Meru Networks VIEW Certified Configuration Guide

November 2011 | 1725-36067-001 Rev. G

Trademark Information

POLYCOM®, the Polycom "Triangles" logo and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

Patent Information

The accompanying product is protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Disclaimer

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

Copyright Notice

4750 Willow Road
Pleasanton, CA 94588-2708
USA

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

Contents

Introduction

Polycom's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between Polycom Wireless Telephones and WLAN infrastructure products.

The products listed below have been thoroughly tested in Polycom’s lab and have passed the VIEW Certification Test Plan. This document details how to configure Meru Networks Wireless LAN System and AP3xx with Polycom Wireless Telephones.

Certified Product Summary

Table 1

Manufacturer:	Meru Networks: *www.merunetworks.com*	
Certified products:	Controllers: MC5000 MC4100 MC3000 [1] MC1500 MC1000 [1]	APs: AP3xx [1]
AP Radio(s):	2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n)	
Security:	None, WPA-PSK, WPA2-PSK, WPA2-PEAP with OKC	
QoS:	Wi-Fi Standard	
AP software version certified:	4.0-SR5-5	
Network topology:	Switched Ethernet (recommended)	

[1] Denotes products directly used in VIEW Certification

Table 2

SpectraLink 8400 Series test parameters	
Handset[1] radio mode:	Meets VIEW minimum call capacity per AP:
802.11b	6 calls[2]
802.11b/g	10 calls[2]
802.11bgn	8 calls[2]
802.11a & 802.11an	10 calls[2]

[1] SpectraLink handset models and their OEM derivatives are verified compatible with the WLAN hardware and software identified in the table. Throughout the remainder of this document they will be referred to collectively as “SpectraLink Wireless Telephones”, “phones” or “handsets”.

[2] Maximum calls tested during VIEW Certification. The certified product may actually support a higher number of maximum calls for 802.11a and 802.11g radio modes.

Table 3

SpectraLink 8020/8030 test parameters	
Handset[1] radio mode	Meets VIEW minimum call capacity per AP
802.11b & b/g mixed & gn	6 (Wi-Fi Standard QoS) [2]
802.11a and 802.11an	8 (Wi-Fi Standard QoS) [2]

[1] SpectraLink handset models and their OEM derivatives are verified compatible with the WLAN hardware and software identified in the table. Throughout the remainder of this document they will be referred to collectively as “SpectraLink Wireless Telephones”, “phones” or “handsets”.

[2] Maximum calls tested during VIEW Certification. The certified product may actually support a higher number of maximum calls for 802.11a and 802.11g radio modes.

Known Limitations

- There should be a one-on-one mapping to ESSID and VLAN.
  If not, Multicast will not work
- EAP-FAST is not supported
- Only Virtual Cell/Virtual Port and the tunneled dataplane mode were tested. It is not known how well a layered deployment or bridged dataplane mode would perform.

Polycom References

Please refer to the Polycom *Deploying Enterprise-Grade Wi-Fi Telephony* white papers which are available at
http://www.polycom.com/products/voice/wireless_solutions/wifi_communications/handsets/SpectraLink_8020_wireless.html or
http://www.polycom.com/global/documents/products/voice/datasheets/best-practices-for-deploying-plcm-spectralink-8400.pdf

This document covers the security, coverage, capacity and QoS considerations necessary for ensuring excellent voice quality with enterprise Wi-Fi networks.

For more detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets, please see the *Best Practices Guide to Network Design Considerations for SpectraLink Wireless Telephones*, which is available at
http://support.polycom.com/PolycomService/support/us/support/voice/wi-fi/index.html.

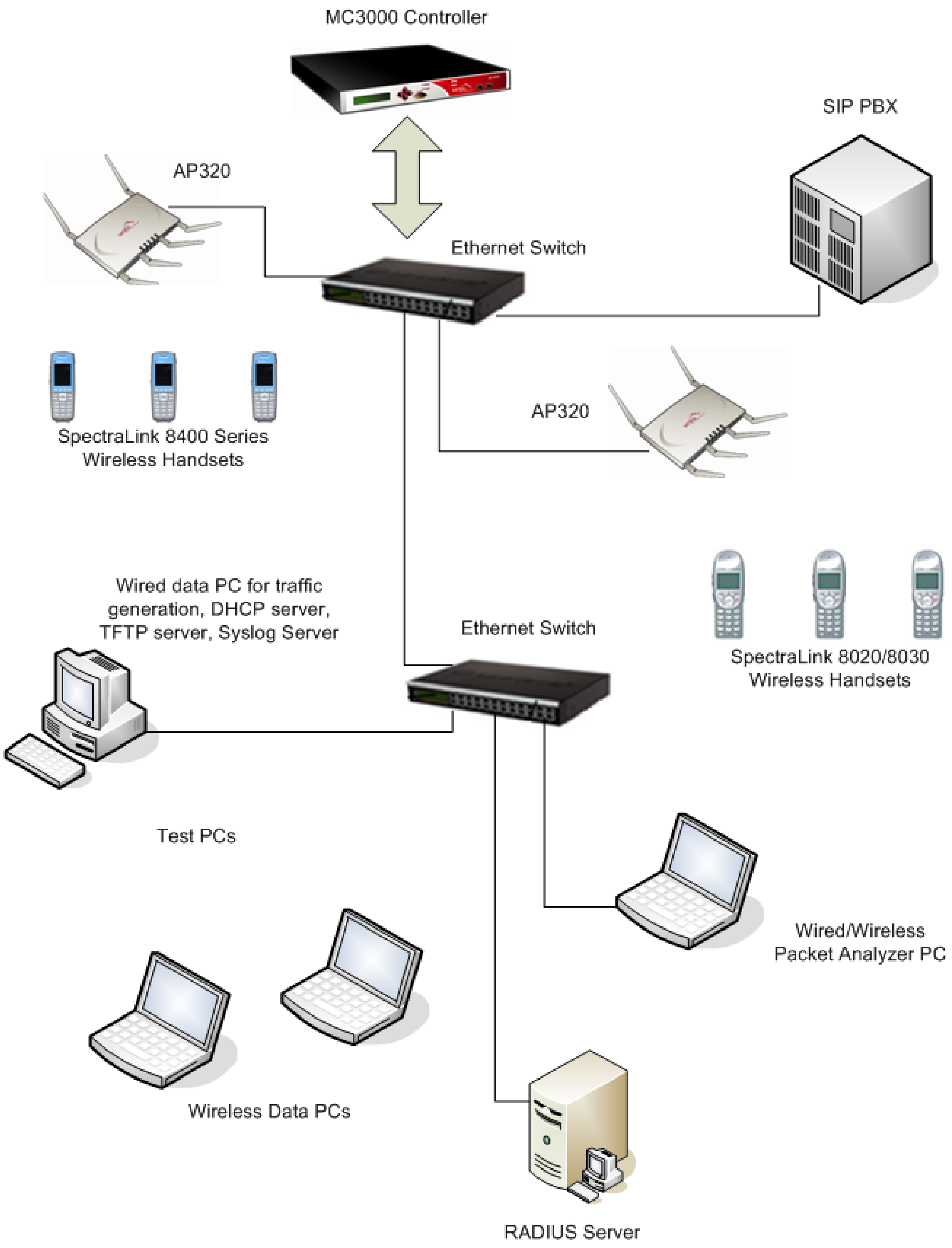
This document identifies issues and solutions based on Polycom's extensive experience in enterprise-class Wi-Fi telephony. It provides recommendations for ensuring that a network environment is adequately optimized for use with SpectraLink Wireless Telephones.

Product Support

Installation and configuration guides for Meru Wireless LAN Controllers and Access Points can be found on the Meru Networks website at http://www.merunetworks.com.

Network Topology

The following topology was used during VIEW Certification testing:



Chapter 1: Initial Setup for Meru Wireless Infrastructure

The Meru network enterprise LAN solution is a controller-based solution. The controller should be initially configured before setting up the Access Points and its parameters for deploying and servicing the wireless clients

Configuring a New Controller Starting from Factory Defaults

Initial setup of a controller requires a serial connection to a PC or laptop to configure the controller network identification settings. After that, the controller management interface is accessed through the network via an SSH2 connection for using the CLI or secure HTTP connection from the Web UI.

Startup

1. Before applying power to the controller, make sure the controller is connected to an Ethernet switch.
2. Set up a serial connection from the PC or laptop to the controller. For the initial controller configuration, you must connect to the controller using the serial port. Plug the Null modem serial cable into the controller serial port and the other end into the serial port of the PC or laptop.
3. On the PC or laptop, set up an ANSI or VT100 compatible terminal session with the following settings:

   115200 baud

   8 bits

   no parity

   1 stop bit

   no flow control
4. Plug the controller into the AC power source.
5. Press the controller Power On/Off switch. When the controller boots for the first time, it shows a series of informational messages and then presents the default login prompt.
6. Log in as admin using the default password, also admin:

   ```
   default login: admin
   Password:
   ```

Enter parameters

1. Run setup, the initial configuration script:

   ```
   default# setup
   Begin system configuration ...
   Country code configuration for this machine.
   The country code is currently set to US
   Would you like to change it [yes/no/quit]?
   ```

2. Type the hostname for the controller (the hostname must be less than 32 characters, cannot start with integers, or contain all integers). In the following example, we choose the hostname controller for our controller:

   ```
   Please enter host name, or q to quit: controller
   Is controller correct [yes/no/quit]?: y
   IP Configuration for this machine.
   ```

3. Change the default admin password to prevent any security breaches:

   ```
   Currently default password is used for admin
   Would you like to change the password [yes/no/quit]?: yes
   Changing password for user admin.
   New password:
   Retype new password:
   passwd: all authentication tokens updated successfully.
   ```

4. Configure IP addressing for the controller

   At this stage, we will assign a static IP address and a netmask to the controller, as well as a gateway address, so a telnet or browser connection can be made. (If your controller and APs are on different subnets, you can assign DHCP addressing for the controller now or later with the CLI or Web Interface.)

   ```
   Would you like to configure networking? y
   Would you like to use Dynamic IP configuration (DHCP)[yes/no/quit]: n
   Please enter the IP configuration for this machine.
   ```

   Each item should be entered as an IP version 4 style address in dotted-decimal notation (for example, 10.20.30.40)

   ```
   Enter IP address, or q to quit: nnn.nnn.nnn.nnn
   Is nnn.nnn.nnn.nnn correct [yes/no/quit]? y
   Enter netmask, or q to quit: nnn.nnn.nnn.nnn
   Is nnn.nnn.nnn.nnn correct [yes/no/quit]? y
   Enter default gateway (IP), or q to quit: nnn.nnn.nnn.nnn
   Is nnn.nnn.nnn.nnn correct [yes/no/quit]? Y
   ```

5. For the initial start-up, if your controller is to be on a different subnet from the APs (Layer 3 configuration), enter the appropriate DNS server information for your WLAN.

```
Would you like to configure a Domain Name Server [yes/no/quit]? y
Domain Name Server (DNS) configuration for this machine.
Enter one or more DNS name servers.
For this prompt only use q when finished entering name servers.
Enter Name Server IP Address, or q to quit: controller#nnn.nnn.nnn.nnn
```

6. If desired, change the controller’s index number. If you select Yes, you will be prompted to set the desired number, which can be any integer from 0-31. If you select No, the controller’s index will remain at the default (0).

7. You are now prompted to set the time zone. You can set it now or later, using the timezone command.

   Synchronize the system time with a Network Time Protocol server so that the controller time is extremely accurate, or set the time from the CLI with the calendar set command.

   ```
   Synchronize time with a Network Time Protocol (NTP) server
   [yes/no/quit]?: n
   You can use the "calendar set" option of the cli to set the time
   ```

8. The system asks for permission to reboot. Tell it to reboot, when prompted:

   ```
   System Configuration completed.
   Do you want to commit your changes and reboot? [yes/no/quit] yes
   Broadcast message from root (Wed Aug 17 11:30:32 2005):
   Now rebooting system...
   The system is going down for reboot NOW!
   ```

   The controller restarts. The full restart process can take up to 5 minutes.

Verification

1. Once the server has completely booted up, verify that you can connect to the controller using the Web UI or the CLI.
   - ○ To start the Web UI, open a browser window and provide the IP address of the Controller you have just configured (http://nnn.nnn.nnn.nnn). Note that you may need to accept a security certificate and/or confirm a security exception before accessing the interface. This can vary depending on the Internet browser in use.
   - ○ To use the CLI, start a SSH2 session using the IP address of the controller.

2. Verify that each access point receives power. If the access point is receiving power, the power LED glows green.

Now the network is ready for configuration

Installing Software

The following section describes step by step details on how to load the controller with the required System Director release to support Polycom phones. The certified System Director version is 4.0-SR5.

1. Upload the new controller image from the FTP server (where xxxx is based on the model of the WLAN controller).

   ```
   controller# copy ftp://ftpuser:ftppasswd@offbox-ip-address/ meru-
   4.0.SR5-xxxx.tar<space> .
   ```

   To check for successful ftp upload, type:

   ```
   controller# sh flash
   ```

   The filename meru-4.0.SR5-xxxx.tar should be present in the listing.

2. Upgrade the controller with the following command. The controller version must be 3.6.1-X or later before the upgrade.

   ```
   controller# upgrade controller 4.0.SR5-5
   ```

3. Plug the access points into the layer 2 or layer 3 switch.

4. Access Points can obtain their power from 802.3af standard Power over Ethernet (PoE). The power can be supplied by a PoE-compatible network switch or PoE power injector installed between the switch and the AP.

Chapter 2: Configuration Guidelines

During configuration of the Meru system, different parameters are configured as described in the following sections:

- Configure VLAN
- Configure a Security Profile
- Configure an ESS Profile

Configure VLAN

It is recommended to separate the voice and data traffic onto different VLAN's. An example configuration for a Polycom only VLAN follows. VLANs for other devices should be configured to provide the necessary separation.

Configuration can be done using the GUI or the CLI. Connect to the Meru CLI either by using a serial cable connected to the serial port of the controller or by connecting via Secure Shell using a tool like Secure CRT or HyperTerminal.

CLI Steps

```
controller# configure terminal
controller (config)#vlan polycom tag nnn
controller (config-vlan)# interface FastEthernet  1
```

(This represents the index of the port on the front of the controller.)

```
controller (config-vlan)# ip address nnn.nnn.nnn.nnn
controller (config-vlan)# ip default-gateway nnn.nnn.nnn.nnn
controller (config-vlan)# ip dhcp-server nnn.nnn.nnn.nnn
controller (config-vlan)# ip dhcp-passthrough
controller (config-vlan)# no ip dhcp-override
controller (config-vlan)# exit
```

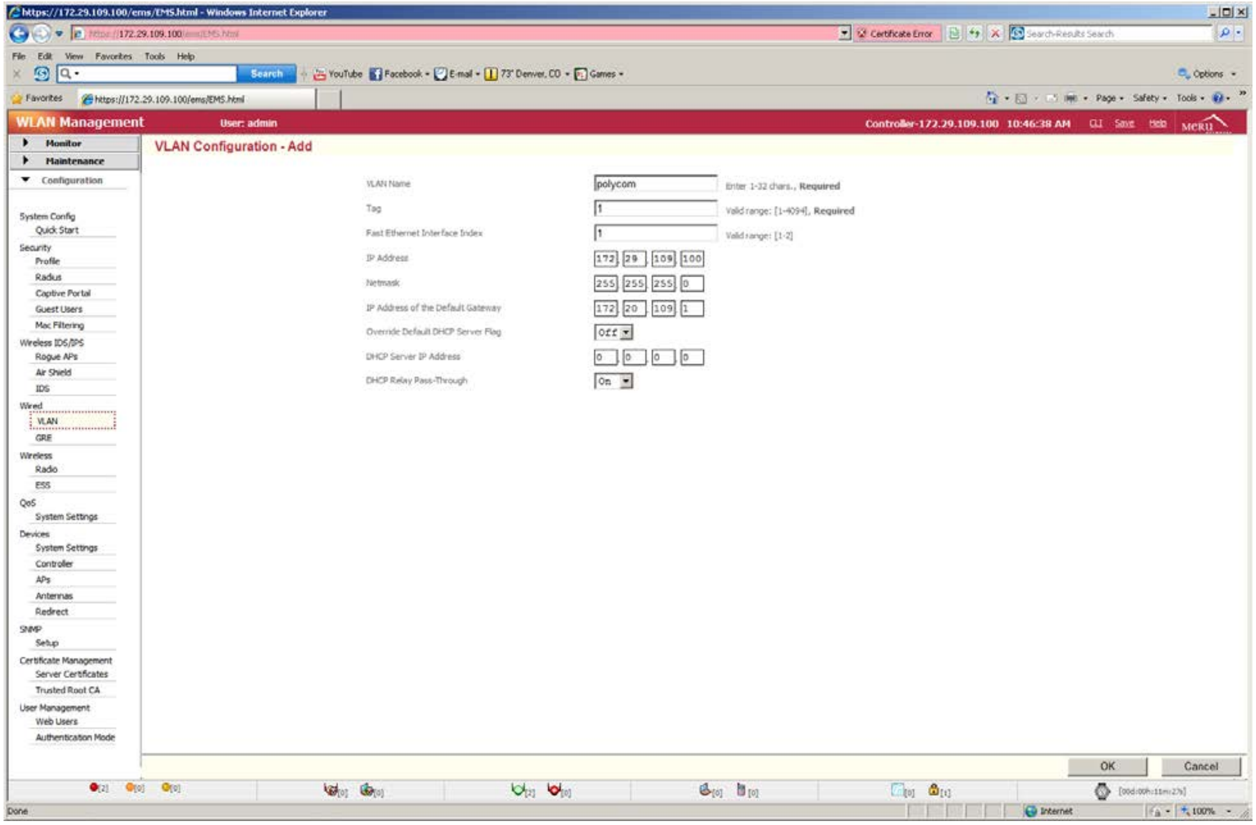
GUI Steps

1. Navigate to System Config->Quick Start and click on the **VLAN** tab.
2. Click on **Add**.
3. Enter the VLAN Name, Tag, Fast Ethernet Interface Index (the index of the port on the front of the controller), IP Address, Netmask, IP Address of the Default Gateway, and DHCP Server IP Address.

4 Set **Override DHCP Server Flag** to **Off**. (The address entered when initially provisioning the controller will be used for the DHCP server.)

5 Set **DHCP Relay Pass-through** to **On**. (The DHCP requests will be sent through unchanged.)

6 Click on **OK**.



VLAN Configuration - Add

VLAN Name: polycom — Enter 1-32 chars., **Required**

Tag: 1 — Valid range: [1-4094], **Required**

Fast Ethernet Interface Index: 1 — Valid range: [1-2]

IP Address: 172 . 29 . 109 . 100

Netmask: 255 . 255 . 255 . 0

IP Address of the Default Gateway: 172 . 20 . 109 . 1

Override Default DHCP Server Flag: Off

DHCP Server IP Address: 0 . 0 . 0 . 0

DHCP Relay Pass-Through: On

Configure Radius Profile

Meru supports the use of a Radius server to provide WPA2-Enterprise PEAP security.

GUI Steps

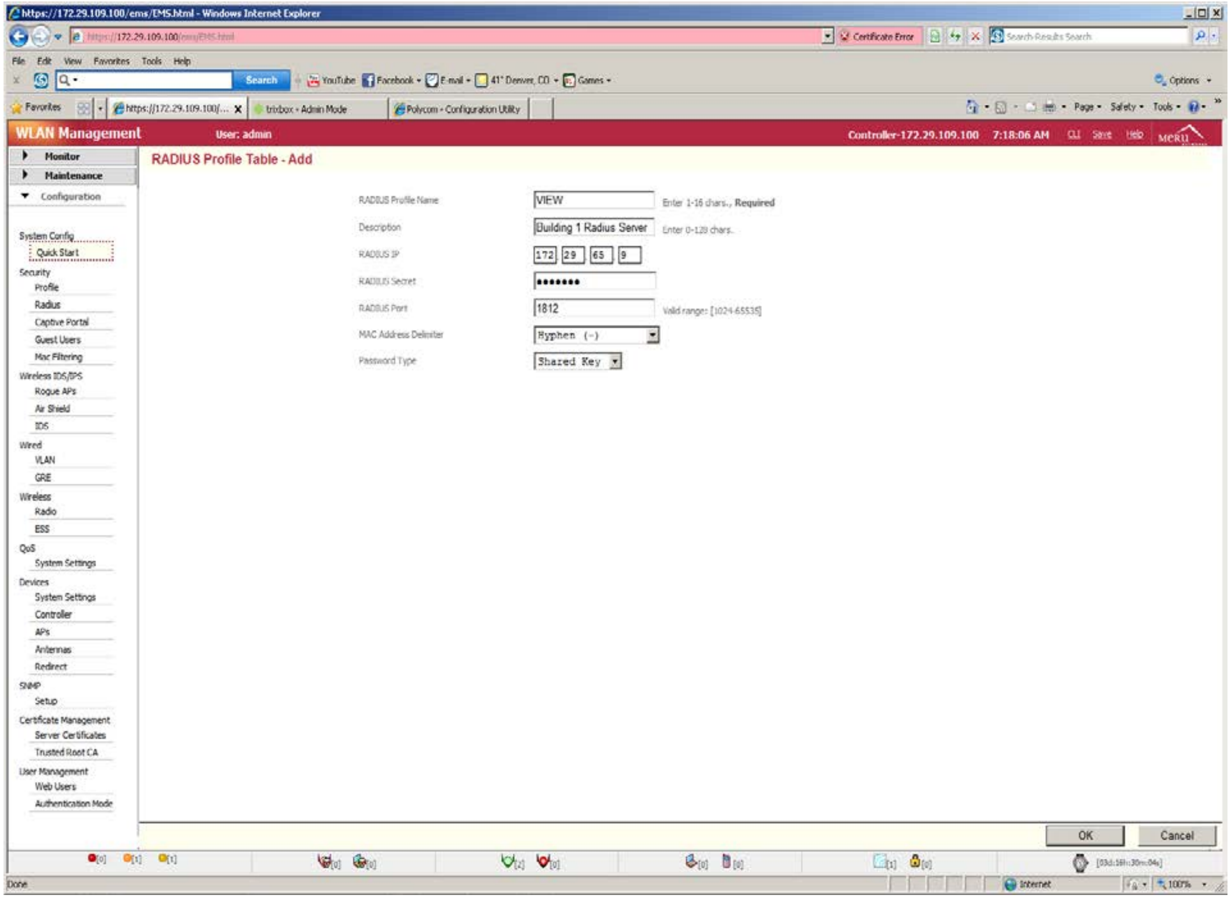
1 Navigate to System Config->Quick Start and click on the **Radius profile** tab.

2 Click on **Add**.

3 Enter the RADIUS Profile Name, Description, RADIUS IP, RADIUS Secret, and RADIUS Port.

4 Leave the **MAC Address Delimiter** set to the default of **Hyphen (-)** and the **Password Type** to the default of **Shared Key**.

5 Click on **OK**.



RADIUS Profile Table - Add

RADIUS Profile Name: VIEW — Enter 1-16 chars., **Required**
Description: Building 1 Radius Server — Enter 0-128 chars.
RADIUS IP: 172 . 29 . 65 . 9
RADIUS Secret: •••••••
RADIUS Port: 1812 — Valid range: [1024-65535]
MAC Address Delimiter: Hyphen (-)
Password Type: Shared Key

CLI Steps

```
controller# configure terminal
controller(config-radius)# radius-profile VIEW
controller(config-radius)# description VIEW
controller(config-radius)# ip-address nnn.nnn.nnn.nnn
controller(config-radius)# key aaasharedsecret
controller(config-radius)# port 1812
```

(The default port is usually the correct one, so this entry is probably unnecessary.)

```
controller(config-radius)# exit
controller# exit
```

Configure Security Profile

Meru supports the following 802.11 security mechanisms for the Polycom phones:

- Open (will not work with the phones in n-enabled radio modes)
- WPA-PSK
- WPA2-PSK
- WPA2-PEAP

The Meru WLAN System supports n security on radios that are not n-enabled. It is often useful for initial provisioning. A security profile with the name of default is automatically created on each VLAN.

The Meru WLAN System supports WPA-PSK mode with Polycom Wireless Telephones and can be configured as follows. Note that the pre-shared key (PSK) in the controller can be entered in hexadecimal or ASCII formats. If it is entered in hexadecimal, it must be preceded with 0x.

CLI Steps

```
controller# configure terminal
controller(config-security)# security-profile wpapass
controller(config-security)# allowed-l2-modes wpa-psk
controller(config-security)# encryption-modes tkip
controller(config-security)# psk key merupolycom
controller(config-security)# exit
controller# exit
```

GUI Steps

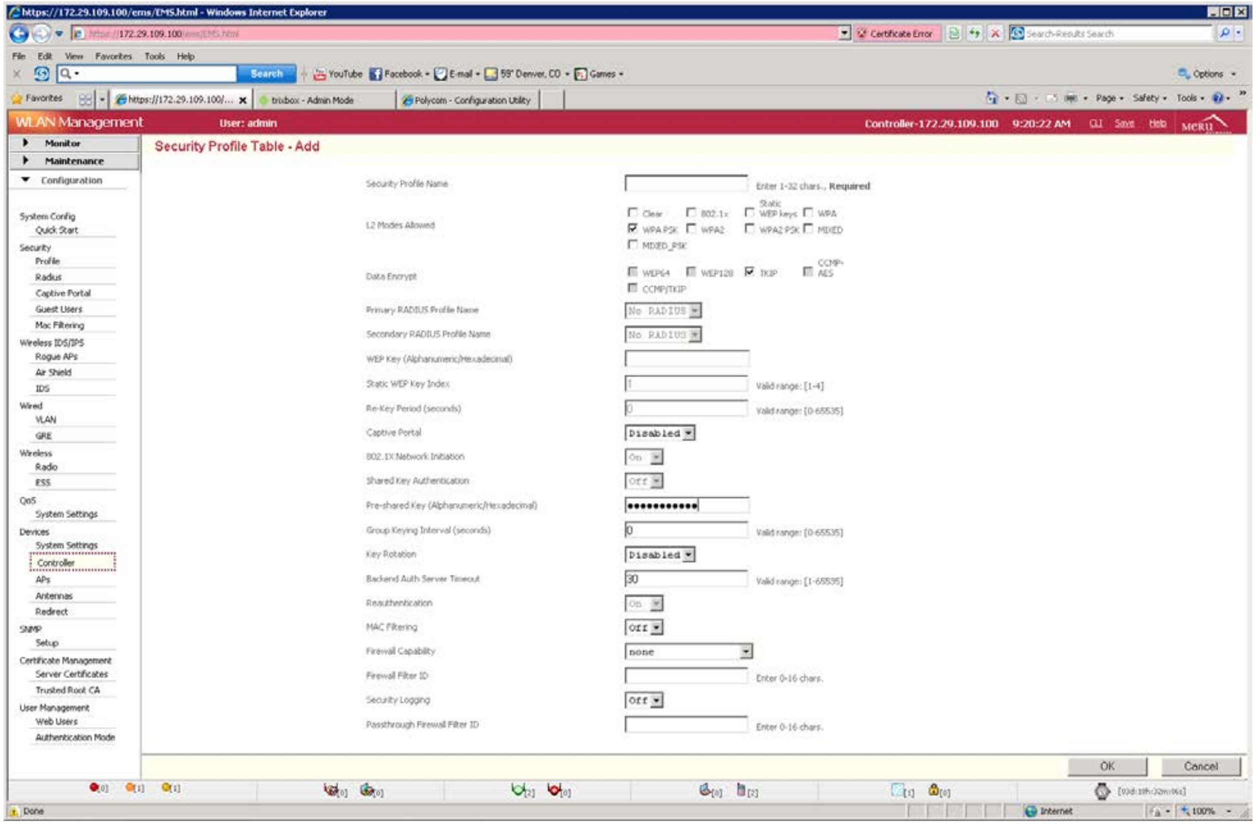
1 Navigate to System Config->Quick Start and click on the **Security Profile** tab.

2 Click on **Add**.

3 Enter the Security Profile Name and the Pre-shared Key (Alphanumeric/Hexadecimal).

4 Check the radio button **WPAPSK**.

5 Click on **OK**.



Security Profile Table - Add

Security Profile Name: Enter 1-32 chars., **Required**

L2 Modes Allowed: □ Clear □ 802.1x □ Static WEP keys □ WPA ☑ WPA PSK □ WPA2 □ WPA2 PSK □ MIXED □ MIXED_PSK

Data Encrypt: □ WEP64 □ WEP128 ☑ TKIP □ CCMP-AES □ CCMP/TKIP

Primary RADIUS Profile Name: No RADIUS

Secondary RADIUS Profile Name: No RADIUS

WEP Key (Alphanumeric/Hexadecimal):

Static WEP Key Index: 1 Valid range: [1-4]

Re-Key Period (seconds): 0 Valid range: [0-65535]

Captive Portal: Disabled

802.1X Network Initiation: On

Shared Key Authentication: Off

Pre-shared Key (Alphanumeric/Hexadecimal): ●●●●●●●●●●●

Group Keying Interval (seconds): 0 Valid range: [0-65535]

Key Rotation: Disabled

Backend Auth Server Timeout: 30 Valid range: [1-65535]

Reauthentication: On

MAC Filtering: Off

Firewall Capability: none

Firewall Filter ID: Enter 0-16 chars.

Security Logging: Off

Passthrough Firewall Filter ID: Enter 0-16 chars.

The Meru WLAN System supports WPA2-PSK mode with Polycom Wireless Telephones and is configured as follows. Note that the pre-shared key (PSK) in the controller is entered in hexadecimal or ASCII formats. If it is entered in hexadecimal, it must be preceded with 0x.

CLI Steps

```
controller# configure terminal
controller(config-security)# security-profile wpa2pass
controller(config-security)# allowed-l2-modes wpa2-psk
controller(config-security)#  encryption-modes ccmp
controller(config-security)#  psk key merupolycom
controller(config-security)#  exit
controller# exit
```

GUI Steps

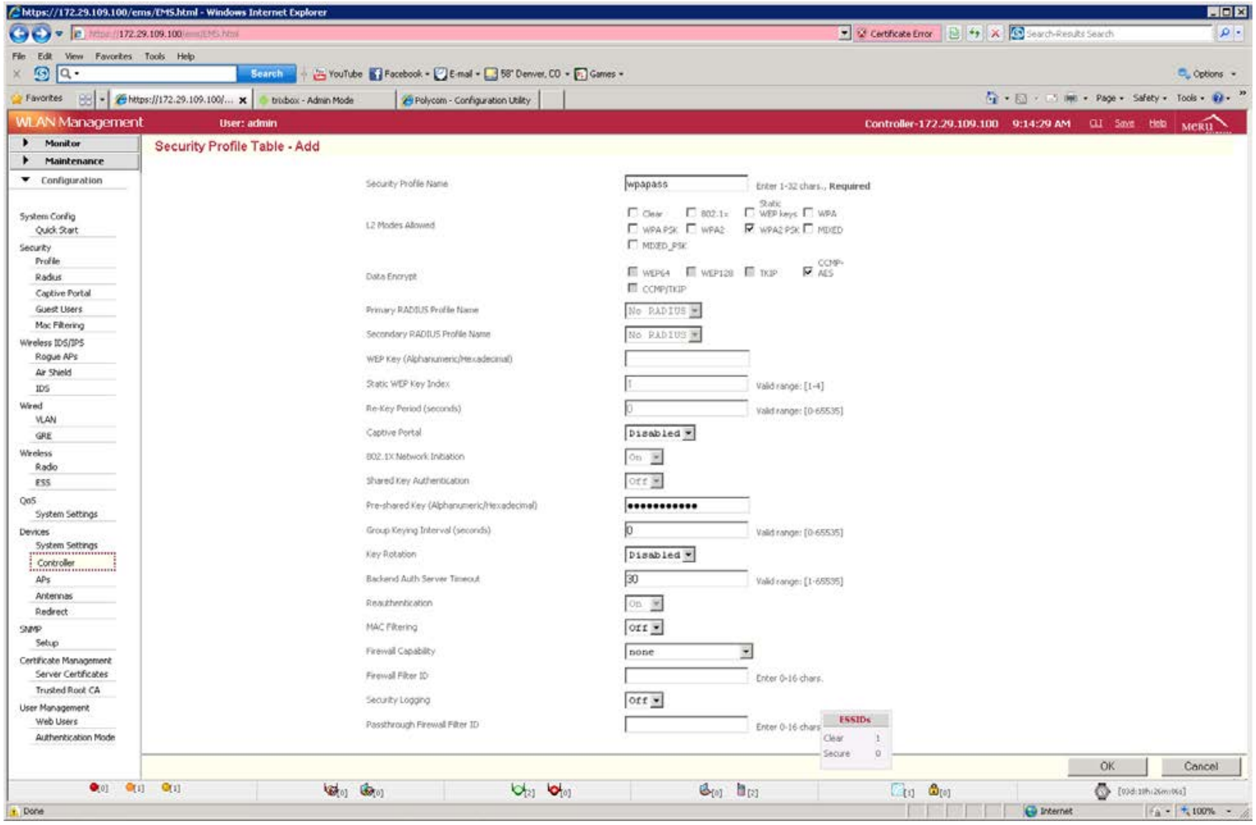
1 Navigate to System Config->Quick Start and click on the **Security Profile** tab.

2 Click on **Add**.

3 Enter the Security Profile Name and the Pre-shared Key (Alphanumeric/Hexadecimal).

4 Check the radio button **WPA2PSK**.

5 Click on **OK**.



Security Profile Table - Add

Security Profile Name	wpapass	Enter 1-32 chars., **Required**
L2 Modes Allowed	□ Clear □ 802.1x □ Static WEP keys □ WPA □ WPA PSK □ WPA2 ☑ WPA2 PSK □ MIXED □ MIXED_PSK	
Data Encrypt	□ WEP64 □ WEP128 □ TKIP ☑ CCMP-AES □ CCMP/TKIP	
Primary RADIUS Profile Name	No RADIUS	
Secondary RADIUS Profile Name	No RADIUS	
WEP Key (Alphanumeric/Hexadecimal)		
Static WEP Key Index	1	Valid range: [1-4]
Re-Key Period (seconds)	0	Valid range: [0-65535]
Captive Portal	Disabled	
802.1X Network Initiation	On	
Shared Key Authentication	Off	
Pre-shared Key (Alphanumeric/Hexadecimal)	●●●●●●●●●●●●	
Group Keying Interval (seconds)	0	Valid range: [0-65535]
Key Rotation	Disabled	
Backend Auth Server Timeout	30	Valid range: [1-65535]
Reauthentication	On	
MAC Filtering	Off	
Firewall Capability	none	
Firewall Filter ID		Enter 0-16 chars.
Security Logging	Off	
Passthrough Firewall Filter ID		Enter 0-16 chars

The Polycom phones support EAP-PEAPv0/MSCHAPv2. The Meru WLAN controller system is configured as follows.

CLI Steps

```
controller# configure terminal
controller(config-security)# security-profile wpapeap
controller(config-security)# allowed-l2-modes wpa2
controller(config-security)#  encryption-modes ccmp
controller(config-security)#  exit
controller# exit
```

GUI Steps

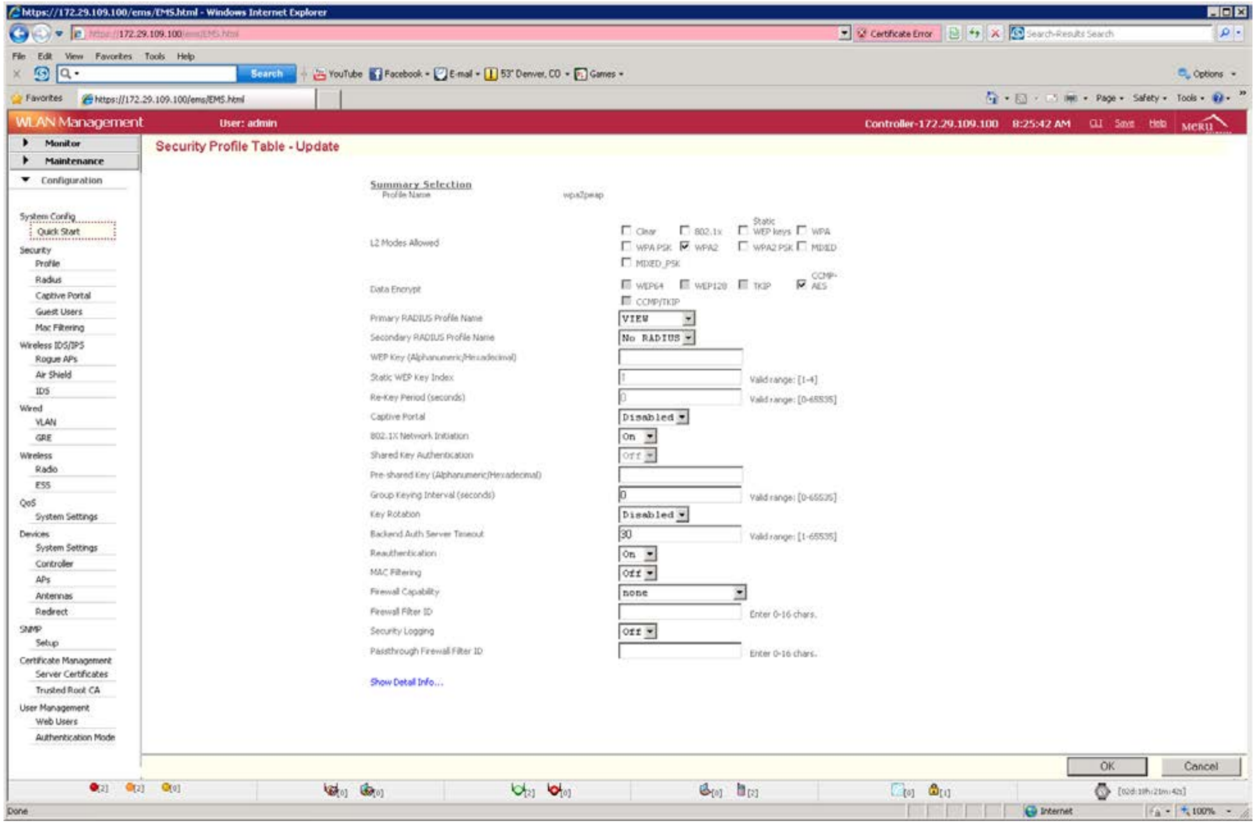
1 Navigate to System Config->Quick Start and click on the **Security Profile** tab.

2 Click on **Add**.

3 Select the previously created RADIUS profile from the **Primary RADIUS Profile Name** dropdown list.

4 Check the radio buttons **WPA2** and **CCMP-AES**.

5 Click on **OK**.



Security Profile Table - Update

Summary Selection

Profile Name	wpa2peap
L2 Modes Allowed	□ Clear □ 802.1x □ Static WEP keys □ WPA □ WPA PSK ☑ WPA2 □ WPA2 PSK □ MIXED □ MIXED_PSK
Data Encrypt	□ WEP64 □ WEP128 □ TKIP ☑ CCMP-AES □ CCMP/TKIP
Primary RADIUS Profile Name	VIEW
Secondary RADIUS Profile Name	No RADIUS
WEP Key (Alphanumeric/Hexadecimal)	
Static WEP Key Index	1 Valid range: [1-4]
Re-Key Period (seconds)	0 Valid range: [0-65535]
Captive Portal	Disabled
802.1X Network Initiation	On
Shared Key Authentication	Off
Pre-shared Key (Alphanumeric/Hexadecimal)	
Group Keying Interval (seconds)	0 Valid range: [0-65535]
Key Rotation	Disabled
Backend Auth Server Timeout	30 Valid range: [1-65535]
Reauthentication	On
MAC Filtering	Off
Firewall Capability	none
Firewall Filter ID	Enter 0-16 chars.
Security Logging	Off
Passthrough Firewall Filter ID	Enter 0-16 chars.

Show Detail Info...

Configure ESS Profile

The ESSID for Polycom Wireless Telephones should be configured as follows. Note: When enabling the multicast support (for the server discovery and PTT feature) there must be only one ESSID per VLAN; otherwise multicast traffic is not passed. The Meru WLAN system supports WMM and SIP. There are no additional QoS rules that need to configure for the phones. Please Note – one should enable the UAPSD feature in the ESS profile. These are switched off by default.

CLI Steps

```
controller# configure terminal
controller(config-essid)# essid polycom
controller(config-essid)# multicast-enable
controller(config-essid)# virtual-port
controller(config-essid)# countermeasure
controller(config-essid)#  security-profile wpa2pass
controller(config-essid)# dataplane  tunneled
controller(config-essid)# tunnel-type configured-vlan-only
controller(config-essid)# vlan name polycom
controller(config-essid)# ssid view
controller(config-essid)#  wmm-support
controller(config-essid)#  apsd-support
controller(config-essid)# beacon dtim-period 1
controller(config-essid)# beacon period  100
controller(config-essid)# exit
controller(config)#exit
```

GUI Steps

1 Navigate to System Config->Quick Start and click on the **ESS Profile** tab.

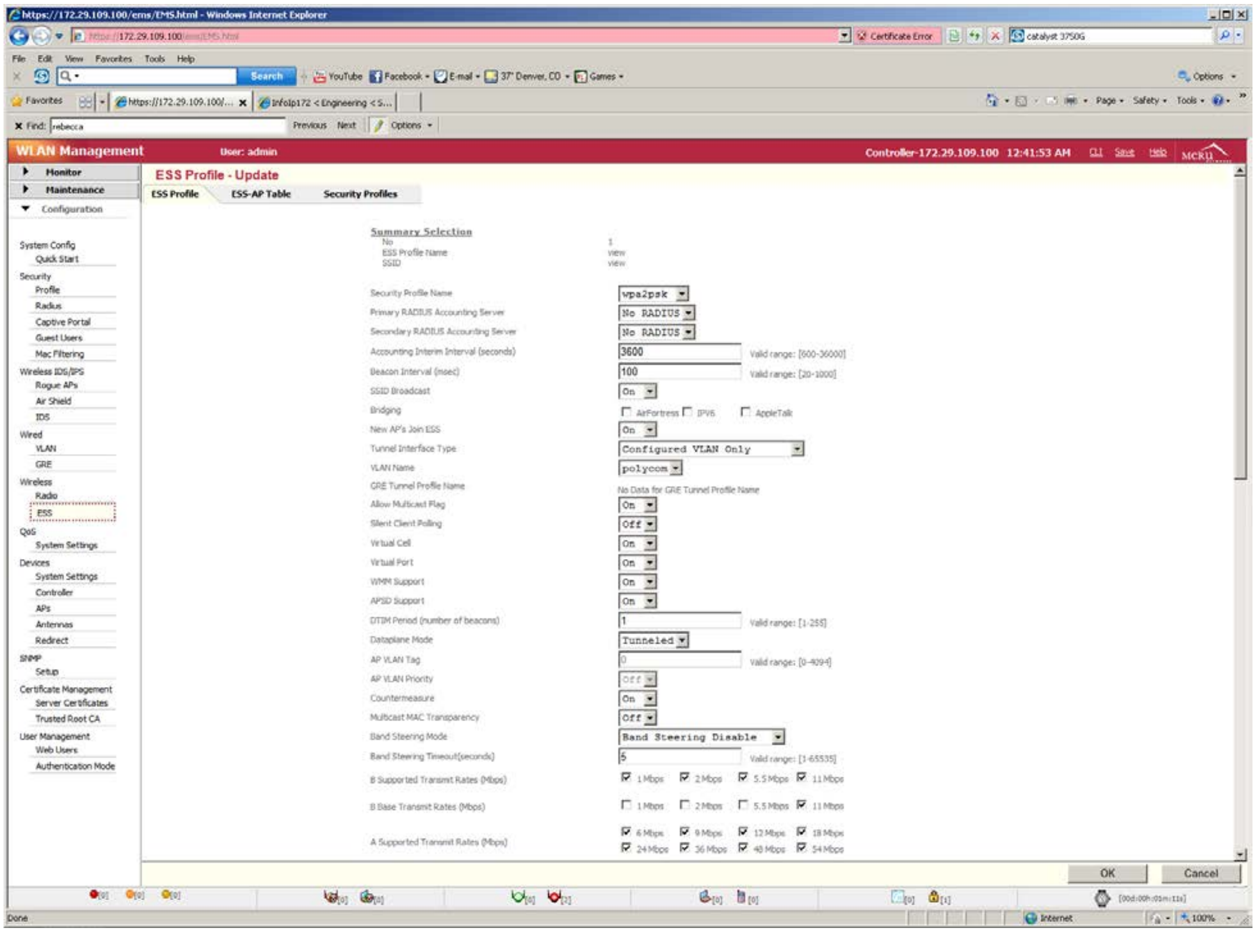
2 Click on **Add**.

3 Set Virtual Cell, Virtual Port, WMM Support, and APSD Support to On.

4 Set the Tunnel Interface Type to Configured VLAN Only and the VLAN Name to the VLAN name defined above (polycom).

5 Set the DTIM Period to 1.

6 Click on **OK**.



ESS Profile - Update

Summary Selection
No 1
ESS Profile Name view
SSID view

Security Profile Name: wpa2psk
Primary RADIUS Accounting Server: No RADIUS
Secondary RADIUS Accounting Server: No RADIUS
Accounting Interim Interval (seconds): 3600 Valid range: [600-36000]
Beacon Interval (msec): 100 Valid range: [20-1000]
SSID Broadcast: On
Bridging: □ AirFortress □ IPV6 □ AppleTalk
New AP's Join ESS: On
Tunnel Interface Type: Configured VLAN Only
VLAN Name: polycom
GRE Tunnel Profile Name: No Data for GRE Tunnel Profile Name
Allow Multicast Flag: On
Silent Client Polling: Off
Virtual Cell: On
Virtual Port: On
WMM Support: On
APSD Support: On
DTIM Period (number of beacons): 1 Valid range: [1-255]
Dataplane Mode: Tunneled
AP VLAN Tag: 0 Valid range: [0-4094]
AP VLAN Priority: Off
Countermeasure: On
Multicast MAC Transparency: Off
Band Steering Mode: Band Steering Disable
Band Steering Timeout(seconds): 5 Valid range: [1-65535]
B Supported Transmit Rates (Mbps): ☑ 1 Mbps ☑ 2 Mbps ☑ 5.5 Mbps ☑ 11 Mbps
B Base Transmit Rates (Mbps): □ 1 Mbps □ 2 Mbps □ 5.5 Mbps ☑ 11 Mbps
A Supported Transmit Rates (Mbps): ☑ 6 Mbps ☑ 9 Mbps ☑ 12 Mbps ☑ 18 Mbps ☑ 24 Mbps ☑ 36 Mbps ☑ 48 Mbps ☑ 54 Mbps

Radio Interface Configuration

The Polycom Wireless Telephones can utilize 802.11a, 802.11b, 802.11g, 802.11bg, 802.11an, or 802.11bgn modes. Additionally, it is recommended to configure the interface for Short Preamble mode.

The AP320s interface 1 supports 802.11b, 802.11g, 802.11bg, and 802.11bgn modes, while interface 2 supports 802.11a and 802.11an modes for the phones.

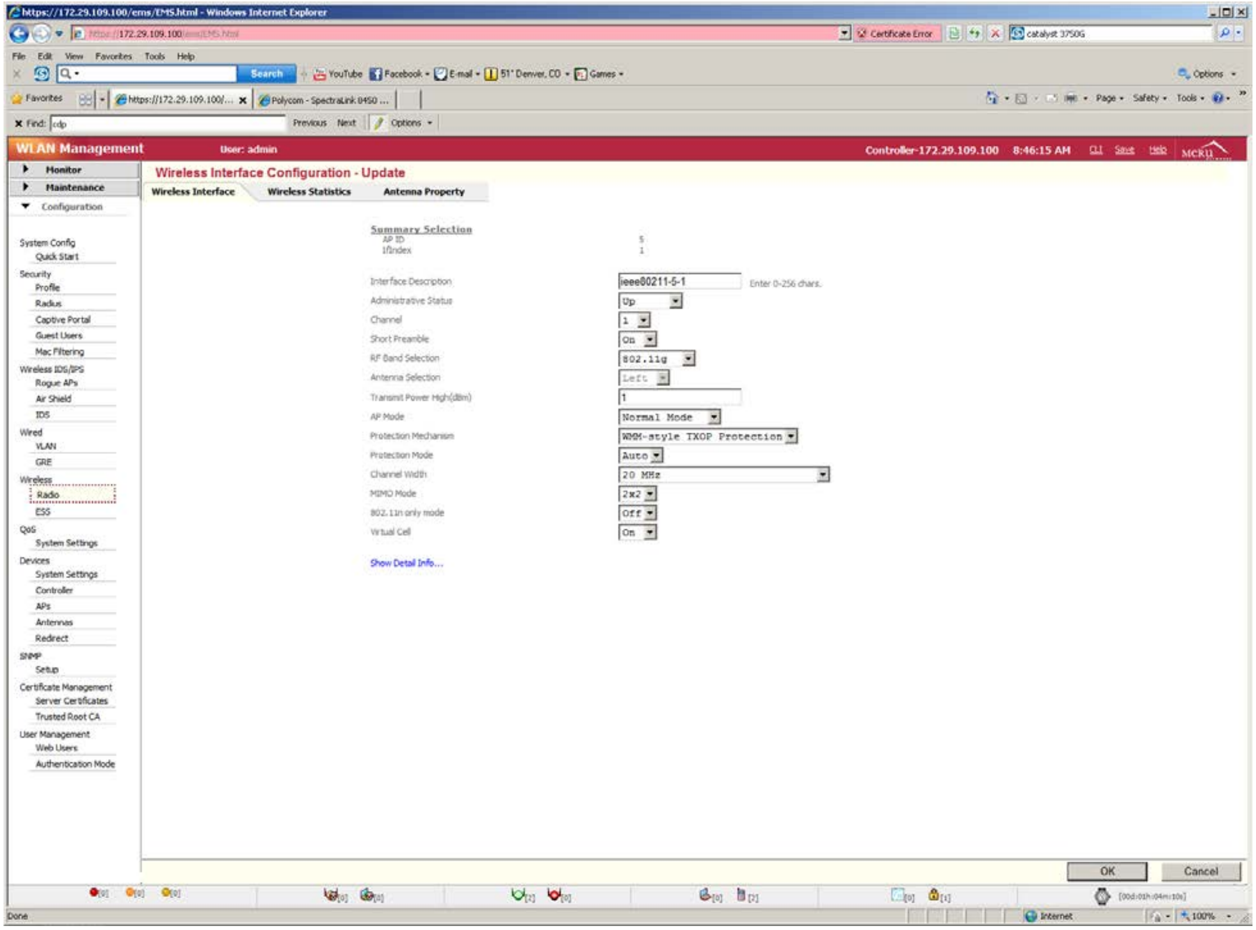
The following commands are used in order to configure the interface of an AP. In this example, access point 5 is configured for 802.11g operation with Short Preamble and channel width to be 20 MHz.

CLI Steps

```
controller#configure terminal
controller(config-if-802)# interface Dot11Radio 5 1
controller(config-if-802)# rf-mode 802.11g
controller(config-if-802)# preamble-short
controller(config-if-802)# channel 1
controller(config-if-802)#  channel-width 20-mhz
controller(config-if-802)# exit
controller#exit
```

GUI Steps

1. Navigate to Configuration->Wireless->Radio.
2. Select the desired radio interface of the connected AP.
3. Select the band from the **RF Band Selection** dropdown list.
4. Select the Channel Width.
5. Set Short Preamble to Off.
6. Click on **OK**.



Wireless Interface Configuration - Update

Summary Selection

AP ID	5
IfIndex	1
Interface Description	ieee80211-5-1 (Enter 0-256 chars.)
Administrative Status	Up
Channel	1
Short Preamble	On
RF Band Selection	802.11g
Antenna Selection	Left
Transmit Power High(dBm)	1
AP Mode	Normal Mode
Protection Mechanism	WMM-style TXOP Protection
Protection Mode	Auto
Channel Width	20 MHz
MIMO Mode	2x2
802.11n only mode	Off
Virtual Cell	On

Show Detail Info...

CLI Steps

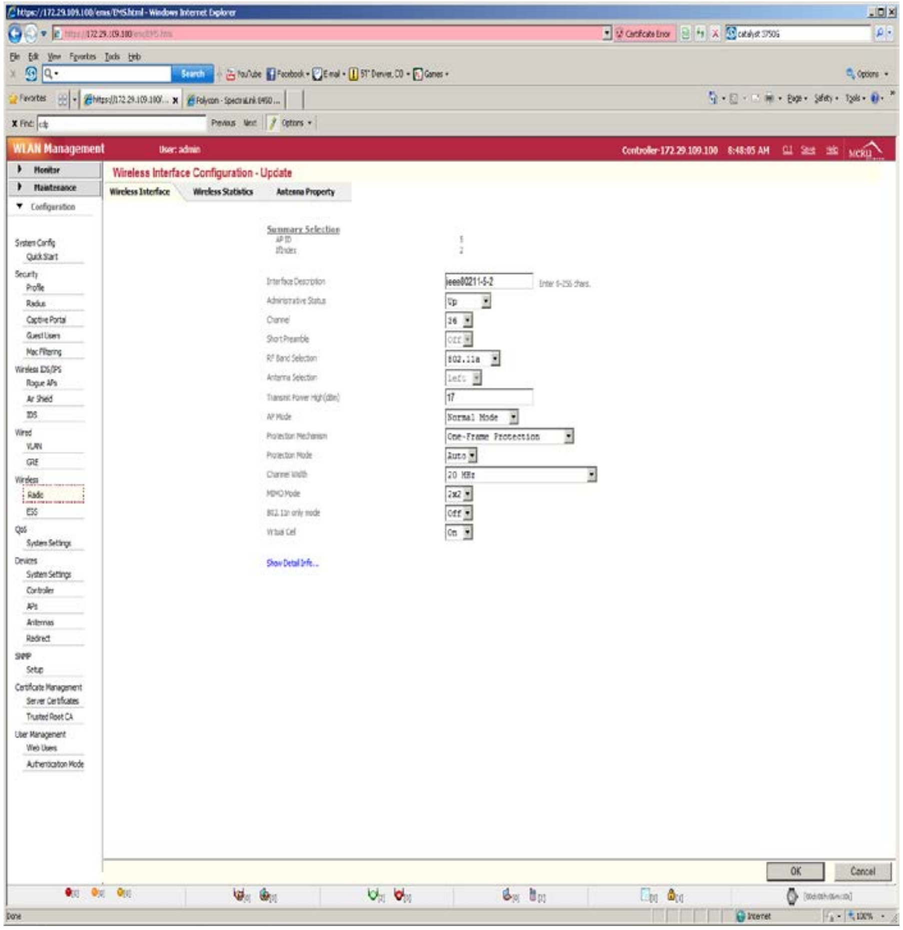
Following is a similar example of configuration for 802.11a operation with the Polycom 8020/8030 Wireless Telephones where we configure access point 5 for channel 36 on 802.11a and channel width configuration to be 40 MHz with extension channel to be the one above.

```
controller#configure terminal
controller(config-if-802)# interface Dot11Radio 5 2
controller(config-if-802)# rf-mode 802.11a
controller(config-if-802)# channel 36
controller(config-if-802)# channel-width 40-mhz-extension-channel-above
controller(config-if-802)# exit
controller# exit
```

GUI Steps

1. Navigate to Configuration->Wireless->Radio.
2. Select the desired radio interface of the connected AP.
3. Select the band from the **RF Band Selection** dropdown list.
4. Select the Channel Width.

5 Click on **OK**.



Wireless Interface Configuration - Update

Wireless Interface | Wireless Statistics | Antenna Property

Summary Selection
AP ID 5
IfIndex 2

Interface Description	ieee80211-5-2 Enter 0-255 chars.
Administrative Status	Up
Channel	36
Short Preamble	Off
RF Band Selection	802.11a
Antenna Selection	Left
Transmit Power High (dBm)	17
AP Mode	Normal Mode
Protection Mechanism	One-Frame Protection
Protection Mode	Auto
Channel Width	20 MHz
MIMO Mode	2x2
802.11n only mode	Off
Virtual Cell	On

Show Detail Info...

Note: Additional details on RF deployment

For additional details on RF deployment please see the Deploying Enterprise-Grade Wi-Fi Telephony white paper and the Best Practices Guide for Deploying Polycom 8020/8030 Wireless Telephones or Best Practices for Deploying Polycom® SpectraLink® 8400 Series Handsets. It is always practice to deploy the APs with an overlapping coverage of at least -60 dBm across the infrastructure for an effective voice solution.

Chapter 3: TSPEC Configuration

In version 4.0-SR5, TSPEC is not enabled by default in the Meru Infrastructure. TSPEC parameters are enabled by using a boot script. There are no additional commands that are needed to enable TSPEC.

Define and Upload a Boot Script to Enable WMM Access

An additional script, tspec.scr, is required in order to enable the TSPEC parameters. The script is run each time the AP's are booted. This script enables TSPEC and other settings to enhance voice quality of service and set the maximum voice call limit. By default the maximum calls is set to 8 for the 2.4 GHz band and 10 for the 5 GHz band.

The bootscript tspec.scr must be downloaded from the Meru Networks support portal.

In the boot script 2 radios will be involved. Radio0 is the 2.4 GHz radio and Radio1 is the 5 GHz radio. By default radio01 and radio11 are used in some of the commands in the boot script. These are virtual radio numbers assigned due to the definition of the SSID. These can change depending on the number of SSID's defined on the controller. *Thus, the bootscript must be edited if the SSID is not the only one defined.*

Note: Checking the bootscript

The bootscript must be checked for the need for editing and a system reload whenever new SSID's are defined.

Note: Loading the bootscript

The bootscript must be loaded even if access control is not used as it provides important performance tuning.

1 To determine the virtual radio number, perform the following:

2 Ensure that both radios are online and enabled for an AP using the information from "Configure Radios". Note the AP number.

3 Connect using the CLI as described in "Configuring a New Controller Starting from Factory Defaults".

4 Type **connect ap n**, where **n** is the AP number noted in step 1. The result will look like the following:

```
ap 6> vap display
```

```
Device          BSSID           State  Assc  PwrS  Essid
--------  ----------------- -----  ----  ---- -------
radio01   00:0c:e6:3a:be:6c  RUN    0     0    view
radio11   00:0c:e6:c1:24:43  RUN    0     0    view
radio01-1 06:06:01:07:21:3d  RUN    1     1    view
radio11-1 06:2c:01:0c:d6:0c  RUN    1     1    view
```

The virtual radios are read from the first and second line of the Device column. In this example, they are “radio01” and “radio11”.

5 Edit the boot script (tspec.scr) available from the Meru support portal, replacing every use of radio01 and radio11 in the script with the virtual radio identifies found.

6 Copy the script into the controller using the following:

```
controller# cd ATS/scripts
controller# copy ftp://ftpuser:ftppasswd@offbox-ip-address/tspec.scr.
controller# configure terminal
controller (config)# boot-script tspec.scr
controller (config)# end
```

This script will set the TSPEC parameters during initialization of all the Access Points during boot-up. Once the script is set up the APs will come up with TSPEC parameters all enabled.

Useful AP Level TSPEC Commands

AP level commands are used to monitor TSPEC related functionalities. The number of supported phone calls per AP is changed using the CLI. TSPEC commands will be integrated into the controller CLI and GUI in future releases.

To use these commands, connect to the CLI using the method described in “Configuring a New Controller Starting from Factory Defaults”.

```
controller# connect ap n
ap n> radio tspec radio0/1 show
```

(This shows the details of the bandwidth allocated for different phones. It also shows if TSPEC is enabled by looking at highest available Access Category Mandatory (acm) queue. If highest acm is > 1 TSPEC is disabled. Otherwise, it is enabled. **radio0** indicates the 2.4 GHz radio and **radio1** indicates the 5 GHz radio.)

```
ap n> radio tspec radio0/1 weightage 10 10 10 70
```

(This command changes the bandwidth allocation for different access categories. Starting from the left, the values set the percentages for the background, best effort, video, and voice classes of service. Option **radio0** indicates the 2.4 GHz radio and **radio1** indicates the 5 GHz radio.)

```
ap n> dev cmd radio0/1 maxvoicecall <value>
```

(This command sets the upper limit of the number of Voice calls per AP. Option **radio0** indicates the 2.4 GHz radio and **radio1** indicates the 5 GHz radio.)

Script File Modification

The section "Define and Upload a Boot Script to Enable WMM Access" discussed how to download a script file into the controller. If parameters like the Maximum Voice Calls per AP, or the weight-age of the TSPEC parameter need to be changed globally, tspec.scr is updated using an editor.

There are two global parameters that can be changed/added in the script file. They are:

1 Weightage

The weight-age given to the different access categories of the TSPEC is changed globally by introducing the command into the script file.

```
radio tspec radio0 weightage [bk] [be] [vi] [vo]
```

(command for 2.4 GHz radio)

```
radio tspec radio1 weightage [bk] [be] [vi] [vo]
```

(command for 5 GHz radio)

By default the weight-age that is allocated to different access categories are 5 for background, 5 for best effort, 5 for video and 85 for voice. Note that the total of the 4 values should be 100.

2 Maximum Voice Calls

The maximum voice calls for each APs can also be changed globally by adding/changing the command in the script file

```
dev cmd radio0 maxvoicecall [value]
```

(command for 2.4 GHz radio)

```
dev cmd radio1 maxvoicecall [value]
```

(command for 5 GHz radio)

By default the maximum voice calls set for 2.4 GHz is 8 calls and 5 GHz is 10 calls.

Once these changes are made, the script is uploaded to the controller in the same way as explained earlier. Once uploaded, all the APs should be rebooted for the new settings to take effect.