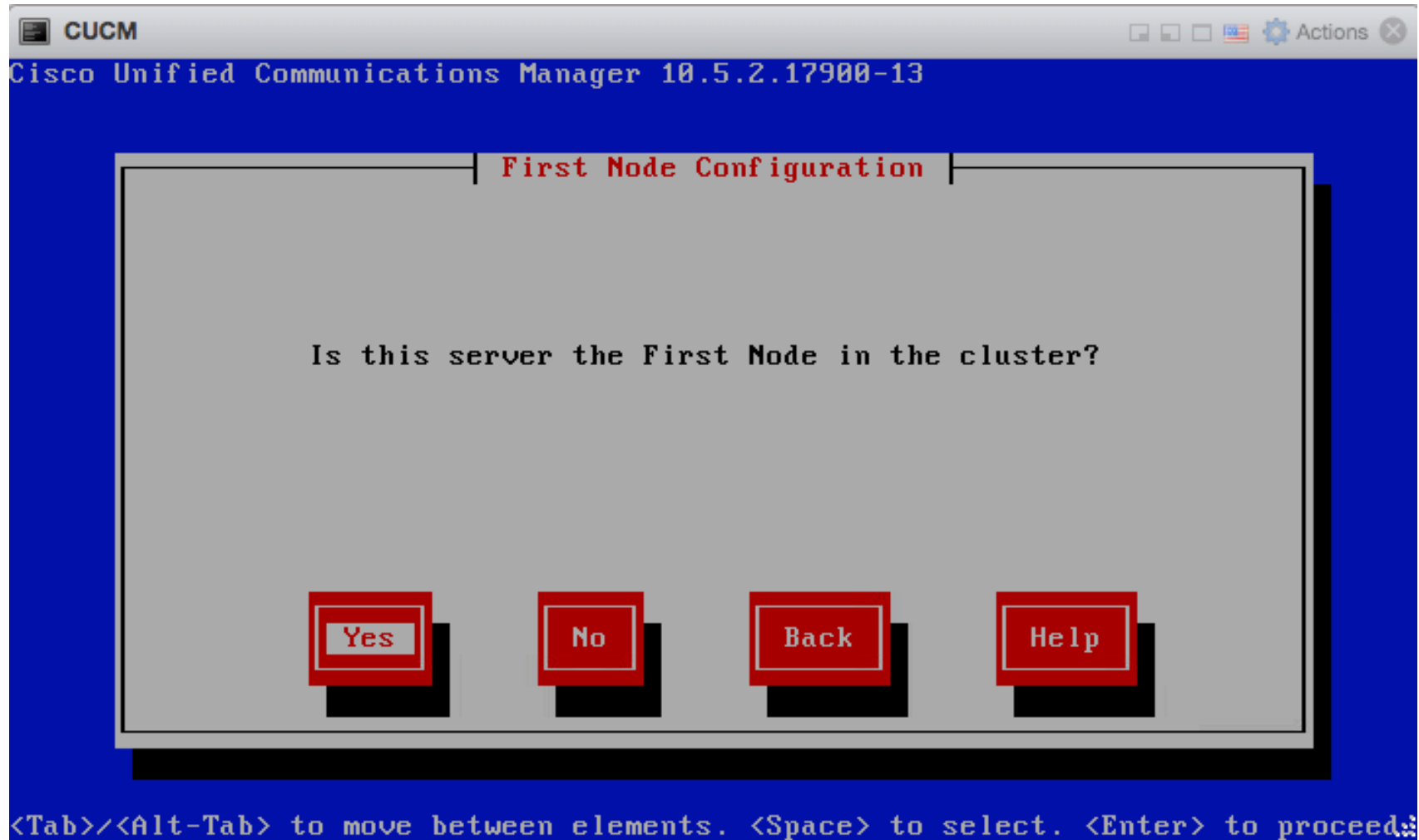
State Cundinamarca

Country Cocos (Keeling) Islands
Colombia
Comoros

OK Back Help

<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

First Node in cluster (Publisher)



Enter NTP server

CUCM

Cisco Unified Communications Manager 10.5.2.17900-13

Network Time Protocol Client Configuration

NTP Server 1 200.160.7.193____

NTP Server 2 _____

NTP Server 3 _____

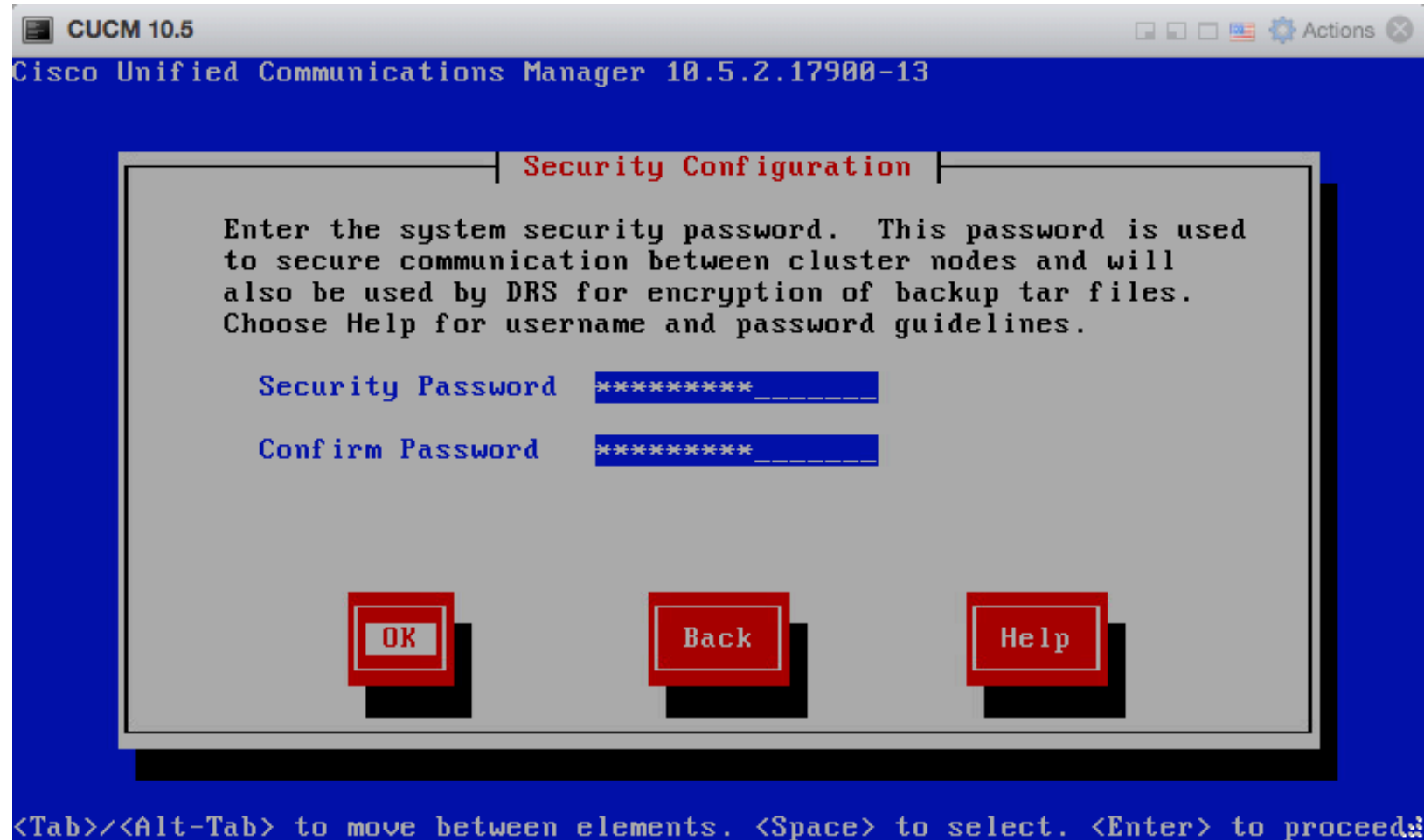
NTP Server 4 _____

NTP Server 5 _____

OK Back Help

<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

Enter password



The screenshot shows a terminal window titled "CUCM 10.5" with a subtitle "Cisco Unified Communications Manager 10.5.2.17900-13". The main content is a "Security Configuration" dialog box. It contains instructions to enter a system security password, which is used for securing communication between cluster nodes and for DRS backup encryption. Below the instructions are two input fields: "Security Password" and "Confirm Password", both masked with asterisks. At the bottom of the dialog are three buttons: "OK", "Back", and "Help". A footer at the bottom of the terminal window provides navigation instructions: "<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed."

CUCM 10.5

Cisco Unified Communications Manager 10.5.2.17900-13

Security Configuration

Enter the system security password. This password is used to secure communication between cluster nodes and will also be used by DRS for encryption of backup tar files. Choose Help for username and password guidelines.

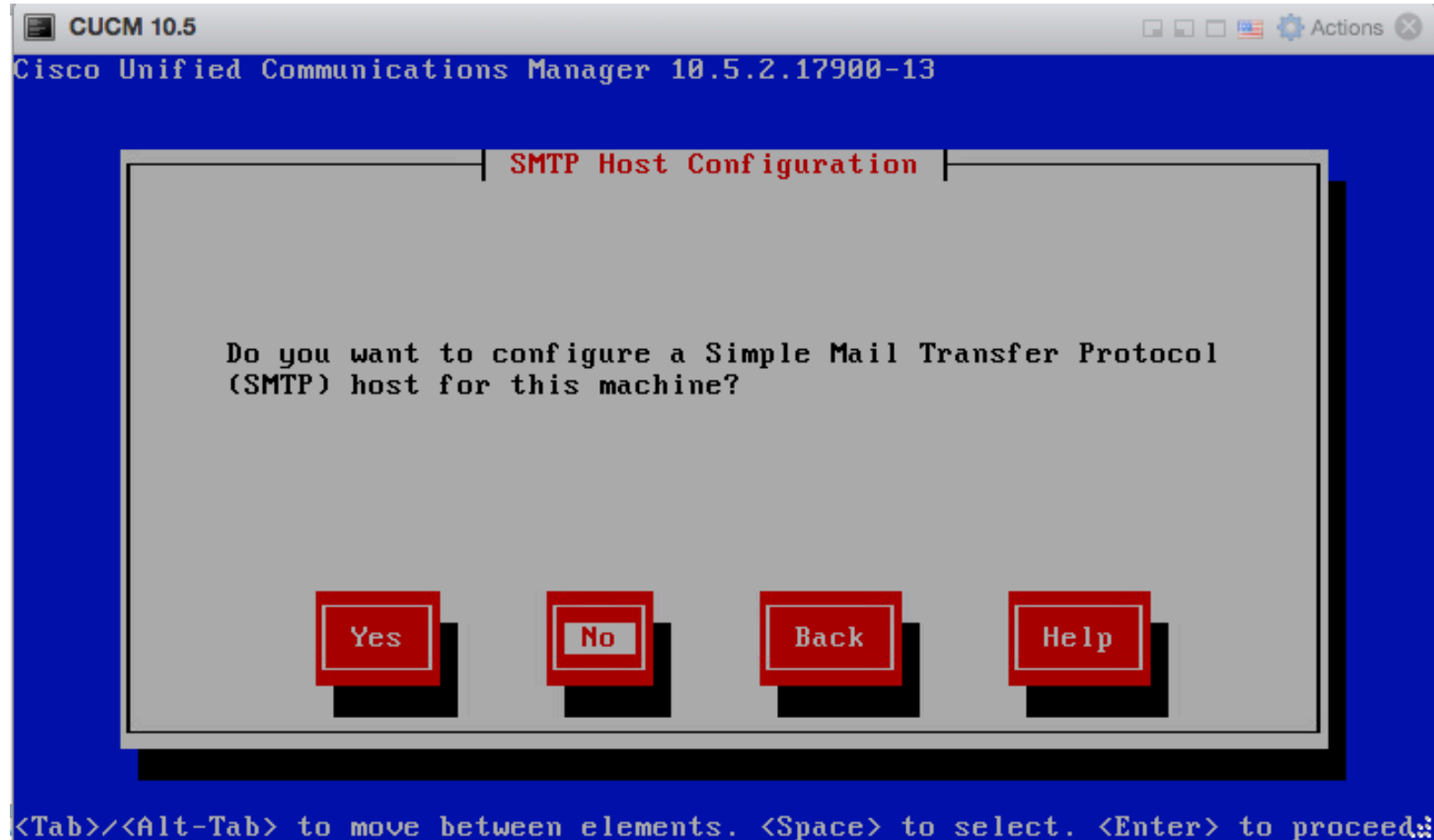
Security Password *****

Confirm Password *****

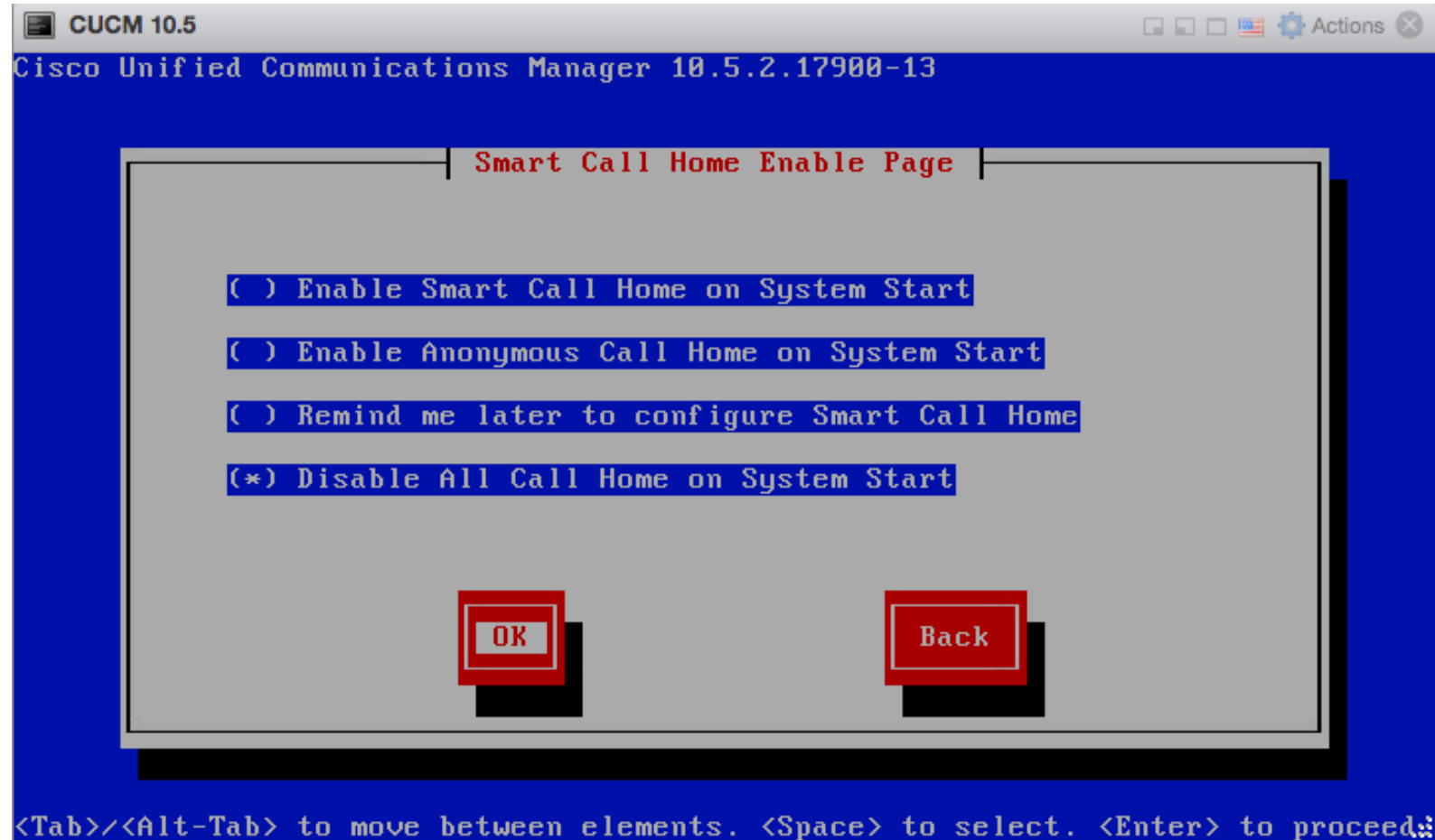
OK Back Help

<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed

Not enable SMTP



Disable Call Home (remote Cisco support)



Enter username password

CUCM 10.5

Cisco Unified Communications Manager 10.5.2.17900-13

Application User Configuration

The Application User username and password are used to log into the Application administrative webpage(s).

Application User Username adminapp_____

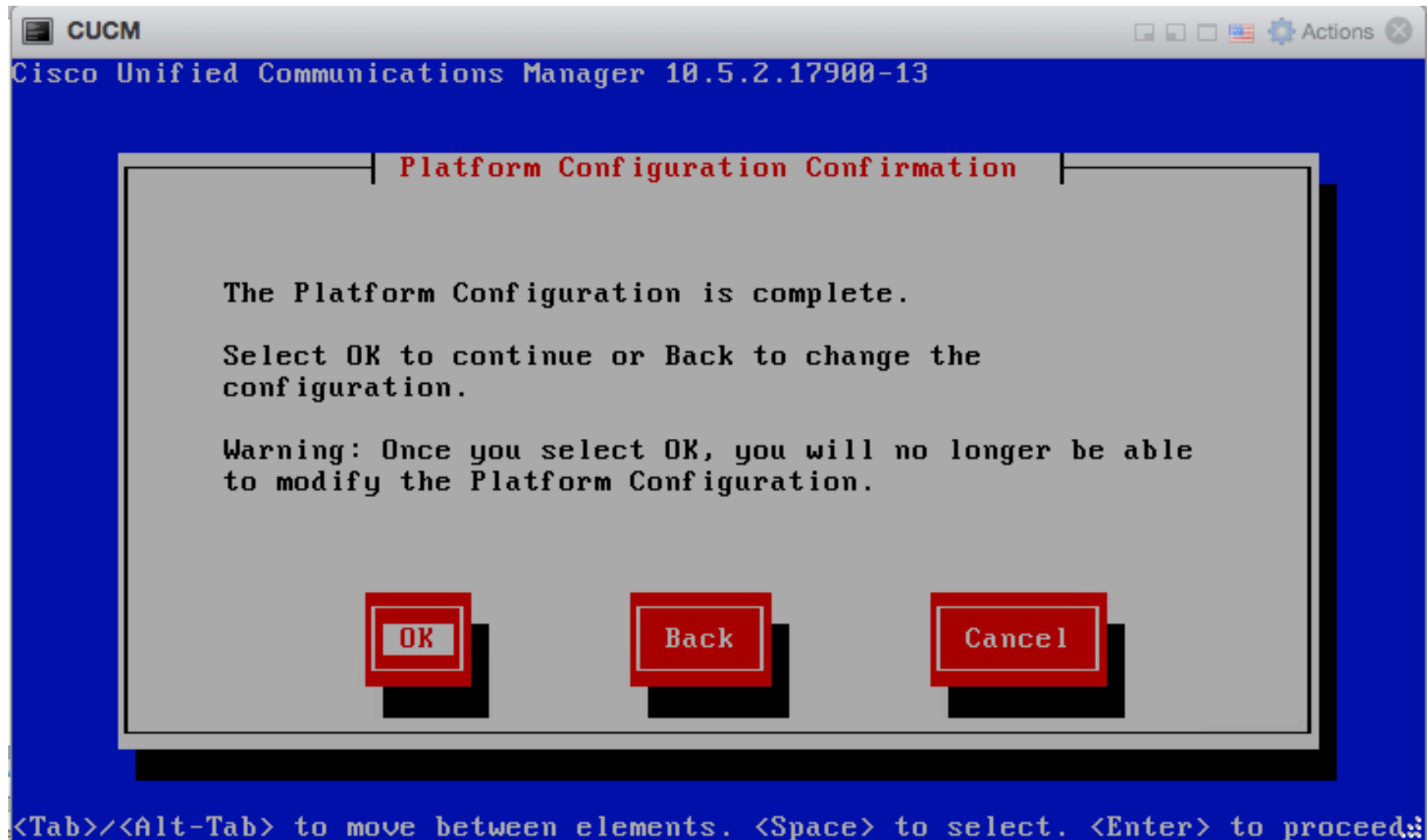
Application User Password *****

Confirm Application User Password *****

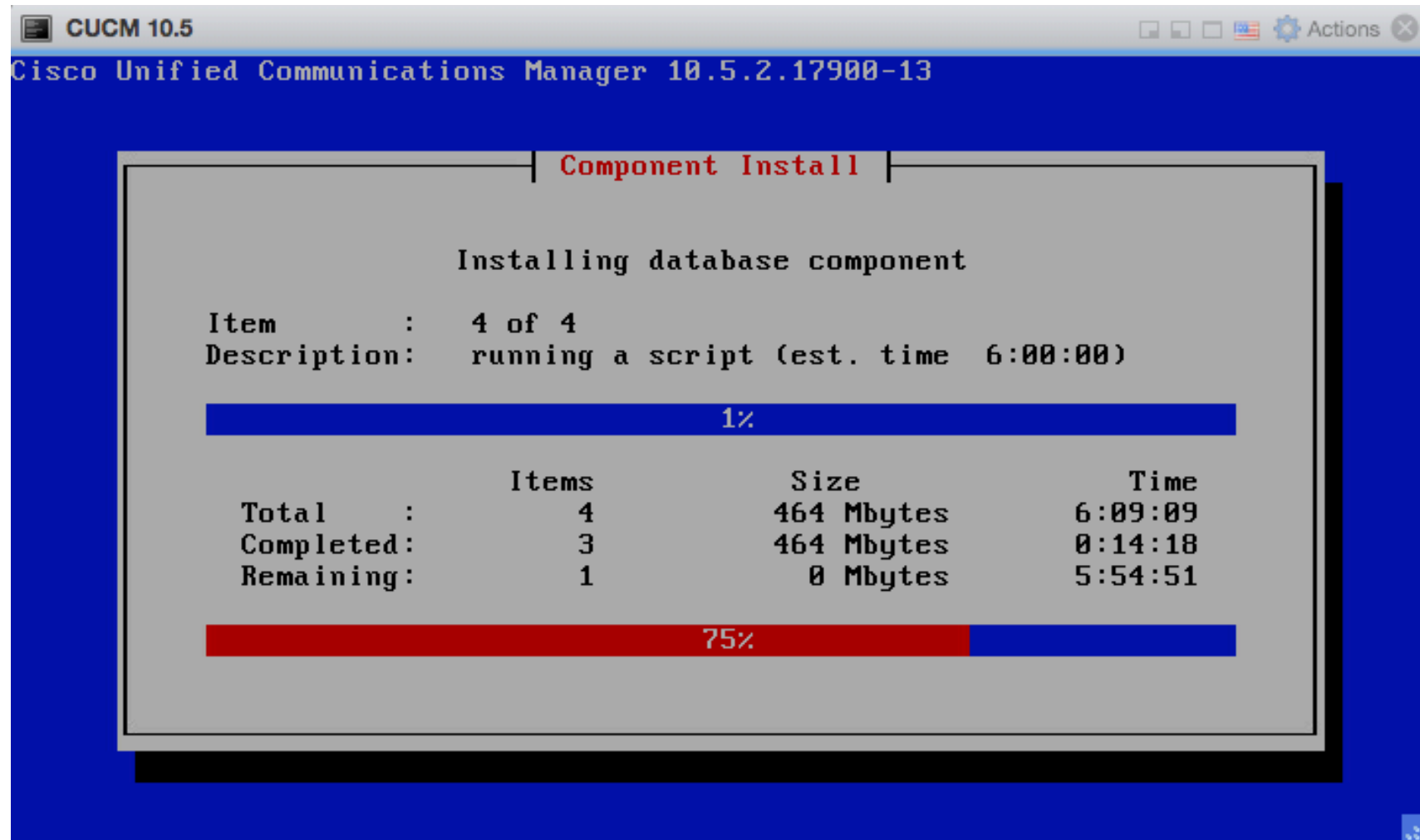
OK Back Help

<Tab>/<Alt-Tab> to move between elements. <Space> to select. <Enter> to proceed.

Confirm configuration



Installation starts



After 20min – CCUCM is ready to be configured



```
CUCM 10.5

The installation of Cisco Unified Communications Manager has completed successfully.

Cisco Unified Communications Manager 10.5.2.17900-13
CUCM login:

The installation of Cisco Unified Communications Manager has completed successfully.


Cisco Unified Communications Manager 10.5.2.17900-13
CUCM login: admin
Password:
Command Line Interface is starting up, please wait ...

Welcome to the Platform Command Line Interface

VMware Installation:
  2 vCPU: Intel(R) Core(TM) i5-7260U CPU @ 2.20GHz
  Disk 1: 80GB, Partitions aligned
  4096 Mbytes RAM

admin:
```


Access via browser


**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation **Cisco Unified CM Administration** **Go**

adminapp | [Search Documentation](#) | [About](#) | [Logout](#)

System ▾ | [Call Routing](#) ▾ | [Media Resources](#) ▾ | [Advanced Features](#) ▾ | [Device](#) ▾ | [Application](#) ▾ | [User Management](#) ▾ | [Bulk Administration](#) ▾ | [Help](#) ▾


 **The system is operating on demo licenses that will expire in 60 days. Add this system to a Cisco Prime License Manager and install sufficient licenses to cover its usage before expiration in order to avoid losing the ability to provision users and devices.**

 **WARNING: No backup device is configured. This is required to recover your system in case of failure.**

Cisco Unified CM Administration

System version: 10.5.2.17900-13

VMware Installation: 2 vCPU Intel(R) Core(TM) i5-7260U CPU @ 2.20GHz, disk 1: 80Gbytes, 4096Mbytes RAM, Partitions aligned



Last Successful Logon: Unavailable

Copyright © 1999 - 2015 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

Click on System -> Servers

The screenshot displays the Cisco Unified CM Administration web interface. On the left, a navigation menu is open, showing the 'Server' category selected. The main content area features a search bar with the text 'address' and a filter dropdown set to 'begins with'. Below the search bar, a table lists servers. The table has three columns: 'Host Name/IP Address', 'Description', and 'Server Type'. The first row shows 'CUCM Voice/Video' in the 'Server Type' column. The URL at the bottom of the browser window is 'https://172.16.0.90/ccmadmin/serverFindList.do'.

Cisco Unified CM Administration

Navigation: Cisco Unified CM Administration Go

adminapp | Search Documentation | About | Logout

Resources Advanced Features Device Application User Management Bulk Administration Help

Server

- Cisco Unified CM
- Cisco Unified CM Group
- Presence Redundancy Groups
- Phone NTP Reference
- Date/Time Group
- BLF Presence Group
- Region Information
- Device Pool
- Device Mobility
- DHCP
- LDAP
- SAML Single Sign-On
- Cross-Origin Resource Sharing (CORS)
- Location Info
- MLPP
- Physical Location
- SRST
- Enterprise Parameters
- Enterprise Phone Configuration
- Service Parameters
- Security
- Application Server
- Licensing
- Geolocation Configuration
- Geolocation Filter
- E911 Messages


Rows per Page 50

address begins with Find Clear Filter

Host Name/IP Address	Description	Server Type
		CUCM Voice/Video

https://172.16.0.90/ccmadmin/serverFindList.do

Click on CUCM


**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation **Cisco Unified CM Administration** **Go**


adminapp | [Search Documentation](#) | [About](#) | [Logout](#)

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾



Find and List Servers

 Add New

Status

 1 records found


Servers (1 - 1 of 1) **Rows per Page** 50 ▾

Find Servers where **Host Name/IP Address** ▾ begins with ▾ **Find** **Clear Filter**  

Host Name/IP Address [▲]	Description	Server Type
CUCM		CUCM Voice/Video

Add New

Change the Name by IP Address




**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation **Cisco Unified CM Administration** **Go**


adminapp | [Search Documentation](#) | [About](#) | [Logout](#)

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Server Configuration **Related Links:** [Back To Find/List](#) **Go**

 Save  Delete  Add New

Status


 Status: Ready

Server Information


Server Type	CUCM Voice/Video
Database Replication	Publisher
Host Name/IP Address*	<input type="text" value="172.16.0.90"/>
IPv6 Address (for dual IPv4/IPv6)	<input type="text"/>
MAC Address	<input type="text"/>
Description	CUCM


Location Bandwidth Management Information

LBM Intercluster Replication Group View Details

 *- indicates required item.


Enable Auto registration




**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions


Navigation Cisco Unified CM Administration  Go

adminapp | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Cisco Unified CM Configuration Related Links: Back To Find/List  Go

 Save  Reset  Apply Config

 Status: Ready

Cisco Unified Communications Manager Information

Cisco Unified Communications Manager: CM_CUCM (used by 10 devices)


Server Information

CTI ID 1


Cisco Unified Communications Manager Server* 172.16.0.90


Cisco Unified Communications Manager Name* CM_CUCM

Description CUCM

Location Bandwidth Manager Group < None > 

Auto-registration Information

Universal Device Template* Sample Device Template with TAG usage examples 


Universal Line Template* Sample Line Template with TAG usage examples 

Starting Directory Number* 1000

Ending Directory Number* 1010

☐ Auto-registration Disabled on this Cisco Unified Communications Manager

Enter CUCM Group name


**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go
adminapp | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Cisco Unified CM Group Configuration Related Links: Back To Find/List Go

Save Delete Copy Reset Apply Config Add New

Status
 Status: Ready

Cisco Unified Communications Manager Group Information
Cisco Unified Communications Manager Group: CUCM-GP (used by 6 devices)

Cisco Unified Communications Manager Group Settings
Name*
☒ Auto-registration Cisco Unified Communications Manager Group


Cisco Unified Communications Manager Group Members
Available Cisco Unified Communications Managers

Selected Cisco Unified Communications Managers*

CM_CUCM

Save Delete Copy Reset Apply Config Add New

Enter NTP server

**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions


Navigation **Cisco Unified CM Administration**

adminapp | [Search Documentation](#) | [About](#) | [Logout](#)

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾


Phone NTP Reference Configuration Related Links: [Back To Find/List](#)

Status


 Update successful

Phone NTP Reference Information

IP Address*	<input type="text" value="146.164.48.5"/>
Description	<input type="text" value="NTP South America"/>
Mode*	<input type="text" value="Unicast"/>

 *- indicates required item.

Click on CMLocal





 **Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go


adminapp | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾



Find and List Date/Time Groups


 Add New  Select All  Clear All  Delete Selected

Status

 1 records found


Date/Time Group (1 - 1 of 1) Rows per Page 50 ▾

Find Date/Time Group where Group Name ▾ begins with ▾ Find Clear Filter  

<input type="checkbox"/>	Name ^	Time Zone	Copy
<input type="checkbox"/>	CMLocal	Etc/GMT	

Add New Select All Clear All Delete Selected

Enter timezone

**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation **Cisco Unified CM Administration** Go

adminapp | Search Documentation | About | Logout


System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Date/Time Group Configuration

Related Links: Back To Find/List Go

Save Delete Copy Reset Apply Config Add New

Status

 Status: Ready

Date/Time Group Information

Date/Time Group: CUCM-Time (used by 6 devices)

Group Name*

Time Zone* Entries with + are compatible with [legacy_phone loads](#)

Separator* (applies to Date Format only)

Date Format*

Time Format*

Phone NTP References for this Date/Time Group

Selected Phone NTP References**

Add Phone NTP References Remove Phone NTP References

Save Delete Copy Reset Apply Config Add New

Go to “Region”

The screenshot displays the Cisco Unified CM Administration web interface. On the left, a navigation menu is open, showing a tree structure of configuration options. The 'Region' option is highlighted. The main content area shows the 'Region' configuration page, which includes a table for defining regions. The table has columns for 'Region Name', 'Country Code', 'Area Code', 'City', 'State', and 'Zip'. The first row is populated with 'Bogota', '5', '164', 'Bogota', 'C', and '164.48.5'. Below the table, there are buttons for 'Add New', 'Apply Config', and 'Remove Phone NTP References'. The URL bar at the bottom shows 'https://172.16.0.90/ccmadmin/regionFindList.do'.

Cisco Unified CM Administration

Navigation: Cisco Unified CM Administration Go

adminapp | Search Documentation | About | Logout

Related Links: Back To Find/List Go

Reset Apply Config Add New

Server

- Cisco Unified CM
- Cisco Unified CM Group
- Presence Redundancy Groups
- Phone NTP Reference
- Date/Time Group
- BLF Presence Group
- Region Information**
- Device Pool
- Device Mobility
- DHCP
- LDAP
- SAML Single Sign-On
- Cross-Origin Resource Sharing (CORS)
- Location Info
- MLPP
- Physical Location
- SRST
- Enterprise Parameters
- Enterprise Phone Configuration
- Service Parameters
- Security
- Application Server
- Licensing
- Geolocation Configuration
- Geolocation Filter
- E911 Messages

Audio Codec Preference List

Region

by 6 devices)

rica/Bogota Entries with # are compatible with [legacy_phone loads](#)

(applies to Date Format only)

Date/Time Group

6.164.48.5


Add Phone NTP References Remove Phone NTP References

Apply Config Add New

es are ordered by highest priority

https://172.16.0.90/ccmadmin/regionFindList.do

New Region


**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go

[adminapp](#) | [Search Documentation](#) | [About](#) | [Logout](#)

System ▾ | Call Routing ▾ | Media Resources ▾ | Advanced Features ▾ | Device ▾ | Application ▾ | User Management ▾ | Bulk Administration ▾ | Help ▾


Region Configuration Related Links: [Back To Find/List](#) Go

 Save


Region Information

Name*

Save

 *- indicates required item.

CUCM-Region to CUCM-Region → 64Kbps



**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go
adminapp | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Region Configuration Related Links: Back To Find/List Go

Save Delete Reset Apply Config Add New

Status
 Add successful
 Click on the Reset button to have the changes take effect.

Region Information
Name* CUCM-Region


Region Relationships

Region	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls	Maximum Session Bit Rate for Immersive Video Calls
NOTE: Regions not displayed	Use System Default	Use System Default	Use System Default	Use System Default


Modify Relationship to other Regions

Regions	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls	Maximum Session Bit Rate for Immersive Video Calls
CUCM-Region Default	Keep Current Setting ▾	<div>64 kbps (G.722, G.711) ▾</div> <div><input type="radio"/> kbps</div>	<div><input checked="" type="radio"/> Keep Current Setting</div> <div><input type="radio"/> Use System Default</div> <div><input type="radio"/> None</div> <div><input type="radio"/> kbps</div>	<div><input checked="" type="radio"/> Keep Current Setting</div> <div><input type="radio"/> Use System Default</div> <div><input type="radio"/> None</div> <div><input type="radio"/> kbps</div>

Save Delete Reset Apply Config Add New

 *- indicates required item.

Config Device Pool


**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation **Cisco Unified CM Administration** [Go](#)

adminapp | [Search Documentation](#) | [About](#) | [Logout](#)

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Device Pool Configuration Related Links: [Back To Find/List](#) [Go](#)

 Save


Device Pool Information
Device Pool: New


Device Pool Settings
Device Pool Name*
Cisco Unified Communications Manager Group*
Calling Search Space for Auto-registration
Adjunct CSS
Reverted Call Focus Priority
Intercompany Media Services Enrolled Group

Roaming Sensitive Settings
Date/Time Group*
Region*
Media Resource Group List
Location
Network Locale
SRST Reference*
Connection Monitor Duration***
Single Button Barge*
Join Across Lines*
Physical Location
Device Mobility Group
Wireless LAN Profile Group [View Details](#)

Local Route Group Settings

Change names by IP Address





**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration  Go

adminapp | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Enterprise Parameters Configuration

 Save  Set to Default  Reset  Apply Config

Phone URL Parameters

URL Authentication	<input type="text" value="http://172.16.0.90:8080/ccmcip/authenticate.jsp"/>	
URL Directories	<input type="text" value="http://172.16.0.90:8080/ccmcip/xmldirectory.jsp"/>	
URL Idle	<input type="text"/>	
URL Idle Time	<input type="text" value="0"/>	<input type="text" value="0"/>
URL Information	<input type="text" value="http://172.16.0.90:8080/ccmcip/GetTelecasterHelpText.js"/>	
URL Messages	<input type="text"/>	
IP Phone Proxy Address	<input type="text"/>	
URL Services	<input type="text" value="http://172.16.0.90:8080/ccmcip/getservicesmenu.jsp"/>	

Secured Phone URL Parameters

Secured Authentication URL	<input type="text" value="https://172.16.0.90:8443/ccmcip/authenticate.jsp"/>	
Secured Directory URL	<input type="text" value="https://172.16.0.90:8443/ccmcip/xmldirectory.jsp"/>	
Secured Idle URL	<input type="text"/>	
Secured Information URL	<input type="text" value="https://172.16.0.90:8443/ccmcip/GetTelecasterHelpText.j"/>	
Secured Messages URL	<input type="text"/>	
Secured Services URL	<input type="text" value="https://172.16.0.90:8443/ccmcip/getservicesmenu.jsp"/>	

User Data Service Parameters


Enable All User Search *	<input type="text" value="True"/>	True
User Search Limit *	<input type="text" value="64"/>	64
Number of Digits to Match *	<input type="text" value="4"/>	4
Personal Directory Timeout *	<input type="text" value="86400"/>	86400

Go to Unified Serviceability → Service Activation

The screenshot displays the Cisco Unified Serviceability web interface. The top navigation bar includes the Cisco logo, the title "Cisco Unified Serviceability For Cisco Unified Communications Solutions", and a navigation menu with "Navigation", "Cisco Unified Serviceability", and "Go". Below this, there's a secondary navigation bar with "adminapp", "About", and "Logout". A main menu bar contains "Alarm", "Trace", "Tools", "Snmp", "CallHome", and "Help". The "Service Activation" menu is open, showing options: "Service Activation", "Control Center - Feature Services", "Control Center - Network Services", "Serviceability Reports Archive", "Audit Log Configuration", "Locations", and "CDR Management". The "Status" section shows "Ready". The "Select Server" section has a "Server*" dropdown and a "Go" button. Below this is a "CM Services" table with columns "Service Name" and "Activation Status".

Service Name	Activation Status
<input type="checkbox"/> Cisco CallManager	Deactivated
<input type="checkbox"/> Cisco Unified Mobile Voice Access Service	Deactivated
<input type="checkbox"/> Cisco IP Voice Media Streaming App	Deactivated
<input type="checkbox"/> Cisco CTIManager	Deactivated
<input type="checkbox"/> Cisco Extension Mobility	Deactivated
<input type="checkbox"/> Cisco Extended Functions	Deactivated
<input type="checkbox"/> Cisco DHCP Monitor Service	Deactivated
<input type="checkbox"/> Cisco Intercluster Lookup Service	Deactivated
<input type="checkbox"/> Cisco Location Bandwidth Manager	Deactivated
<input type="checkbox"/> Cisco Directory Number Alias Sync	Deactivated
<input type="checkbox"/> Cisco Directory Number Alias Lookup	Deactivated
<input type="checkbox"/> Cisco Dialed Number Analyzer Server	Deactivated
<input type="checkbox"/> Cisco Dialed Number Analyzer	Deactivated
<input type="checkbox"/> Cisco Tftp	Deactivated

Check All Services → Save


**Cisco Unified Serviceability**
For Cisco Unified Communications Solutions


Navigation Cisco Unified Serviceability Go


adminapp | About | Logout


Alarm Trace Tools Snmp CallHome Help

Service Activation Related Links: Control Center - Feature Services Go

 Save

 Set to Default

 Refresh

Status:
 Ready

Select Server
Server* 172.16.0.90--CUCM Voice/Video Go
☒ Check All Services


CM Services

	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CallManager	Deactivated
<input checked="" type="checkbox"/>	Cisco Unified Mobile Voice Access Service	Deactivated
<input checked="" type="checkbox"/>	Cisco IP Voice Media Streaming App	Deactivated
<input checked="" type="checkbox"/>	Cisco CTIManager	Deactivated
<input checked="" type="checkbox"/>	Cisco Extension Mobility	Deactivated
<input checked="" type="checkbox"/>	Cisco Extended Functions	Deactivated
<input checked="" type="checkbox"/>	Cisco DHCP Monitor Service	Deactivated
<input checked="" type="checkbox"/>	Cisco Intercluster Lookup Service	Deactivated
<input checked="" type="checkbox"/>	Cisco Location Bandwidth Manager	Deactivated
<input checked="" type="checkbox"/>	Cisco Directory Number Alias Sync	Deactivated
<input checked="" type="checkbox"/>	Cisco Directory Number Alias Lookup	Deactivated
<input checked="" type="checkbox"/>	Cisco Dialed Number Analyzer Server	Deactivated
<input checked="" type="checkbox"/>	Cisco Dialed Number Analyzer	Deactivated
<input checked="" type="checkbox"/>	Cisco Tftp	Deactivated

CTI Services

	Service Name	Activation Status
--	--------------	-------------------

Services activated

**Cisco Unified Serviceability**
For Cisco Unified Communications Solutions

Navigation Cisco Unified Serviceability Go

adminapp About Logout

Alarm Trace Tools Snmp CallHome Help

Service Activation Related Links: Control Center - Feature Services Go

Save Set to Default Refresh

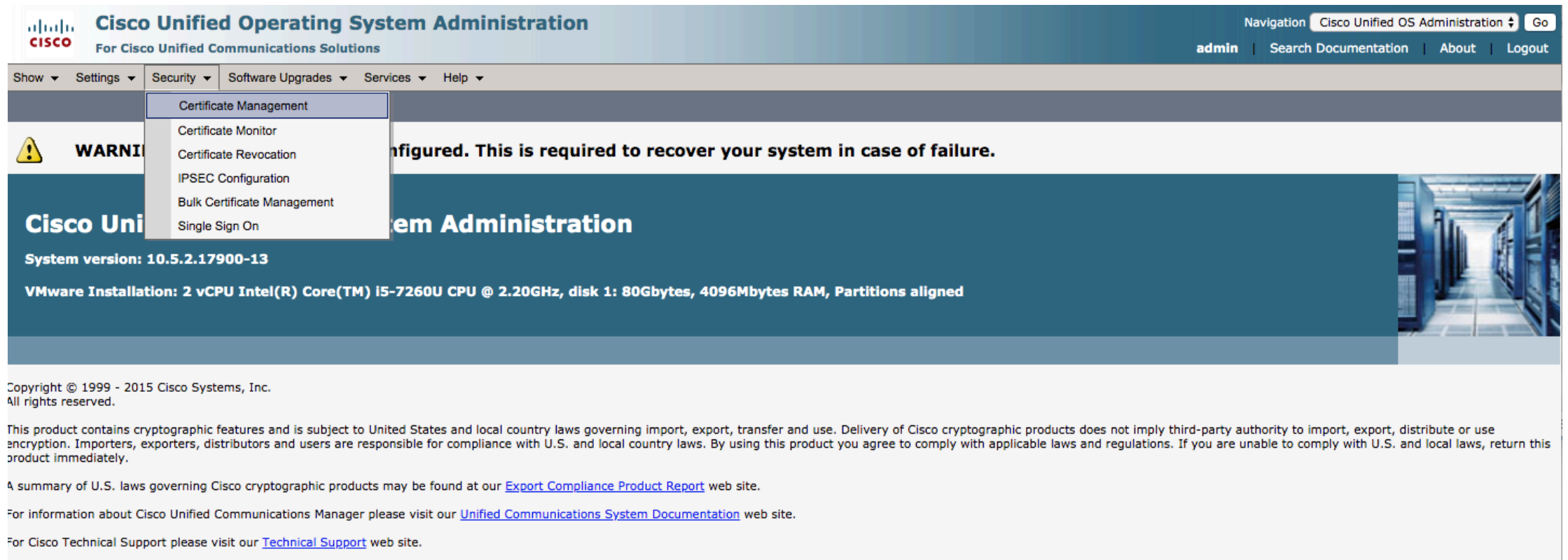
Status:
Ready

Select Server
Server* 172.16.0.90--CUCM Voice/Video Go
☐ Check All Services

CM Services

	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CallManager	Activated
<input checked="" type="checkbox"/>	Cisco Unified Mobile Voice Access Service	Activated
<input checked="" type="checkbox"/>	Cisco IP Voice Media Streaming App	Activated
<input checked="" type="checkbox"/>	Cisco CTIManager	Activated
<input checked="" type="checkbox"/>	Cisco Extension Mobility	Activated
<input checked="" type="checkbox"/>	Cisco Extended Functions	Activated
<input checked="" type="checkbox"/>	Cisco DHCP Monitor Service	Activated
<input checked="" type="checkbox"/>	Cisco Intercluster Lookup Service	Activated
<input checked="" type="checkbox"/>	Cisco Location Bandwidth Manager	Activated
<input checked="" type="checkbox"/>	Cisco Directory Number Alias Sync	Activated
<input checked="" type="checkbox"/>	Cisco Directory Number Alias Lookup	Activated
<input checked="" type="checkbox"/>	Cisco Dialed Number Analyzer Server	Activated
<input checked="" type="checkbox"/>	Cisco Dialed Number Analyzer	Activated
<input checked="" type="checkbox"/>	Cisco Tftp	Activated

Go to OS Administration → Certificate Management



Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration Go

admin | Search Documentation | About | Logout

Show Settings Security Software Upgrades Services Help

Certificate Management

- Certificate Monitor
- Certificate Revocation
- IPSEC Configuration
- Bulk Certificate Management
- Single Sign On

WARNI

Cisco Unified Operating System Administration

System version: 10.5.2.17900-13

VMware Installation: 2 vCPU Intel(R) Core(TM) i5-7260U CPU @ 2.20GHz, disk 1: 80Gbytes, 4096Mbytes RAM, Partitions aligned

Copyright © 1999 - 2015 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

Download the Manufacturing root certificate

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration Go
admin | Search Documentation | About | Logout

Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

CallManager-trust	Cisco_Manufacturing_CA	CA-signed	Cisco_Manufacturing_CA	Cisco_Root_CA_2048	05/14/2029	
CallManager-trust	ACT2_SUDI_CA	CA-signed	ACT2_SUDI_CA	Cisco_Root_CA_2048	05/14/2029	
CAPF	CAPF-f4b5a296	Self-signed	CAPF-f4b5a296	CAPF-f4b5a296	04/07/2024	Self-signed certificate generated by system
CAPF-trust	Cisco_Manufacturing_CA_SHA2	CA-signed	Cisco_Manufacturing_CA_SHA2	Cisco_Root_CA_M2	11/12/2037	
CAPF-trust	Cisco_Root_CA_2048	Self-signed	Cisco_Root_CA_2048	Cisco_Root_CA_2048	05/14/2029	
CAPF-trust	Cisco_Root_CA_M2	Self-signed	Cisco_Root_CA_M2	Cisco_Root_CA_M2	11/12/2037	
CAPF-trust	CAPF-f4b5a296	Self-signed	CAPF-f4b5a296	CAPF-f4b5a296	04/07/2024	
CAPF-trust	CAP-RTP-001	Self-signed	CAP-RTP-001	CAP-RTP-001	02/06/2023	
CAPF-trust	CAP-RTP-002	Self-signed	CAP-RTP-002	CAP-RTP-002	10/10/2023	
CAPF-trust	Cisco_Manufacturing_CA	CA-signed	Cisco_Manufacturing_CA	Cisco_Root_CA_2048	05/14/2029	
CAPF-trust	ACT2_SUDI_CA	CA-signed	ACT2_SUDI_CA	Cisco_Root_CA_2048	05/14/2029	
ipsec	CUCM	Self-signed	CUCM	CUCM	04/07/2024	Self-signed certificate generated by system
ipsec-trust	CUCM	Self-signed	CUCM	CUCM	04/07/2024	Trust Certificate
ITLRecovery	ITLRECOVERY_CUCM	Self-signed	ITLRECOVERY_CUCM	ITLRECOVERY_CUCM	04/04/2039	Self-signed certificate generated by system
tomcat	CUCM	Self-signed	CUCM	CUCM	04/07/2024	Self-signed certificate generated by system
tomcat-trust	VeriSign_Class_3_Secure_Server_CA_-_G3	CA-signed	VeriSign_Class_3_Secure_Server_CA_-_G3	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/07/2020	Call Home Server Certificate
tomcat-trust	CUCM	Self-signed	CUCM	CUCM	04/07/2024	Trust Certificate
TVS	CUCM	Self-signed	CUCM	CUCM	04/07/2024	Self-signed certificate generated by system

.PEM file to your computer

Cisco

Cisco Unified Operating System

For Cisco Unified Communications Solutions

Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾

Certificate List

Generate Self-signed

Upload Certificate/Certificate chain

CallManager-trust	Cisco_Manufacturing_CA
CallManager-trust	ACT2_SUDI_CA
CAPF	CAPF-f4b5a296
CAPF-trust	Cisco_Manufacturing_CA_SHA2
CAPF-trust	Cisco_Root_CA_2048
CAPF-trust	Cisco_Root_CA_M2
CAPF-trust	CAPF-f4b5a296
CAPF-trust	CAP-RTP-001
CAPF-trust	CAP-RTP-002
CAPF-trust	Cisco_Manufacturing_CA
CAPF-trust	ACT2_SUDI_CA
ipsec	CUCM
ipsec-trust	CUCM
ITLRecovery	ITLRECOVERY_CUCM
tomcat	CUCM
tomcat-trust	VeriSign_Class_3_Secure_Server_CA_-_G3
tomcat-trust	CUCM
TVS	CUCM

Delete

Download .PEM File

Status

Status: Ready

Certificate Settings

File Name: Cisco_Root_CA_2048.pem
Certificate Purpose: CAPF-trust
Certificate Type: trust-certs
Certificate Group: product-cm
Description(friendly name):

Certificate File Data

[
Version: V3
Serial Number: 5FF87B282B54DC8D42A315B568C9ADFF
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=Cisco Root CA 2048, O=Cisco Systems
Validity From: Fri May 14 15:17:12 COT 2004
To: Mon May 14 15:25:42 COT 2029
Subject Name: CN=Cisco Root CA 2048, O=Cisco Systems
Key: RSA (1.2.840.113549.1.1.1)
Key value:
308201080282010100b09ab9aba7af0a77a7e271b6b4666294788847c66255844032bfc0ab2ea51c71d6bc6e7ba8aaba6ed2158848459da2fc83d0ccb98ce02668704a78df21179ef46105c915c8cf16da3561899443a884a83198789bb94e6f2c53126ccd1dad2b24bb31c42bff83446fb63d247709eabf2aa81f6a56f6200f1154978175a725ce596a8265efb7eae7e28d758b6ef2dd4fa65e629ccf100a64d04e6dce2bcc5bf560a527478d69f47fce1b70de701b20d66ecda601a83c12d2a93fa06b5ebb8e208b7a91e3b568eea0e7c40

Delete

Download .PEM File

Close

Navigation Cisco Unified OS Administration ▾ Go


admin | Search Documentation | About | Logout

05/14/2029	
05/14/2029	
04/07/2024	Self-signed certificate generated by system
11/12/2037	
05/14/2029	
11/12/2037	
04/07/2024	
02/06/2023	
10/10/2023	
05/14/2029	
05/14/2029	
04/07/2024	Self-signed certificate generated by system
04/07/2024	Trust Certificate
04/04/2039	Self-signed certificate generated by system
04/07/2024	Self-signed certificate generated by system
02/07/2020	Call Home Server Certificate
04/07/2024	Trust Certificate
04/07/2024	Self-signed certificate generated by system

Enable 802.1X on Cisco IP Phones

- Out of the box, Cisco IP phones are capable of 802.1X but they are not enabled for 802.1X. it is possible to enable 802.1X on phones by enabling 802.1X in the phone configuration file.
- Next time the phone resets and downloads its configuration file, 802.1X is enabled for all supported EAP methods. There is no way to disable individual EAP methods on a Cisco IP phone.
- Enabling 802.1X on phones first is a best practice:
 - Bring up new phones in a physically secure staging area where the access ports are not enabled for 802.1X. This allows the phones to access the network and download the needed configuration files.

Register the Cisco IP Phone to CUCM

**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go

adminapp | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Find and List Phones Related Links: [Actively Logged In Device Report](#) Go

+ Add New ⌘ Select All ⌘ Clear All ✖ Delete Selected ↺ Reset Selected ✎ Apply Config to Selected




Status

i 1 records found

Phone (1 - 1 of 1) Rows per Page 50 ▾


Find Phone where Device Type contains 7821 Find Clear Filter + -

Select item or enter search text ▾

<input type="checkbox"/>		Device Name(Line) ^	Description	Device Type	Device Protocol	Status	IPv4 Address	Copy	Super Copy
<input type="checkbox"/>	 7821	SEPE0D173E55320	Auto 1002	Cisco 7821	SIP	Registered with 172.16.0.90	10.10.0.5		

Add New Select All Clear All Delete Selected Reset Selected Apply Config to Selected

Enable 802.1X Authentication







 **Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration

adminapp | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Phone Configuration Related Links: Back To Find/List

 Save  Delete  Copy  Reset  Apply Config  Add New

IPv6 Log Server	<input type="text"/>	<input type="checkbox"/>
Outbound Rollover*	Disabled ▾	<input type="checkbox"/>
Cisco Discovery Protocol (CDP): Switch Port*	Enabled ▾	<input type="checkbox"/>
Cisco Discovery Protocol (CDP): PC Port*	Enabled ▾	<input type="checkbox"/>
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port*	Enabled ▾	<input type="checkbox"/>
Link Layer Discovery Protocol (LLDP): PC Port*	Enabled ▾	<input type="checkbox"/>
LLDP Asset ID	<input type="text"/>	
LLDP Power Priority*	Unknown ▾	
802.1x Authentication*	Enabled ▾	<input checked="" type="checkbox"/>
Automatic Port Synchronization*	Disabled ▾	<input type="checkbox"/>
Switch Port Remote Configuration*	Disabled ▾	<input type="checkbox"/>
PC Port Remote Configuration*	Disabled ▾	<input type="checkbox"/>
SSH Access*	Disabled ▾	<input type="checkbox"/>
Incoming Call Toast Timer*	5 ▾	<input type="checkbox"/>
Line Key Barge*	cBarge ▾	
Ring Locale*	Default ▾	<input type="checkbox"/>
TLS Resumption Timer*	3600 <input type="text"/>	<input type="checkbox"/>
FIPS Mode*	Disabled ▾	<input type="checkbox"/>
HOLD/RESUME Key*	HOLD/RESUME Key ▾	<input type="checkbox"/>



a Hewlett Packard
Enterprise company

Task: Config Clearpass

Add the switch as Device

The screenshot displays the Aruba ClearPass Policy Manager web interface. The left sidebar contains a navigation menu with sections: Dashboard, Monitoring, Configuration, Posture, Enforcement, Network, Profile and Network Scan, Policy Simulation, and Administration. The 'Configuration' section is expanded, showing a tree view where 'Network' > 'Devices' is selected. The main content area shows the breadcrumb 'Configuration » Network » Devices' and a list of network devices. An 'Add' button is visible. A modal dialog titled 'Edit Device Details' is open, showing tabs for 'Device', 'SNMP Read Settings', 'SNMP Write Settings', 'CLI Settings', 'OnConnect Enforcement', and 'Attributes'. The 'Device' tab is active, displaying fields for Name, IP or Subnet Address, Description, RADIUS Shared Secret, TACACS+ Shared Secret, Vendor Name, Enable RADIUS CoA, and Enable RadSec. The 'Name' field contains '2930F switch', 'IP or Subnet Address' contains '172.16.100.1', 'Description' contains 'Aruba Access Switch', 'Vendor Name' is set to 'Aruba', and 'Enable RADIUS CoA' is checked with 'RADIUS CoA Port' set to '3799'. At the bottom of the dialog are 'Copy', 'Save', and 'Cancel' buttons. The footer of the interface shows copyright information for Hewlett Packard Enterprise Development LP, the date and time 'May 28, 2019 07:29:31 COT', and the version 'ClearPass Policy Manager 6.7.9.109195 on CLABV platform'.

aruba ClearPass Policy Manager

Configuration » Network » Devices

Network Devices

Add

Edit Device Details

Device SNMP Read Settings SNMP Write Settings CLI Settings OnConnect Enforcement Attributes

Name: 2930F switch

IP or Subnet Address: 172.16.100.1 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)

Description: Aruba Access Switch

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Vendor Name: Aruba

Enable RADIUS CoA: ☒ RADIUS CoA Port: 3799

Enable RadSec: ☐

Copy Save Cancel

© Copyright 2018 Hewlett Packard Enterprise Development LP May 28, 2019 07:29:31 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Import Cisco Root certificates

aruba ClearPass Policy Manager Menu

Administration » Certificates » Trust List

Certificate Trust List

[+ Add](#)

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Show records

#	<input type="checkbox"/>	Subject	Validity	Enabled
1.	<input type="checkbox"/>	CN=Cisco Manufacturing CA,O=Cisco Systems	Valid	Enabled
2.	<input type="checkbox"/>	CN=Cisco Root CA 2048,O=Cisco Systems	Valid	Enabled
3.	<input type="checkbox"/>	CN=CAP-RTP-001,O=Cisco Systems	Valid	Disabled
4.	<input type="checkbox"/>	CN=CAP-RTP-002,O=Cisco Systems	Valid	Disabled
5.	<input type="checkbox"/>	CN=Cisco Manufacturing CA SHA2,O=Cisco	Valid	Disabled

Showing 1-5 of 5

© Copyright 2018 Hewlett Packard Enterprise Development LP May 28, 2019 09:29:39 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Create the role “IP-Phone”

The screenshot displays the Aruba ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with categories like Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'ClearPass Policy Manager' and shows the 'Roles' configuration page. A modal dialog box titled 'Add New Role' is open in the center, allowing the user to create a new role. The 'Name' field is populated with 'IP-Phone' and the 'Description' field contains 'Role in Clearpass'. The background shows a table of existing roles, including [AirGroup v1], [Guest], [MAC Caching], and various [Onboard] roles for different operating systems.

Aruba ClearPass Policy Manager

Configuration » Identity » Roles

Roles

Roles exist independently of an individual service and can be accessed globally through the role-mapping policy of any service.

Filter: Name contains [] Go Clear Filter

Show 20 records

Add New Role

Name: IP-Phone

Description: Role in Clearpass

Save Cancel

#	Name	Description
1.	[AirGroup v1]	Role for an AirGroup protocol version 1 request
2.	[AirGroup v2]	Role for an AirGroup protocol version 2 request
3.	[AirGroup v3]	Role for an AirGroup protocol version 3 request
4.	[AirGroup v4]	Role for an AirGroup protocol version 4 request
5.	[BYOD]	Role for a BYOD device
6.	[Cisco Duo]	Role for a Cisco Duo device
7.	[Cisco Duo v2]	Role for a Cisco Duo v2 device
8.	[Cisco Duo v3]	Role for a Cisco Duo v3 device
9.	[Cisco Duo v4]	Role for a Cisco Duo v4 device
10.	[Cisco Duo v5]	Role for a Cisco Duo v5 device
11.	[Guest]	Default role for a Guest
12.	[Guest]	Default role for a Guest
13.	[MAC Caching]	Default role applied during MAC caching
14.	[Onboard Android]	Role for an Android device being provisioned
15.	[Onboard Chromebook]	Role for Chromebook device being provisioned
16.	[Onboard iOS]	Role for an iOS device being provisioned
17.	[Onboard Linux]	Role for Linux device being provisioned
18.	[Onboard Mac OS X]	Role for a Mac OS X device being provisioned
19.	[Onboard Windows]	Role for a Windows device being provisioned
20.	[Other]	Default role for another user or device

© Copyright 2018 Hewlett Packard Enterprise Development LP Apr 12, 2019 16:18:44 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Create the role “CiscoPhone”

Edit Role [X]

Name:	<input type="text" value="CiscoPhone"/>
Description:	<div>Cisco Phone - Role Definition</div>

Save **Cancel**

Tag Cisco Phone MAC Addresses

Edit Role [X]

Name:	<input type="text" value="IP-Phone"/>
Description:	<div>Role in Clearpass</div>

Save **Cancel**

Map Cisco Phones to “IP-Phone” Tag

Click on “Guest Roles”

The screenshot displays the Aruba ClearPass Policy Manager web interface. The left sidebar contains a navigation menu with categories: Dashboard, Monitoring, Configuration, Identity, Posture, Enforcement, Network, Profile and Network Scan, and Administration. The 'Configuration' menu is expanded, showing sub-items like Methods, Sources, Single Sign-On (SSO), Local Users, Endpoints, Static Host Lists, Roles, and Role Mappings. The 'Role Mappings' item is selected. The main content area shows the breadcrumb 'Configuration » Identity » Role Mappings' and the title 'Role Mappings'. A descriptive paragraph explains that after authentication, a ClearPass service invokes its role-mapping policy to assign roles to the client. Below this is a filter section with a dropdown for 'Name', a search box, and buttons for 'Go' and 'Clear Filter'. A table lists two role mappings: '[AirGroup Version Match]' and '[Guest Roles]'. The '[Guest Roles]' entry is highlighted in yellow. At the bottom of the table, it says 'Showing 1-2 of 2' and provides buttons for 'Copy', 'Export', and 'Delete'.

aruba ClearPass Policy Manager Menu

Configuration » Identity » Role Mappings

Role Mappings

After authenticating a request, a ClearPass service invokes its role-mapping policy, resulting in assignment of a role(s) to the client. This role becomes the identity component of enforcement policy decisions.

Filter: Name contains [] Go Clear Filter Show 20 records

#	Name	Description	Default Role
1.	[AirGroup Version Match]	System-defined mapping to identify the protocol version of an AirGroup request	[AirGroup v1]
2.	[Guest Roles]	The roles used by Guest.	[Employee]

Showing 1-2 of 2 Copy Export Delete

Click on “Add Rule”

The screenshot shows the Aruba ClearPass Policy Manager web interface. The left sidebar contains a navigation menu with sections: Dashboard, Monitoring, Configuration (highlighted), Identity, Posture, Enforcement, Network, Profile and Network Scan, and Administration. Under Configuration, there are sub-items: Methods, Sources, Single Sign-On (SSO), Local Users, Endpoints, Static Host Lists, Roles, and Role Mappings (highlighted). The main content area is titled 'ClearPass Policy Manager' and shows the breadcrumb 'Configuration » Identity » Role Mappings » Edit - [Guest Roles]'. Below this is the 'Role Mappings - [Guest Roles]' section with tabs for Summary, Policy, and Mapping Rules (highlighted). The Mapping Rules tab displays the 'Rules Evaluation Algorithm' set to 'Select first match' and a table of 'Role Mapping Rules'. The table has two columns: 'Conditions' and 'Role Name'. It lists three rules: 1. (GuestUser:Role ID EQUALS 1) for [Contractor], 2. (GuestUser:Role ID EQUALS 2) for [Guest], and 3. (GuestUser:Role ID EQUALS 3) for [Employee]. Below the table is an 'Add Rule' button (highlighted with a red box), along with 'Move Up', 'Move Down', 'Edit Rule', and 'Remove Rule' buttons. At the bottom of the main area are 'Back to Role Mappings', 'Copy', 'Save', and 'Cancel' buttons. The footer contains copyright information, a timestamp 'Apr 11, 2019 16:41:46 COT', and the version 'ClearPass Policy Manager 6.7.9.109195 on CLABV platform'.

aruba ClearPass Policy Manager Menu

Configuration » Identity » Role Mappings » Edit - [Guest Roles]

Role Mappings - [Guest Roles]

Summary Policy **Mapping Rules**

Rules Evaluation Algorithm: ☒ Select first match ☐ Select all matches

Role Mapping Rules:

Conditions	Role Name
1. (GuestUser:Role ID EQUALS 1)	[Contractor]
2. (GuestUser:Role ID EQUALS 2)	[Guest]
3. (GuestUser:Role ID EQUALS 3)	[Employee]

Add Rule Move Up ↑ Move Down ↓ Edit Rule Remove Rule

← Back to Role Mappings Copy Save Cancel

© Copyright 2018 Hewlett Packard Enterprise Development LP Apr 11, 2019 16:41:46 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform



Map the “CiscoPhone” Role

The screenshot displays the ClearPass Policy Manager interface. The left sidebar shows the navigation menu with sections like Dashboard, Monitoring, Configuration, Identity, Posture, Enforcement, Network, and Administration. The main header area shows the breadcrumb path: Configuration » Identity » Role Mappings » Edit - [Guest Roles]. Below this, the 'Role Mappings - [Guest Roles]' section has tabs for Summary, Policy, and Mapping Rules. The 'Mapping Rules' tab is active, showing the 'Rules Editor' dialog box.

The 'Rules Editor' dialog box is divided into two main sections: 'Conditions' and 'Actions'.

Conditions Section:

Matches ☒ ANY or ☐ ALL of the following conditions:

	Type	Name	Operator	Value	
1.	GuestUser	Role ID	EQUALS	4	 
2.	Click to add...				



Actions Section:

Role Name: CiscoPhone

At the bottom right of the dialog are 'Save' and 'Cancel' buttons. Below the dialog, there is a 'Back to Role Mappings' link and another set of 'Copy', 'Save', and 'Cancel' buttons.

© Copyright 2018 Hewlett Packard Enterprise Development LP Apr 11, 2019 16:46:17 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Click on “save”

 ClearPass Policy Manager Menu 

Dashboard

Monitoring

Configuration

Identity

Posture

Enforcement

Network

Profile and Network Scan

Administration

Methods

Sources

Single Sign-On (SSO)

Local Users

Endpoints

Static Host Lists

Roles

Role Mappings

Policies

Profiles

Devices

Device Groups

Proxy Targets

Event Sources

Network Scan

Profile Settings

Configuration » Identity » Role Mappings » Edit - [Guest Roles]

Role Mappings - [Guest Roles]

SummaryPolicyMapping Rules

Rules Evaluation Algorithm: ☒ Select first match ☐ Select all matches

Role Mapping Rules:

Conditions	Role Name
1. (GuestUser:Role ID EQUALS 1)	[Contractor]
2. (GuestUser:Role ID EQUALS 2)	[Guest]
3. (GuestUser:Role ID EQUALS 3)	[Employee]
4. (GuestUser:Role ID EQUALS 4)	CiscoPhone

Add Rule

Move Up ↑

Move Down ↓

Edit Rule

Remove Rule

← Back to Role Mappings

Copy

Save

Cancel

© Copyright 2018 Hewlett Packard Enterprise Development LP

Apr 11, 2019 16:47:20 COT

ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Create a role mapping

aruba ClearPass Policy Manager Menu

Configuration » Identity » Role Mappings » Add

Role Mappings

Policy Mapping Rules Summary

Policy Name:

Description:

Default Role: [View Details](#) [Modify](#) [Add New Role](#)

[< Back to Role Mappings](#) [Next ->](#) [Save](#) [Cancel](#)

Copyright 2018 Hewlett Packard Enterprise Development LP Apr 12, 2019 16:20:04 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

“IP-Phone” role is mapped to “CiscoPhone” Guest role

The screenshot shows the Aruba ClearPass Policy Manager web interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, Posture, Enforcement, Network, Profile and Network Scan, and Administration. The main content area is titled 'Role Mappings' and includes tabs for Policy, Mapping Rules, and Summary. The 'Mapping Rules' tab is active, showing a 'Rules Evaluation Algorithm' set to 'Select first match' and a 'Role Mapping Rules' section with a table of conditions. A 'Rules Editor' modal is open, allowing the configuration of a new rule. In the 'Conditions' section, the 'Matches' are set to 'ANY'. A table lists the conditions with columns for Type, Name, Operator, and Value. The first condition is 'Authorization:[Guest Device Repository]' with Name 'Device Role ID', Operator 'EQUALS', and Value '4'. The 'Actions' section shows the 'Role Name' dropdown set to 'IP-Phone'. Red boxes highlight the 'Add Rule' button, the first condition row, the 'IP-Phone' dropdown, and the 'Save' button. At the bottom of the modal are 'Save' and 'Cancel' buttons. The footer of the interface shows the copyright notice 'Copyright 2018 Hewlett Packard Enterprise Development LP', the date and time 'Apr 12, 2019 16:22:19 COT', and the version 'ClearPass Policy Manager 6.7.9.109195 on CLABV platform'.

aruba ClearPass Policy Manager

Configuration » Identity » Role Mappings » Add

Role Mappings

Policy Mapping Rules Summary

Rules Evaluation Algorithm: ☒ Select first match ☐ Select all matches

Role Mapping Rules:

Conditions	Role Name
	<input type="button" value="Add Rule"/> <input type="button" value="Move Up ↑"/> <input type="button" value="Move Down ↓"/> <input type="button" value="Edit Rule"/> <input type="button" value="Remove Rule"/>

Rules Editor

Conditions

Matches ☒ ANY or ☐ ALL of the following conditions:

Type	Name	Operator	Value
1. Authorization:[Guest Device Repository]	Device Role ID	EQUALS	4
2. Click to add...			

Actions

Role Name:

© Copyright 2018 Hewlett Packard Enterprise Development LP Apr 12, 2019 16:22:19 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Map anything else to “Other” role

The screenshot shows the ClearPass Policy Manager web interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, Posture, Enforcement, Network, Profile and Network Scan, and Administration. The main content area is titled 'Role Mappings' and shows a configuration for a role named 'IP-Phone'. A 'Rules Editor' modal is open, showing a table of conditions. The first condition is 'Authorization:[Guest Device Repository]:Device Role ID EQUALS 4'. The 'Actions' section shows the 'Role Name' dropdown set to '[Other]'. The 'Save' button is highlighted with a red box.

ClearPass Policy Manager

Configuration » Identity » Role Mappings » Add

Role Mappings

Policy Mapping Rules Summary

Rules Evaluation Algorithm: ☒ Select first match ☐ Select all matches

Role Mapping Rules:

Conditions	Role Name
1. (Authorization:[Guest Device Repository]:Device Role ID EQUALS 4)	IP-Phone

Add Rule Move Up ↑ Move Down ↓ Edit Rule Remove Rule

Rules Editor

Matches ☒ ANY or ☐ ALL of the following conditions:

Type	Name	Operator	Value
1.	Authorization:[Guest Device Repository]	Device Role ID	NOT_EQUALS 4
2.	Click to add...		

Actions

Role Name: [Other]

Save Cancel

© Copyright 2018 Hewlett Packard Enterprise Development LP Apr 12, 2019 16:23:57 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

“Wired-Policy” Role mapping

The screenshot displays the Aruba ClearPass Policy Manager web interface. The left sidebar contains a navigation menu with categories: Dashboard, Monitoring, Configuration (selected), Posture, Enforcement, Network, Profile and Network Scan, and Administration. Under Configuration, the 'Role Mappings' option is highlighted. The main content area shows the 'Role Mappings' configuration page with tabs for Policy, Mapping Rules (selected), and Summary. The breadcrumb trail is 'Configuration » Identity » Role Mappings » Add'. The 'Rules Evaluation Algorithm' is set to 'Select first match'. Below, the 'Role Mapping Rules' table lists two rules:

Conditions	Role Name
1. (Authorization:[Guest Device Repository]:Device Role ID EQUALS 4)	IP-Phone
2. (Authorization:[Guest Device Repository]:Device Role ID NOT_EQUALS 4)	[Other]

At the bottom of the rules list are buttons: Add Rule, Move Up ↑, Move Down ↓, Edit Rule, and Remove Rule. The footer of the interface includes a copyright notice: '© Copyright 2018 Hewlett Packard Enterprise Development LP', a timestamp: 'Apr 12, 2019 16:25:26 COT', and the version information: 'ClearPass Policy Manager 6.7.9.109195 on CLABV platform'.

Create IP Phone Enforcement Profile

aruba ClearPass Policy Manager Menu

Configuration » Enforcement » Profiles » Edit Enforcement Profile - IP Phone Enforcement

Enforcement Profiles - IP Phone Enforcement

Summary **Profile** Attributes

Name: **IP Phone Enforcement**

Description: IP Phone Enforcement

Type: RADIUS

Action: ☒ Accept ☐ Reject ☐ Drop

Device Group List:

[Remove](#) [View Details](#) [Modify](#) [Add New Device Group](#)

--Select--

[Back to Enforcement Profiles](#) [Copy](#) [Save](#) [Cancel](#)

© Copyright 2018 Hewlett Packard Enterprise Development LP May 28, 2019 10:21:08 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Create the Enforcement Profile to send the VOICE-ROLE as Radius VSA

aruba ClearPass Policy Manager

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile Attributes Summary

	Type	Name	Value	
1.	Radius:Hewlett-Packard	HPE-User-Role (25)	=	VOICE-ROLE
2.	Click to add...			

Navigation: < Back to Enforcement Profiles Next → Save Cancel

© Copyright 2018 Hewlett Packard Enterprise Development LP Apr 12, 2019 16:32:55 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

“IP Phone” Enforcement Profile summary

aruba ClearPass Policy Manager Menu

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Enforcement profile has not been saved

Profile Attributes Summary

Profile:

Template:	Aruba RADIUS Enforcement
Name:	IP Phone Role Enforcement
Description:	IP Phone Role Enforcement
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name	Value
1.	Radius:Hewlett-Packard-Enterprise	HPE-User-Role	= VOICE-ROLE

[Back to Enforcement Profiles](#) [Next ->](#) [Save](#) [Cancel](#)

© Copyright 2018 Hewlett Packard Enterprise Development LP Apr 12, 2019 16:33:36 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Create the Enforcement Policy to authenticate Cisco Phones via EAP-TLS

The screenshot displays the Aruba ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with categories: Identity, Posture, Enforcement, Network, Profile and Network Scan, and Administration. The 'Enforcement' category is expanded, and 'Policies' is selected. The main content area shows the configuration for an Enforcement Policy named 'Wired-IP-Phone_TLS EP'. The policy is configured with the following details:

- Name:** Wired-IP-Phone_TLS EP
- Description:** IP Phone Enforcement Policy
- Enforcement Type:** RADIUS
- Default Profile:** [Deny Access Profile]

Buttons for 'View Details' and 'Modify' are visible next to the Default Profile. A link 'Add New Enforcement Profile' is also present. At the bottom of the configuration area, there are buttons for 'Back to Enforcement Policies', 'Copy', 'Save', and 'Cancel'.

© Copyright 2018 Hewlett Packard Enterprise Development LP May 28, 2019 08:02:26 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Create the rules

ClearPass Policy Manager

Configuration » Enforcement » Policies » Edit - Wired-IP-Phone_TLS EP

Enforcement Policies - Wired-IP-Phone_TLS EP

Rules Editor

Match ALL of the following conditions:

Type	Name	Operator	Value
2. Authorization:[Guest Device Repository]	AccountStatus	EQUALS	0
3. Tips	Role	EQUALS	IP-Phone
4. Certificate	Issuer-DN	EQUALS	CN=Cisco Manufacturing CA,O=Cisco Systems
5. Certificate	Subject-CN	BEGINS_WITH	CP-

Enforcement Profiles

Profile Names: [RADIUS] IP Phone Enforcement

Move Up ↑
Move Down ↓
Remove

--Select to Add--

Save Cancel

Back to Enforcement Policies

Copy Save Cancel

© Copyright 2018 Hewlett Packard Enterprise Development LP May 28, 2019 08:06:25 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Account Status:
225 = disabled
226 = expired
0 = enabled and valid

“Wired-IP-Phone_TLS” Enforcement Policy summary

The screenshot displays the Aruba ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with categories like Dashboard, Monitoring, Configuration, Authentication, Identity, Posture, Enforcement, Network, and Administration. The 'Configuration' section is expanded, and 'Enforcement' > 'Policies' is selected. The main content area shows the 'Edit - Wired-IP-Phone_TLS EP' page. It has tabs for Summary, Enforcement, and Rules. The 'Summary' tab is active, showing details about the policy: Name (Wired-IP-Phone_TLS EP), Description (IP Phone Enforcement Policy), Enforcement Type (RADIUS), and Default Profile ([Deny Access Profile]). Below this, the 'Rules' section shows the 'Rules Evaluation Algorithm' set to 'First applicable'. A table lists the rules, with rule 1 having specific conditions and the action 'IP Phone Enforcement'. At the bottom, there are buttons for 'Back to Enforcement Policies', 'Copy', 'Save', and 'Cancel'. The footer contains copyright information, a timestamp, and the software version.

aruba ClearPass Policy Manager Menu

Configuration » Enforcement » Policies » Edit - Wired-IP-Phone_TLS EP

Enforcement Policies - Wired-IP-Phone_TLS EP

Summary Enforcement Rules

Enforcement:

Name:	Wired-IP-Phone_TLS EP
Description:	IP Phone Enforcement Policy
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm: First applicable

	Conditions	Actions
1.	(Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) AND (Authorization:[Guest Device Repository]:AccountStatus EQUALS 0) AND (Tips:Role EQUALS IP-Phone) AND (Certificate:Issuer-DN EQUALS CN=Cisco Manufacturing CA,O=Cisco Systems) AND (Certificate:Subject-CN BEGINS_WITH CP-)	IP Phone Enforcement

[Back to Enforcement Policies](#) Copy Save Cancel

© Copyright 2018 Hewlett Packard Enterprise Development LP May 28, 2019 08:08:47 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Create the Enforcement Policy to authenticate Cisco Phones via MAC-AUTH

The screenshot displays the ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with categories: Dashboard, Monitoring, Configuration (selected), Identity, Posture, Enforcement, Network, Profile and Network Scan, and Administration. Under the Configuration menu, the path 'Enforcement > Policies' is highlighted. The main content area shows the 'Edit - Wired-IP-Phone_MAC EP' page. The 'Enforcement' tab is active, displaying the following fields:

- Name:** Wired-IP-Phone_MAC EP (highlighted with a red box)
- Description:** IP Phone Enforcement Policy
- Enforcement Type:** RADIUS
- Default Profile:** [Deny Access Profile] (highlighted with a red box) with a dropdown arrow, a 'View Details' button, and a 'Modify' button.

At the bottom of the main content area, there is a link 'Add New Enforcement Profile'. The footer of the interface includes a 'Back to Enforcement Policies' link, and buttons for 'Copy', 'Save', and 'Cancel'. The footer text reads: '© Copyright 2018 Hewlett Packard Enterprise Development LP May 28, 2019 10:01:10 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform'.

Create the rules

ClearPass Policy Manager

Configuration » Enforcement » Policies » Edit - Wired-IP-Phone_MAC EP

Rules Editor

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Date	Day-of-Week	BELONGS_TO	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday
2. Authorization:[Guest Device Repository]	AccountStatus	EQUALS	0
3. Tips	Role	EQUALS	IP-Phone
4. Click to add...			

Enforcement Profiles

Profile Names: [RADIUS] IP Phone Enforcement

Move Up ↑
Move Down ↓
Remove

--Select to Add--

Save Cancel

Back to Enforcement Policies

Copy Save Cancel

© Copyright 2018 Hewlett Packard Enterprise Development LP May 28, 2019 10:06:38 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Account Status:
225 = disabled
226 = expired
0 = enabled and valid

“Wired-IP-Phone_MAC” Enforcement Policy summary

aruba

Dashboard

Monitoring

Configuration

Identity

- Single Sign-On (SSO)
- Local Users
- Endpoints
- Static Host Lists
- Roles
- Role Mappings

Posture

- Posture Policies
- Audit Servers

Enforcement

- Policies
- Profiles

Network

- Devices
- Device Groups
- Proxy Targets
- Event Sources

Profile and Network Scan

- Network Scan
- Profile Settings

Administration

ClearPass Policy Manager

Menu

Configuration » Enforcement » Policies » Edit - Wired-IP-Phone_MAC EP

Enforcement Policies - Wired-IP-Phone_MAC EP

Summary

Enforcement

Rules

Enforcement:

Name:	Wired-IP-Phone_MAC EP
Description:	IP Phone Enforcement Policy
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm:	First applicable
-----------------------------	------------------

Conditions	Actions
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) AND (Authorization:[Guest Device Repository]:AccountStatus EQUALS 0) AND (Tips:Role EQUALS IP-Phone)	IP Phone Enforcement

Back to Enforcement Policies

Copy

Save


Cancel

© Copyright 2018 Hewlett Packard Enterprise Development LP

May 28, 2019 10:11:05 COT

ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Create the 802.1X EAP-TLS service



ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Identity

Posture

Enforcement

Network

Administration

Configuration » Services » Edit - 802.1X EAP-TLS Wired Phone

Services - 802.1X EAP-TLS Wired Phone

SummaryServiceAuthenticationRolesEnforcement

Name:802.1X EAP-TLS Wired Phone

Description:802.1X Wired Access Service

Type:802.1X Wired

Status:Enabled

Monitor Mode:☐ Enable to monitor network access without enforcement

More Options:☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3. Connection	NAD-IP-Address	EQUALS	172.16.100.1
4. Radius:IETF	User-Name	BEGINS_WITH	CP-
5. Connection	Client-Mac-Vendor	EQUALS	Cisco Systems, Inc

Back to Services

DisableCopySaveCancel

EAP-TLS as Authentication Method

The screenshot displays the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, Services, Authentication, Identity, Posture, Enforcement, Network, and Administration. The main content area is titled 'ClearPass Policy Manager' and shows the configuration for 'Services - 802.1X EAP-TLS Wired Phone'. The 'Authentication' tab is selected, showing a list of authentication methods with 'EAP TLS' highlighted. Below this, there are sections for authentication sources, strip username rules, and service certificates. At the bottom, there are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'.

aruba ClearPass Policy Manager Menu

Configuration » Services » Edit - 802.1X EAP-TLS Wired Phone

Services - 802.1X EAP-TLS Wired Phone

Summary Service Authentication Roles Enforcement

Authentication Methods: **EAP TLS** Add New Authentication Method

Move Up ↑
Move Down ↓
Remove
View Details
Modify

--Select to Add--

Authentication Sources: Add New Authentication Source

[Local User Repository] [Local SQL DB]
[Guest Device Repository] [Local SQL DB]

Move Up ↑
Move Down ↓
Remove
View Details
Modify

--Select to Add--

Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Service Certificate: --Select to Add-- View Certificate Details

[Back to Services](#) Disable Copy Save Cancel

Select “Wired-Policy” as Role Mapping policy

aruba ClearPass Policy Manager Menu

Configuration » Services » Edit - 802.1X EAP-TLS Wired Phone

Services - 802.1X EAP-TLS Wired Phone

Summary Service Authentication **Roles** Enforcement

Role Mapping Policy: **Wired-Policy** [Modify](#) [Add New Role Mapping Policy](#)

Role Mapping Policy Details

Description:

Default Role: [Other]

Rules Evaluation Algorithm: first-applicable

Conditions	Role
1. (Authorization:[Guest Device Repository]:Device Role ID EQUALS 4)	IP-Phone
2. (Authorization:[Guest Device Repository]:Device Role ID EQUALS 6)	AccessPoint
3. (Authorization:[Guest Device Repository]:Device Role ID NOT_EQUALS 4)	[Other]

[Back to Services](#) [Disable](#) [Copy](#) [Save](#) [Cancel](#)

Select “Wired-IP-Phone_TLS” Enforcement policy

aruba ClearPass Policy Manager Menu

Configuration » Services » Edit - 802.1X EAP-TLS Wired Phone

Services - 802.1X EAP-TLS Wired Phone

Summary **Service** **Authentication** **Roles** **Enforcement**

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: **Wired-IP-Phone_TLS EP** Modify Add New Enforcement Policy

Enforcement Policy Details

Description: IP Phone Enforcement Policy

Default Profile: **[Deny Access Profile]**


Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
<p>(Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)</p> <p>AND (Authorization:[Guest Device Repository]:AccountStatus EQUALS 0)</p> <p>1. AND (Tips:Role EQUALS IP-Phone)</p> <p>AND (Certificate:Issuer-DN EQUALS CN=Cisco Manufacturing CA,O=Cisco Systems)</p> <p>AND (Certificate:Subject-CN BEGINS_WITH CP-)</p>	IP Phone Enforcement

[Back to Services](#) Disable Copy Save Cancel

© Copyright 2018 Hewlett Packard Enterprise Development LP May 28, 2019 10:45:00 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

802.1X EAP-TLS Wired Phone summary



ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Identity

Posture

Enforcement

Network

Administration

Configuration » Services » Edit - 802.1X EAP-TLS Wired Phone

Services - 802.1X EAP-TLS Wired Phone

SummaryServiceAuthenticationRolesEnforcement

Service:

Name:

802.1X EAP-TLS Wired Phone

Description:

802.1X Wired Access Service

Type:

802.1X Wired

Status:

Enabled

Monitor Mode:

Disabled

More Options:

-

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Connection	NAD-IP-Address	EQUALS	172.16.100.1
4.	Radius:IETF	User-Name	BEGINS_WITH	CP-
5.	Connection	Client-Mac-Vendor	EQUALS	Cisco Systems, Inc

Back to Services

Disable

Copy

Save


Cancel

© Copyright 2018 Hewlett Packard Enterprise Development LP

May 28, 2019 10:49:12 COT

ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Create the MAC Authentication service

ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Identity

Posture

Enforcement

Network

Administration

Configuration » Services » Edit - 2930F MAC Authentication

Services - 2930F MAC Authentication

SummaryServiceAuthenticationRolesEnforcement

Name:2930F MAC Authentication

Description:MAC-based Authentication Service 2930F

Type:MAC Authentication

Status:Enabled

Monitor Mode:☐ Enable to monitor network access without enforcement

More Options:☐ Authorization ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

	Type	Name	Operator	Value		
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15)		
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)		
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}		
4.	Connection	NAD-IP-Address	EQUALS	172.16.100.1		
5.	Click to add...					

Back to Services

DisableCopySaveCancel

© Copyright 2018 Hewlett Packard Enterprise Development LP

May 28, 2019 10:55:37 COT

ClearPass Policy Manager 6.7.9.109195 on CLABV platform

“Allow all MAC AUTH” as Authentication Method

The screenshot displays the Aruba ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with categories: Dashboard, Monitoring, Configuration (selected), Identity, Posture, Enforcement, and Network. Under Configuration, the path is Services > Authentication > Methods. The main content area is titled 'Services - 2930F MAC Authentication' and has tabs for Summary, Service, Authentication (selected), Roles, and Enforcement. The 'Authentication Methods' section shows a list with '[Allow All MAC AUTH]' selected and highlighted with a red box. To the right of the list are buttons for Move Up, Move Down, Remove, View Details, and Modify. Below the list is a dropdown menu labeled '--Select to Add--'. The 'Authentication Sources' section shows a list with '[Guest Device Repository] [Local SQL DB]' and '[Endpoints Repository] [Local SQL DB]'. To the right are buttons for Move Up, Move Down, Remove, View Details, and Modify. Below the list is a dropdown menu labeled '--Select to Add--'. The 'Strip Username Rules' section has a checkbox labeled 'Enable to specify a comma-separated list of rules to strip username prefixes or suffixes'. At the bottom of the main content area are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'.

aruba ClearPass Policy Manager Menu

Configuration » Services » Edit - 2930F MAC Authentication

Services - 2930F MAC Authentication

Summary Service Authentication Roles Enforcement

Authentication Methods: [Allow All MAC AUTH]

Move Up ↑ Move Down ↓ Remove View Details Modify

--Select to Add--

Add New Authentication Method

Authentication Sources: [Guest Device Repository] [Local SQL DB] [Endpoints Repository] [Local SQL DB]

Move Up ↑ Move Down ↓ Remove View Details Modify

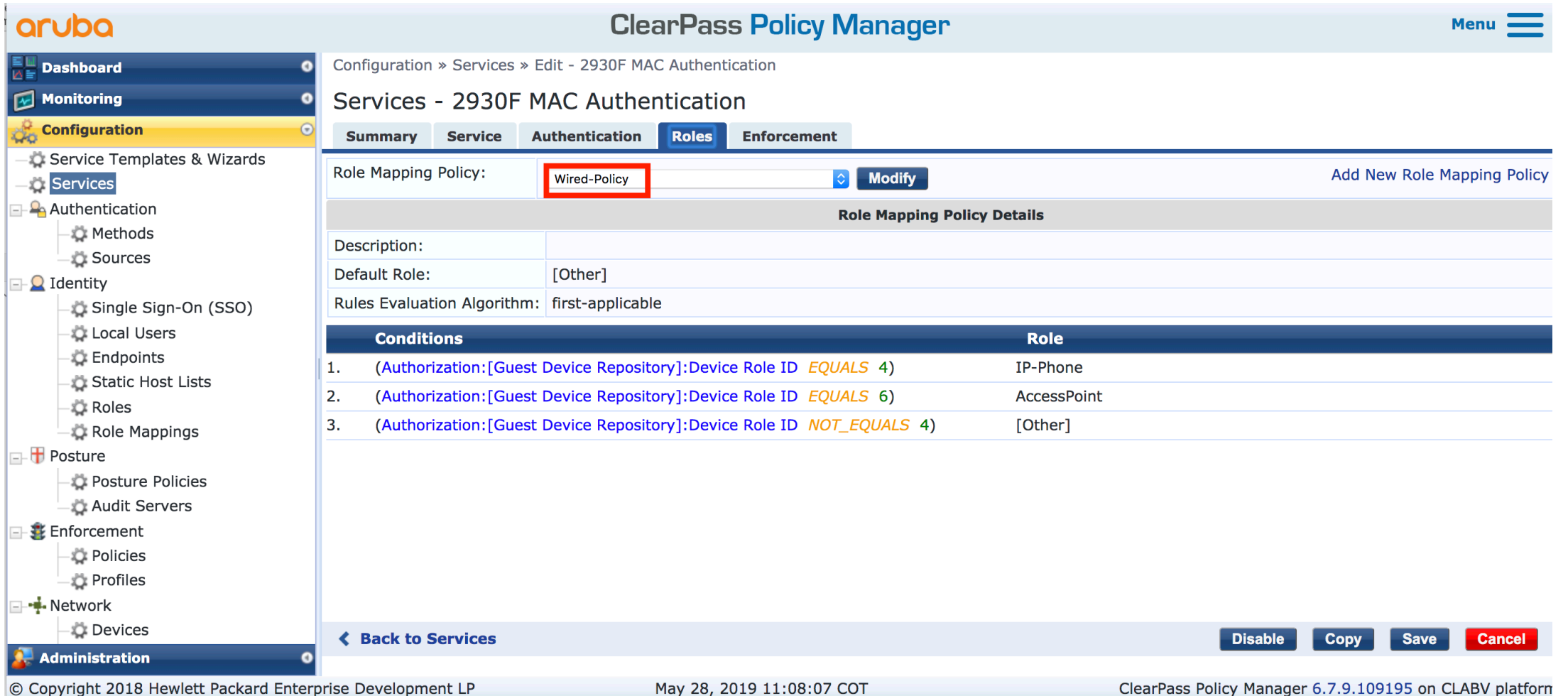
--Select to Add--

Add New Authentication Source

Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Back to Services Disable Copy Save Cancel

Select “Wired-Policy” as Role Mapping policy



aruba ClearPass Policy Manager Menu

Configuration » Services » Edit - 2930F MAC Authentication

Services - 2930F MAC Authentication

Summary **Service** **Authentication** **Roles** **Enforcement**

Role Mapping Policy: **Wired-Policy** Modify Add New Role Mapping Policy

Role Mapping Policy Details

Description:

Default Role: [Other]

Rules Evaluation Algorithm: first-applicable

Conditions	Role
1. (Authorization:[Guest Device Repository]:Device Role ID EQUALS 4)	IP-Phone
2. (Authorization:[Guest Device Repository]:Device Role ID EQUALS 6)	AccessPoint
3. (Authorization:[Guest Device Repository]:Device Role ID NOT_EQUALS 4)	[Other]

[Back to Services](#) Disable Copy Save Cancel

© Copyright 2018 Hewlett Packard Enterprise Development LP May 28, 2019 11:08:07 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

Select “Wired-IP-Phone_MAC” Enforcement policy

aruba ClearPass Policy Manager Menu

Configuration » Services » Edit - 2930F MAC Authentication

Services - 2930F MAC Authentication

Summary **Service** **Authentication** **Roles** **Enforcement**

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: **Wired-IP-Phone_MAC EP** Modify [Add New Enforcement Policy](#)

Enforcement Policy Details

Description: IP Phone Enforcement Policy

Default Profile: **[Deny Access Profile]**


Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Date:Day-of-Week <i>BELONGS_TO</i> Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) AND (Authorization:[Guest Device Repository]:AccountStatus <i>EQUALS</i> 0) AND (Tips:Role <i>EQUALS</i> IP-Phone)	IP Phone Enforcement

[Back to Services](#) Disable Copy Save Cancel

© Copyright 2018 Hewlett Packard Enterprise Development LP May 28, 2019 11:09:16 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

MAC Authentication summary

ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Identity

Posture

Enforcement

Network

Administration

Configuration » Services » Edit - 2930F MAC Authentication

Services - 2930F MAC Authentication

SummaryServiceAuthenticationRolesEnforcement

Service:

Name:

2930F MAC Authentication

Description:

MAC-based Authentication Service 2930F

Type:

MAC Authentication

Status:

Enabled

Monitor Mode:

Disabled

More Options:

-

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
4.	Connection	NAD-IP-Address	EQUALS	172.16.100.1

Authentication:

Back to Services

DisableCopySaveCancel

© Copyright 2018 Hewlett Packard Enterprise Development LP

May 28, 2019 11:11:57 COT


ClearPass Policy Manager 6.7.9.109195 on CLABV platform



a Hewlett Packard
Enterprise company

Task: Upload Phone MAC Addresses to Clearpass

Click on Export phone details

**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration Go

adminapp | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Find and List Phones To Export

[Next](#)





Status

4 records found

Browse the complete search result before submitting the job.

Phones (1 - 4 of 4)

Find Phones where Device Name ▾ begins with ▾ Using AND ▾ Find

	Device Name(Line) ^	Description	Device Pool
 7960	SEP001BD584D932	Auto 1001	Default
 7975	SEP006440B58F2D	Auto 1000	Default
 7975	SEP64168DBB9670	Auto 1003	Default
 7821	SEPE0D173E55320	Auto 1002	Default

[Next](#)

Upload/Download Files

Phones ▾

Users ▾

Phones & Users ▾

Managers/Assistants ▾

User Device Profiles ▾

Gateways ▾

Forced Authorization Codes ▾

Client Matter Codes ▾

Call Pickup Group ▾

Mobility ▾

Region Matrix ▾

Import/Export ▾

Phone Migration ▾

EMCC ▾

Intercompany Media Services ▾

Confidential Access Level ▾

TAPS ▾

Directory URIs and Patterns ▾

Job Scheduler

Phone Template

Phone File Format ▾

Validate Phones

Insert Phones

Update Phones ▾

Delete Phones ▾

Export Phones ▾

Add/Update Lines ▾

Reset/Restart Phones ▾

Wipe And Lock Phones ▾

Generate Phone Reports

Migrate Phones ▾

Add/Update Intercom ▾

Related Links: [View Device Summary](#) Go

Specific Details

All Details

100 ▾

IP Address

[10.10.0.8](#)


[10.10.0.5](#)


[10.10.0.10](#)

[10.10.0.9](#)

https://172.16.0.90/ccmadmin/bulkphoneexportallEdit.do

Submit bulk export


**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions

Navigation Cisco Unified CM Administration  Go


adminapp | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾


Export Phones Configuration

 Submit

Status

 Status: Ready

Export Phones


Select the Device Type *  All Phone Types

File Name *


Job Information

Job Description

☒ Run Immediately ☐ Run Later (To schedule and activate this job, use Job Scheduler page.)

 *- indicates required item.

Download the report






**Cisco Unified CM Administration**
For Cisco Unified Communications Solutions


Navigation Cisco Unified CM Administration Go

adminapp | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Find and List Files

 Add New  Select All  Clear All  Delete Selected  Download Selected

Status
 4 records found

File (1 - 4 of 4)

Find File where Name ▾ begins with ▾ Using AND ▾ Find
 Select item or enter search text ▾

<input type="checkbox"/>	File Name ^
<input type="checkbox"/>	MAC_address_04112019142341.txt
<input type="checkbox"/>	bat.xlt
<input type="checkbox"/>	test_04112019141157.txt
<input type="checkbox"/>	test_04112019141209.txt

Add New Select All Clear All Delete Selected Download Selected

Upload/Download Files

Phones ▾

Users ▾

Phones & Users ▾

Managers/Assistants ▾

User Device Profiles ▾

Gateways ▾

Forced Authorization Codes ▾

Client Matter Codes ▾

Call Pickup Group ▾

Mobility ▾

Region Matrix ▾

Import/Export ▾

Phone Migration ▾

EMCC ▾

Intercompany Media Services ▾

Confidential Access Level ▾

TAPS ▾

Directory URIs and Patterns ▾

Job Scheduler

Rows per Page 100 ▾

Function Type

Phones - All Details

cel CSV Tool

Phones - All Details

Phones - All Details

https://172.16.0.90/ccmadmin/bulkfileuploadFindList.do

Report generated by Callmanager – CSV format

- CSV format report shows IP Phone MAC Addresses:

[illegible]

Click on “Import Guest Accounts”

aruba ClearPass Guest Menu

Home » Guest » Manage Devices

Manage Devices

The following table shows the devices that have been created. Click an account to modify it.

Quick Help Create More Options

Export Guest Accounts
Export a list of all current guest accounts to a file. You can select the format you want to export to here.

Import Guest Accounts
Import a list of guests from a text file and create a guest account for each entry in the list.

Choose Columns
Add or remove columns from the list.

Filter:

MAC Address	Device Name	Expiration	Sponsor	Sharing
There are no devices to display.				

Refresh No matching accounts found 20 rows per page

Back to guests Back to main

Guest
Start Here
Active Sessions
Create Account
Create Device
Create Multiple
Export Accounts
Import Accounts
Manage Accounts
Manage Devices
Manage Multiple Accounts

Onboard
Configuration
Administration

https://172.16.0.65/guest/guest_import.php ClearPass Guest 6.7.9.109195 on CLABV platform

Choose CSV file - Click on “Next Step”

aruba ClearPass Guest Menu

Guest

- Start Here
- Active Sessions
- Create Account
- Create Device
- Create Multiple
- Export Accounts
- Import Accounts**
- Manage Accounts
- Manage Devices
- Manage Multiple Accounts

Onboard

Configuration

Administration

Upload User List

Size Limit: Maximum file upload size: 15.0 MB.
A maximum of 1000 records can be imported at one time.

Accounts File: **Choose File** Cisco Phone MAC Address
Upload a file containing a list of user accounts. This field may be left blank if you provide the list in the field below.

Accounts Text:

Type in or paste the list of user accounts. This field may be left blank if you upload a file.

Advanced: ☐ Show additional import options

Next Step

* required field

[Back to guests](#)

[Back to main](#)

© Copyright 2019 Hewlett Packard Enterprise Development LP ClearPass Guest 6.7.9.109195 on CLABV platform

Click on “Next Step”

aruba

Guest

Start Here

Active Sessions

Create Account

Create Device

Create Multiple

Export Accounts

Import Accounts

Manage Accounts

Manage Devices

Manage Multiple Accounts

Onboard

Configuration

Administration

ClearPass Guest

Menu

Import: Step 2 of 3

Data was imported from the 'csv' format. The first 5 records in the imported data are shown below. There are a total of 5 records in the imported data.

Record	Username	Field 2	Role	Activation	Expiration	Lifetime	Expire Action	MAC Address	Is Device
1	Username	Device Name	Role	Activation	Expiration	Lifetime	Expire Action	MAC Address	Is Device
2	00-64-40-B5-8F-2D	Cisco Phone	CiscoPhone	4/11/19 17:20	N/A	0	0	00-64-40-B5-8F-2D	1
3	00-1B-D5-84-D9-32	Cisco Phone	CiscoPhone	4/11/19 17:20	N/A	0	0	00-1B-D5-84-D9-32	1
4	E0-D1-73-E5-53-20	Cisco Phone	CiscoPhone	4/11/19 17:20	N/A	0	0	E0-D1-73-E5-53-20	1
5	64-16-8D-BB-96-70	Cisco Phone	CiscoPhone	4/11/19 17:20	N/A	0	0	64-16-8D-BB-96-70	1

You can edit this data by returning to Step 1.

To create user accounts from this data, use the form below to match each of the fields in the imported data with each of the parameters needed to create a guest account.

Match Fields

* Username:

Username

The username of the created guest accounts.

* Password:

Generate random passwords

The password for the created guest accounts.

* Role:

Role

The role to assign to each of the created guest accounts.

* Activation Time:

Activation

The date and time at which to enable the guest accounts.

* Expiration Time:

Expiration

The date and time at which a guest account will expire and be deleted.

* Account Lifetime:

Lifetime

The amount of time after the first login before the account will expire and be deleted.

Expire Action:

Expire Action

Select an option for controlling the expiration of this account. Note that a logout can only occur if the NAS is RFC-3576 compliant.

* Notes:

None

A note stored with each of the guest accounts.

Auto-Detected Fields:

☒ MAC Address

☒ Is Device

The above fields were auto-detected in your file. Check the ones you wish to import.

* Header Rows:

1

The number of rows shown in the imported data that do not correspond to user accounts.

Next Step

* required field

© Copyright 2019 Hewlett Packard Enterprise Development LP

ClearPass Guest 6.7.9.109195 on CLABV platform

Click on “Create Guest Accounts”

aruba

Guest

Start Here

Active Sessions

Create Account

Create Device

Create Multiple

Export Accounts

Import Accounts

Manage Accounts

Manage Devices

Manage Multiple Accounts

ClearPass Guest

Menu

Home » Guest » Import Accounts

Import Accounts

Import: Step 3 of 3

There are 4 user accounts in the imported data. These are shown below.

You can change this data by returning to Step 2.

To create user accounts from this data, select the user accounts that should be created.

Import Accounts

Select: This Page (4) • All (4) • None • New (4) • Existing (0)
Total number of records currently selected: 4

	Username	Password	Role	Activation	Expiration	Lifetime	Expire Action	MAC Address	Is Device
<input checked="" type="checkbox"/>	00-64-40-B5-8F-2D	729196	CiscoPhone	2019-04-11 17:20	N/A	N/A	0	00-64-40-B5-8F-2D	1
<input checked="" type="checkbox"/>	00-1B-D5-84-D9-32	043309	CiscoPhone	2019-04-11 17:20	N/A	N/A	0	00-1B-D5-84-D9-32	1
<input checked="" type="checkbox"/>	E0-D1-73-E5-53-20	424335	CiscoPhone	2019-04-11 17:20	N/A	N/A	0	E0-D1-73-E5-53-20	1
<input checked="" type="checkbox"/>	64-16-8D-BB-96-70	640126	CiscoPhone	2019-04-11 17:20	N/A	N/A	0	64-16-8D-BB-96-70	1

Refresh

1

Showing 1 – 4 of 4
20 rows per page

Select the accounts to import.

Create Guest Accounts

Onboard

Configuration

Administration

© Copyright 2019 Hewlett Packard Enterprise Development LP

ClearPass Guest 6.7.9.109195 on CLABV platform

Accounts created in Clearpass Guest

aruba ClearPass Guest Menu

Home » Guest » Create Multiple

Finished Creating Guest Accounts

Finished creating 4 guest accounts.

The details about each of the accounts created are shown below.

Account Details	
MAC Address	00-64-40-B5-8F-2D
Role	CiscoPhone
Current State	Pending
Account Activation	Thursday, 11 April 2019, 5:20 PM
Account Expiration	No expiration time set

Account Details	
MAC Address	00-1B-D5-84-D9-32
Role	CiscoPhone
Current State	Pending
Account Activation	Thursday, 11 April 2019, 5:20 PM
Account Expiration	No expiration time set

Account Details	
MAC Address	E0-D1-73-E5-53-20
Role	CiscoPhone
Current State	Pending
Account Activation	Thursday, 11 April 2019, 5:20 PM
Account Expiration	No expiration time set

Account Details	
MAC Address	64-16-8D-8B-96-70
Role	CiscoPhone
Current State	Pending
Account Activation	Thursday, 11 April 2019, 5:20 PM
Account Expiration	No expiration time set

Open print window using template...

© Copyright 2019 Hewlett Packard Enterprise Development LP ClearPass Guest 6.7.9.109195 on CLABV platform

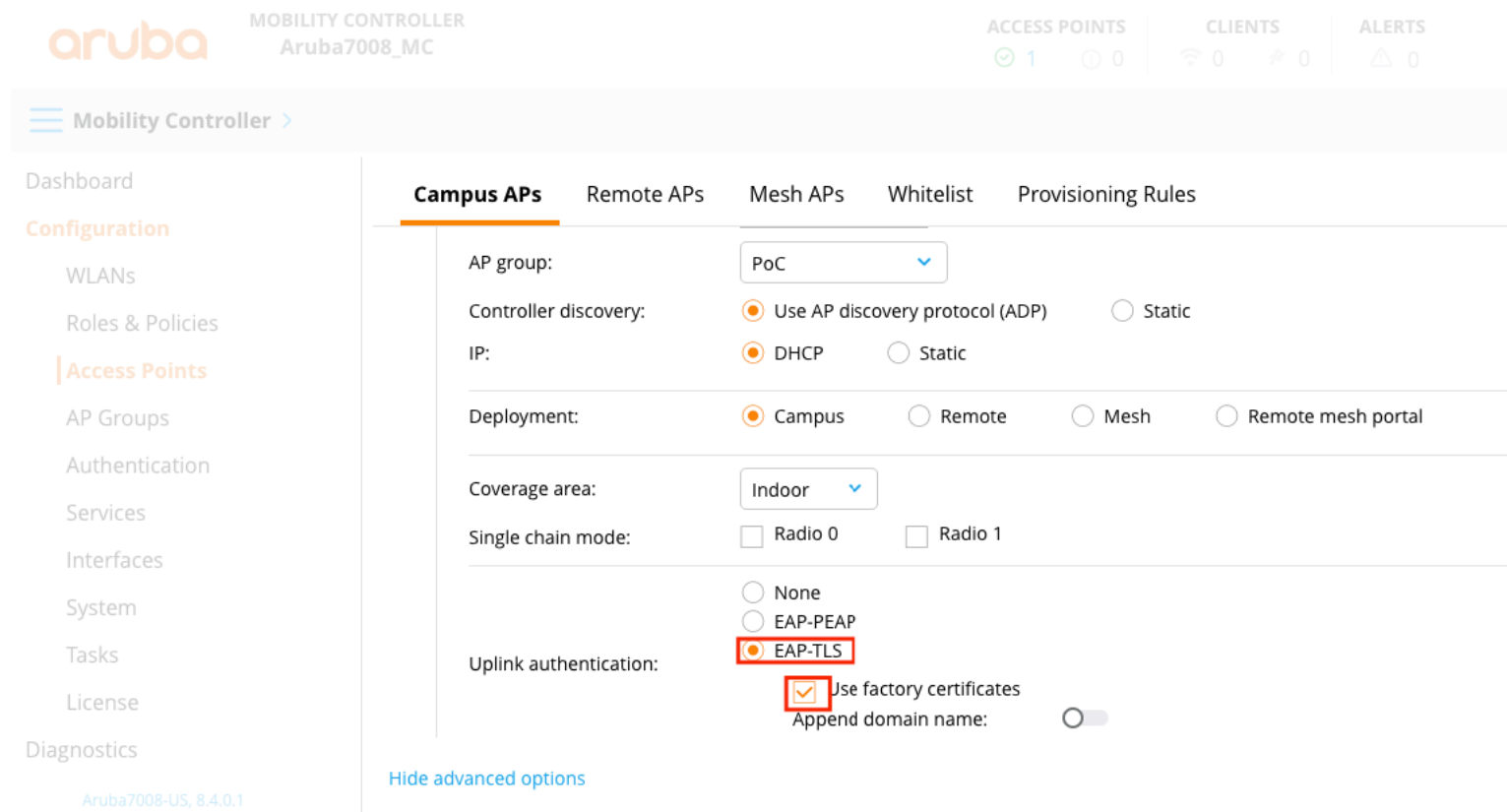


a Hewlett Packard
Enterprise company

Task: Config Aruba Controller to support uplink Auth on APs

Config AP Authentication via

From 8.2.0.0, APs support for both EAP-TLS. APs can use Aruba factory certificate or custom certificate supplied during EAP-TLS exchange <https://arubapedia.arubanetworks.com/arubapedia/index.php/How-To: Aruba Access Point Authentication via EAP-TLS with Factory Certificate>



The image shows the Aruba Mobility Controller configuration interface for Campus APs. The interface is divided into a left sidebar and a main configuration area. The sidebar includes links to Dashboard, Configuration, WLANs, Roles & Policies, Access Points, AP Groups, Authentication, Services, Interfaces, System, Tasks, License, and Diagnostics. The main configuration area is titled 'Campus APs' and includes tabs for Remote APs, Mesh APs, Whitelist, and Provisioning Rules. The configuration fields are as follows:

- AP group: PoC (dropdown)
- Controller discovery: ☒ Use AP discovery protocol (ADP) ☐ Static
- IP: ☒ DHCP ☐ Static
- Deployment: ☒ Campus ☐ Remote ☐ Mesh ☐ Remote mesh portal
- Coverage area: Indoor (dropdown)
- Single chain mode: ☐ Radio 0 ☐ Radio 1
- Uplink authentication: ☒ EAP-TLS (highlighted with a red box) ☐ None ☐ EAP-PEAP
- Use factory certificates: ☒ (highlighted with a red box)
- Append domain name: ☐

At the bottom of the main configuration area, there is a link to 'Hide advanced options'.

Clearpass → Enable Aruba Root certificate

The screenshot displays the Aruba ClearPass Policy Manager web interface. On the left is a navigation sidebar with the 'Administration' menu expanded, showing options like 'Server Configuration', 'Log Configuration', 'Local Shared Folders', 'Licensing', 'External Servers', 'SNMP Trap Receivers', 'Syslog Targets', 'Syslog Export Filters', 'Messaging Setup', 'Endpoint Context Servers', 'File Backup Servers', 'Certificates', 'Certificate Store', 'Trust List' (highlighted), and 'Revocation Lists'. The main header shows the 'aruba' logo, 'ClearPass Policy Manager', and a 'Menu' icon. The breadcrumb trail is 'Administration » Certificates » Trust List'. The page title is 'Certificate Trust List' with an 'Add' button. A description states: 'This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.' A filter bar shows 'Subject' containing 'aruba'. The table below lists four certificates, with the third one selected. The table has columns for '#', 'Subject', 'Validity', and 'Enabled'. The bottom of the table shows 'Showing 1-4 of 4' and a 'Delete' button.

aruba ClearPass Policy Manager Menu

Administration » Certificates » Trust List

Certificate Trust List

+ Add

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject contains aruba + Go Clear Filter Show 20 records

#	Subject	Validity	Enabled
1.	<input type="checkbox"/> emailAddress=dd37d60f-3580-49af-922e-d8c3f3396b43@example.com,CN=ClearPass Onboard Local Certificate Authority (Signing),O=Aruba Networks,L=Sunnyvale,ST=California,C=US	Valid	Enabled
2.	<input type="checkbox"/> emailAddress=dd37d60f-3580-49af-922e-d8c3f3396b43@example.com,CN=ClearPass Onboard Local Certificate Authority,O=Aruba Networks,L=Sunnyvale,ST=California,C=US	Valid	Enabled
3.	<input checked="" type="checkbox"/> CN=Aruba Networks Trusted Computing Root CA 1.0,C=US,O=Aruba Networks,OU=Operations,OU=DeviceTrust	Valid	Disabled
4.	<input type="checkbox"/> L=Bogota,ST=Cundinamarca,CN=CAPF-f4b5a296,OU=Aruba,O=Test-CUCM,C=CO	Valid	Disabled

Showing 1-4 of 4 Delete

Click on Enable

The screenshot shows the ClearPass Policy Manager interface. On the left is a navigation menu with sections like Dashboard, Monitoring, Configuration, and Administration. The 'Administration' section is expanded, showing 'Certificates' and 'Trust List'. The main area displays the 'Trust List' with a table of certificates. A 'View Certificate Details' dialog box is open, showing details for a selected certificate. The dialog includes fields for Subject DN, Issuer DN, Issue Date/Time, Expiry Date/Time, Validity Status, Signature Algorithm, Public Key Format, Serial Number, and Enabled status. The 'Enabled' status is currently 'false', and the 'Enable' button is highlighted with a red box. The background table shows a list of certificates with columns for #, Subject, Validity, and Enabled status.

View Certificate Details

Subject DN:	CN=Aruba Networks Trusted Computing Root CA 1.0,C=US,O=Aruba Networks,OU=Operations,OU=DeviceTrust
Issuer DN:	CN=Aruba Networks Trusted Computing Root CA 1.0,C=US,O=Aruba Networks,OU=Operations,OU=DeviceTrust
Issue Date/Time:	Sep 13, 2007 22:12:06 COT
Expiry Date/Time:	Sep 13, 2032 22:21:14 COT
Validity Status:	Valid
Signature Algorithm:	SHA1WithRSAEncryption
Public Key Format:	X.509
Serial Number:	155386889284515228762147431949179635633
Enabled:	false

Enable **Export** **Close**

© Copyright 2018 Hewlett Packard Enterprise Development LP May 02, 2019 16:00:14 COT ClearPass Policy Manager 6.7.9.109195 on CLABV platform

References

- https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/IP_Tele/IP_Telephony_DIG.html
- <https://community.cisco.com/t5/policy-and-access/cisco-ise-authenticating-ip-phone-7942/td-p/2442348>
- <https://www.ipstorming.com/cisco-ise-ip-phones-and-eap-tls-authentication/>
- <https://zigbits.tech/zbise11-cisco-ise-2-3-cisco-voip-phone-with-mab-auth-on-wired/>
- <https://community.cisco.com/t5/identity-services-engine-ise/phones-prefer-to-connect-to-data-domain-instead-of-voice-domain/td-p/3814242>
- <https://community.cisco.com/t5/identity-services-engine-ise/ise-and-cisco-ip-phones/td-p/3467053>
- <https://community.arubanetworks.com/t5/Security/ClearPass-Solution-Guide-Wired-Policy-Enforcement/td-p/298161>



a Hewlett Packard
Enterprise company

Thanks