Avaya Solution & Interoperability Test Lab

Application Notes for a Motorola Wireless Solution consisting of the Motorola RFS Series RF Switch and Motorola AP300 Access Points with an Avaya Aura™ Telephony Infrastructure in a Converged VoIP and Data Network - Issue 1.0

Abstract

These Application Notes describe the configuration of a wireless Voice over IP (VoIP) solution consisting of Motorola RFS Series RF Switch managing multiple Motorola AP300 Access Points with an Avaya Aura™ telephony infrastructure. Emphasis of the testing was placed on verifying prioritization of VoIP Wireless traffic on calls associated with the Avaya 3631 wireless IP telephones.

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 consisting of a Motorola RFS Series Switch managing multiple Motorola AP300 Access Points with an Avaya Aura™ telephony infrastructure consisting of Avaya Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services, Avaya Modular Messaging, 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 Motorola AP300 Access Points and registered with Communication Manager.

1.1. Interoperability Compliance Testing

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

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/Motorola 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

Technical support for Motorola can be obtained through the following:

- Phone: +1 (800) 6535350
- Web support in the form of an online form at http://support.symbol.com

2. Reference Configuration

The network diagram shown in **Figure 1** illustrates the testing environment used for compliance testing. The network consists of Communication Manager running on an Avaya S8300 Server with an Avaya G450 Media Gateway, an Avaya S8500 server running SIP Enablement Services, one Avaya Modular Messaging Application Server, one Avaya Modular Messaging Storage Server, one Avaya 9630 IP Telephone (SIP), one Avaya 9620 IP Telephone (H.323), one Avaya 2420 Digital Telephone, one Motorola RFS4000 RF Switch, and three Motorola AP300 Access Points. One computer is present in the network providing network services such as Radius, DHCP, HTTP, and TFTP.

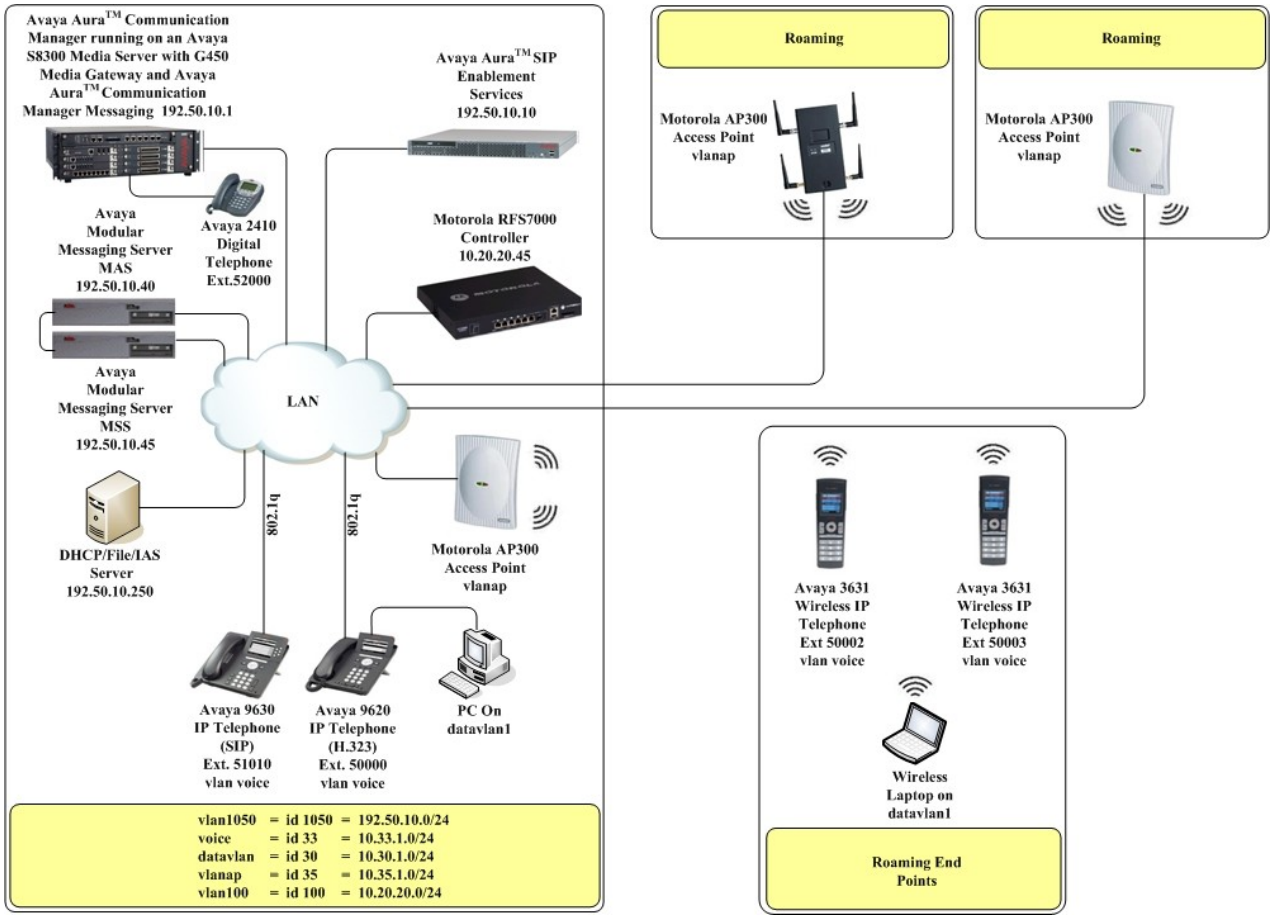


Figure 1: Avaya and Motorola Wireless LAN Configuration

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 5.2.1
Avaya G450 Media Gateway (Corporate Site) MGP MM712 DCP Media Module	 28.22.0 HW9
Avaya Aura™ SIP Enablement Services (SES)	
Avaya Aura™ SIP Enablement Services	5.2.1
Avaya Messaging (Voice Mail) Products	
Avaya Modular Messaging - Messaging Application Server (MAS)	5.0
Avaya Modular Messaging - Message Storage Server (MSS)	5.0
Avaya Aura™ Communication Manager Messaging (CMM)	5.2.1-13.0
Avaya Telephony Sets	
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone Edition 3.0.1
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone SIP 2.4
Avaya 3631 Wireless Telephone	1.5.08
Avaya 2410 Digital Telephone	5.0
Motorola Products	
Motorola RFS4000 RF Switch	4.1.0.0-042R
Motorola AP300 Access Point	4.1.0.0-042R
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 for wired IP Telephones

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**.

1. 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
```

2. On **Page 3,** add the following options for **des rgn**:

- **codec** set set to **1**

Note: **direct WAN**, **Units** and **IGAR** will propagate automatically.

```
change ip-network-region 1                                      Page   3 of  19

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    s
 1    1                                                               all
 2
 3    1     y    NoLimit                                            n
```

4.2. Configure the ip-network-region for the Wireless IP Telephones

The Differentiated Services Code Point (DSCP) value of 52 will be used for both PHB values. DSCP 52 represents the traffic class of premium and the traffic type voice. Set the **Call Control PHB Value** to **52** and the **Audio PHB Value** to **52**. **Call Control 802.1p Priority** and **Audio 802.1p Priority** are set to **6**.

1. From the SAT, use the **change ip-network-region 3** command to change the DIFFSERV/TOS PARAMETERS and 802.1P/Q PARAMETERS settings. Change the following:

- **Call Control PHB Value** set to **52**
- **Audio PHB Value** set to **52**
- **Call Control 802.1p Priority** set to **6**
- **Audio 802.1p Priority** set to **6**

```
change ip-network-region 3                                      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: 52      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 52       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
```

4.3. Configure the wireless Avaya IP Telephones to use ip-network-region 3

The Avaya 3631 Wireless IP Telephones use Wi-Fi Multimedia (WMM), for Quality of Service. WMM puts DSCP value 46 in the video queue and needs to be changed to 52 so the traffic is placed in the voice queue. This step is needed to assign the Avaya 3631 Wireless IP Telephones to use the ip-network-region 3 and DSCP value 52, configured in **Section 4.2 Step 1**.

Step	Description
1.	From the SAT, use the **change ip-network map** command to add the IP address of the Avaya 3631 Wireless IP Telephones individually or the subnet of where all of the Avaya 3631 Wireless IP Telephones reside. For compliance each Avaya 3631 Wireless IP Telephone was entered individually. • **FROM:** set to **IP address of the** Avaya 3631 Wireless IP Telephone • **TO:** set to **IP address of the** Avaya 3631 Wireless IP Telephone • **Subnet Bits:** set to **32** • **Network Region:** set to **3**

```
change ip-network-map                                          Page   1 of  63
                              IP ADDRESS MAPPING

                                                   Subnet Network     Emergency
 IP Address                                        Bits   Region VLAN Location Ext
 ------------------------------------------------ ------ ------ ---- -------------
 FROM: 10.33.1.131                                 /32    3      n
   TO: 10.33.1.131
 FROM: 10.33.1.132                                 /32    3      n
   TO: 10.33.1.132
```

5. Configure Motorola RFS4000 RF Switch and Motorola AP300 Access Points

The following steps detail the initial configuration for the Motorola Mobility Solution used for the compliance testing. Layer2 roaming was compliance tested. These Application Notes will cover Layer2.

The initial configuration on the Motorola RFS4000 RF Switch, i.e. assign management IP address, vlan, etc. was administered via the command line interface. The rest was administered via the web configuration tool. Except where stated, the parameters in all steps are the default settings and are supplied for reference. For more information on configuring Motorola RFS4000 RF Switch and Motorola AP300 Access points, please refer to **Section 10, [9]** and **[10].**

5.1. Motorola RFS4000 RF Switch (CLI)

Configure Motorola RFS4000 RF Switch as depicted in **Figure 1**.

To perform the initial configuration on the Motorola RFS4000 RF Switch, setup a serial connection from a PC. Setup a terminal session with the following parameters:

Bits per second	**"19200"**
Data Bits	**"8"**
Parity	**"None"**
Stop bits	**"1"**
Flow control	**"None"**

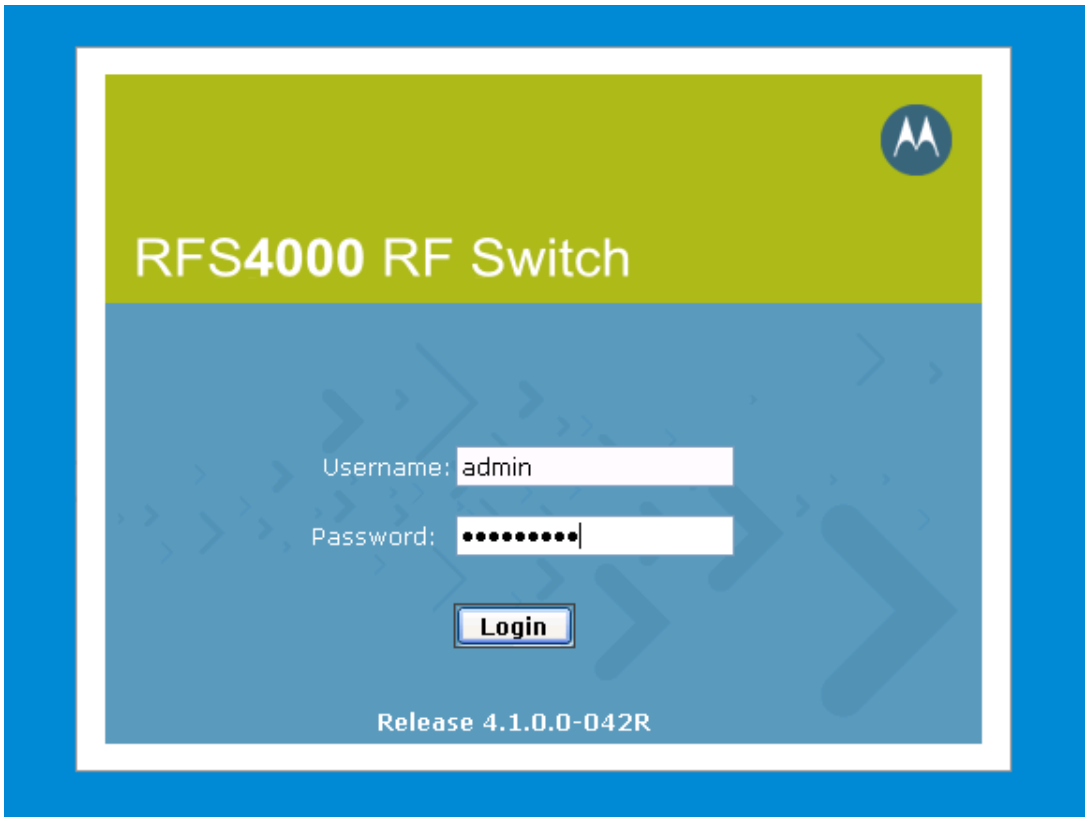
Log in to the Motorola RFS4000 RF Switch using default credentials which can be obtained from **Section 10, [10]**. Add the following information typed in **BOLD:**

RFS4000 login:
RFS4000 login: **cli**

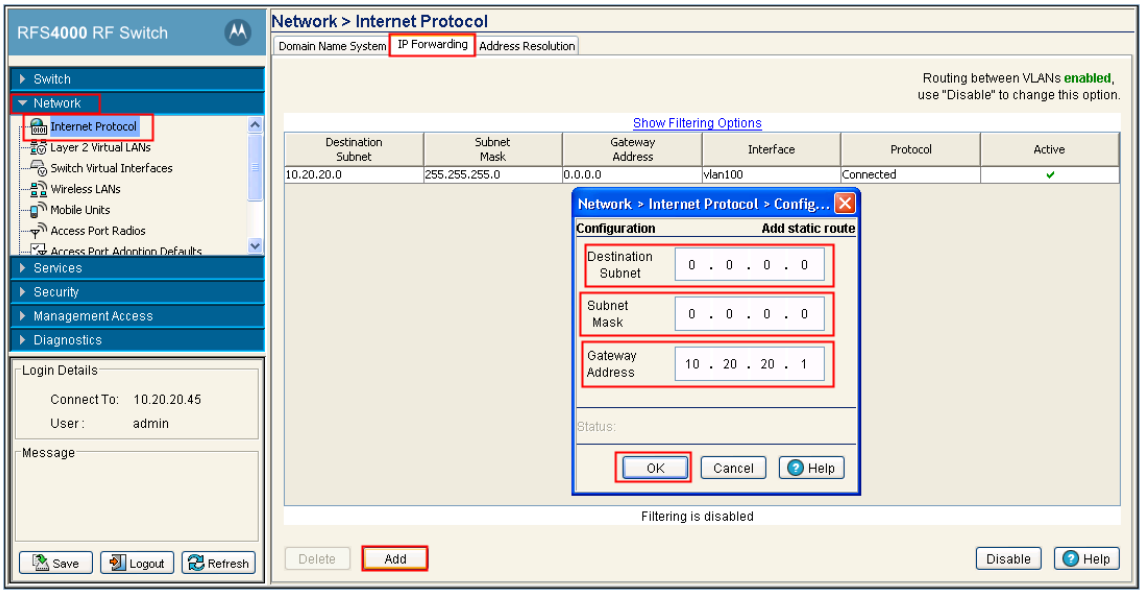
User Access Verification

Username: **admin**
Password: **XXXXXXX**
Welcome to CLI
RFS4000>**enable**
RFS4000#**config terminal**
Enter configuration commands, one per line. End with CNTL/Z.
RFS4000(config)#**interface vlan100**
RFS4000(config-if)#**management**
RFS4000(config-if)#**ip address 10.20.20.45/24**
RFS4000(config-if)#**exit**
RFS4000(config)#**interface up1**
RFS4000(config-if)# **switchport mode trunk**
RFS4000(config-if)# **switchport trunk native vlan 100**
RFS4000(config-if)# **switchport trunk allowed vlan none**
RFS4000(config-if)#**switchport trunk allowed vlan add 100**
RFS4000(config-if)#**exit**
RFS4000(config)# **no ip dhcp pool Default**
RFS4000(config)#**interface vlan 1**
RFS4000(config-if)#**no ip address 192.168.0.1/24**
RFS4000(config-if)#**no ip nat inside**
RFS4000(config-if)#**exit**
RFS4000(config)#**write memory**

5.2. Configure Motorola RFS4000 RF Switch (Web)

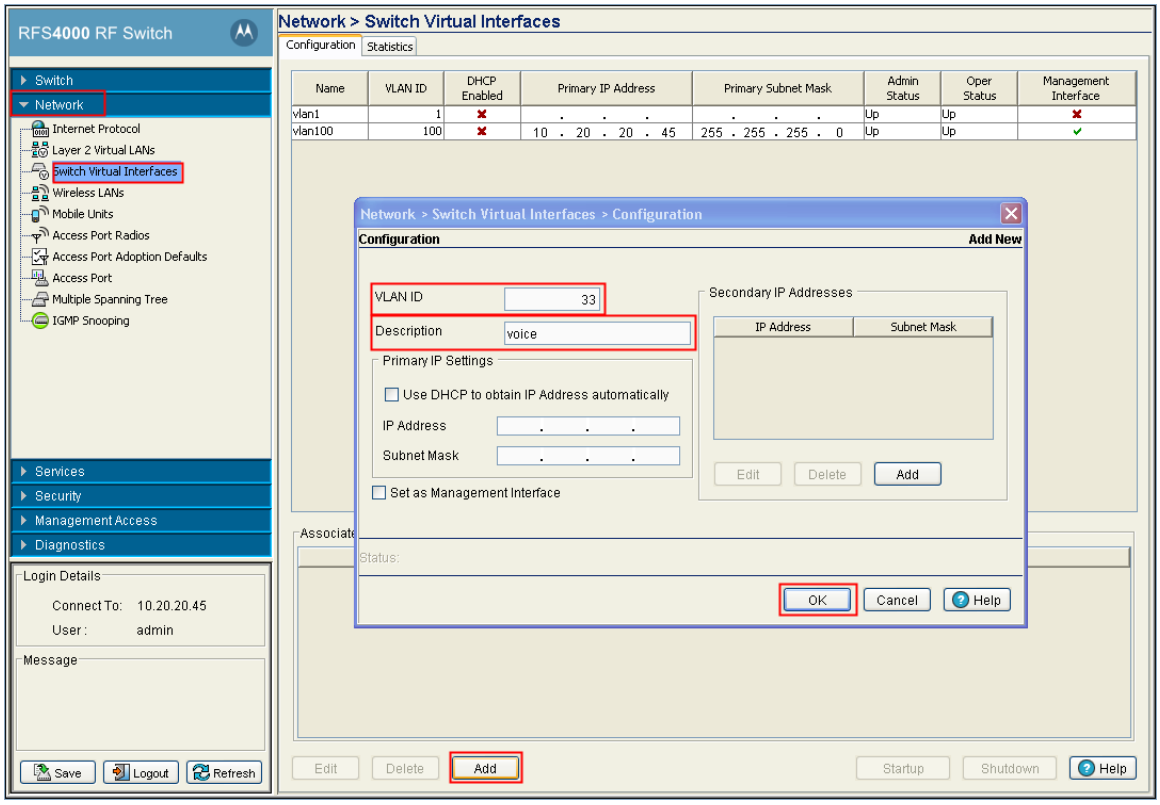
Step	
1.	Configure the Motorola RFS4000 RF Switch using the built-in web-based **Management Tool.** Access this tool by establishing a web browser connection to the Motorola RFS4000 RF Switch. For more information on configuring Motorola RFS4000 RF Switch and Motorola AP300 Access points, please refer to **Section 10, [9] & [10].** 1. Connect the LAN port of the computer being used to the LAN port on the Motorola RFS4000 Wireless RF Switch. 2. Start the **Management Tool** as follows: Start your web browser and enter **https://10.20.20.45**. Press Enter. 3. Log in to the Motorola RFS4000 RF Switch using default credentials which can be obtained from the Motorola RFS4000 RF Switch documentation. Note: After logging in, the default Motorola Web page will appear, (NOT shown) and requests the Country information to be set. For compliance testing, **United States – us** was used. This will only need to be set on the first time that the Motorola RFS4000 RF Switch is logged into. **Click Apply.** 

Create the default gateway

Step	
2.	Navigate to **Network → Internet Protocol → IP Forwarding**. Select **Add**. The **Network** > **Internet Protocol > Configuration** box will appear. To create the default gateway, enter **0.0.0.0** for the **Destination Subnet** and **Subnet Mask,** and specify the IP address of the router for **Gateway Address.** Select **OK** to continue. 

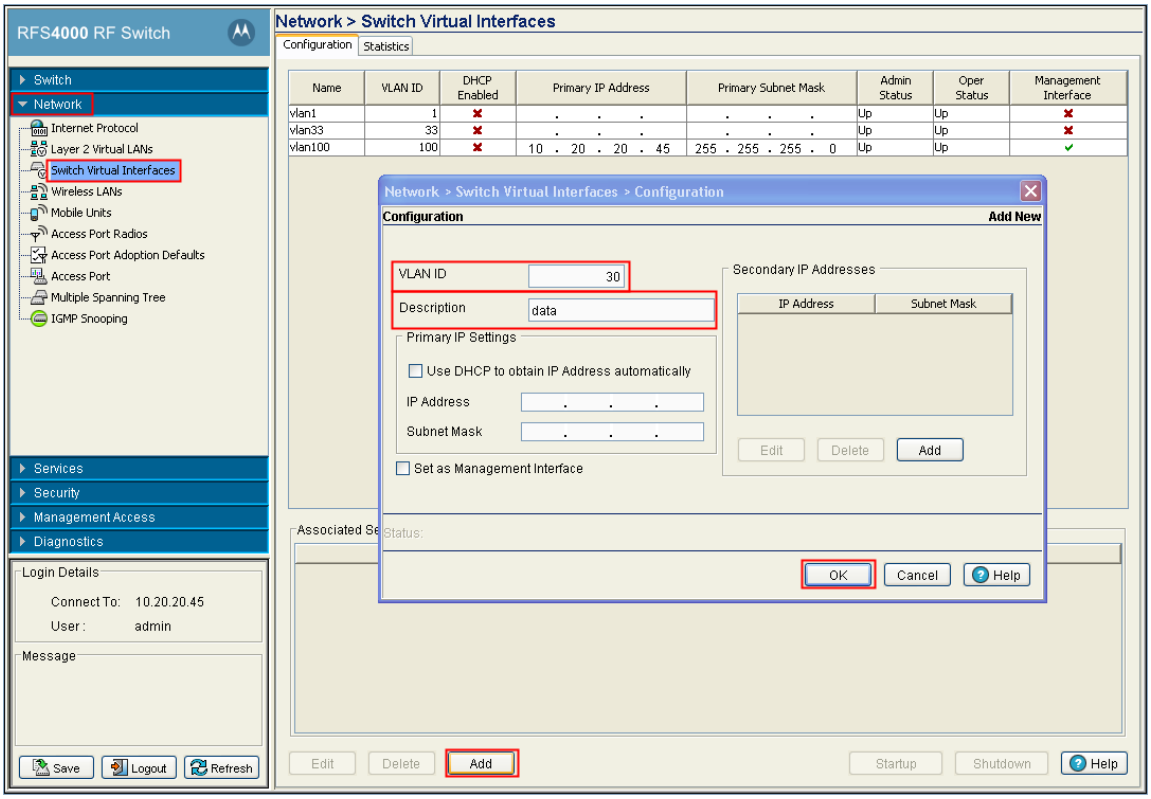
Create a VLAN for the voice network

Step	
3.	Navigate to **Network → Switch Virtual Interfaces → Configuration**. Select **Add**. The **Network** > **Switch Virtual Interfaces > Configuration** box will appear. Enter the **VLAN ID** and **Description** for the **voice VLAN.** Select **OK** to continue.



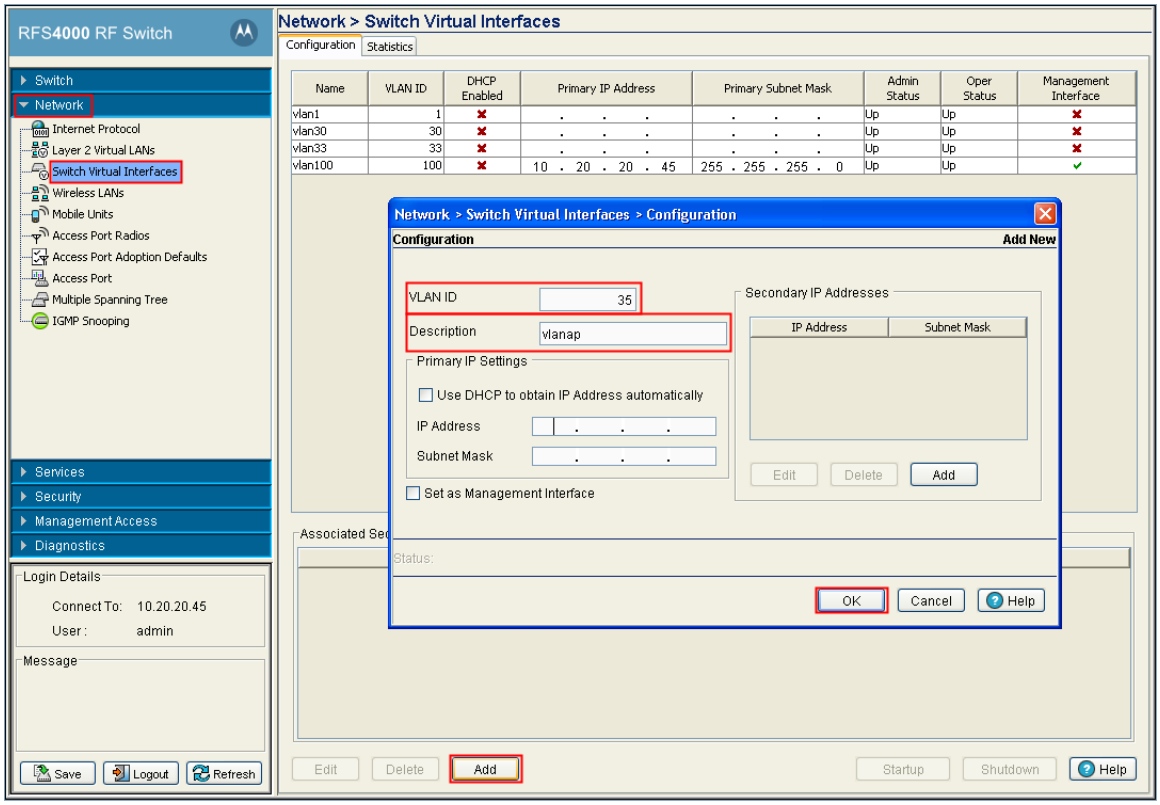
Create a VLAN for the data network

Step	
4.	Navigate to **Network → Switch Virtual Interfaces → Configuration**. Select **Add**. The **Network** > **Switch Virtual Interfaces > Configuration** box will appear. Enter the **VLAN ID** and **Description** for the **data VLAN.** Select **OK** to continue.

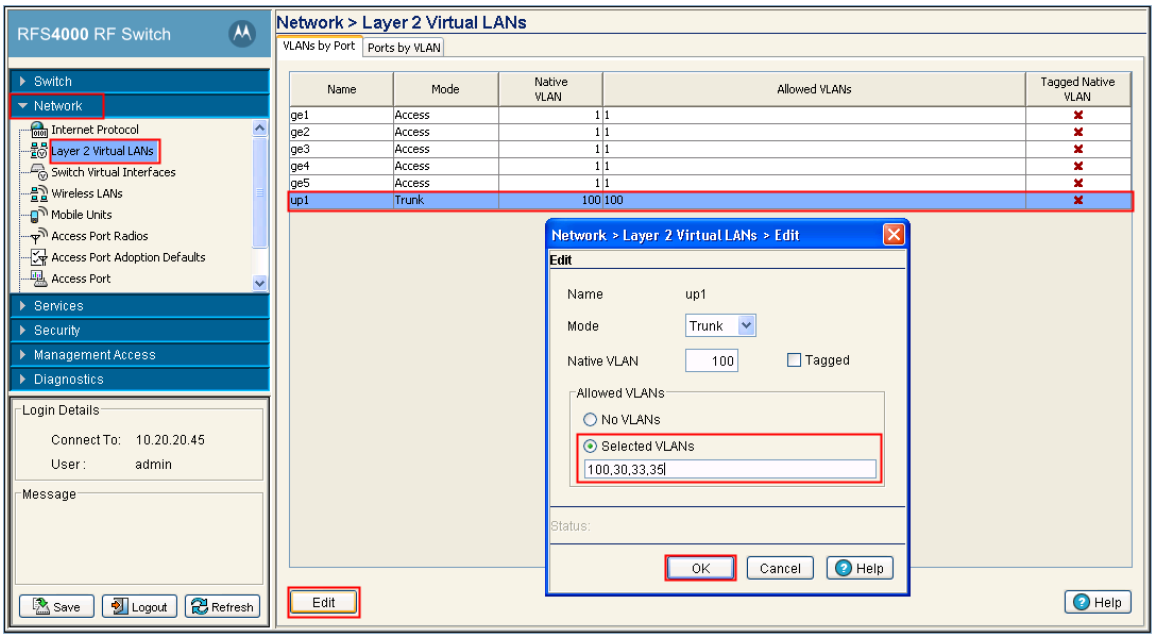


Create a VLAN for the Motorola Access Points

Step	
5.	Navigate to **Network → Switch Virtual Interfaces → Configuration**. Select **Add**. The **Network** > **Switch Virtual Interfaces > Configuration** box will appear. Enter the **VLAN ID** and **Description** for the **AP VLAN.** Select **OK** to continue.



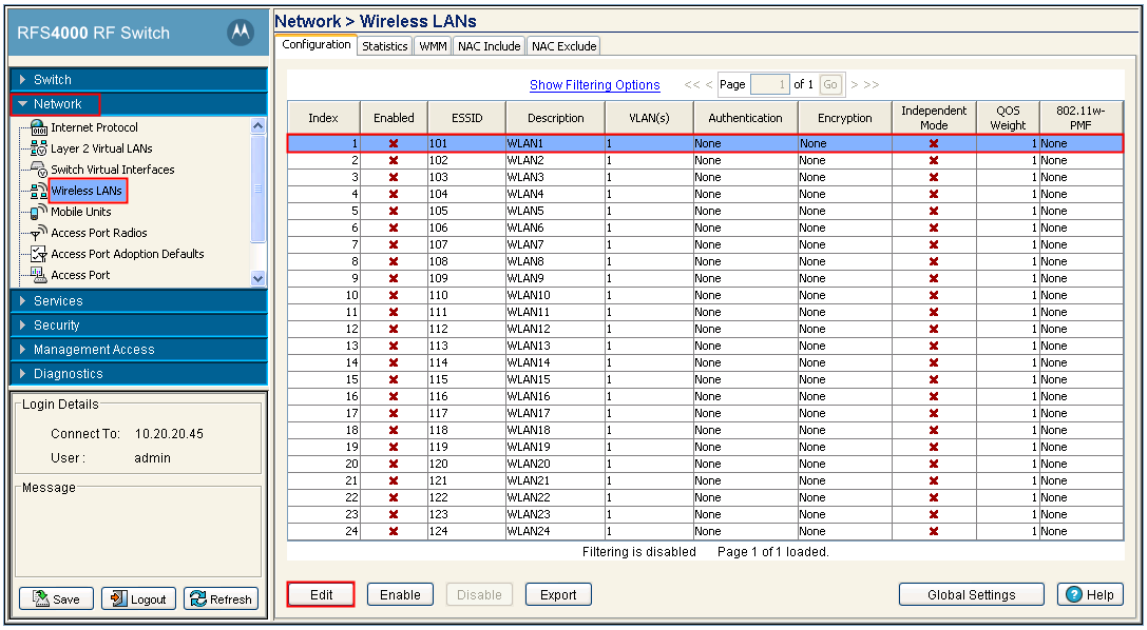
Enable VLAN trunking for the wireless networks. It is assumed VLAN trunking is enabled on the port of the Ethernet switch that is connected to the wireless switch, and that the VLANs created in **Section 5.2 Steps 3** through **5,** are assigned.

Step	
6.	Navigate to **Network → Layer 2 Virtual LANs** and highlight the **up1** interface and click **Edit**. The **Network** > **Layer 2 Virtual LANs > Edit** box will appear. Click the **Selected VLANs** radio button**,** and enter the VLANS created in **Section 5.2 Steps 3** through **5** separated by comas, under **Allowed VLANs.** Select **OK** to continue. 

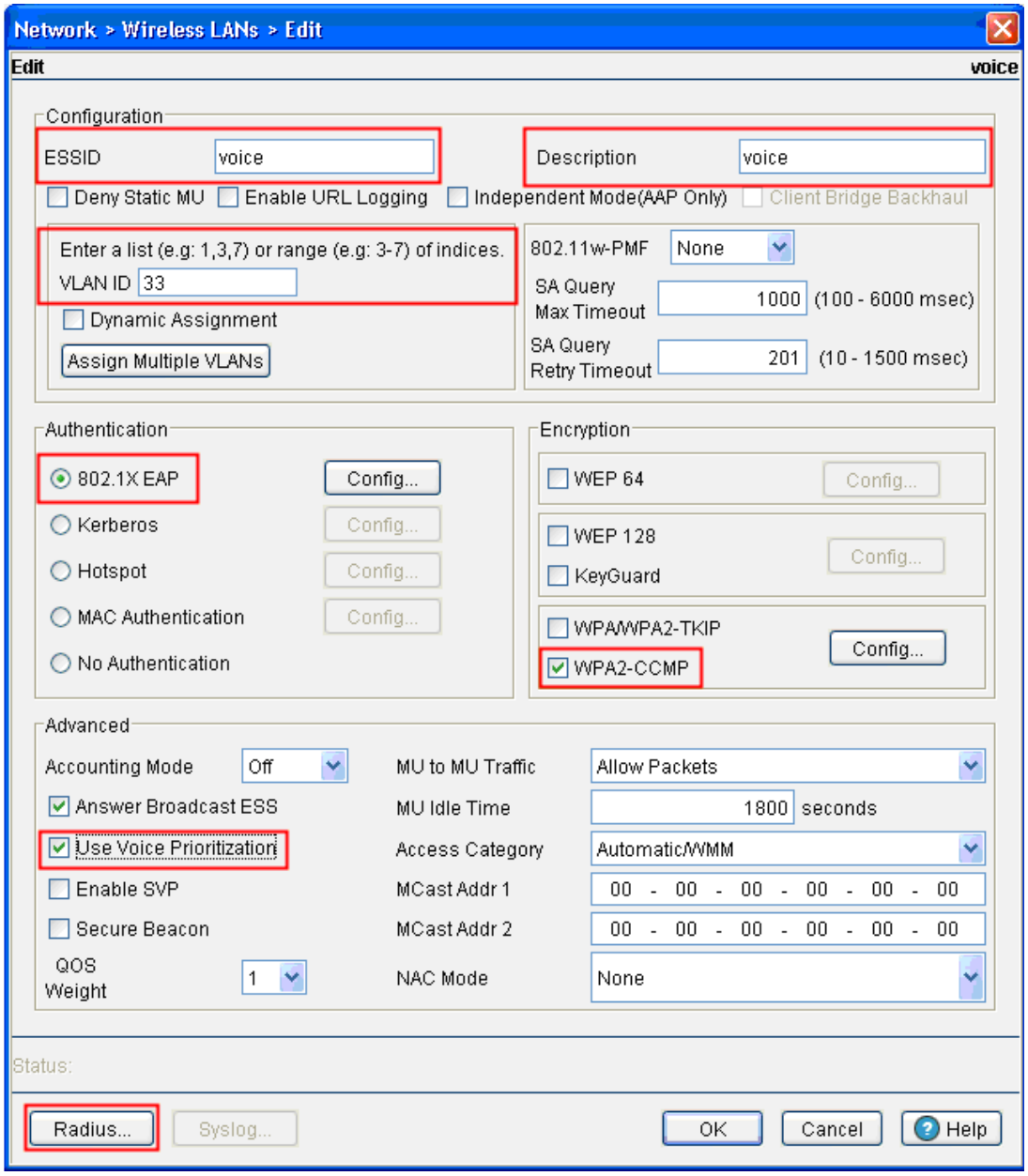
Create ESSIDs for the voice and data networks. Three different security schemas were tested for the voice wireless traffic - Clear, WPA2-PSK CCMP and WPA2 CCMP with 802.1x authentication. Administration of the Clear and WPA2 CCMP ESSIDs will not be covered in these Application Notes.

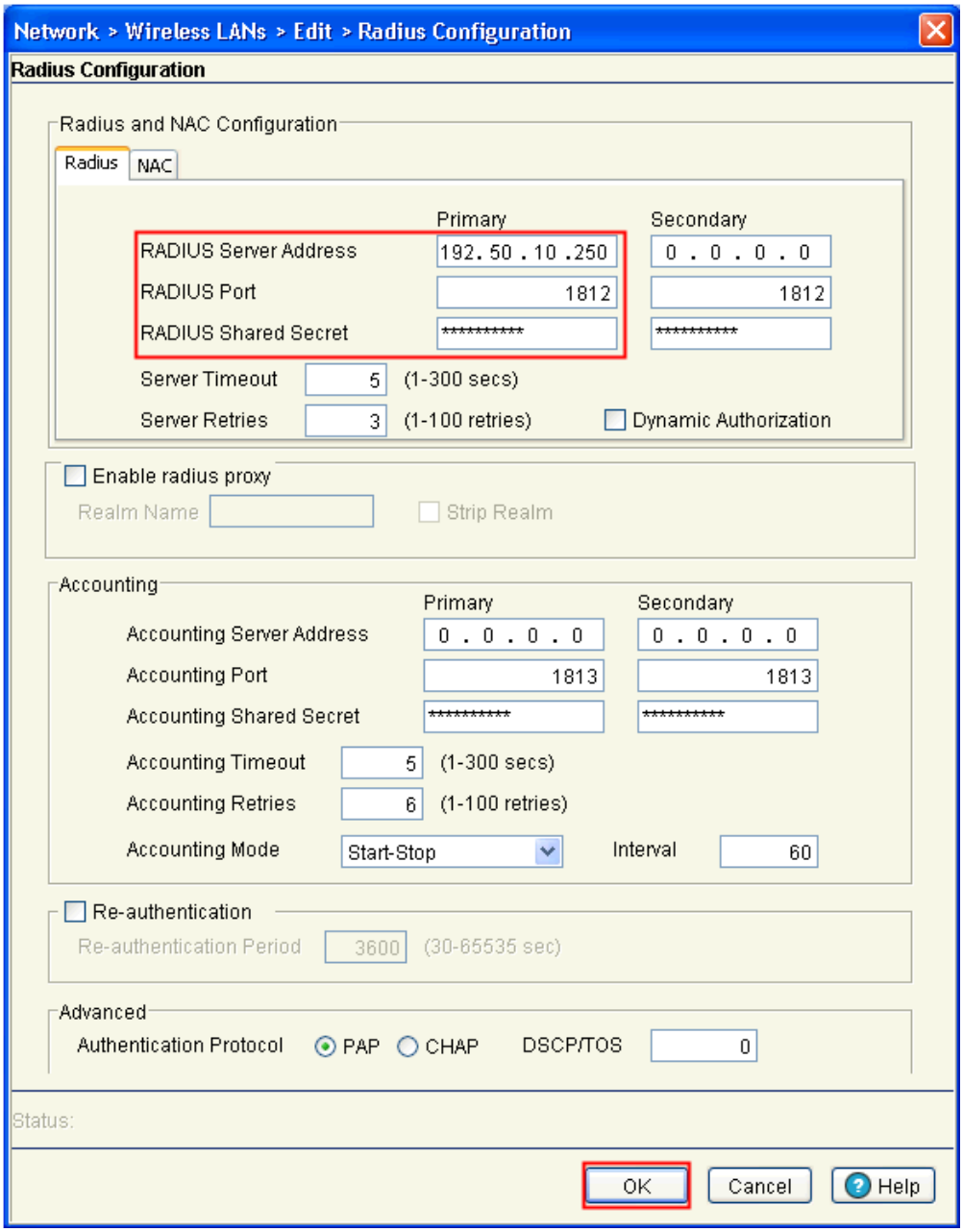
Create the voice ESSID

Step	
7.	Navigate to **Network → Wireless LANs → Configuration.** Highlight an unused ESSID (e.g., **101)** and click **Edit**.



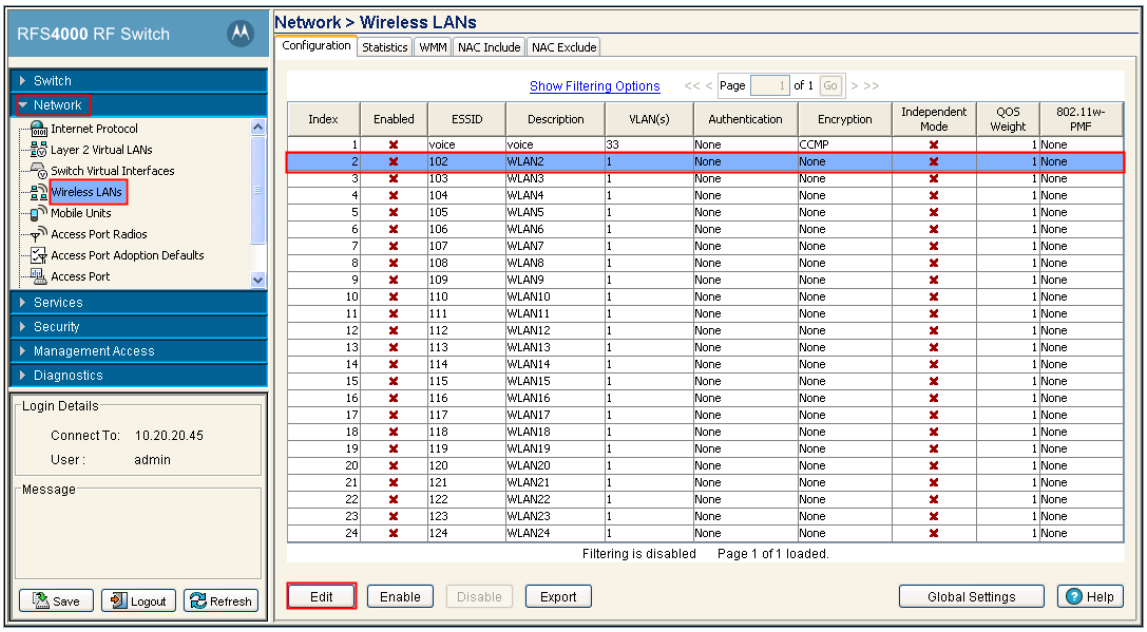
Step	
8.	The **Network > Wireless LANs > Edit** dialogue box will appear Enter the **ESSID, VLAN ID,** and **Description.** Under **Advanced,** check the **Use Voice Prioritization.** Under **Authentication,** select the radio button for **802.1X EAP**. Under **Encryption,** check the **WPA2-CCMP** box**.** Select **Radius…** to continue**.**



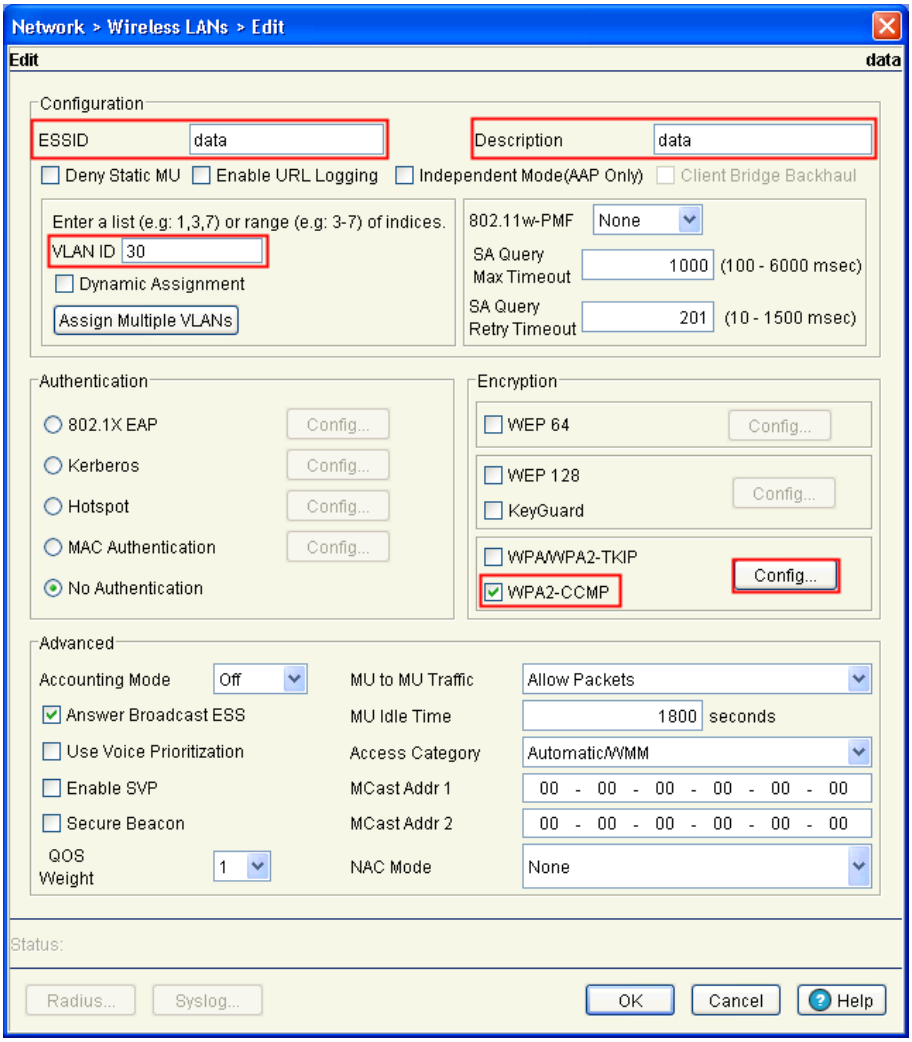
Step	
9.	The **Network > Wireless LANs > Edit > Radius Configuration** dialogue box will appear**.** Enter the **RADIUS Server Address, RADIUS Port** and **RADIUS Shared Secret.** Select **OK** and then select **OK** on the **Network > Wireless LANs > Edit** dialogue box from **Step 8**, (not shown) to continue. Note: The RADIUS Shared Secret musts match the one configured on the Radius server and should be obtained from the Radius administrator. 

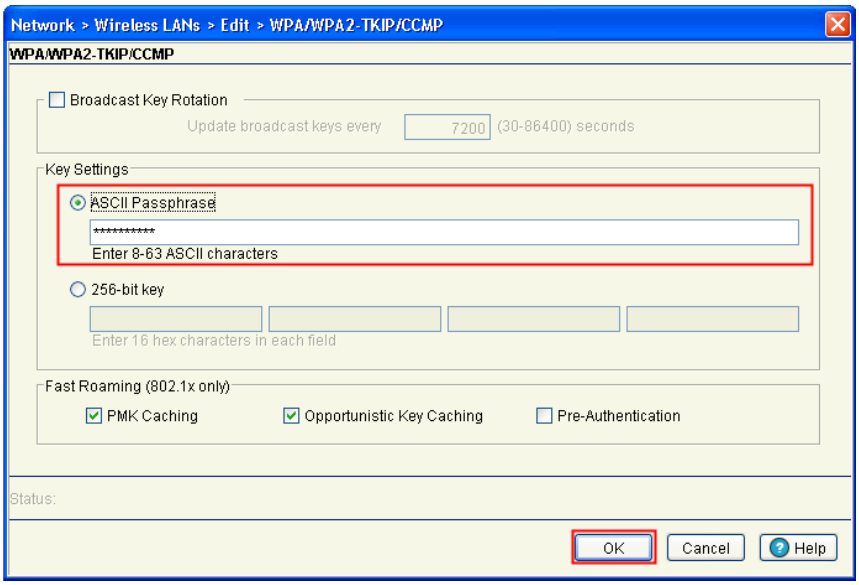
Create the data ESSID

Step	
10.	Navigate to **Network → Wireless LANs → Configuration.** Highlight an unused ESSID (e.g., **102)** and click **Edit**.



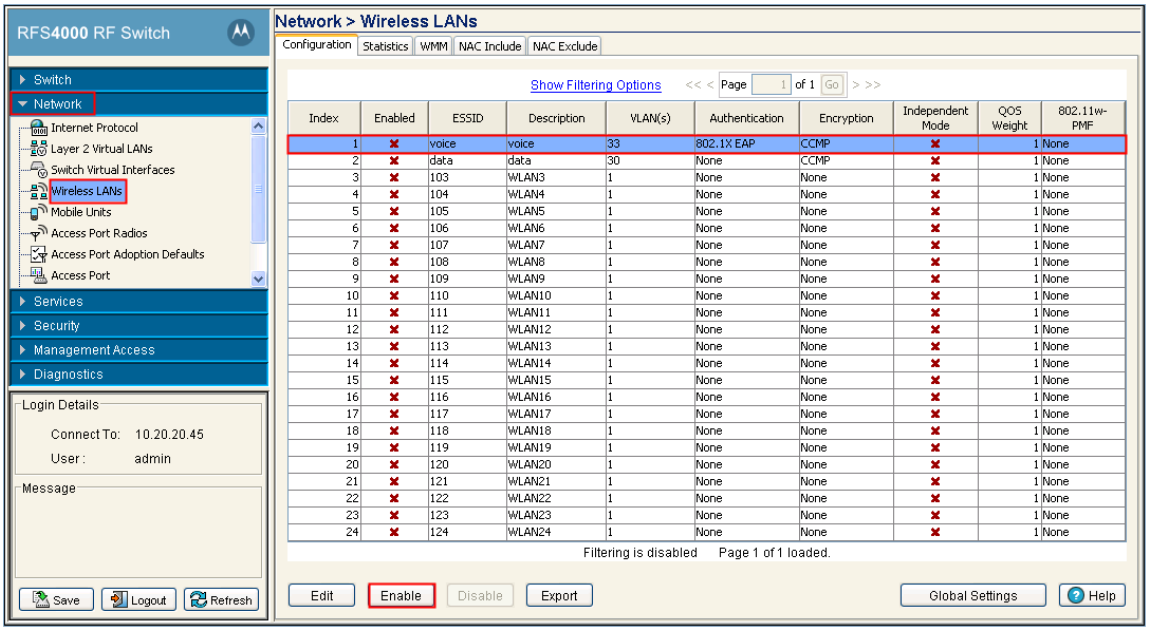
Step	
11.	The **Network > Wireless LANs > Edit** dialogue box will appear**.** Enter the **ESSID, VLAN ID,** and **Description.** Under **Encryption,** check the **WPA2-CCMP** box and select **Config** to continue.



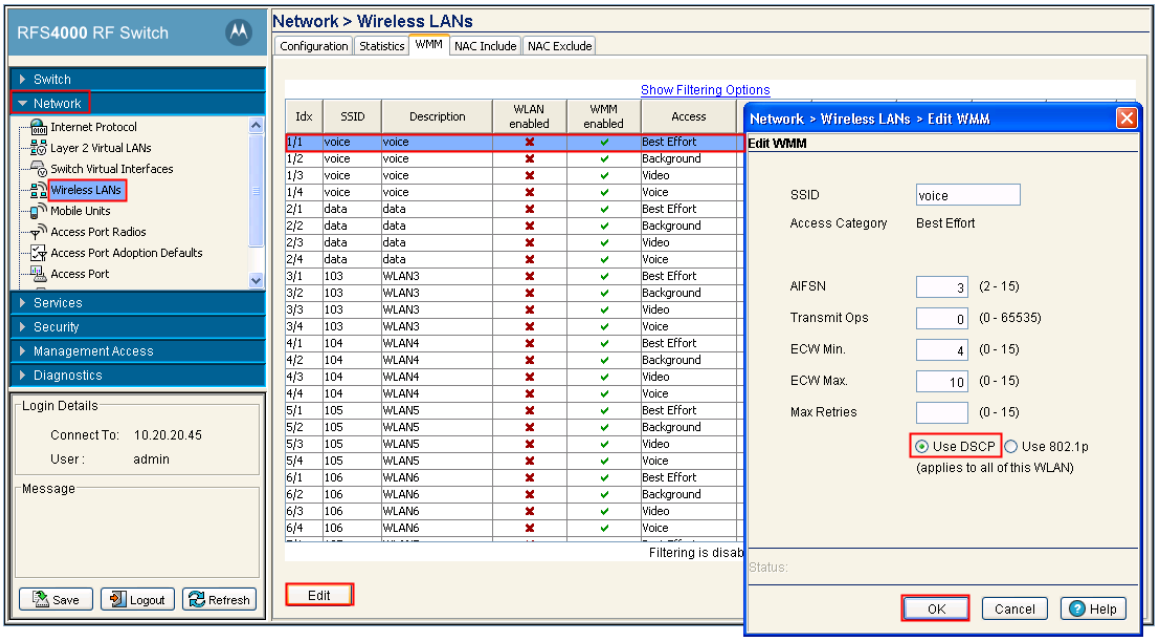
Step	
12.	The **Network > Wireless LANs > Edit > WPA/WPA2 – TKIP/CCMP** dialogue box will appear**. Enter** the **ASCII Passphrase.** Select **OK** and then select **OK** on the **Network > Wireless LANs > Edit** dialogue box from **Step 11**, (not shown). 

Enable wireless LANs

Step	
13.	Navigate to **Network → Wireless LANs → Configuration.** Highlight the **voice** ESSID and click **Enable**. Repeat this for the **data** ESSID.

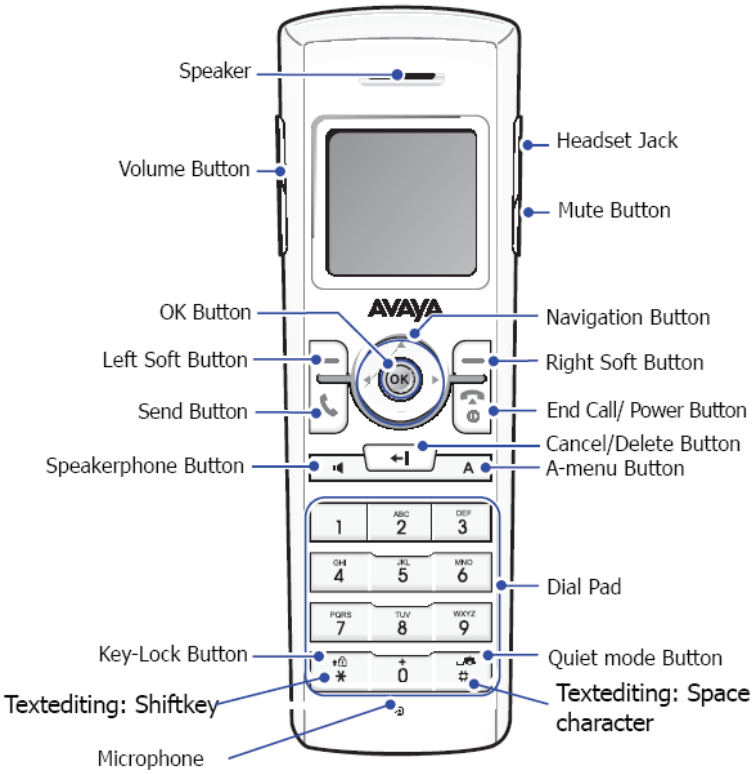


Edit WMM Policy

Step	
14.	Navigate to **Network → Wireless LANs → WMM.** Highlight **voice** (there will be 4 entries, highlight any one) and click **Edit**. Check the **Use DSCP** radio button. Click **OK** to continue. **Note**: Repeat this step for **data**. 

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 **voice, Encryption** type **is WPA2-CCMP** and the Authentication type **802.1x,** as create in **Section 5.2 Step 8.** Add the following information to the 46xxsettings.txt setting file.

```
SET WTPROF1      " voice"
SET WTSSIDP1     " voice"
SET DNSSRVRP1    "192.50.10.1"
SET WTWMMP1      "1"
SET DOMAIN       "dev4.com"
SET WTSECP1      "5"
SET ENCRYPTP1    "4"
SET EAPTYPEP1    "4"
SET TRUSTCERTS "cacert1.pem"
```

After the phone reboots, the user is prompted to enter **802.1X ID**, **username**, and **password**. (For PEAP-MSCHAPV2, only specify **ID** and **password**; leave **username** blank.) This is a one-time-only data entry. Data is stored in flash and presented automatically on subsequent authentications. Alternately, the user can enter 802.1x/EAP information as part of Access Profile configuration through phone's display interface.

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:

Step	**Description:** Configuring DHCP Option 242
1.	1. On the DHCP server, open the **DHCP server administration** tool by clicking **Start → Administration Tools → DHCP**. 2. Find the DHCP server and right-click on the server name. Select **Set Predefined Options**. 3. In the Predefined Options and Values dialog box, click the **Add** button. 4. In the Option Type dialog box, enter the following information: • **Name = 242** • **Data type = String** • **Code = 242** 5. Click the **OK** button to save this information. 6. Add the following **String** under **Value**: **MCIPADD=192.50.10.1,MCPORT=1719,HTTPSRVR=10.20.20.250**

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 Communication Manager through the Motorola Wireless Solution.
- Verify Message Waiting Indicator and message retrieval from Avaya Modular Messaging Server and 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, voicemail, DTMF while traversing the Motorola RFS Series 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 Communication Manager utilizing the Motorola Wireless Solution. The Avaya Wireless 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/Motorola 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 **ESSID** value of the wireless network matches the **ESSID** field value configured in **Section 5.2 Step 7,** 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 Motorola RFS Series RF Switch and multiple Motorola AP300 Access Points with an Avaya Aura™ telephony infrastructure. The Motorola RFS Series RF Switch and Motorola AP300 Access Points were successfully compliance-tested in a wireless converged voice and data network configuration. All feature functionality test cases described in **Section 7** passed.

10. Additional References

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

[1] *Administering Avaya Aura™ Communication Manager,* May 2009, Issue 5.0, Document Number 03-300509.

[2] *Administering Avaya Aura™ SIP Enablement Services*, May 2009, Issue 2.1, Document 03-602508.

[3] *Avaya Aura™ SIP Enablement Services (SES) Implementation Guide*, May 2009, Issue 6, Document 16-300140.

[4] *Avaya 3631 Wireless Telephone Administrator Guide,* March 2007, Issue 2, Document Number 16-602203.

[5] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.0,* Document Number 16-300698.

[6] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.0,* Document Number 16-601944.

[7] *Modular Messaging, Release 5.0 with the Avaya MSS Messaging Application Server (MAS) Administration Guide,* January 2009.

[8] *Avaya Aura™ Communication Manager Messaging Installation and Initial Configuration*.

The following product documentation is provided by Motorola. For additional product and company information, visit http://www.motorola.com.

[9] *Motorola RFS Series Wireless LAN Switches WiNG CLI Reference Guide* (Part No. 72E-131208-01 Rev. A).

[10] *Motorola RFS Series Wireless LAN Switches WiNG System Reference Guide* (Part No. 72E-132942-01 Rev. A).

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.