



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.

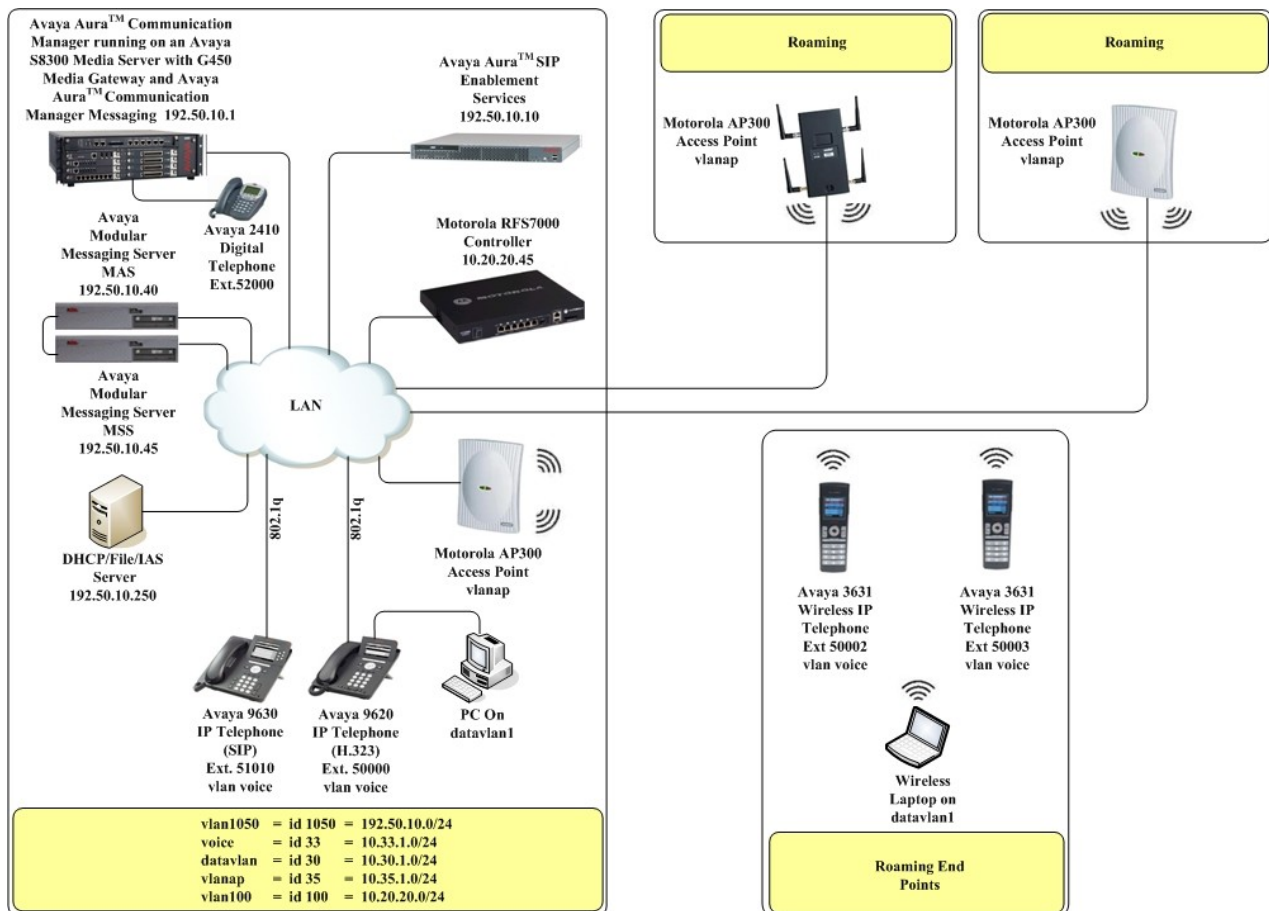


Figure 1: Avaya and Motorola Wireless LAN Configuration

3. Equipment and Software Validated

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

Equipment	Software/Firmware
<i>Avaya PBX Products</i>	
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
<i>Avaya Aura™ SIP Enablement Services (SES)</i>	
Avaya Aura™ SIP Enablement Services	5.2.1
<i>Avaya Messaging (Voice Mail) Products</i>	
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
<i>Avaya Telephony Sets</i>	
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
<i>Motorola Products</i>	
Motorola RFS4000 RF Switch	4.1.0.0-042R
Motorola AP300 Access Point	4.1.0.0-042R
<i>MS Products</i>	
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.	<p>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:</p> <ul style="list-style-type: none"> • 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 <pre> 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 </pre>
2.	<p>On Page 3, add the following options for des rgn:</p> <ul style="list-style-type: none"> • codec set set to 1 <p>Note: direct WAN, Units and IGAR will propagate automatically.</p> <pre> 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 2 3 1 y NoLimit n </pre>

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.	<p>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:</p> <ul style="list-style-type: none">• 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
	<pre>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</pre>

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.	<p>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.</p> <ul style="list-style-type: none">• 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																													
	<div>change ip-network-map<div>IP ADDRESS MAPPING</div><div>Page 1 of 63</div><table><tr><th>IP Address</th><th>Subnet Bits</th><th>Network Region</th><th>VLAN</th><th>Emergency Location</th><th>Ext</th></tr><tr><td>FROM: 10.33.1.131</td><td>/32</td><td>3</td><td>n</td><td></td><td></td></tr><tr><td>TO: 10.33.1.131</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>FROM: 10.33.1.132</td><td>/32</td><td>3</td><td>n</td><td></td><td></td></tr><tr><td>TO: 10.33.1.132</td><td></td><td></td><td></td><td></td><td></td></tr></table></div>	IP Address	Subnet Bits	Network Region	VLAN	Emergency 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				
IP Address	Subnet Bits	Network Region	VLAN	Emergency 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**

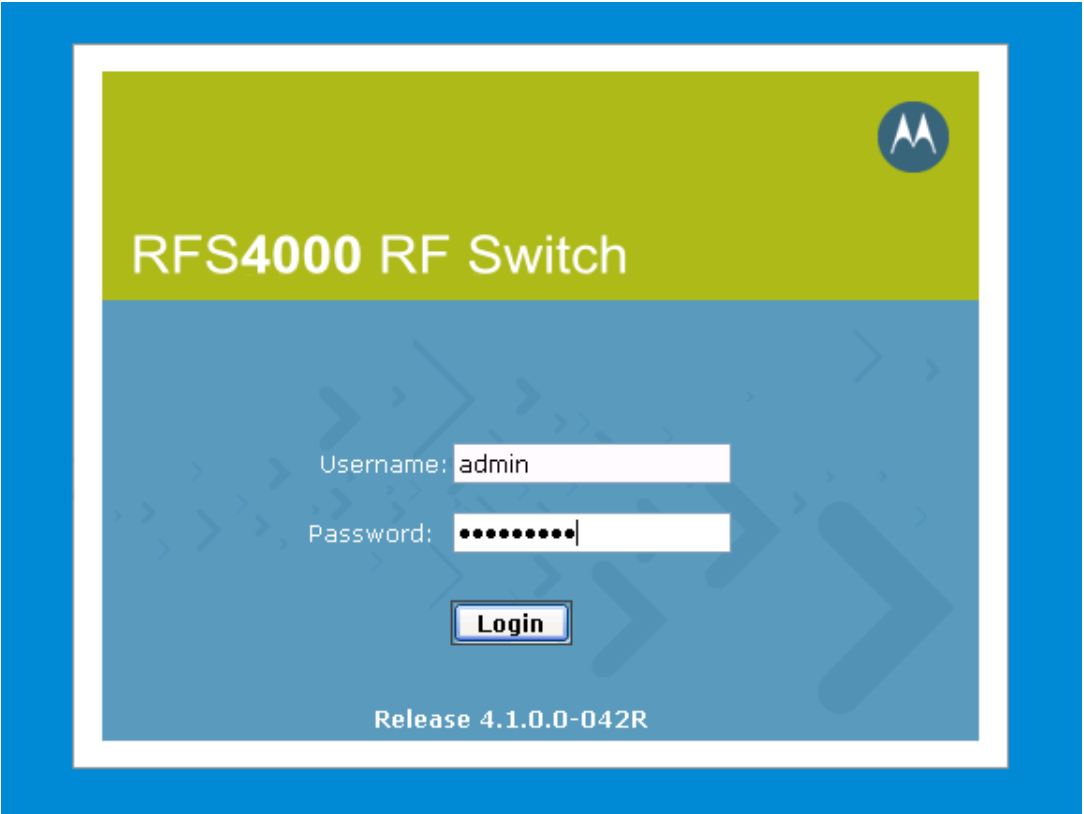
RFS4000(config-if)#**no ip address 192.168.0.1/24**

RFS4000(config-if)#**no ip nat inside**

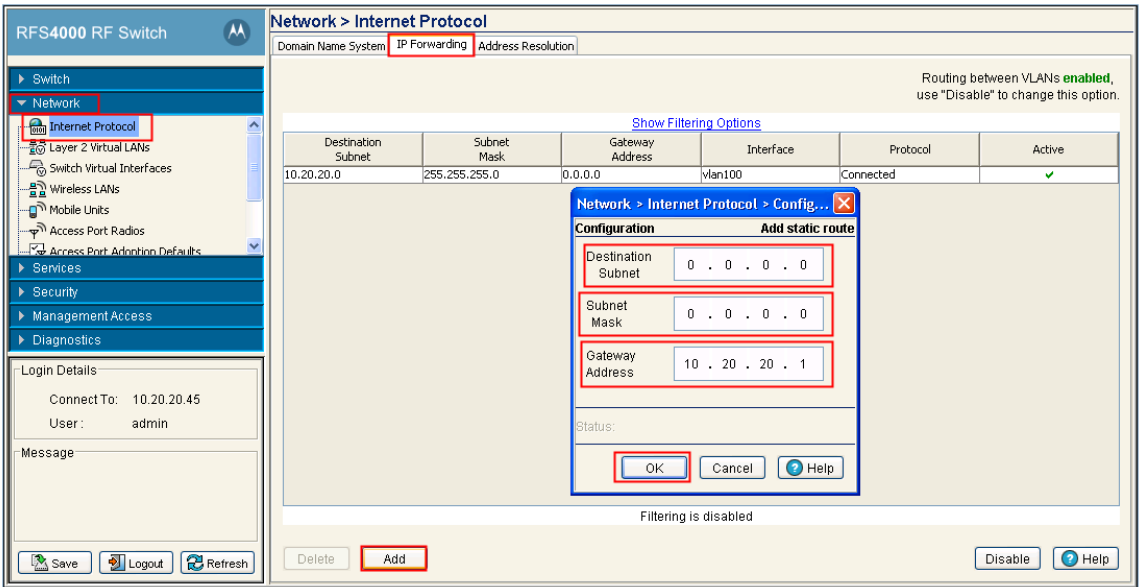
RFS4000(config-if)#**exit**

RFS4000(config)#**write memory**

5.2. Configure Motorola RFS4000 RF Switch (Web)

Step	
1.	<p>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].</p> <ol style="list-style-type: none">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. <p>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.</p> 

Create the default gateway

Step													
2.	<p>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.</p>  <p>The screenshot shows the RFS4000 RF Switch configuration interface. On the left, the 'Network' menu is expanded, and 'Internet Protocol' is selected. The main window displays the 'Network > Internet Protocol' configuration page. The 'IP Forwarding' tab is active. A table lists a static route with the following details:</p> <table border="1"> <thead> <tr> <th>Destination Subnet</th> <th>Subnet Mask</th> <th>Gateway Address</th> <th>Interface</th> <th>Protocol</th> <th>Active</th> </tr> </thead> <tbody> <tr> <td>10.20.20.0</td> <td>255.255.255.0</td> <td>0.0.0.0</td> <td>vlan100</td> <td>Connected</td> <td>✓</td> </tr> </tbody> </table> <p>A configuration dialog box titled 'Network > Internet Protocol > Config...' is open, showing the 'Add static route' configuration. The fields are:</p> <ul style="list-style-type: none"> Destination Subnet: 0 . 0 . 0 . 0 Subnet Mask: 0 . 0 . 0 . 0 Gateway Address: 10 . 20 . 20 . 1 <p>The 'Status' field is empty. The 'OK' button is highlighted. At the bottom of the main window, the 'Add' button is also highlighted.</p>	Destination Subnet	Subnet Mask	Gateway Address	Interface	Protocol	Active	10.20.20.0	255.255.255.0	0.0.0.0	vlan100	Connected	✓
Destination Subnet	Subnet Mask	Gateway Address	Interface	Protocol	Active								
10.20.20.0	255.255.255.0	0.0.0.0	vlan100	Connected	✓								

Create a VLAN for the voice network

Step	
3.	<p>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.</p>

The screenshot displays the RFS4000 RF Switch configuration interface. On the left, a navigation tree shows 'Network' expanded, with 'Switch Virtual Interfaces' selected. The main area shows the 'Configuration' tab for 'Switch Virtual Interfaces'. A table lists existing VLANs:

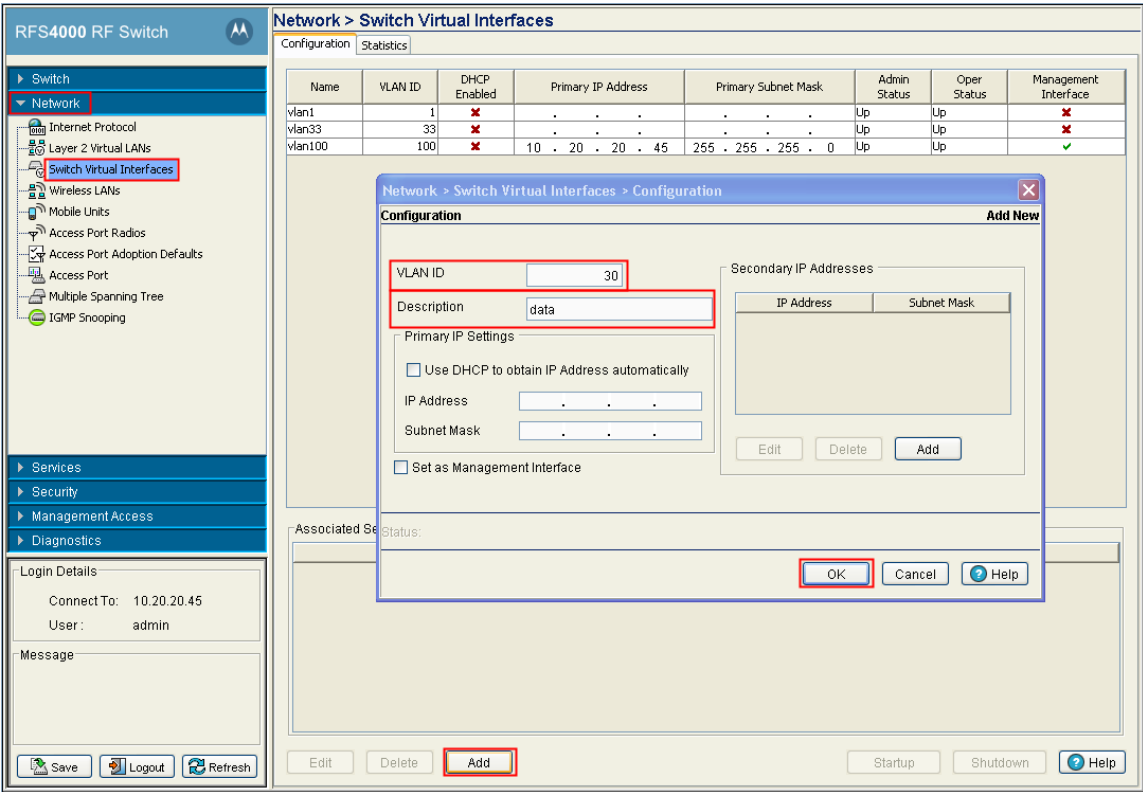
Name	VLAN ID	DHCP Enabled	Primary IP Address	Primary Subnet Mask	Admin Status	Oper Status	Management Interface
vlan1	1	✗	Up	Up	✗
vlan100	100	✗	10 . 20 . 20 . 45	255 . 255 . 255 . 0	Up	Up	✓

Overlaid on this is the 'Network > Switch Virtual Interfaces > Configuration' dialog box. It contains the following fields and options:

- VLAN ID:** 33
- Description:** voice
- Primary IP Settings:**
 - ☐ Use DHCP to obtain IP Address automatically
 - IP Address:** . . .
 - Subnet Mask:** . . .
 - ☐ Set as Management Interface
- Secondary IP Addresses:** (Table with columns for IP Address and Subnet Mask)
- Buttons:** Edit, Delete, Add (in the dialog), and OK, Cancel, Help (at the bottom of the dialog).

The 'Add' button in the dialog box is highlighted with a red box. The background interface also has an 'Add' button highlighted with a red box at the bottom.

Create a VLAN for the data network

Step	
4.	<p>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.</p>  <p>The screenshot shows the RFS4000 RF Switch configuration interface. On the left is a navigation tree with 'Network' expanded and 'Switch Virtual Interfaces' selected. The main area displays a table of existing VLANs and a configuration dialog for a new VLAN. The dialog box is titled 'Network > Switch Virtual Interfaces > Configuration' and contains the following fields and options:</p> <ul style="list-style-type: none"> VLAN ID: 30 Description: data Primary IP Settings: <ul style="list-style-type: none"> <input type="checkbox"/> Use DHCP to obtain IP Address automatically IP Address: . . . Subnet Mask: . . . <input type="checkbox"/> Set as Management Interface Secondary IP Addresses: A table with columns 'IP Address' and 'Subnet Mask', and buttons 'Edit', 'Delete', and 'Add'. <p>At the bottom of the dialog box, the 'OK' button is highlighted with a red box. Below the dialog box, there are buttons for 'Edit', 'Delete', and 'Add' (highlighted with a red box) for the main table, and 'Startup', 'Shutdown', and 'Help' buttons at the bottom right.</p>

Create a VLAN for the Motorola Access Points

Step	
5.	<p>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.</p>

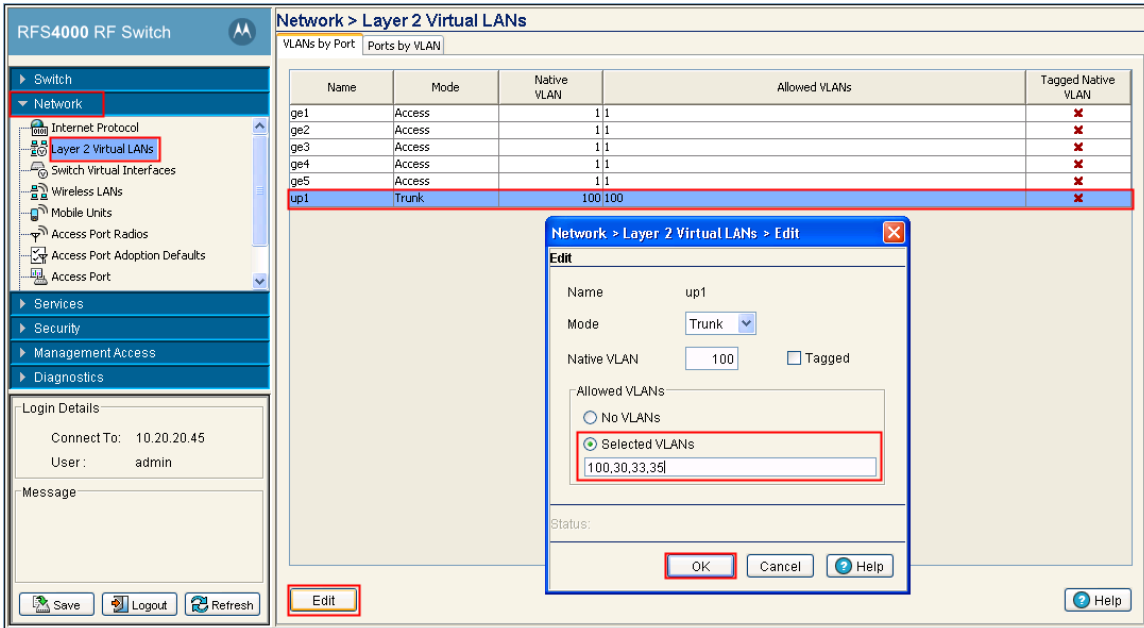
The screenshot shows the RFS4000 RF Switch configuration interface. On the left is a navigation tree with 'Network' expanded and 'Switch Virtual Interfaces' selected. The main area displays the 'Network > Switch Virtual Interfaces > Configuration' dialog box. This dialog box contains the following elements:

- VLAN ID:** A text field containing the value '35'.
- Description:** A text field containing the value 'vlanap'.
- Primary IP Settings:** A section with a checkbox 'Use DHCP to obtain IP Address automatically' (unchecked), and fields for 'IP Address' and 'Subnet Mask'.
- Secondary IP Addresses:** A table with columns 'IP Address' and 'Subnet Mask', and buttons 'Edit', 'Delete', and 'Add'.
- Buttons:** 'OK', 'Cancel', and 'Help' buttons at the bottom right of the dialog box.

The 'Add' button in the bottom right of the dialog box is highlighted with a red rectangle. In the background, a table lists existing VLANs:

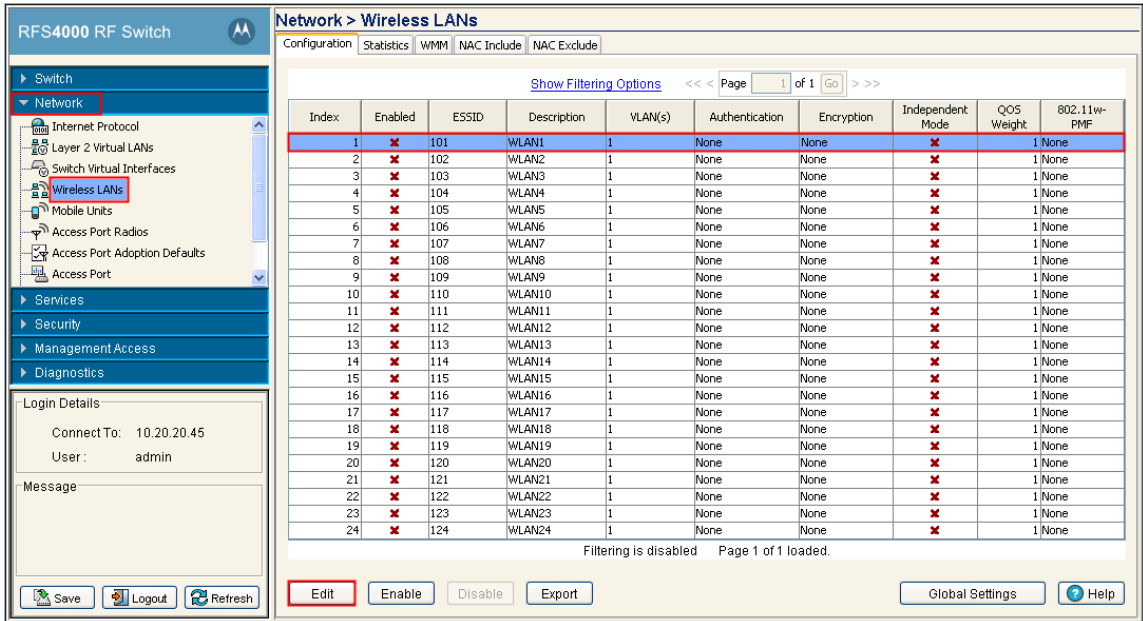
Name	VLAN ID	DHCP Enabled	Primary IP Address	Primary Subnet Mask	Admin Status	Oper Status	Management Interface
vlan1	1	✗	Up	Up	✗
vlan30	30	✗	Up	Up	✗
vlan33	33	✗	Up	Up	✗
vlan100	100	✗	10 . 20 . 20 . 45	255 . 255 . 255 . 0	Up	Up	✓

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.	<p>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.</p>  <p>The screenshot shows the RFS4000 RF Switch configuration interface. On the left is a navigation tree with 'Network' expanded and 'Layer 2 Virtual LANs' selected. The main area displays a table of Layer 2 Virtual LANs. The 'up1' interface is highlighted in blue. An 'Edit' dialog box is open, showing the 'Allowed VLANs' section with the 'Selected VLANs' radio button selected and the text '100,30,33,35' entered in the text field. The 'OK' button is highlighted in red.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Mode</th> <th>Native VLAN</th> <th>Allowed VLANs</th> <th>Tagged Native VLAN</th> </tr> </thead> <tbody> <tr> <td>ge1</td> <td>Access</td> <td>1</td> <td>1</td> <td>×</td> </tr> <tr> <td>ge2</td> <td>Access</td> <td>1</td> <td>1</td> <td>×</td> </tr> <tr> <td>ge3</td> <td>Access</td> <td>1</td> <td>1</td> <td>×</td> </tr> <tr> <td>ge4</td> <td>Access</td> <td>1</td> <td>1</td> <td>×</td> </tr> <tr> <td>ge5</td> <td>Access</td> <td>1</td> <td>1</td> <td>×</td> </tr> <tr> <td>up1</td> <td>Trunk</td> <td>100</td> <td>100</td> <td>×</td> </tr> </tbody> </table>	Name	Mode	Native VLAN	Allowed VLANs	Tagged Native VLAN	ge1	Access	1	1	×	ge2	Access	1	1	×	ge3	Access	1	1	×	ge4	Access	1	1	×	ge5	Access	1	1	×	up1	Trunk	100	100	×
Name	Mode	Native VLAN	Allowed VLANs	Tagged Native VLAN																																
ge1	Access	1	1	×																																
ge2	Access	1	1	×																																
ge3	Access	1	1	×																																
ge4	Access	1	1	×																																
ge5	Access	1	1	×																																
up1	Trunk	100	100	×																																

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.	<p>Navigate to Network → Wireless LANs → Configuration. Highlight an unused ESSID (e.g., 101) and click Edit.</p>  <p>The screenshot displays the 'Network > Wireless LANs' configuration page. The left sidebar shows the navigation menu with 'Wireless LANs' selected. The main content area shows a table of 24 wireless LANs. The first row (Index 1, Enabled, ESSID 101, Description WLAN1) is highlighted in red. The 'Edit' button is also highlighted in red. The bottom of the page has buttons for Save, Logout, Refresh, Edit, Enable, Disable, Export, Global Settings, and Help.</p> <table border="1"> <thead> <tr> <th>Index</th> <th>Enabled</th> <th>ESSID</th> <th>Description</th> <th>VLAN(s)</th> <th>Authentication</th> <th>Encryption</th> <th>Independent Mode</th> <th>QOS Weight</th> <th>802.11w-PMF</th> </tr> </thead> <tbody> <tr><td>1</td><td>✗</td><td>101</td><td>WLAN1</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>2</td><td>✗</td><td>102</td><td>WLAN2</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>3</td><td>✗</td><td>103</td><td>WLAN3</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>4</td><td>✗</td><td>104</td><td>WLAN4</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>5</td><td>✗</td><td>105</td><td>WLAN5</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>6</td><td>✗</td><td>106</td><td>WLAN6</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>7</td><td>✗</td><td>107</td><td>WLAN7</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>8</td><td>✗</td><td>108</td><td>WLAN8</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>9</td><td>✗</td><td>109</td><td>WLAN9</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>10</td><td>✗</td><td>110</td><td>WLAN10</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>11</td><td>✗</td><td>111</td><td>WLAN11</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>12</td><td>✗</td><td>112</td><td>WLAN12</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>13</td><td>✗</td><td>113</td><td>WLAN13</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>14</td><td>✗</td><td>114</td><td>WLAN14</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>15</td><td>✗</td><td>115</td><td>WLAN15</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>16</td><td>✗</td><td>116</td><td>WLAN16</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>17</td><td>✗</td><td>117</td><td>WLAN17</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>18</td><td>✗</td><td>118</td><td>WLAN18</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>19</td><td>✗</td><td>119</td><td>WLAN19</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>20</td><td>✗</td><td>120</td><td>WLAN20</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>21</td><td>✗</td><td>121</td><td>WLAN21</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>22</td><td>✗</td><td>122</td><td>WLAN22</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>23</td><td>✗</td><td>123</td><td>WLAN23</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> <tr><td>24</td><td>✗</td><td>124</td><td>WLAN24</td><td>1</td><td>None</td><td>None</td><td>✗</td><td>1</td><td>None</td></tr> </tbody> </table>	Index	Enabled	ESSID	Description	VLAN(s)	Authentication	Encryption	Independent Mode	QOS Weight	802.11w-PMF	1	✗	101	WLAN1	1	None	None	✗	1	None	2	✗	102	WLAN2	1	None	None	✗	1	None	3	✗	103	WLAN3	1	None	None	✗	1	None	4	✗	104	WLAN4	1	None	None	✗	1	None	5	✗	105	WLAN5	1	None	None	✗	1	None	6	✗	106	WLAN6	1	None	None	✗	1	None	7	✗	107	WLAN7	1	None	None	✗	1	None	8	✗	108	WLAN8	1	None	None	✗	1	None	9	✗	109	WLAN9	1	None	None	✗	1	None	10	✗	110	WLAN10	1	None	None	✗	1	None	11	✗	111	WLAN11	1	None	None	✗	1	None	12	✗	112	WLAN12	1	None	None	✗	1	None	13	✗	113	WLAN13	1	None	None	✗	1	None	14	✗	114	WLAN14	1	None	None	✗	1	None	15	✗	115	WLAN15	1	None	None	✗	1	None	16	✗	116	WLAN16	1	None	None	✗	1	None	17	✗	117	WLAN17	1	None	None	✗	1	None	18	✗	118	WLAN18	1	None	None	✗	1	None	19	✗	119	WLAN19	1	None	None	✗	1	None	20	✗	120	WLAN20	1	None	None	✗	1	None	21	✗	121	WLAN21	1	None	None	✗	1	None	22	✗	122	WLAN22	1	None	None	✗	1	None	23	✗	123	WLAN23	1	None	None	✗	1	None	24	✗	124	WLAN24	1	None	None	✗	1	None
Index	Enabled	ESSID	Description	VLAN(s)	Authentication	Encryption	Independent Mode	QOS Weight	802.11w-PMF																																																																																																																																																																																																																																																		
1	✗	101	WLAN1	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
2	✗	102	WLAN2	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
3	✗	103	WLAN3	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
4	✗	104	WLAN4	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
5	✗	105	WLAN5	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
6	✗	106	WLAN6	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
7	✗	107	WLAN7	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
8	✗	108	WLAN8	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
9	✗	109	WLAN9	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
10	✗	110	WLAN10	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
11	✗	111	WLAN11	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
12	✗	112	WLAN12	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
13	✗	113	WLAN13	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
14	✗	114	WLAN14	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
15	✗	115	WLAN15	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
16	✗	116	WLAN16	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
17	✗	117	WLAN17	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
18	✗	118	WLAN18	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
19	✗	119	WLAN19	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
20	✗	120	WLAN20	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
21	✗	121	WLAN21	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
22	✗	122	WLAN22	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
23	✗	123	WLAN23	1	None	None	✗	1	None																																																																																																																																																																																																																																																		
24	✗	124	WLAN24	1	None	None	✗	1	None																																																																																																																																																																																																																																																		

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.

Network > Wireless LANs > Edit

Edit voice

Configuration

ESSID: Description:

☐ Deny Static MU ☐ Enable URL Logging ☐ Independent Mode(AAP Only) ☐ Client Bridge Backhaul

Enter a list (e.g: 1,3,7) or range (e.g: 3-7) of indices.
VLAN ID:

☐ Dynamic Assignment

802.11w-PMF:
SA Query Max Timeout: (100 - 6000 msec)
SA Query Retry Timeout: (10 - 1500 msec)

Authentication

☒ 802.1X EAP
☐ Kerberos
☐ Hotspot
☐ MAC Authentication
☐ No Authentication

Encryption

☐ WEP 64
☐ WEP 128
☐ KeyGuard
☐ WPA/WPA2-TKIP
☒ WPA2-CCMP

Advanced

Accounting Mode:
☒ Answer Broadcast ESS
☒ Use Voice Prioritization
☐ Enable SVP
☐ Secure Beacon
QOS Weight:

MU to MU Traffic:
MU Idle Time: seconds
Access Category:
MCast Addr 1:
MCast Addr 2:
NAC Mode:

Status:

Step	
9.	<p data-bbox="277 275 1432 422">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.</p> <p data-bbox="277 453 1404 527">Note: The RADIUS Shared Secret must match the one configured on the Radius server and should be obtained from the Radius administrator.</p> <div data-bbox="358 569 1349 1829"> </div>

Create the data ESSID

Step

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

RFS4000 RF Switch

Network > Wireless LANs

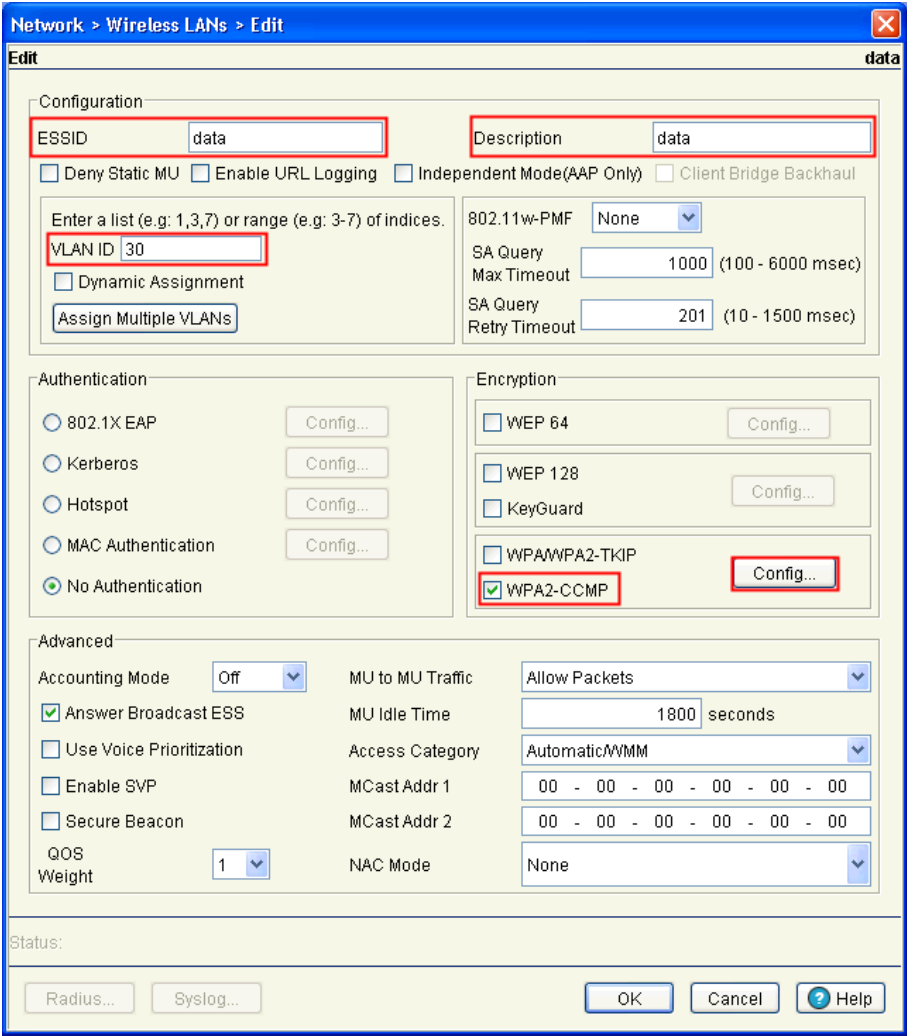
Configuration | Statistics | WMM | NAC Include | NAC Exclude

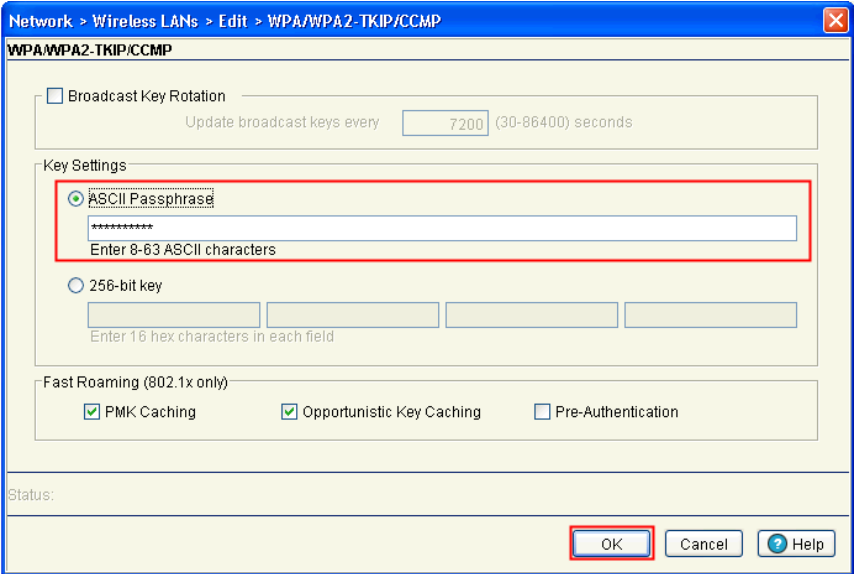
Show Filtering Options << Page 1 of 1 Go >>

Index	Enabled	ESSID	Description	VLAN(s)	Authentication	Encryption	Independent Mode	QOS Weight	802.11w-PMF
1	✗	voice	voice	33	None	CCMP	✗	1	None
2	✗	102	WLAN2	1	None	None	✗	1	None
3	✗	103	WLAN3	1	None	None	✗	1	None
4	✗	104	WLAN4	1	None	None	✗	1	None
5	✗	105	WLAN5	1	None	None	✗	1	None
6	✗	106	WLAN6	1	None	None	✗	1	None
7	✗	107	WLAN7	1	None	None	✗	1	None
8	✗	108	WLAN8	1	None	None	✗	1	None
9	✗	109	WLAN9	1	None	None	✗	1	None
10	✗	110	WLAN10	1	None	None	✗	1	None
11	✗	111	WLAN11	1	None	None	✗	1	None
12	✗	112	WLAN12	1	None	None	✗	1	None
13	✗	113	WLAN13	1	None	None	✗	1	None
14	✗	114	WLAN14	1	None	None	✗	1	None
15	✗	115	WLAN15	1	None	None	✗	1	None
16	✗	116	WLAN16	1	None	None	✗	1	None
17	✗	117	WLAN17	1	None	None	✗	1	None
18	✗	118	WLAN18	1	None	None	✗	1	None
19	✗	119	WLAN19	1	None	None	✗	1	None
20	✗	120	WLAN20	1	None	None	✗	1	None
21	✗	121	WLAN21	1	None	None	✗	1	None
22	✗	122	WLAN22	1	None	None	✗	1	None
23	✗	123	WLAN23	1	None	None	✗	1	None
24	✗	124	WLAN24	1	None	None	✗	1	None

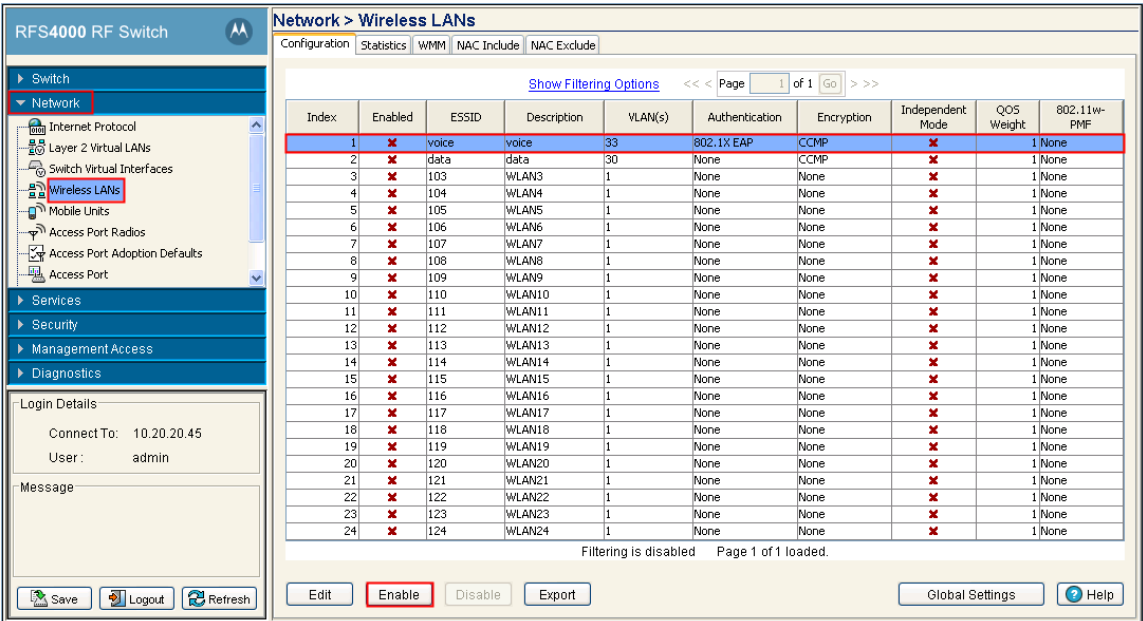
Filtering is disabled Page 1 of 1 loaded.

Save Logout Refresh Edit Enable Disable Export Global Settings Help

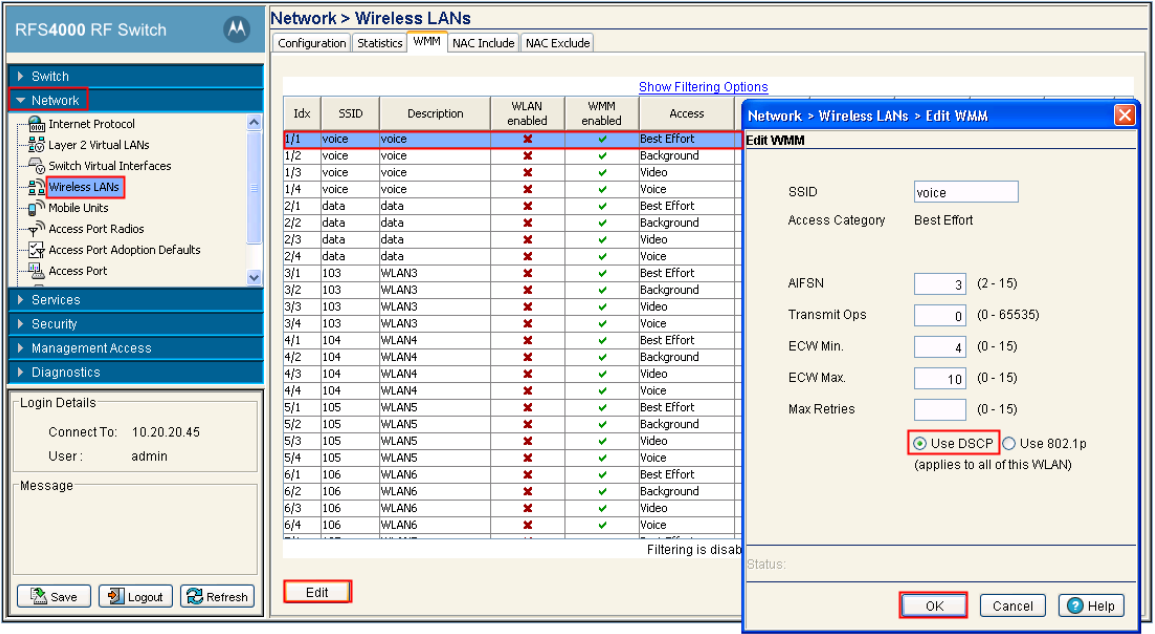
Step	
11.	<p>The Network > Wireless LANs > Edit dialogue box will appear. Enter the ESSID, VLAN ID, and Description. Under Encryption, check the WPA2-CCMP box and select Config to continue.</p> 

Step	
12.	<p>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).</p> 

Enable wireless LANs

Step																																																																																																																																																																																																																																																											
13.	<p>Navigate to Network → Wireless LANs → Configuration. Highlight the voice ESSID and click Enable. Repeat this for the data ESSID.</p>  <p>The screenshot shows the 'Network > Wireless LANs' configuration page. On the left, the 'Wireless LANs' menu item is highlighted. The main area displays a table of wireless LAN configurations. The first row, representing the 'voice' ESSID, is highlighted. At the bottom, the 'Enable' button is highlighted.</p> <table border="1"> <thead> <tr> <th>Index</th> <th>Enabled</th> <th>ESSID</th> <th>Description</th> <th>VLAN(s)</th> <th>Authentication</th> <th>Encryption</th> <th>Independent Mode</th> <th>QOS Weight</th> <th>802.11w-PMF</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input checked="" type="checkbox"/></td> <td>voice</td> <td>voice</td> <td>33</td> <td>802.1X EAP</td> <td>CCMP</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>2</td> <td><input checked="" type="checkbox"/></td> <td>data</td> <td>data</td> <td>30</td> <td>None</td> <td>CCMP</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>3</td> <td><input checked="" type="checkbox"/></td> <td>103</td> <td>WLAN3</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>4</td> <td><input checked="" type="checkbox"/></td> <td>104</td> <td>WLAN4</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>5</td> <td><input checked="" type="checkbox"/></td> <td>105</td> <td>WLAN5</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>6</td> <td><input checked="" type="checkbox"/></td> <td>106</td> <td>WLAN6</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>7</td> <td><input checked="" type="checkbox"/></td> <td>107</td> <td>WLAN7</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>8</td> <td><input checked="" type="checkbox"/></td> <td>108</td> <td>WLAN8</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>9</td> <td><input checked="" type="checkbox"/></td> <td>109</td> <td>WLAN9</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>10</td> <td><input checked="" type="checkbox"/></td> <td>110</td> <td>WLAN10</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>11</td> <td><input checked="" type="checkbox"/></td> <td>111</td> <td>WLAN11</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>12</td> <td><input checked="" type="checkbox"/></td> <td>112</td> <td>WLAN12</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>13</td> <td><input checked="" type="checkbox"/></td> <td>113</td> <td>WLAN13</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>14</td> <td><input checked="" type="checkbox"/></td> <td>114</td> <td>WLAN14</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>15</td> <td><input checked="" type="checkbox"/></td> <td>115</td> <td>WLAN15</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>16</td> <td><input checked="" type="checkbox"/></td> <td>116</td> <td>WLAN16</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>17</td> <td><input checked="" type="checkbox"/></td> <td>117</td> <td>WLAN17</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>18</td> <td><input checked="" type="checkbox"/></td> <td>118</td> <td>WLAN18</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>19</td> <td><input checked="" type="checkbox"/></td> <td>119</td> <td>WLAN19</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>20</td> <td><input checked="" type="checkbox"/></td> <td>120</td> <td>WLAN20</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>21</td> <td><input checked="" type="checkbox"/></td> <td>121</td> <td>WLAN21</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>22</td> <td><input checked="" type="checkbox"/></td> <td>122</td> <td>WLAN22</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>23</td> <td><input checked="" type="checkbox"/></td> <td>123</td> <td>WLAN23</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> <tr> <td>24</td> <td><input checked="" type="checkbox"/></td> <td>124</td> <td>WLAN24</td> <td>1</td> <td>None</td> <td>None</td> <td><input checked="" type="checkbox"/></td> <td>1</td> <td>None</td> </tr> </tbody> </table>	Index	Enabled	ESSID	Description	VLAN(s)	Authentication	Encryption	Independent Mode	QOS Weight	802.11w-PMF	1	<input checked="" type="checkbox"/>	voice	voice	33	802.1X EAP	CCMP	<input checked="" type="checkbox"/>	1	None	2	<input checked="" type="checkbox"/>	data	data	30	None	CCMP	<input checked="" type="checkbox"/>	1	None	3	<input checked="" type="checkbox"/>	103	WLAN3	1	None	None	<input checked="" type="checkbox"/>	1	None	4	<input checked="" type="checkbox"/>	104	WLAN4	1	None	None	<input checked="" type="checkbox"/>	1	None	5	<input checked="" type="checkbox"/>	105	WLAN5	1	None	None	<input checked="" type="checkbox"/>	1	None	6	<input checked="" type="checkbox"/>	106	WLAN6	1	None	None	<input checked="" type="checkbox"/>	1	None	7	<input checked="" type="checkbox"/>	107	WLAN7	1	None	None	<input checked="" type="checkbox"/>	1	None	8	<input checked="" type="checkbox"/>	108	WLAN8	1	None	None	<input checked="" type="checkbox"/>	1	None	9	<input checked="" type="checkbox"/>	109	WLAN9	1	None	None	<input checked="" type="checkbox"/>	1	None	10	<input checked="" type="checkbox"/>	110	WLAN10	1	None	None	<input checked="" type="checkbox"/>	1	None	11	<input checked="" type="checkbox"/>	111	WLAN11	1	None	None	<input checked="" type="checkbox"/>	1	None	12	<input checked="" type="checkbox"/>	112	WLAN12	1	None	None	<input checked="" type="checkbox"/>	1	None	13	<input checked="" type="checkbox"/>	113	WLAN13	1	None	None	<input checked="" type="checkbox"/>	1	None	14	<input checked="" type="checkbox"/>	114	WLAN14	1	None	None	<input checked="" type="checkbox"/>	1	None	15	<input checked="" type="checkbox"/>	115	WLAN15	1	None	None	<input checked="" type="checkbox"/>	1	None	16	<input checked="" type="checkbox"/>	116	WLAN16	1	None	None	<input checked="" type="checkbox"/>	1	None	17	<input checked="" type="checkbox"/>	117	WLAN17	1	None	None	<input checked="" type="checkbox"/>	1	None	18	<input checked="" type="checkbox"/>	118	WLAN18	1	None	None	<input checked="" type="checkbox"/>	1	None	19	<input checked="" type="checkbox"/>	119	WLAN19	1	None	None	<input checked="" type="checkbox"/>	1	None	20	<input checked="" type="checkbox"/>	120	WLAN20	1	None	None	<input checked="" type="checkbox"/>	1	None	21	<input checked="" type="checkbox"/>	121	WLAN21	1	None	None	<input checked="" type="checkbox"/>	1	None	22	<input checked="" type="checkbox"/>	122	WLAN22	1	None	None	<input checked="" type="checkbox"/>	1	None	23	<input checked="" type="checkbox"/>	123	WLAN23	1	None	None	<input checked="" type="checkbox"/>	1	None	24	<input checked="" type="checkbox"/>	124	WLAN24	1	None	None	<input checked="" type="checkbox"/>	1	None
Index	Enabled	ESSID	Description	VLAN(s)	Authentication	Encryption	Independent Mode	QOS Weight	802.11w-PMF																																																																																																																																																																																																																																																		
1	<input checked="" type="checkbox"/>	voice	voice	33	802.1X EAP	CCMP	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
2	<input checked="" type="checkbox"/>	data	data	30	None	CCMP	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
3	<input checked="" type="checkbox"/>	103	WLAN3	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
4	<input checked="" type="checkbox"/>	104	WLAN4	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
5	<input checked="" type="checkbox"/>	105	WLAN5	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
6	<input checked="" type="checkbox"/>	106	WLAN6	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
7	<input checked="" type="checkbox"/>	107	WLAN7	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
8	<input checked="" type="checkbox"/>	108	WLAN8	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
9	<input checked="" type="checkbox"/>	109	WLAN9	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
10	<input checked="" type="checkbox"/>	110	WLAN10	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
11	<input checked="" type="checkbox"/>	111	WLAN11	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
12	<input checked="" type="checkbox"/>	112	WLAN12	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
13	<input checked="" type="checkbox"/>	113	WLAN13	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
14	<input checked="" type="checkbox"/>	114	WLAN14	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
15	<input checked="" type="checkbox"/>	115	WLAN15	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
16	<input checked="" type="checkbox"/>	116	WLAN16	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
17	<input checked="" type="checkbox"/>	117	WLAN17	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
18	<input checked="" type="checkbox"/>	118	WLAN18	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
19	<input checked="" type="checkbox"/>	119	WLAN19	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
20	<input checked="" type="checkbox"/>	120	WLAN20	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
21	<input checked="" type="checkbox"/>	121	WLAN21	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
22	<input checked="" type="checkbox"/>	122	WLAN22	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
23	<input checked="" type="checkbox"/>	123	WLAN23	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		
24	<input checked="" type="checkbox"/>	124	WLAN24	1	None	None	<input checked="" type="checkbox"/>	1	None																																																																																																																																																																																																																																																		

Edit WMM Policy

Step																																																																																																																																																							
14.	<p>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.</p> <p>Note: Repeat this step for data.</p>  <p>The screenshot shows the RFS4000 RF Switch configuration interface. The left sidebar shows the navigation tree with 'Network' expanded and 'Wireless LANs' selected. The main area displays the 'Network > Wireless LANs' configuration page with tabs for Configuration, Statistics, WMM, NAC Include, and NAC Exclude. The 'WMM' tab is active, showing a table of WMM entries. The 'voice' entry is highlighted. The 'Edit WMM' dialog box is open, showing the 'voice' entry selected. The 'Use DSCP' radio button is checked, and the 'OK' button is highlighted.</p> <table border="1"> <thead> <tr> <th>Idx</th> <th>SSID</th> <th>Description</th> <th>WLAN enabled</th> <th>WMM enabled</th> <th>Access</th> </tr> </thead> <tbody> <tr><td>1/1</td><td>voice</td><td>voice</td><td>✗</td><td>✓</td><td>Best Effort</td></tr> <tr><td>1/2</td><td>voice</td><td>voice</td><td>✗</td><td>✓</td><td>Background</td></tr> <tr><td>1/3</td><td>voice</td><td>voice</td><td>✗</td><td>✓</td><td>Video</td></tr> <tr><td>1/4</td><td>voice</td><td>voice</td><td>✗</td><td>✓</td><td>Voice</td></tr> <tr><td>2/1</td><td>data</td><td>data</td><td>✗</td><td>✓</td><td>Best Effort</td></tr> <tr><td>2/2</td><td>data</td><td>data</td><td>✗</td><td>✓</td><td>Background</td></tr> <tr><td>2/3</td><td>data</td><td>data</td><td>✗</td><td>✓</td><td>Video</td></tr> <tr><td>2/4</td><td>data</td><td>data</td><td>✗</td><td>✓</td><td>Voice</td></tr> <tr><td>3/1</td><td>103</td><td>WLAN3</td><td>✗</td><td>✓</td><td>Best Effort</td></tr> <tr><td>3/2</td><td>103</td><td>WLAN3</td><td>✗</td><td>✓</td><td>Background</td></tr> <tr><td>3/3</td><td>103</td><td>WLAN3</td><td>✗</td><td>✓</td><td>Video</td></tr> <tr><td>3/4</td><td>103</td><td>WLAN3</td><td>✗</td><td>✓</td><td>Voice</td></tr> <tr><td>4/1</td><td>104</td><td>WLAN4</td><td>✗</td><td>✓</td><td>Best Effort</td></tr> <tr><td>4/2</td><td>104</td><td>WLAN4</td><td>✗</td><td>✓</td><td>Background</td></tr> <tr><td>4/3</td><td>104</td><td>WLAN4</td><td>✗</td><td>✓</td><td>Video</td></tr> <tr><td>4/4</td><td>104</td><td>WLAN4</td><td>✗</td><td>✓</td><td>Voice</td></tr> <tr><td>5/1</td><td>105</td><td>WLAN5</td><td>✗</td><td>✓</td><td>Best Effort</td></tr> <tr><td>5/2</td><td>105</td><td>WLAN5</td><td>✗</td><td>✓</td><td>Background</td></tr> <tr><td>5/3</td><td>105</td><td>WLAN5</td><td>✗</td><td>✓</td><td>Video</td></tr> <tr><td>5/4</td><td>105</td><td>WLAN5</td><td>✗</td><td>✓</td><td>Voice</td></tr> <tr><td>6/1</td><td>106</td><td>WLAN6</td><td>✗</td><td>✓</td><td>Best Effort</td></tr> <tr><td>6/2</td><td>106</td><td>WLAN6</td><td>✗</td><td>✓</td><td>Background</td></tr> <tr><td>6/3</td><td>106</td><td>WLAN6</td><td>✗</td><td>✓</td><td>Video</td></tr> <tr><td>6/4</td><td>106</td><td>WLAN6</td><td>✗</td><td>✓</td><td>Voice</td></tr> </tbody> </table>	Idx	SSID	Description	WLAN enabled	WMM enabled	Access	1/1	voice	voice	✗	✓	Best Effort	1/2	voice	voice	✗	✓	Background	1/3	voice	voice	✗	✓	Video	1/4	voice	voice	✗	✓	Voice	2/1	data	data	✗	✓	Best Effort	2/2	data	data	✗	✓	Background	2/3	data	data	✗	✓	Video	2/4	data	data	✗	✓	Voice	3/1	103	WLAN3	✗	✓	Best Effort	3/2	103	WLAN3	✗	✓	Background	3/3	103	WLAN3	✗	✓	Video	3/4	103	WLAN3	✗	✓	Voice	4/1	104	WLAN4	✗	✓	Best Effort	4/2	104	WLAN4	✗	✓	Background	4/3	104	WLAN4	✗	✓	Video	4/4	104	WLAN4	✗	✓	Voice	5/1	105	WLAN5	✗	✓	Best Effort	5/2	105	WLAN5	✗	✓	Background	5/3	105	WLAN5	✗	✓	Video	5/4	105	WLAN5	✗	✓	Voice	6/1	106	WLAN6	✗	✓	Best Effort	6/2	106	WLAN6	✗	✓	Background	6/3	106	WLAN6	✗	✓	Video	6/4	106	WLAN6	✗	✓	Voice
Idx	SSID	Description	WLAN enabled	WMM enabled	Access																																																																																																																																																		
1/1	voice	voice	✗	✓	Best Effort																																																																																																																																																		
1/2	voice	voice	✗	✓	Background																																																																																																																																																		
1/3	voice	voice	✗	✓	Video																																																																																																																																																		
1/4	voice	voice	✗	✓	Voice																																																																																																																																																		
2/1	data	data	✗	✓	Best Effort																																																																																																																																																		
2/2	data	data	✗	✓	Background																																																																																																																																																		
2/3	data	data	✗	✓	Video																																																																																																																																																		
2/4	data	data	✗	✓	Voice																																																																																																																																																		
3/1	103	WLAN3	✗	✓	Best Effort																																																																																																																																																		
3/2	103	WLAN3	✗	✓	Background																																																																																																																																																		
3/3	103	WLAN3	✗	✓	Video																																																																																																																																																		
3/4	103	WLAN3	✗	✓	Voice																																																																																																																																																		
4/1	104	WLAN4	✗	✓	Best Effort																																																																																																																																																		
4/2	104	WLAN4	✗	✓	Background																																																																																																																																																		
4/3	104	WLAN4	✗	✓	Video																																																																																																																																																		
4/4	104	WLAN4	✗	✓	Voice																																																																																																																																																		
5/1	105	WLAN5	✗	✓	Best Effort																																																																																																																																																		
5/2	105	WLAN5	✗	✓	Background																																																																																																																																																		
5/3	105	WLAN5	✗	✓	Video																																																																																																																																																		
5/4	105	WLAN5	✗	✓	Voice																																																																																																																																																		
6/1	106	WLAN6	✗	✓	Best Effort																																																																																																																																																		
6/2	106	WLAN6	✗	✓	Background																																																																																																																																																		
6/3	106	WLAN6	✗	✓	Video																																																																																																																																																		
6/4	106	WLAN6	✗	✓	Voice																																																																																																																																																		

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 WTWMP1       "1"
SET DOMAIN       "dev4.com"
SET WTSECP1      "5"
SET ENCRYPTP1     "4"
SET EAPYPEP1     "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.	<ol style="list-style-type: none">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:<ul style="list-style-type: none">• Name = 242• Data type = String• Code = 2425. 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).

©2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.