Avaya Solution & Interoperability Test Lab

Application Notes for a Meraki Wireless Solution with an Avaya Aura™ Telephony Infrastructure and Avaya Wireless 3631 IP Telephones in a Converged Wireless VoIP and Data Network - Issue 1.0

Abstract

These Application Notes describe the configuration of a wireless Voice over IP (VoIP) solution using Meraki's Cloud Managed Enterprise WLAN solution managing multiple Meraki MR14 Access Points with an Avaya Aura™ Telephony Infrastructure and Avaya Wireless 3631 IP Telephones in a Converged wireless VoIP and Data Network. Emphasis of the testing was placed on verifying prioritization of VoIP Wireless traffic on calls associated with the Avaya 3631 wireless IP telephones.

The Meraki Cloud Controller (MCC) provides centralized management, optimization, and monitoring of Meraki wireless Access Points. The MCC is a cloud-based service that is constantly monitoring, optimizing, and reporting on the behavior of the wireless network.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration of a wireless Voice over IP (VoIP) solution using Meraki's Cloud Managed Enterprise WLAN solution managing multiple Meraki MR14 Access Points with an Avaya Aura™ Telephony Infrastructure consisting of Avaya Aura™ Communication Manager, Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager Messaging and Avaya 3631 Wireless IP Telephones in a converged wired/wireless Voice over IP and Data Network. The Avaya 3631 Wireless IP Telephones gained network access through the Meraki MR14 Access Points and registered with Communication Manager.

1.1. Interoperability Compliance Testing

Interoperability compliance testing covered feature functionality, serviceability, and quality of service (QoS).

Compliance testing emphasis was placed on verifying Layer 2 roaming, Multiple Encryption & Authentication types, Wi-Fi Multimedia (WMM) QoS and the prioritization of wireless VoIP traffic and voice quality in a converged VoIP and Data network scenario.

Feature functionality tested:

- QoS - Wi-Fi Multimedia (WMM)
- Multiple ESSIDs
- Multiple Encryption & Authentication types - Clear, WPA2-CCMP and WPA2 CCMP with 802.1x authentication
- VLANs
- Layer 2 roaming

The telephony features verified to operate correctly included:

- Attended/Unattended transfer
- Conference call add/drop/participation
- Multiple call appearances
- Caller ID operation
- Call forwarding
- Call Park,/Call pick-up
- Bridged call appearances
- Voicemail using Communication Manager Messaging
- Message Waiting Indicator (MWI)
- Hold/Return from hold
- Direct IP Media (Shuffling)
- G.711 and G.729 codecs

Serviceability testing:

- Serviceability testing was conducted to verify the ability of the Avaya/ Meraki solution to recover from adverse conditions, such as power cycling network devices and disconnecting cables between the LAN interfaces. In all cases, the ability to recover after the network normalized was verified.

1.2. Support

For technical support on Meraki products, consult the support pages at:
http://meraki.com/support/

2. Reference Configuration

The network diagram shown in **Figure 1** illustrates the testing environment used for compliance testing. The network consists of an Avaya Aura™ Communication Manager and Avaya Aura™ Communication Manager Messaging running on an Avaya S8300 Server with an Avaya G450 Media Gateway, one Avaya S8800 server running Avaya Aura™ Session Manager, one Avaya S8800 server running Avaya Aura™ System Manager, multiple Avaya 9600 Series IP Telephones, SIP and H.323, one Avaya 2410 Digital Telephone and three Meraki MR14 Access Points. One computer is present in the network providing network services such as Radius, DHCP, HTTP, and TFTP.

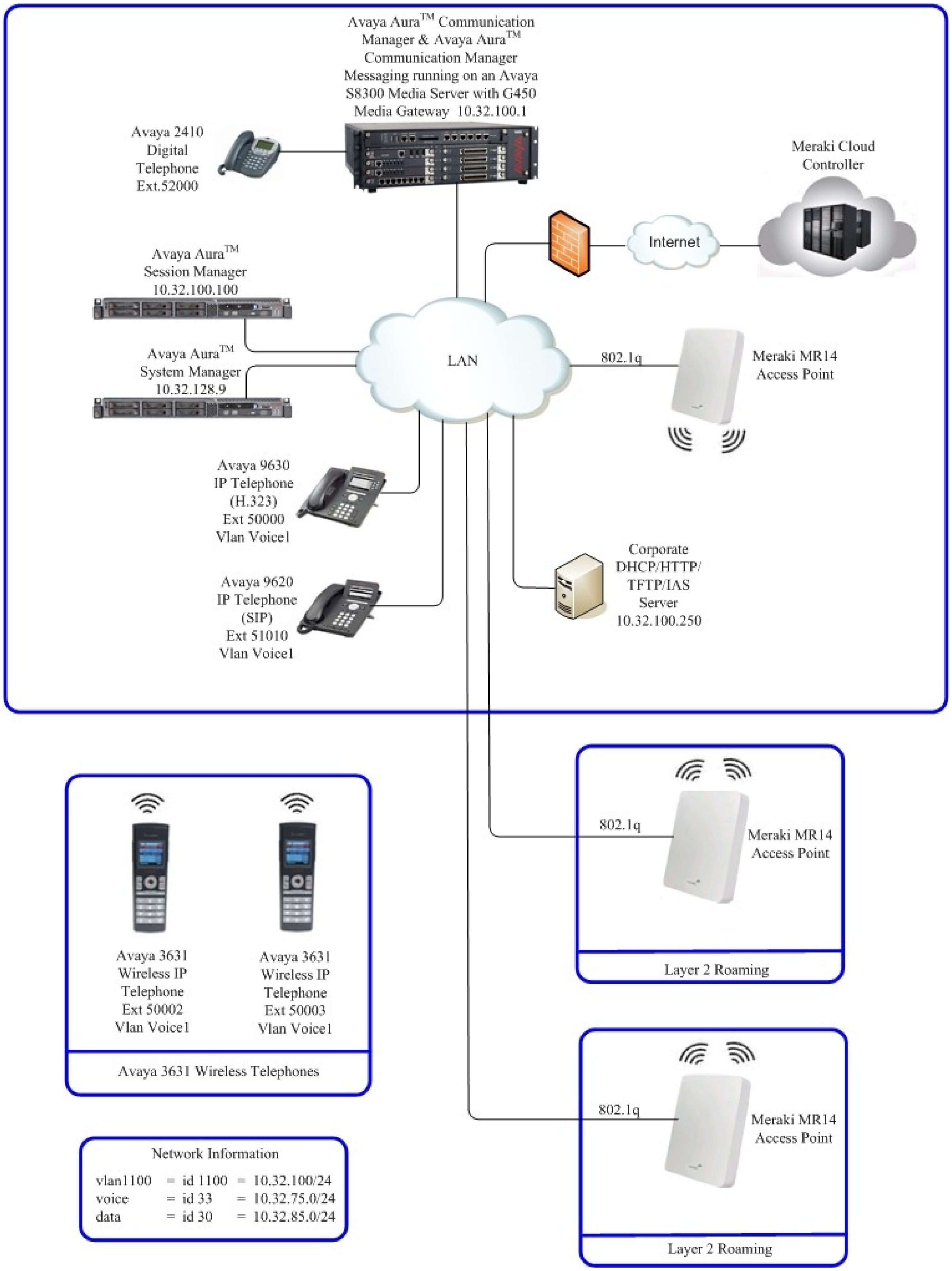

Avaya Aura™ Communication Manager & Avaya Aura™ Communication Manager Messaging running on an Avaya S8300 Media Server with G450 Media Gateway 10.32.100.1
Avaya 2410 Digital Telephone Ext.52000
Meraki Cloud Controller
Internet
Avaya Aura™ Session Manager 10.32.100.100
Avaya Aura™ System Manager 10.32.128.9
LAN
802.1q
Meraki MR14 Access Point
Avaya 9630 IP Telephone (H.323) Ext 50000 Vlan Voice1
Avaya 9620 IP Telephone (SIP) Ext 51010 Vlan Voice1
Corporate DHCP/HTTP/TFTP/IAS Server 10.32.100.250
802.1q
Meraki MR14 Access Point
Layer 2 Roaming
Avaya 3631 Wireless IP Telephone Ext 50002 Vlan Voice1
Avaya 3631 Wireless IP Telephone Ext 50003 Vlan Voice1
Avaya 3631 Wireless Telephones
802.1q
Meraki MR14 Access Point
Layer 2 Roaming
Network Information
vlan1100 = id 1100 = 10.32.100/24
voice = id 33 = 10.32.75.0/24
data = id 30 = 10.32.85.0/24

Figure 1: Network Configuration

3. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software/Firmware
Avaya PBX Products	
Avaya S8300 Server running Avaya Aura™ Communication Manager	Avaya Aura™ Communication Manager 6.0
Avaya G450 Media Gateway (Corporate Site) MGP MM712 DCP Media Module	 30 .13 .2 HW9
Avaya Aura™ Session Manager	
Avaya Aura™ Session Manager	6.0
Avaya Messaging (Voice Mail) Products	
Avaya Aura™ Communication Manager Messaging (CMM)	6.0
Avaya Telephony Sets	
Avaya 9600 Series IP Telephones	(H.323 3.1.1) and (SIP 2.6)
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone SIP 2.6
Avaya 3631 Wireless Telephone	V1.509
Avaya 2410 Digital Telephone	5.0
Meraki Products	
Meraki MR14 Access Point	14-50196
MS Products	
Microsoft Windows 2003 Server	Microsoft Windows 2003 Server

4. Configure QoS on Communication Manager

This section describes the steps required for Communication Manager to support the configuration shown in **Figure 1**. The following pages provide instructions on how to administer the required configuration parameters. The assumption is that the appropriate license and authentication files have been installed on the servers and that login and password credentials are available. It is assumed that the reader has a basic understanding of the administration of Communication Manager and has access to the System Administration Terminal (SAT) screen. For detailed information on the installation, maintenance, and configuration of Communication Manager, please consult references in **Section 10 [1]** through **[3].**

IP networks were originally designed to carry data on a best-effort delivery basis, which meant that all traffic had equal priority and an equal chance of being delivered in a timely manner. As a result, all traffic had an equal chance of being dropped when congestion occurred. QoS is now utilized to prioritize VoIP traffic and should be implemented throughout the entire network.

In order to achieve prioritization of VoIP traffic, the VoIP traffic must be classified. The Avaya Aura™ telephony infrastructure supports both IEEE 802.1p and DiffServ.

There were two ip-network-region's used for this sample configuration, one for Avaya wired IP Telephones and one for Avaya wireless IP Telephones. The DiffServ and 802.1p/Q values configured here will be downloaded to the Avaya H.323 IP wired and wireless Telephones via Communication Manager. Avaya SIP IP Telephones will get QoS settings by downloading the 46xxsettings file from the HTTP server (not shown in this document). For more information on QoS settings please refer to **Section 10 [1]** through **[3]**.

4.1. Configure the ip-network-region

The Differentiated Services Code Point (DSCP) value of 46 will be used for both PHB values. DSCP 46 represents the traffic class of premium and the traffic type voice. Set the **Call Control PHB Value** to **46** and the **Audio PHB Value** to **46**. **Call Control 802.1p Priority** and **Audio 802.1p Priority** are set to **6**.

From the SAT, use the **change ip-network-region 1** command to change the DIFFSERV/TOS PARAMETERS and 802.1P/Q PARAMETERS settings. Change the following:

- **Call Control PHB Value** set to **46**
- **Audio PHB Value** set to **46**
- **Call Control 802.1p** set to **6**
- **Audio 802.1p priority** set to **6**

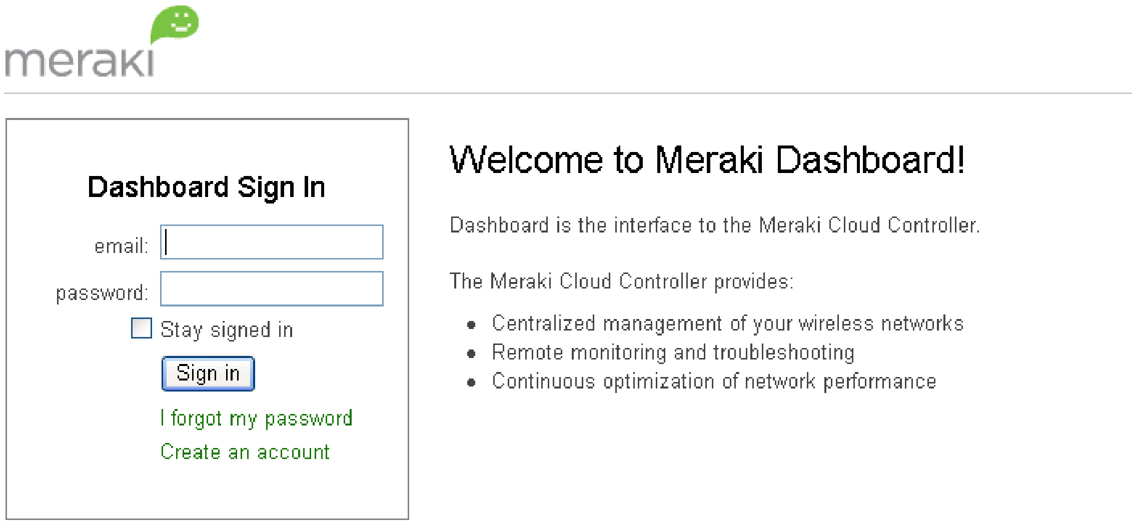
```
change ip-network-region 1                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: dev4.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 3027
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46     RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46      Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

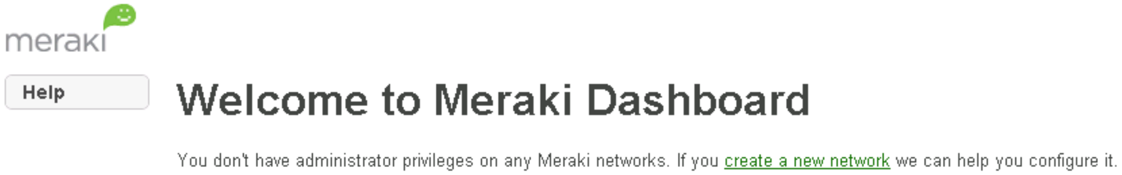
5. Configure the Meraki Cloud and Meraki MR14 Access Points

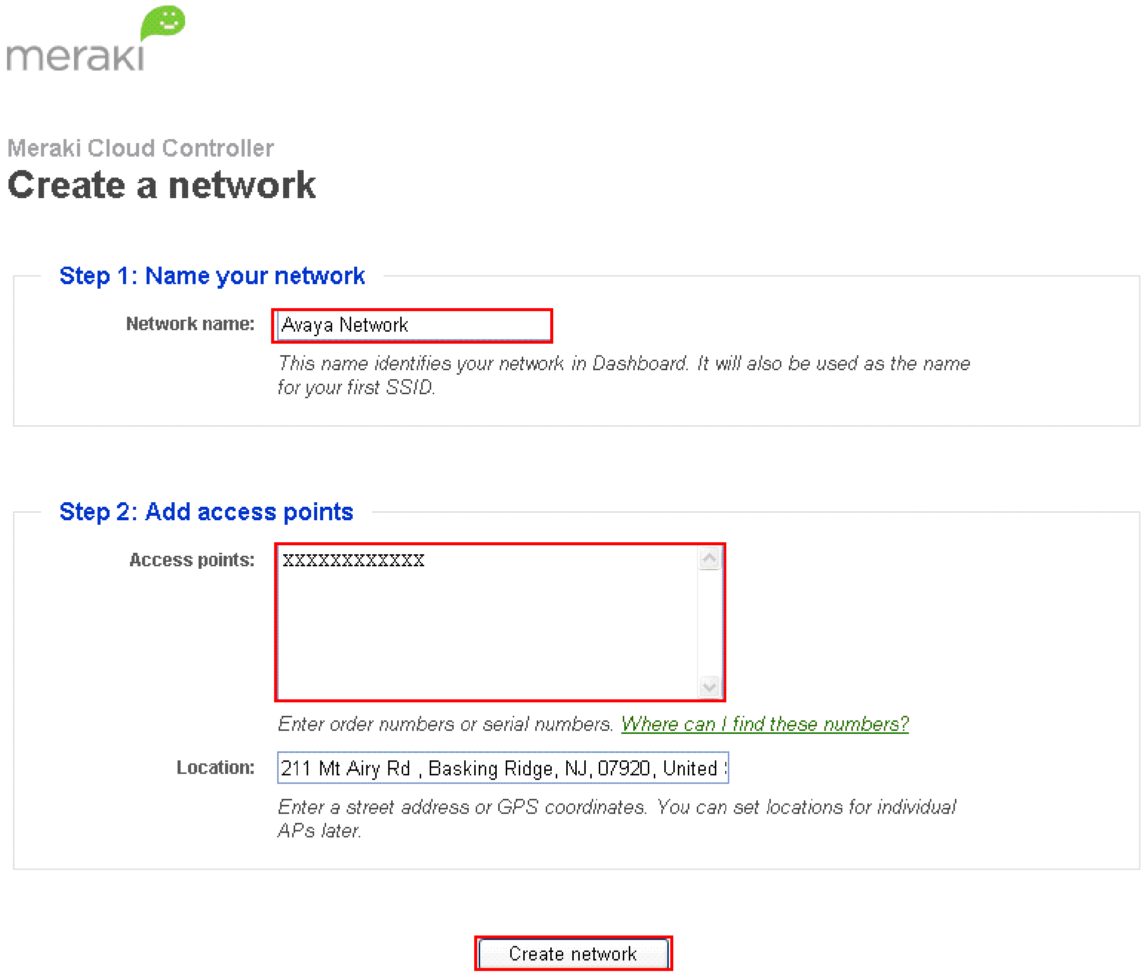
The following steps detail the initial configuration for the Meraki Cloud Solution used for the compliance testing. The configuration on the Meraki Cloud was administered via the following Public address: https://dashboard.meraki.com.

Except where stated the parameters in all steps are the default settings and are supplied for reference. Refer to **Section 10 [5]** for additional information regarding the configuration displayed in this section.

5.1. Configure Meraki Cloud

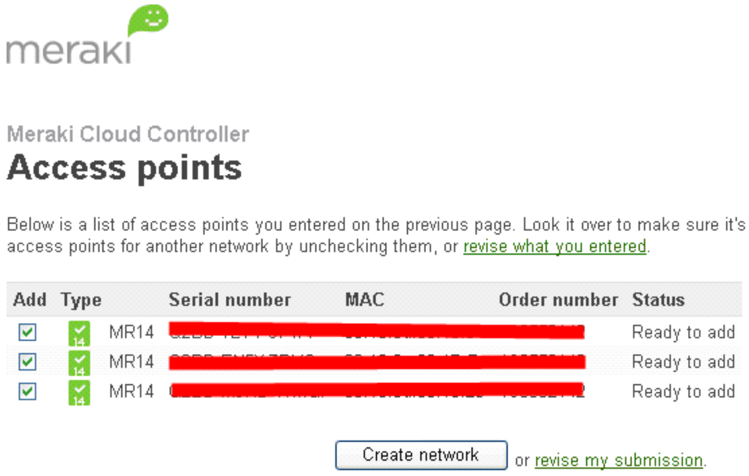
Step	Meraki Cloud as depicted in **Figure 1**.
1.	1. Start the web browser and enter the address https://dashboard.meraki.com**.** 2. Log in to the Meraki Cloud. For new users, create a new account, otherwise, login with the credentials previously created. Select **Sign in** to continue.  meraki Dashboard Sign In email: password: ☐ Stay signed in Sign in I forgot my password Create an account Welcome to Meraki Dashboard! Dashboard is the interface to the Meraki Cloud Controller. The Meraki Cloud Controller provides: • Centralized management of your wireless networks • Remote monitoring and troubleshooting • Continuous optimization of network performance

Step	
2.	The Welcome to Meraki Dashboard window will appear, select **create a new network** to continue.  Welcome to Meraki Dashboard You don't have administrator privileges on any Meraki networks. If you create a new network we can help you configure it.

Step	
3.	The Create a network window will appear. Go to **Step 1:Name your network,** add a unique **Network name**. Go to **Step 2**: **Add access points**, add the purchased **Access points** information supplied by Meraki. Select **Create network** to continue.  Meraki Cloud Controller Create a network Step 1: Name your network Network name: Avaya Network *This name identifies your network in Dashboard. It will also be used as the name for your first SSID.* Step 2: Add access points Access points: XXXXXXXXXXXX *Enter order numbers or serial numbers. Where can I find these numbers?* Location: 211 Mt Airy Rd , Basking Ridge, NJ, 07920, United *Enter a street address or GPS coordinates. You can set locations for individual APs later.*

Step 4.

The **Access points** window will appear. It will list the Access points that were purchased. As shown below, three access points were used for compliance testing. Select **Create network** to continue.



Meraki Cloud Controller

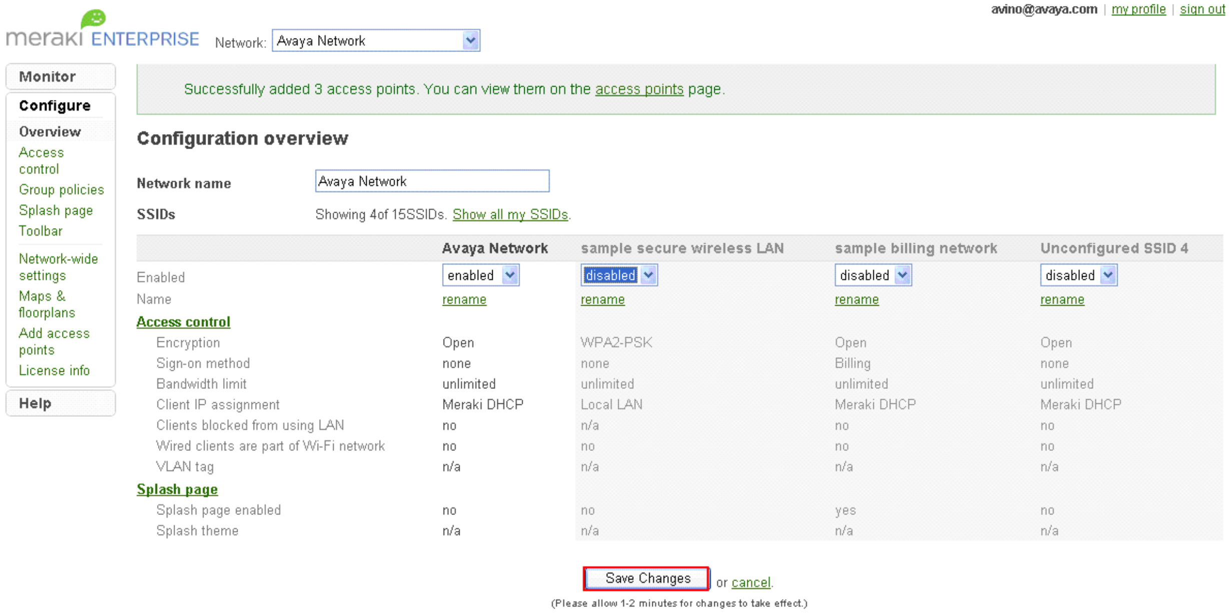
Access points

Below is a list of access points you entered on the previous page. Look it over to make sure it's what you expect. You can withhold access points for another network by unchecking them, or revise what you entered.

Add	Type	Serial number	MAC	Order number	Status
☑	MR14	[redacted]	[redacted]	[redacted]	Ready to add
☑	MR14	[redacted]	[redacted]	[redacted]	Ready to add
☑	MR14	[redacted]	[redacted]	[redacted]	Ready to add

Step 5.

The **Configuration overview** window will appear. It will list the pre-configured SSID's. Select **Save Changes** to continue.



Network: Avaya Network

Successfully added 3 access points. You can view them on the access points page.

Configuration overview

Network name: Avaya Network

SSIDs: Showing 4of 15SSIDs. Show all my SSIDs.

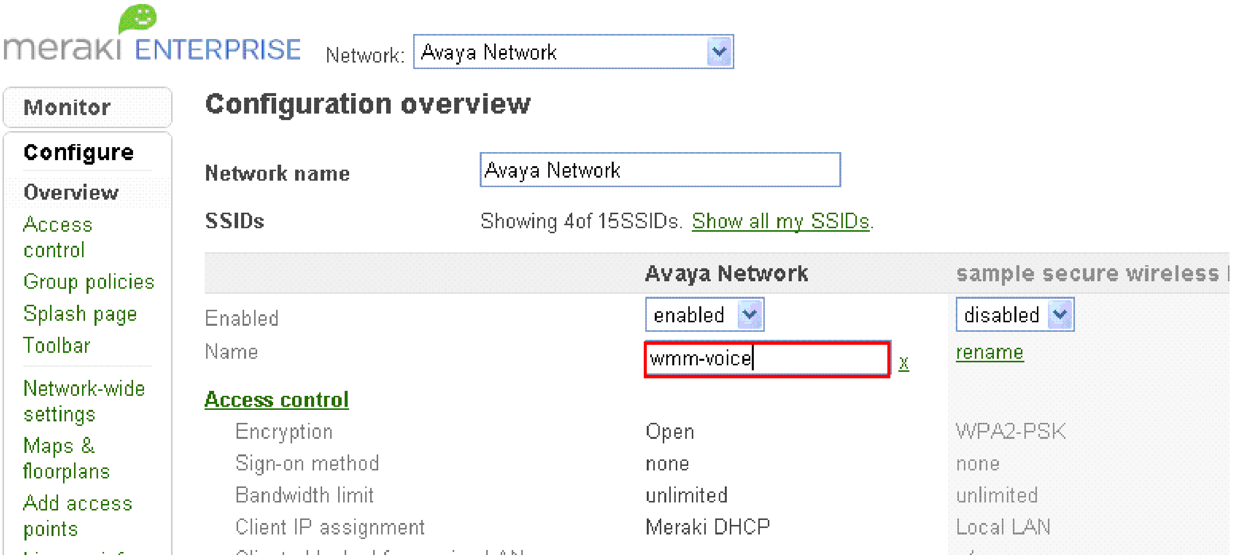
	Avaya Network	sample secure wireless LAN	sample billing network	Unconfigured SSID 4
Enabled	enabled	disabled	disabled	disabled
Name	rename	rename	rename	rename
Access control				
Encryption	Open	WPA2-PSK	Open	Open
Sign-on method	none	none	Billing	none
Bandwidth limit	unlimited	unlimited	unlimited	unlimited
Client IP assignment	Meraki DHCP	Local LAN	Meraki DHCP	Meraki DHCP
Clients blocked from using LAN	no	n/a	no	no
Wired clients are part of Wi-Fi network	no	no	no	no
VLAN tag	n/a	n/a	n/a	n/a
Splash page				
Splash page enabled	no	no	yes	no
Splash theme	n/a	n/a	n/a	n/a

(Please allow 1-2 minutes for changes to take effect.)

5.2. Create and Configure the SSID for the Voice Network

Three different security schemas were tested for the voice wireless traffic - Clear, WPA2-PSK AES/CCMP and WPA2 AES/CCMP with 802.1x authentication. Administration of the Clear and WPA2 AES/CCMP with 802.1x authentication SSIDs will not be covered in these Application Notes.

It is assumed VLAN trunking is enabled on the ports of the Ethernet switch that is connected to each Meraki Access Point, and that the VLANs assigned in this section are assigned.

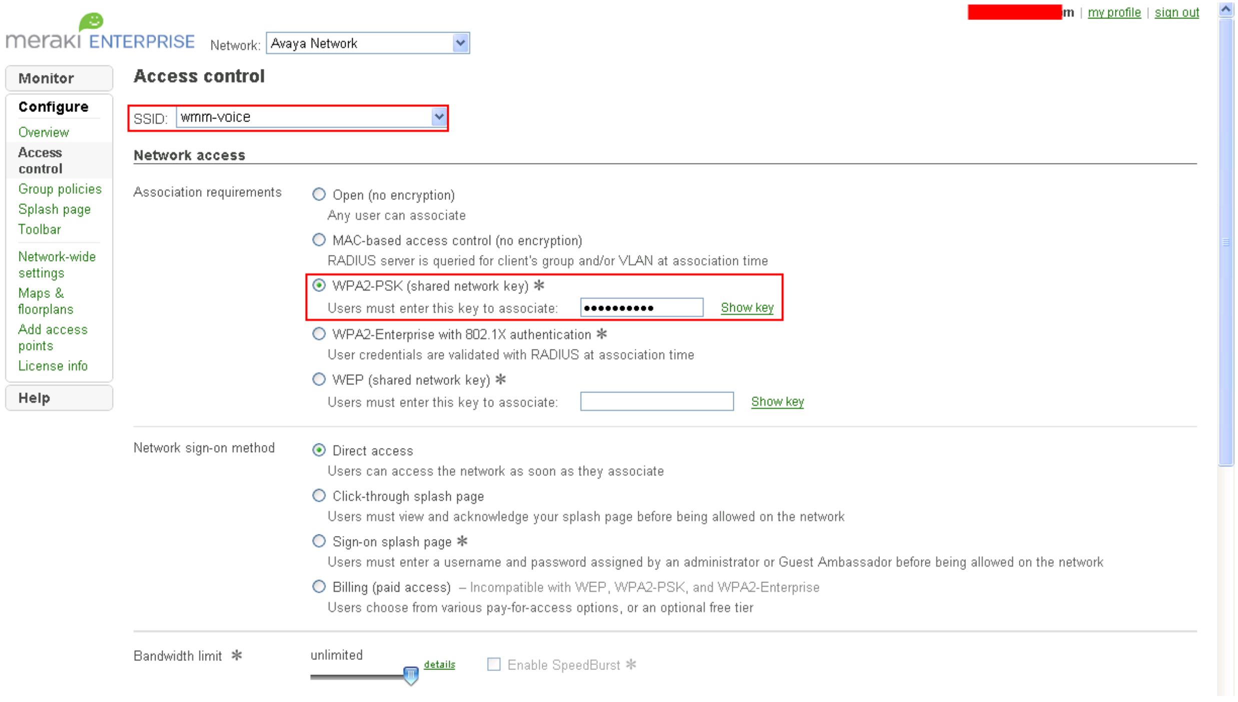
Step	
1.	From the left configuration tree, select **Configure → Overview.** Select **rename** (not shown), under the SSID, **Avaya Network**, change the name to **wmm-voice**. Select **Save Changes** at the bottom of the page (not show), to continue. 

Configuration overview

Network name: Avaya Network

SSIDs: Showing 4of 15SSIDs. Show all my SSIDs.

	Avaya Network	sample secure wireless
Enabled	enabled	disabled
Name	wmm-voice x	rename
Access control		
Encryption	Open	WPA2-PSK
Sign-on method	none	none
Bandwidth limit	unlimited	unlimited
Client IP assignment	Meraki DHCP	Local LAN

Step	
2.	From the left configuration tree, select **Configure → Access control.** Under **Access control**, select **wmm-voice** from the **SSID** drop-down list. Under **Network access** , select the radio button for **WPA2-PSK (shared network key)** and enter a unique key. Scroll down to **Addressing and traffic** to continue. 

[redacted]m | my profile | sign out

meraki ENTERPRISE Network: Avaya Network

Monitor
Configure
Overview
Access control
Group policies
Splash page
Toolbar
Network-wide settings
Maps & floorplans
Add access points
License info
Help

Access control

SSID: wmm-voice

Network access

Association requirements

○ Open (no encryption)
Any user can associate

○ MAC-based access control (no encryption)
RADIUS server is queried for client's group and/or VLAN at association time

● WPA2-PSK (shared network key) ✻
Users must enter this key to associate: •••••••••• Show key

○ WPA2-Enterprise with 802.1X authentication ✻
User credentials are validated with RADIUS at association time

○ WEP (shared network key) ✻
Users must enter this key to associate: Show key

Network sign-on method

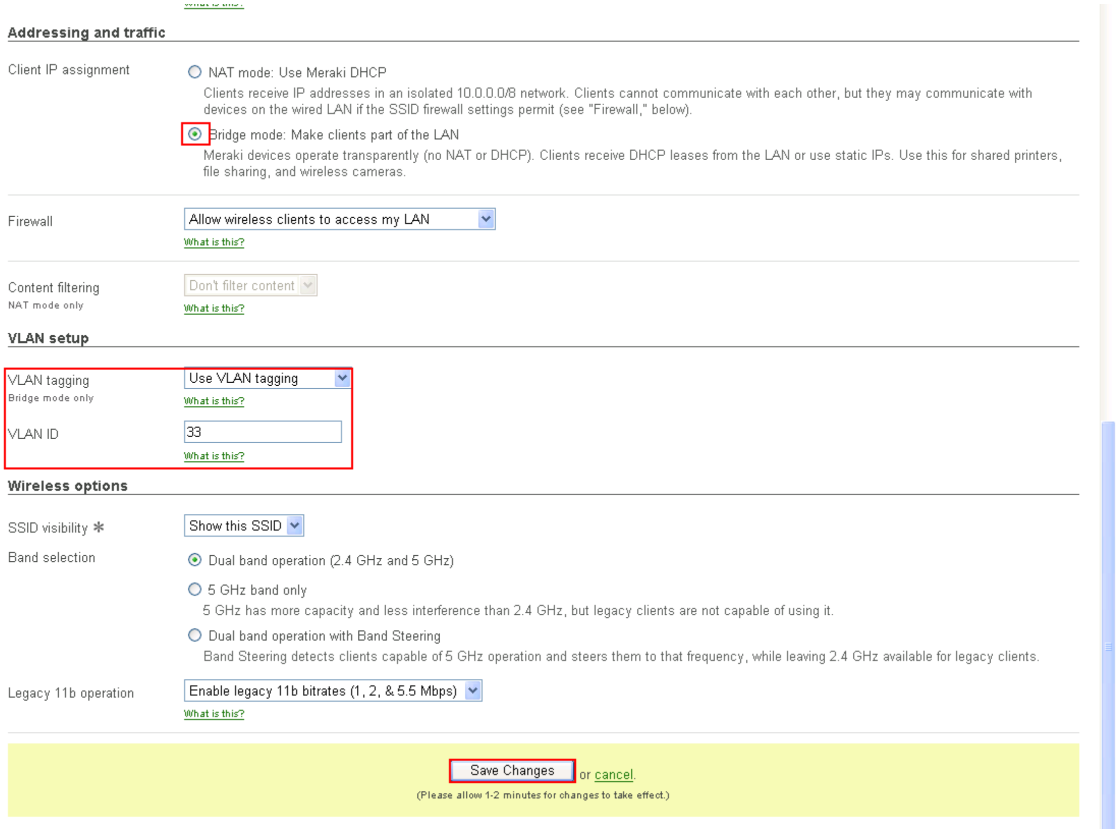
● Direct access
Users can access the network as soon as they associate

○ Click-through splash page
Users must view and acknowledge your splash page before being allowed on the network

○ Sign-on splash page ✻
Users must enter a username and password assigned by an administrator or Guest Ambassador before being allowed on the network

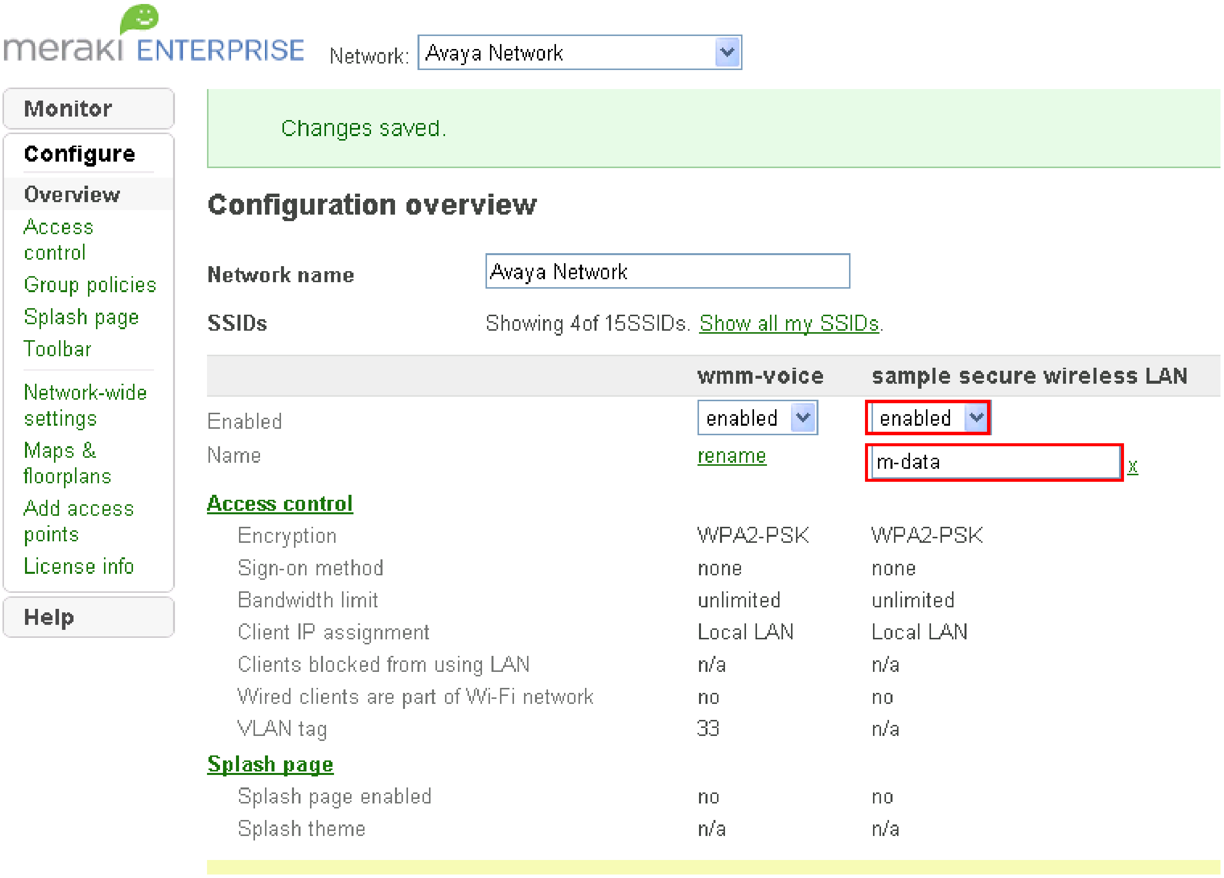
○ Billing (paid access) – Incompatible with WEP, WPA2-PSK, and WPA2-Enterprise
Users choose from various pay-for-access options, or an optional free tier

Bandwidth limit ✻ unlimited details ☐ Enable SpeedBurst ✻

Step	
3.	Under **Addressing and traffic**, select the **Bridge mode: Make clients part of the LAN** radio button. Under **VLAN setup,** select **Use VLAN tagging** from the **VLAN tagging** drop-down list and enter the VLAN ID for the voice network. For compliance testing 33 was used. Select **Save Changes** to continue.  **Addressing and traffic** Client IP assignment ○ NAT mode: Use Meraki DHCP Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the SSID firewall settings permit (see "Firewall," below). ● Bridge mode: Make clients part of the LAN Meraki devices operate transparently (no NAT or DHCP). Clients receive DHCP leases from the LAN or use static IPs. Use this for shared printers, file sharing, and wireless cameras. Firewall: Allow wireless clients to access my LAN Content filtering (NAT mode only): Don't filter content **VLAN setup** VLAN tagging (Bridge mode only): Use VLAN tagging VLAN ID: 33 **Wireless options** SSID visibility: Show this SSID Band selection ● Dual band operation (2.4 GHz and 5 GHz) ○ 5 GHz band only 5 GHz has more capacity and less interference than 2.4 GHz, but legacy clients are not capable of using it. ○ Dual band operation with Band Steering Band Steering detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients. Legacy 11b operation: Enable legacy 11b bitrates (1, 2, & 5.5 Mbps) Save Changes or cancel. (Please allow 1-2 minutes for changes to take effect.)

5.3. Create and Configure the SSID for the Data Network

It is assumed VLAN trunking is enabled on the ports of the Ethernet switch that is connected to each Meraki Access Point, and that the VLANs assigned in this section are assigned

Step	
1.	From the left configuration tree, select **Configure → Overview.** Select **rename** (not shown), under the SSID, **sample secure wireless LAN,** change the name to **m-data**. Select **Save Changes** at the bottom of the page, (not show), to continue. 

Network: Avaya Network

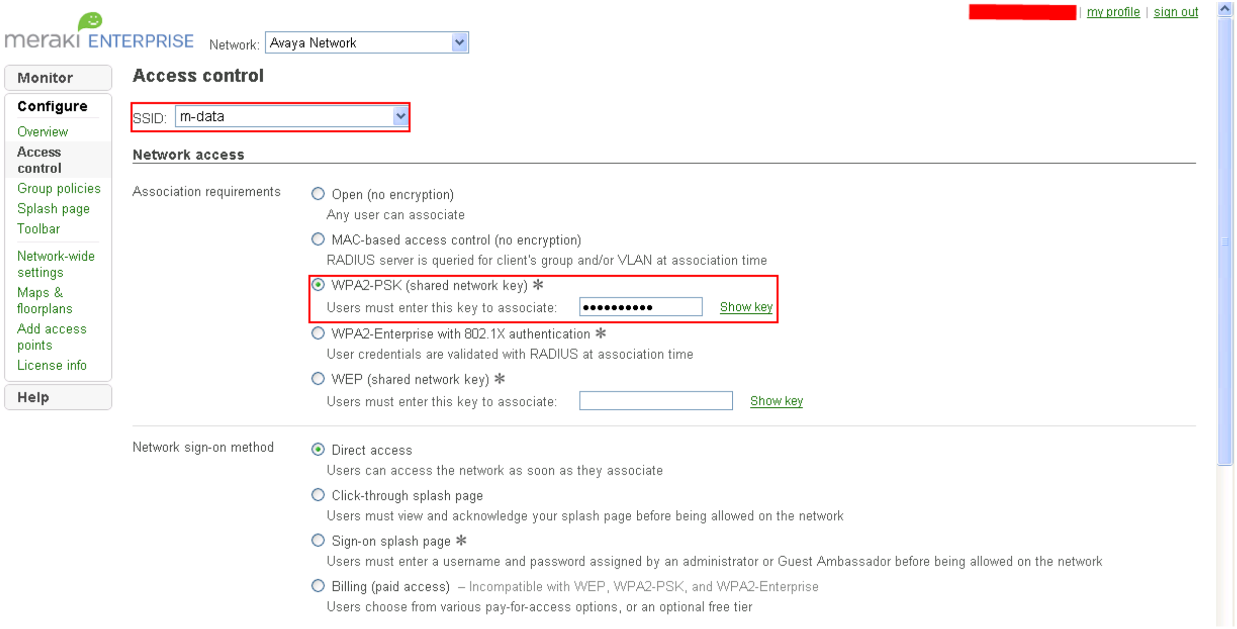
Changes saved.

Configuration overview

Network name Avaya Network

SSIDs Showing 4of 15SSIDs. Show all my SSIDs.

	wmm-voice	**sample secure wireless LAN**
Enabled	enabled	enabled
Name	rename	m-data x
Access control		
Encryption	WPA2-PSK	WPA2-PSK
Sign-on method	none	none
Bandwidth limit	unlimited	unlimited
Client IP assignment	Local LAN	Local LAN
Clients blocked from using LAN	n/a	n/a
Wired clients are part of Wi-Fi network	no	no
VLAN tag	33	n/a
Splash page		
Splash page enabled	no	no
Splash theme	n/a	n/a

Step	
2.	From the left configuration tree, select **Configure → Access control.** Under **Access control**, select **m-data** from the **SSID** drop-down list. Under **Network access,** select the radio button for **WPA2-PSK (shared network key)** and enter a unique key. Scroll down to **Addressing and traffic** to continue. 

[redacted] | my profile | sign out

meraki ENTERPRISE Network: Avaya Network

Access control

SSID: m-data

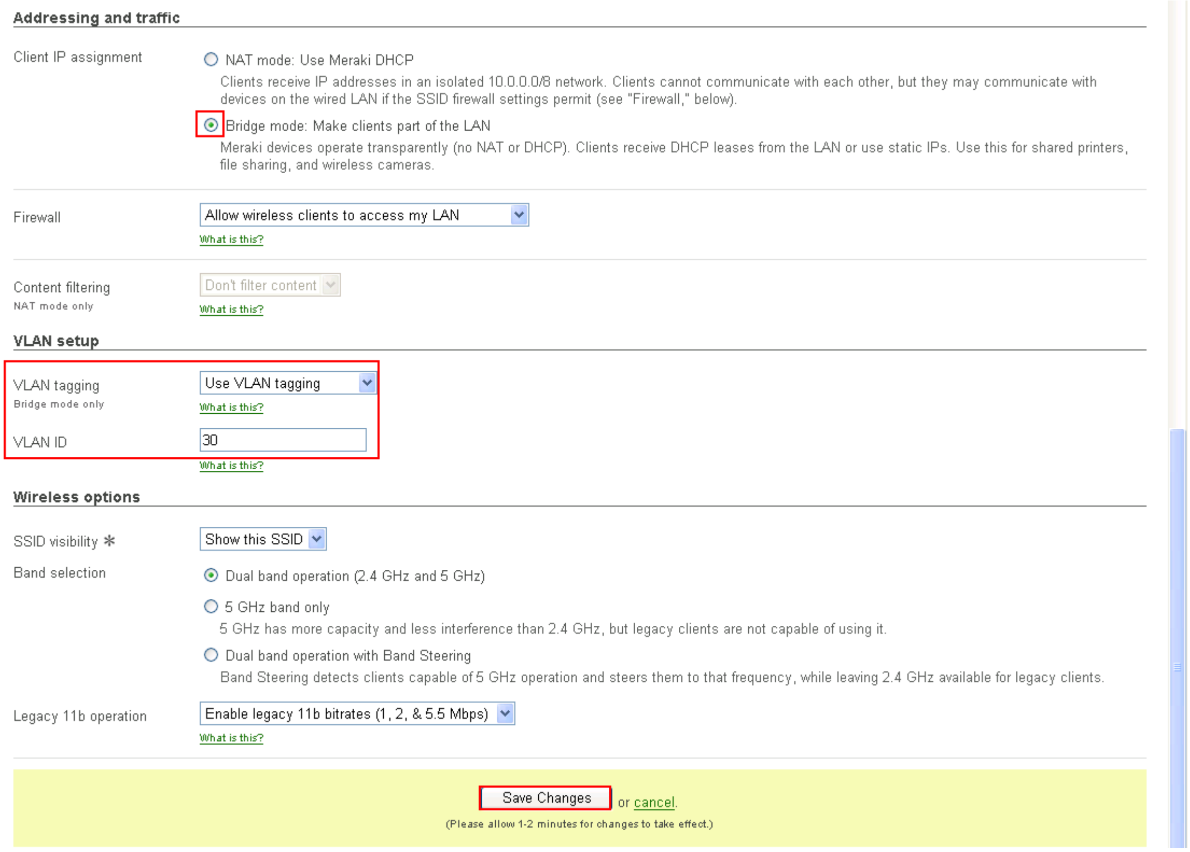
Network access

Association requirements
- ○ Open (no encryption)
  Any user can associate
- ○ MAC-based access control (no encryption)
  RADIUS server is queried for client's group and/or VLAN at association time
- ● WPA2-PSK (shared network key) ✻
  Users must enter this key to associate: •••••••••• Show key
- ○ WPA2-Enterprise with 802.1X authentication ✻
  User credentials are validated with RADIUS at association time
- ○ WEP (shared network key) ✻
  Users must enter this key to associate: Show key

Network sign-on method
- ● Direct access
  Users can access the network as soon as they associate
- ○ Click-through splash page
  Users must view and acknowledge your splash page before being allowed on the network
- ○ Sign-on splash page ✻
  Users must enter a username and password assigned by an administrator or Guest Ambassador before being allowed on the network
- ○ Billing (paid access) – Incompatible with WEP, WPA2-PSK, and WPA2-Enterprise
  Users choose from various pay-for-access options, or an optional free tier

Step

3. Under **Addressing and traffic**, select the **Bridge mode: Make clients part of the LAN** radio button. Under **VLAN setup,** select **Use VLAN tagging** from the **VLAN tagging** drop-down list and enter the VLAN ID for the data network. For compliance testing 30 was used. Select **Save Changes** to continue.



Addressing and traffic

Client IP assignment

○ NAT mode: Use Meraki DHCP

Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the SSID firewall settings permit (see "Firewall," below).

● Bridge mode: Make clients part of the LAN

Meraki devices operate transparently (no NAT or DHCP). Clients receive DHCP leases from the LAN or use static IPs. Use this for shared printers, file sharing, and wireless cameras.

Firewall: Allow wireless clients to access my LAN

Content filtering (NAT mode only): Don't filter content

VLAN setup

VLAN tagging (Bridge mode only): Use VLAN tagging

VLAN ID: 30

Wireless options

SSID visibility ✻: Show this SSID

Band selection

● Dual band operation (2.4 GHz and 5 GHz)

○ 5 GHz band only

5 GHz has more capacity and less interference than 2.4 GHz, but legacy clients are not capable of using it.

○ Dual band operation with Band Steering

Band Steering detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients.

Legacy 11b operation: Enable legacy 11b bitrates (1, 2, & 5.5 Mbps)

(Please allow 1-2 minutes for changes to take effect.)

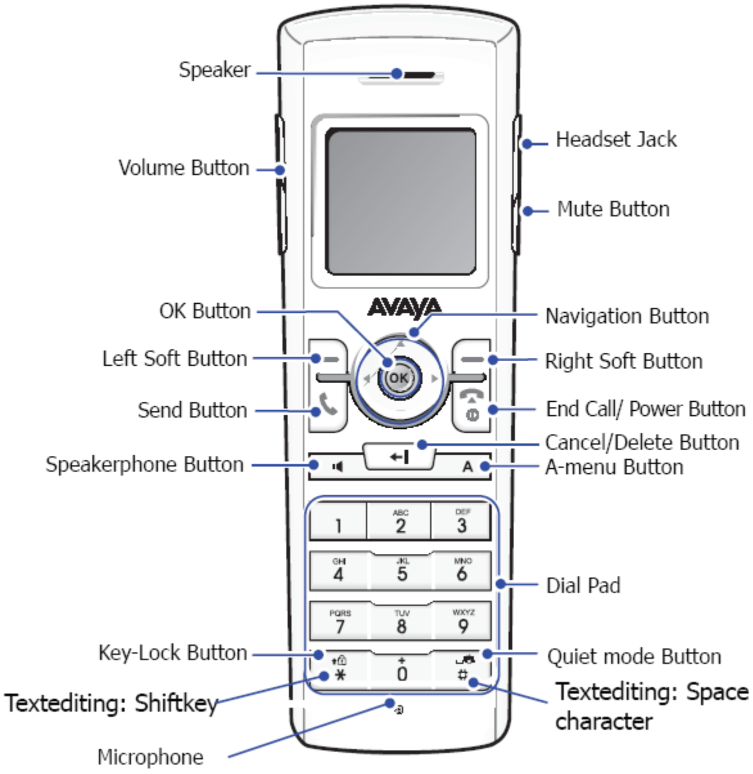
5.4. Configure the Meraki MR14 Access Points

It is assumed VLAN trunking is enabled on the ports of the Ethernet switch that is connected to the each Meraki Access Point, and that the VLANs assigned in this section are assigned.

Step	Assigning IP Addresses to MR14s
1.	All gateway MR14s (MR14s with Ethernet connections to the LAN) must be assigned routable IP addresses. These IP addresses can be dynamically assigned via DHCP or statically assigned. For compliance testing, Static Assignment was used. Static Assignment Static IPs are assigned using the local web server on each AP. The following procedure describes how to set the static IP: 1. Using a client machine (e.g. a laptop), connect to the AP wirelessly by associating to any SSID broadcast by the AP. 2. Using a web browser on the client machine, access the AP's built-in web server by browsing to http://my.meraki.com. Alternatively, browse to http://10.128.128.128. 3. Click on the "Static IP Configuration" tab. Log in. The default user name is "admin". The default password is the AP's serial number, with hyphens included (e.g. Q2BD-551C-ZYW3). 4. Configure the static IP address, net mask, gateway IP address and DNS servers that this AP will use on its wired connection. For most networks, the AP's will be behind a firewall. Policies on the firewall must allow outgoing connections on particular ports to particular IP addresses in order for the MR14 to be able to seamlessly communicate with the Cloud Controller. The most current list of outbound ports and IP addresses can be found here: http://tinyurl.com/y79une3.

6. Configure Avaya 3631 Wireless IP Telephone

The following steps detail the configuration process for the Avaya 3631 Wireless IP Telephone. For complete details on all the supported features on the Avaya 3631 Wireless IP Telephone refer **Section 10 [4].**



6.1. 46xxsettings File Options

The 46xxsettings.txt file is used to specify certain system parameters. It is used by all Avaya 1600, 4600 and 9600 IP & SIP Telephones. The 46xxsettings.txt file can be delivered to the Avaya 3631 Wireless IP Telephone through either of the following two methods:

- Automatically over-the-air from an HTTP server. The file is delivered whenever the Avaya 3631 Wireless IP Telephone is restarted.

- Manually via a USB cable connected between the Avaya 3631 Wireless IP Telephone and a PC

For this compliance test, the 46xxsetting file was delivered manually via a USB cable connected between the Avaya 3631 Wireless IP Telephone and a PC. For more information on configuring 46xxsetting options refer to **Section 10 [4].**

For this example, the ESSID is **wmm-voice, Encryption** type **is WPA2-PSK** as created in **Section 5.2.** Add the following information to the 46xxsetting setting file.

```
SET WTPROF1      " wmm-voice"
SET WTSSIDP1     " wmm-voice "
SET DNSSRVRP1    "10.32.100.250"
SET DOMAIN       "dev4.com"
SET WTSECP1      "3"
SET ENCRYPTP1    "4"
SET WTWMMP1      "1"
SET WTKEYP1      "test123123"
```

6.2. Downloading 46xxsettings File via USB Cable

Only a Samsung cable with an 18-pin connector can be used to support USB operations on the Avaya 3631 Wireless IP Telephone. This cable is orderable through Avaya. This cable works with the standard Windows USB driver; it is not necessary to install a special USB driver to use this cable.

Use the following procedure to download the 46xxsettings.txt file to the phone via a USB cable.

1. On the Avaya 3631 Wireless IP Telephone, access the **Advanced Settings** menu, select the **Admin access mode** and specify the Admin password.

2. From the **Advanced** menu, select the **Service** sub-menu.

3. From the **Service** menu, select **Backup & Restore over USB.**

4. From the **Backup & Restore …** menu, select **Download settings file.**
    - The "Starting USB driver …" status message is displayed

5. When prompted, insert (or remove and re-insert) the USB cable into its connector on the bottom of the phone.
    - A confirmation window appears, with instructions on copying files.

6. From the Windows PC, drag and drop the **46xxsettings.txt** file onto the USB drive folder associated with the phone.

7. Once the file has been copied to the USB drive, return to the phone and select the **Done** softkey.
    - The phone displays a "Downloading file…" status message

8. When the phone displays a "Completed" message, press the **Back** softkey.
    - The phone displays a Confirmation window for restarting the phone.

6.3. Downloading Digital Certificates via USB Cable

The Certificate for the Avaya 3631 Wireless IP Telephone is in the PEM format. Certificate filenames are fixed. The fixed filenames are keyed to the phone Access Profile with which the certificate is associated. So, **cacert1.pem** is filename for certificate used with first Access Profile. To use the certificate with Access Profile 2 or 3, the user must change the filename accordingly.

Only a Samsung cable with an 18-pin connector can be used to support USB operations on the Avaya 3631 Wireless IP Telephone. This cable is orderable through Avaya. This cable works with the standard Windows USB driver; it is not necessary to install a special USB driver to use this cable.

Use the following procedure to download digital certificates to the phone via a USB cable.

1. On the Avaya 3631 Wireless IP Telephone, access the **Advanced Settings** menu, select the **Admin access mode** and specify the Admin password.

2. From the **Advanced** menu, select the **Service** sub-menu.

3. From the Service menu, select **Backup & Restore over USB**

4. From the **Backup & Restore** … menu, select **Download settings file**
    - The "Starting USB driver …" status message is displayed

5. When prompted, insert (or remove and re-insert) the USB cable into its connector on the bottom of the phone.
    - A confirmation window appears, with instructions on copying files.

6. From the Windows PC, drag and drop the **certificate file**(s) onto the USB drive folder associated with the phone.

7. Once the file(s) have been copied to the USB drive, return to the phone and select the Done softkey.
    - The phone displays a "Downloading file…" status message

8. When the phone displays a "Completed" message, press the **Back** softkey.

6.4. Configure DHCP

The Avaya 3631 Wireless IP Telephone supports DHCP for IP address assignment and configuration of other telephone parameters.

The Avaya 3631 Wireless IP Telephone supports Site-Specific Option Numbers (SSON) 242 and 176. The default is 242. Note that this parameter can be changed only through the phone's menu interface.

This section describes how to configure the Vendor Class Identifier Code (option 242) on a Microsoft Windows-based DHCP server. Since option 242 is not a predefined option on a Windows DHCP server, add it to the option list for the server. To configure option 242 on the Windows DHCP server:

Configuring DHCP Option 242

On the DHCP server, open the **DHCP server administration** tool by clicking **Start → Administration Tools → DHCP**.

1. Find the DHCP server and right-click on the server name. Select **Set Predefined Options**.
2. In the Predefined Options and Values dialog box, click the **Add** button.
3. In the Option Type dialog box, enter the following information:

    - **Name = 242**
    - **Data type = String**
    - **Code = 242**

4. Click the **OK** button to save this information.
5. Add the following **String** under **Value**:

MCIPADD=10.32.100.1,MCPORT=1719,HTTPSRVR=10.32.100.250

7. General Test Approach and Test Results

All feature functionality test cases were performed manually. The general test approach entailed verifying the following:

- Registration, re-registration of Avaya 3631 Wireless IP Telephone with Avaya Aura™ Communication Manager through the Meraki's Cloud Managed Enterprise WLAN solution.
- Verify Message Waiting Indicator and message retrieval from Avaya Aura™ Communication Manager Messaging.
- VoIP calls between the Avaya 3631 Wireless IP Telephones and the wired Avaya Digital/SIP/H.323 Telephones.
- Validated G.711MU and G.729A codecs, shuffling, conferencing, Transfer, Hold/Return from hold, Forwarding, Call Park, Call Pickup, Bridged extension, voicemail, DTMF while traversing the Meraki's Cloud Managed Enterprise WLAN solution.
- Wireless Roaming, Wireless Security, Wireless Authentication and Wireless Quality of Service.
- Verified that QoS directed the voice signaling and voice media to the higher priority queue based on WMM QoS.
- Validate QoS queues by making and receiving wireless calls while sending a heavy load of low priority data traffic and verifying that good voice quality was achieved.

All feature functionality, serviceability, and QoS performance test cases passed. The Avaya 3631 Wireless IP Telephones successfully registered with Avaya Aura™ Communication Manager utilizing the Meraki's Cloud Managed Enterprise WLAN solution. The Avaya Wireless 3631 IP Telephones were verified to roam successfully between access points and yielded good voice quality and no calls were lost. Compliance testing also focused on verifying Quality of Service for voice traffic while low priority background traffic was competing for bandwidth. The stability of the Avaya/Meraki solution was successfully verified through QoS performance and serviceability testing.

8. Verification Steps

This section provides the verification steps that may be performed to verify that the wireless IP endpoints have connectivity to the network and that good voice quality is being provided on wireless calls.

- Check that the Avaya 3631 Wireless IP Telephones have successfully registered with Communication Manager by typing the **list registered-ip-station** command on the SAT in Communication Manager.
- Ensure that the **SSID** value of the wireless network matches the **SSID** field value configured in **Section 6.1,** on the Avaya 3631 Wireless IP Telephones.
- Place calls from the Avaya 3631 Wireless IP Telephones and verify two-way audio.
- Place a call to the Avaya 3631 Wireless IP Telephones, allow the call to be directed to voicemail, leave a voicemail message and verify the MWI light is turned on.
- Using the Avaya 3631 Wireless IP Telephone that received the voicemail, connect to the voicemail system to retrieve the voicemail and verify the MWI light is turned off.
- Place calls to the Avaya 3631 Wireless IP Telephones and exercise calling features such as transfer, conference and hold.

9. Conclusion

These Application Notes illustrate the procedures necessary for configuring the Meraki's Cloud Managed Enterprise WLAN solution managing multiple Meraki MR14 Access Points with an Avaya Aura™ telephony infrastructure. The Meraki's Cloud Managed Enterprise WLAN solution managing multiple Meraki MR14 Access Points was successfully compliance-tested in a wireless converged voice and data network configuration. All feature functionality test cases described in **Section 1.1** passed.

10. Additional References

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Installing and Configuring Avaya Aura™ Session Manager, Doc ID 03-603473 Release 6, October, 2010*

[2] *Administering Avaya Aura™ Session Manager, Doc ID 03-603324, Release 6.0, August, 2010*

[3] *Installing and Configuring Avaya Aura™ Communication Manager, Doc ID 03-603558, Release 6.0 September, 2010*

[4] *Avaya one-X™ Deskphone SIP for 9600 Series IP Telephones Administrator Guide Release 2.6, Doc ID 16-601944, June, 2010*

[5] *Avaya one-X™ Deskphone H.323 Administrator Guide, Doc ID 16-300698, Release 6.0, August, 2010*

[6] *3631 Wireless Telephone Administrator Guide, Doc ID 16-602203, March, 2007*

The Meraki product documentation can be found at:
http://meraki.com/support/documentation/#setup_guides

[7] *Meraki Cloud Controller Product Manual, Design and Configuration Guide for Wireless Networks Using the Meraki Cloud Controller, June 2010*

[8] *Meraki MR11/14 Hardware Installation Guide*

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.