Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Symbol Technologies WS5100 Wireless Switch with Wireless Access Point AP300 Access Port and Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe a solution for supporting wireless voice traffic over an Avaya IP Telephony infrastructure using the Symbol Technologies WS5100 Wireless Switch, and the Symbol Technologies wireless access point AP300 Access Port. Avaya wireless IP Telephones, Avaya IP Softphone, and Avaya Phone Manager Pro gained network access through the Symbol Technologies Access Ports and registered with either Avaya Communication Manager or Avaya IP Office. The Avaya Voice Priority Processor was used to support SpectraLink Voice Priority (SVP) on the Avaya Wireless IP Telephones and the Symbol Technologies Access Points. An Extreme Networks Alpine 3804 Ethernet Switch interconnected all the network devices. Emphasis of the testing was placed on verifying good voice quality on calls associated with the Avaya wireless IP endpoints. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a solution for supporting wireless voice traffic over an Avaya IP Telephony infrastructure using the Symbol Technologies Wireless solution. The Symbol Technologies tested configuration consisted of the Symbol Technologies WS5100 Wireless Switch, Access Point AP300 Access Port, and the Avaya IP Softphone running on Symbol Technologies MC50 Pocket PC. The Symbol Technologies AP300 Access Ports connect the Avaya 3616/3626 Wireless IP Telephones and the Avaya IP Softphone and Phone Manager Pro running on wireless laptops to the wired network through the WS5100 Wireless Switch. This allowed the telephones to register with Avaya Communication Manager or the Avaya IP office. The Avaya Voice Priority Processor was used to support the SpectraLink Voice Priority (SVP) Protocol on the Avaya 3616/3626 Wireless IP Telephones and the Symbol Technologies AP300 Access Ports. An Extreme Networks Alpine 3804 Ethernet Switch was used to interconnect all of the network devices. Emphasis of the testing was placed on verifying good voice quality on calls associated with the Avaya wireless IP endpoints.

The compliance test verified the following features supported by the Symbol Wireless LAN System.

- Layer-2 and Layer-3 Connectivity
- Layer-2 roaming
- 802.1X RADIUS authentication and WEP Encryption
- Quality of Service (QoS) based on Weighted Fair Queuing
- VLANs and 802.1Q Trunking
- SpectraLink Voice Protocol (SVP)
- IEEE 802.11b and 802.11g
- Dynamic IP Addressing using DHCP

1.1. Sample Network Configuration

Figures 1 illustrates the wireless LAN (WLAN) configuration used to verify the Symbol Technologies solution. All of the wireless IP devices depicted in the configuration roamed between the Symbol Technologies AP300 Access Ports for full mobility. Note the IP addresses for the Symbol access points in VLAN 2 are not shown because these access points communicate with the WS5100 Wireless Switch in the same subnet at Layer-2 using MAC addresses only. Symbol Technologies AP300 Access Port currently does not support Layer-3 roaming. Avaya IP Softphone running on Symbol Technologies MC50 Pocket PC was used to place and receive calls from the different telephones.

I

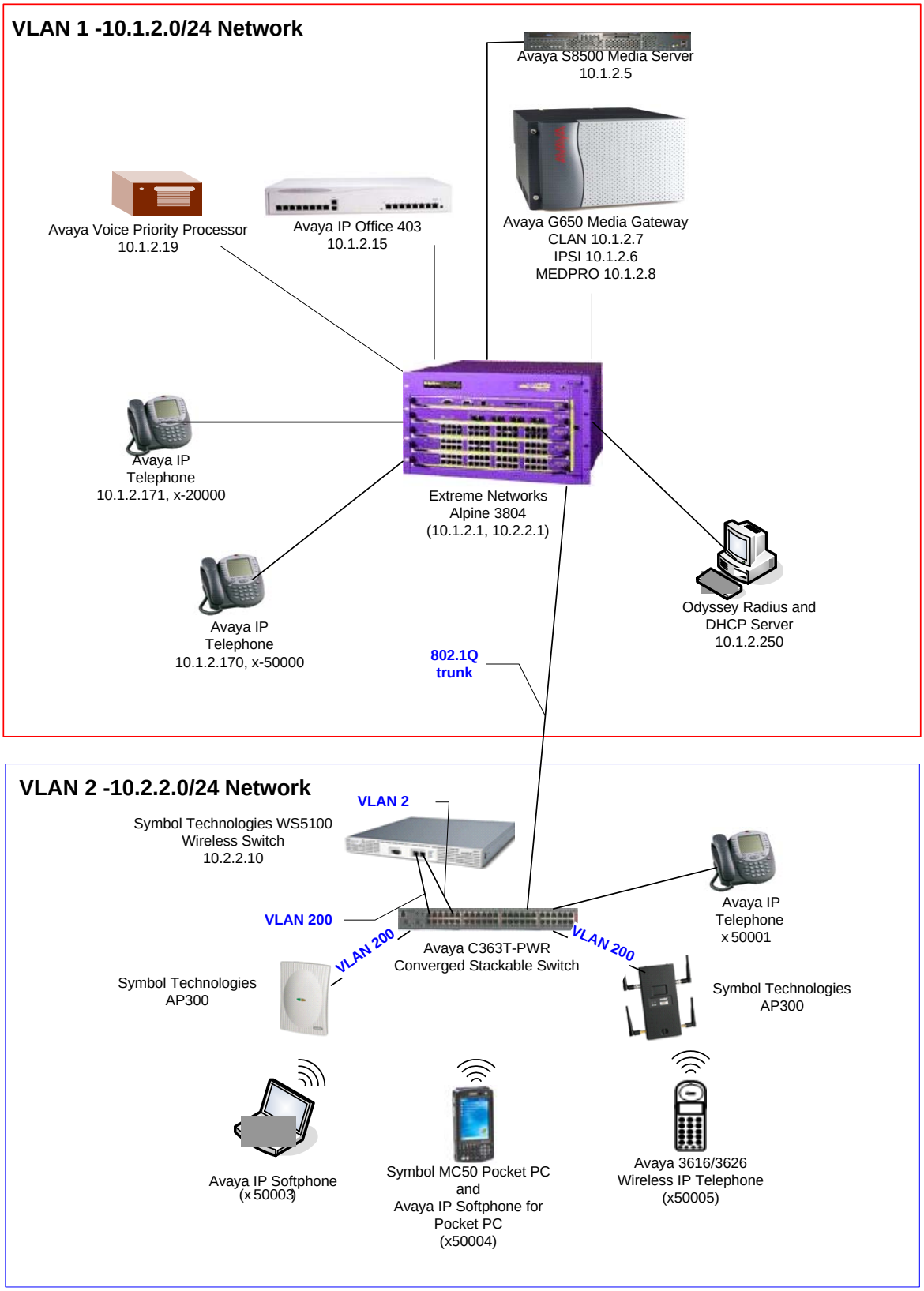


Figure 1: Sample Network Configuration

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8500 Media Server with an Avaya G650 Media Gateway	Avaya Communication Manager 3.0 (R013x.00.0.340.3)
Avaya IP Office 403	3.4(40)
Avaya Voice Priority Processor	33/02
Avaya 4600 Series IP Phones	2.100
Avaya 3616/3626 Wireless IP Telephones	96.040
Extreme Network Alpine 3804 Switch	7.2.0 Build 25
Avaya C363T-PWR Converged Stackable Switch	4.3.12
Avaya IP Softphone	5.2.3.6
Avaya IP Softphone for Pocket PC	Version 3, Load 76
Avaya Phone Manager Pro	3.0.12
Symbol Technologies WS5100 Wireless Switch	1.4.2.0-005R
Symbol Technologies AP 300 Access Ports	0.1.10.0
Symbol Technologies MC50 Pocket PC	Windows Mobile 2003 Second Edition 4.21.1088 (Build 14235.2.0.0)
Odyssey RADIUS Server	2.01.00.653
Funk Odyssey Client	3.03.0.1194

3. Symbol Technologies WS5100 Wireless Switch

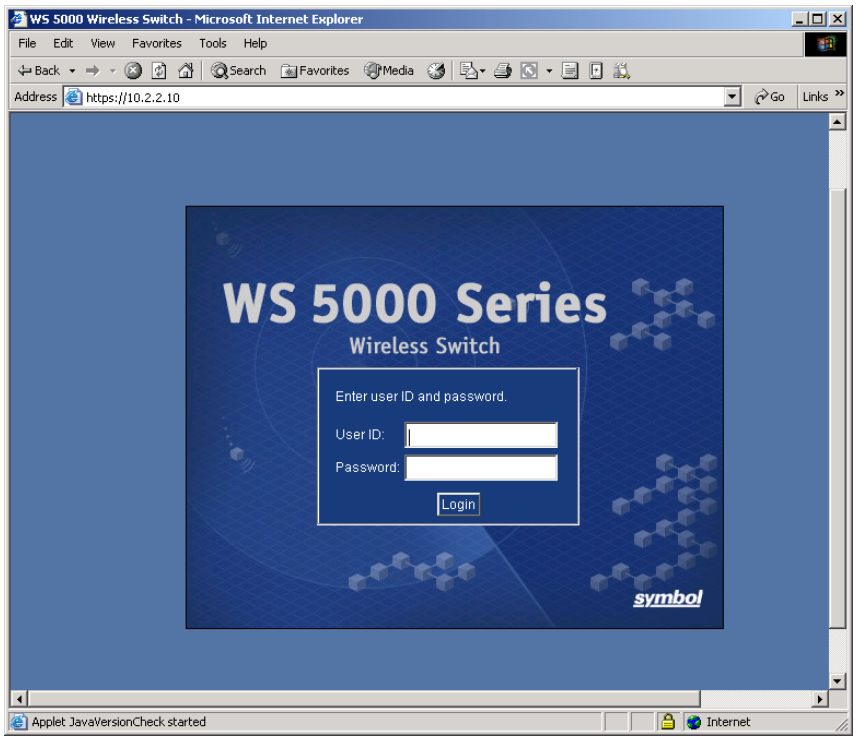
The Symbol WS5100 Wireless Switch bridges together the wireless and wired network. The Symbol WS5100 Wireless Switch has a built-in Network Policy and QoS manager that can classify both upstream traffic (from the wireless network) and downstream traffic (to the wireless network). Based on pre-defined or user configured custom rules and policies, the Wireless Switch applies QoS mechanisms to the classified traffic. The Symbol Technologies AP300 Access Port is managed by the Symbol TechnologiesWS5100 Wireless Switch and does not need to be individually configured.

3.1. Symbol Technologies' Guideline for enabling QoS policy on the Symbol WS5100

Symbol Technologies recommends the following attributes to support Avaya 3616/3626 Wireless IP telephones.

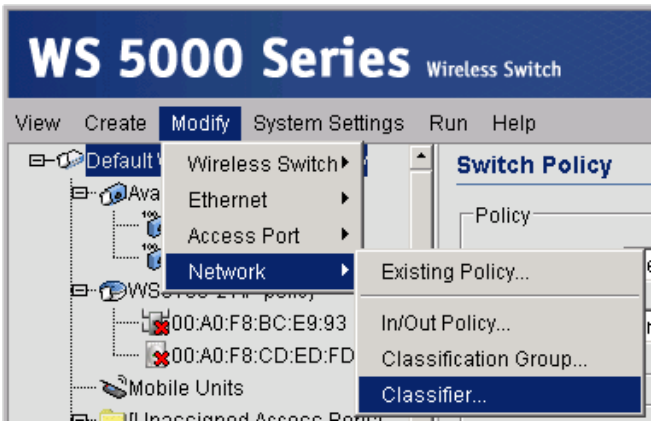
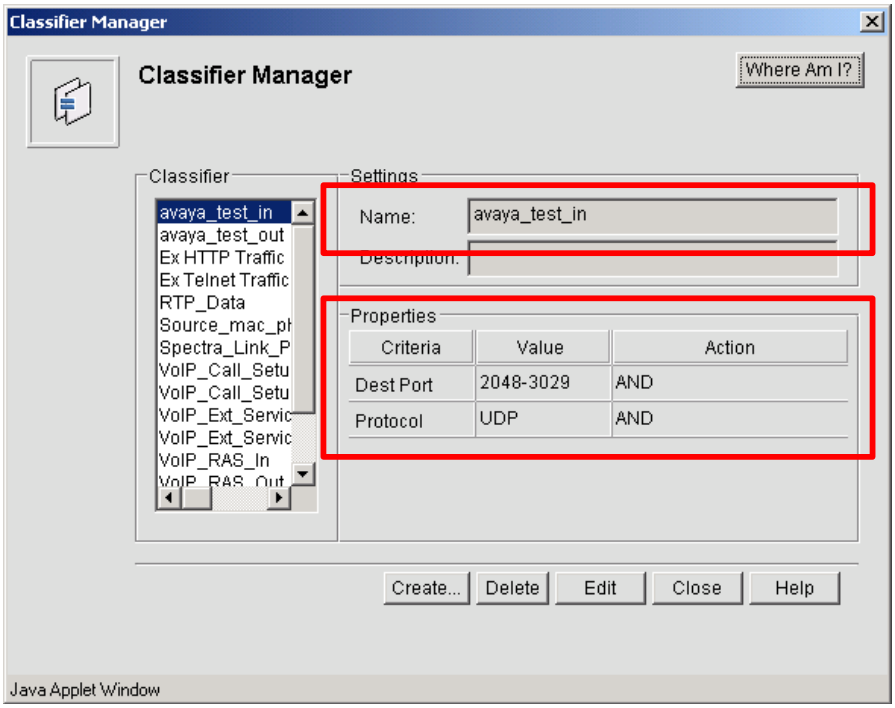
- WS5000 series code 1.4.2.0-005r or later.
- A BSSID (WLAN) exclusively for Avaya 3616/3626 Wireless IP telephone, with at least 70% of the total wireless bandwidth assigned to this voice WLAN.
- DTIM 3
  DTIM or "Delivery Traffic Indication Message"
  A DTIM is sent as part of a beacon by an access port to a client. A client in sleep mode will use this setting to awaken for a packet awaiting delivery.
- RTS 2347(default)
- Outbound network policy applied to the VoIP WLAN specifying
  - Multicast mask 01:00:5e:00:00:00
  - WFQ of at least 70% priority for SpectraLink Voice Priority (SVP)
- Long preamble enabled for Avaya 3616/3626 Wireless IP telephones

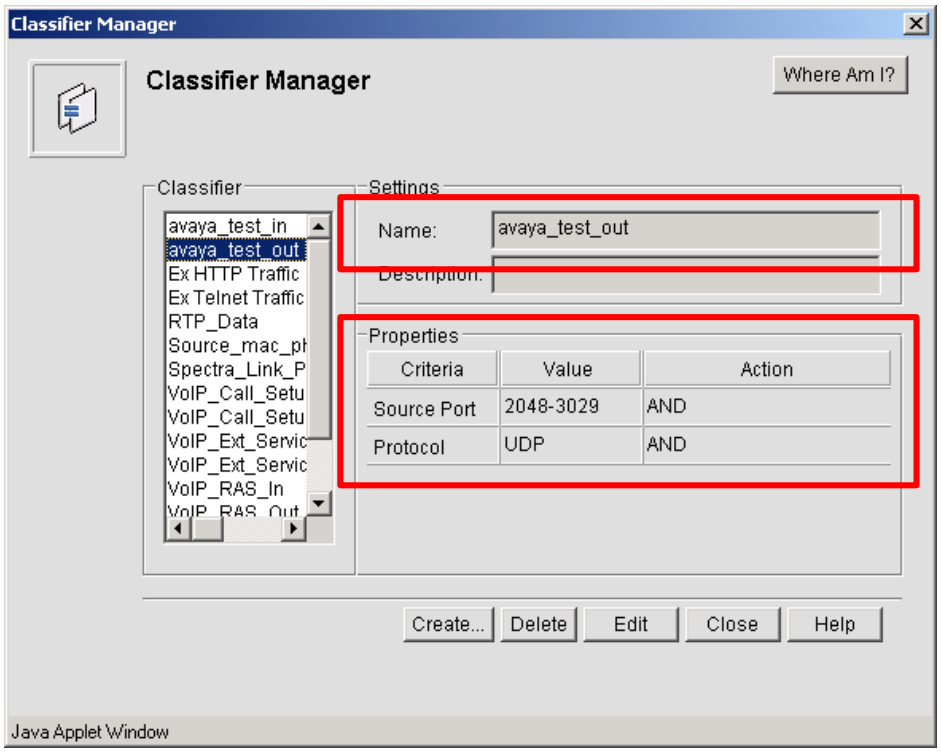
3.2. Accessing Symbol Technologies WS5100 Wireless Switch

Step	Description
1.	Log in to the Symbol Technologies WS5100 Wireless Switch by using in the IP address of the wireless switch on the Web browser, in the format https://x.x.x.x where x.x.x.x is the IP address of the WS5100 Wireless Switch. 

3.2.1. Creating a new Classifier

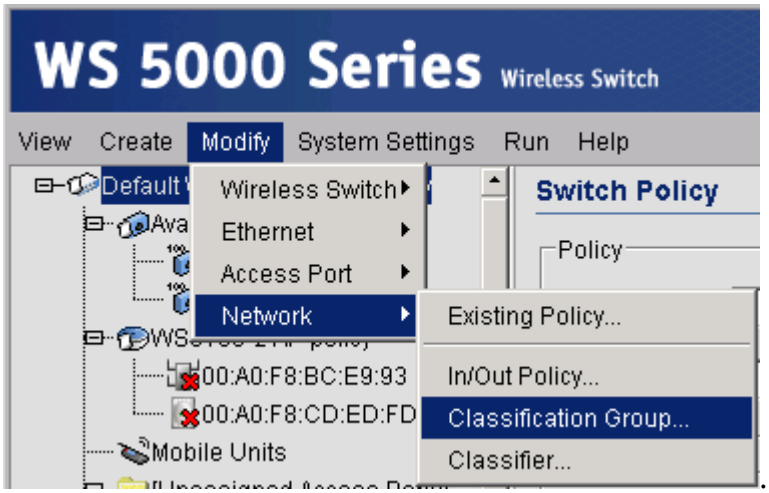
Create two Classifiers, one called "**avaya_test_in**" and the other called "**avaya_test_out**".

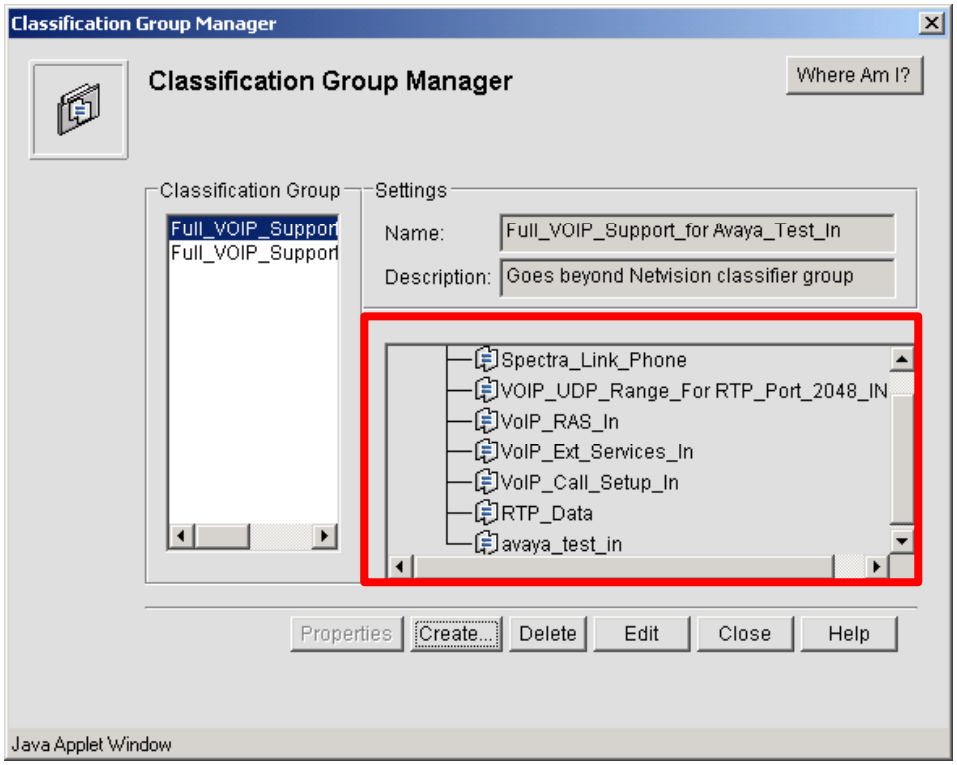
Step	Description
1.	Begin configuration of the Classifier by selecting **Modify → Network → Classifier**. This displays the Classifier Manager. 
2.	Select **Create** and follow the wizard's direction to create a Classifier for inbound VoIP traffic from the Wireless Network. The sample network used the name "**avaya_test_in**" with the UDP port setting as shown highlighted below. The port number is the range of ports used by Avaya Communication Manager for RTP traffic, as configured in the ***ip-network-region*** in section 4.1. 

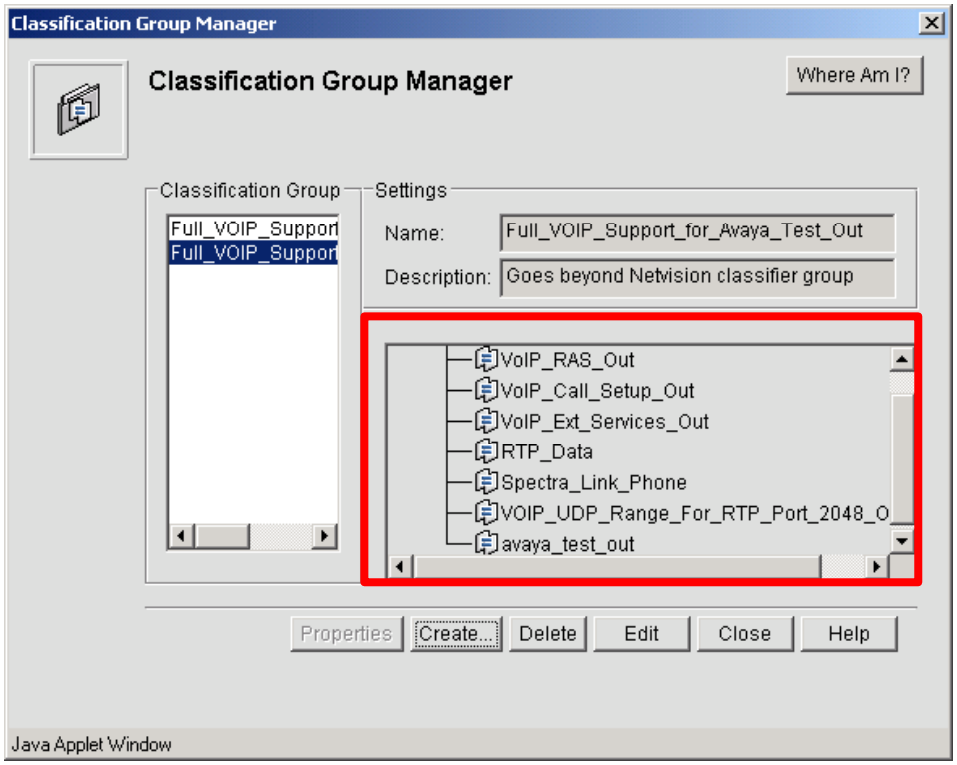
Step	Description
3.	Select **Create** and follow the wizard's direction to create a Classifier for outbound VoIP traffic to the Wireless Network. The sample network used the name "**avaya_test_out**" with the UDP port setting as shown highlighted below. The port number is the range of ports used by Avaya Communication Manager for RTP traffic, as configured in the ***ip-network-region*** in section 4.1. 

3.2.2. Creating a New Classification Group

Create two Classifier Groups, the sample network used "**Full_VOIP_Support_for_Avaya_Test_In**" and "**Full_VOIP_Support_for_Avaya_Test_Out**" for the Classification Group.

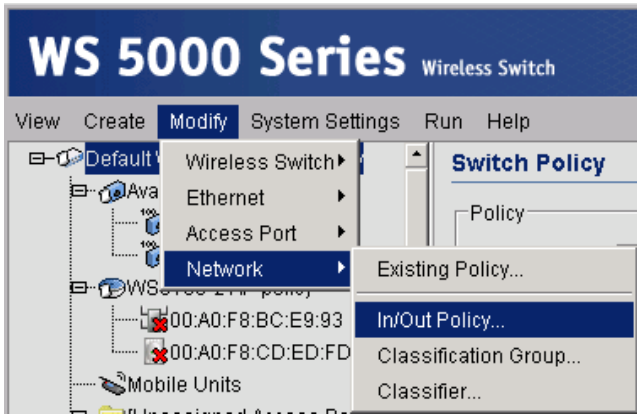
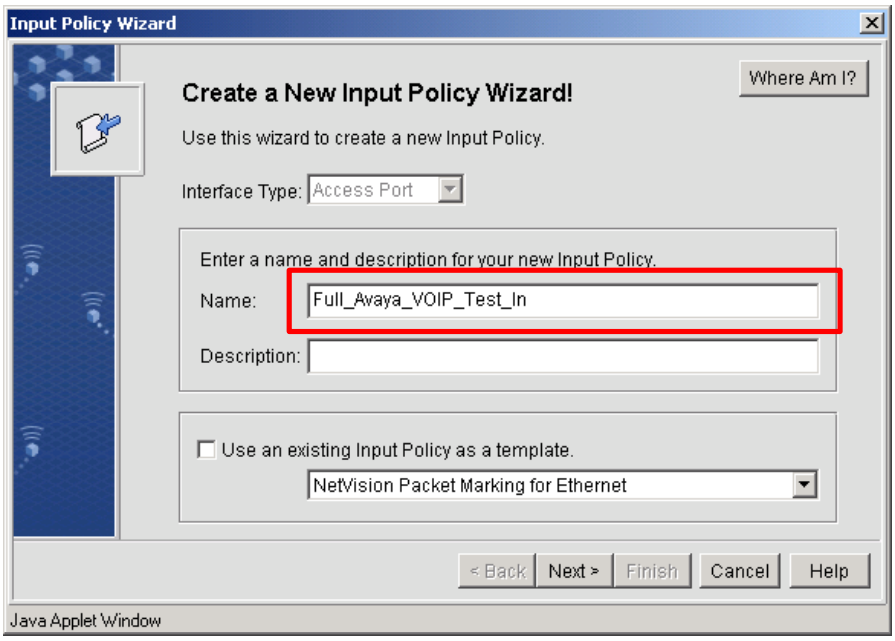
Step	Description
1.	Begin configuration of the Classification Group by select **Modify → Network → Classification Group**. This displays the Classification Group Manager. 

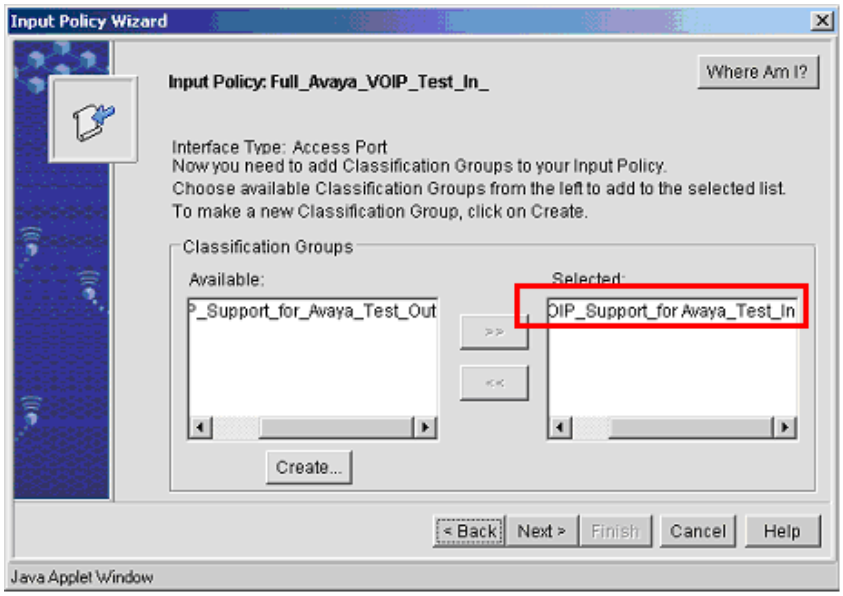
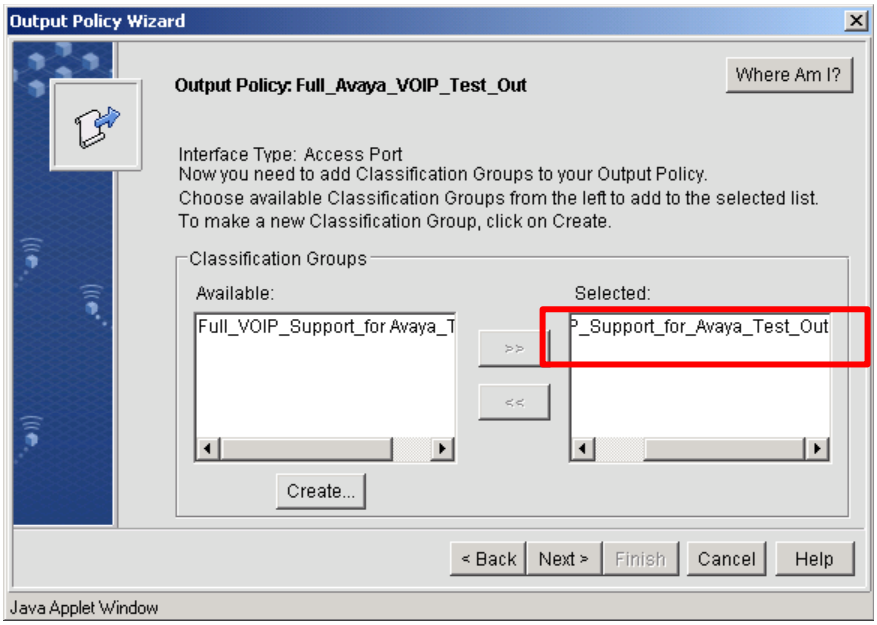
Step	Description
2.	Select **Create** and follow the wizard's direction to create a new Classification Group for upstream VoIP traffic. The sample configuration uses **"Full_VOIP_Support_for_Avaya_Test_In"** as the name for this Classification Group. Make sure to select all the Classifiers listed below. • Spectra_Link_Phone • VOIP_UDP_Range_For RTP_Port 2048_IN • VoIP_RAS_In • VoIP_Ext_Services_In • VoIP_Call_Setup_In • RTP_Data • avaya_test_in The Classifier "avaya_test_in" was created in section 3.2.1. 

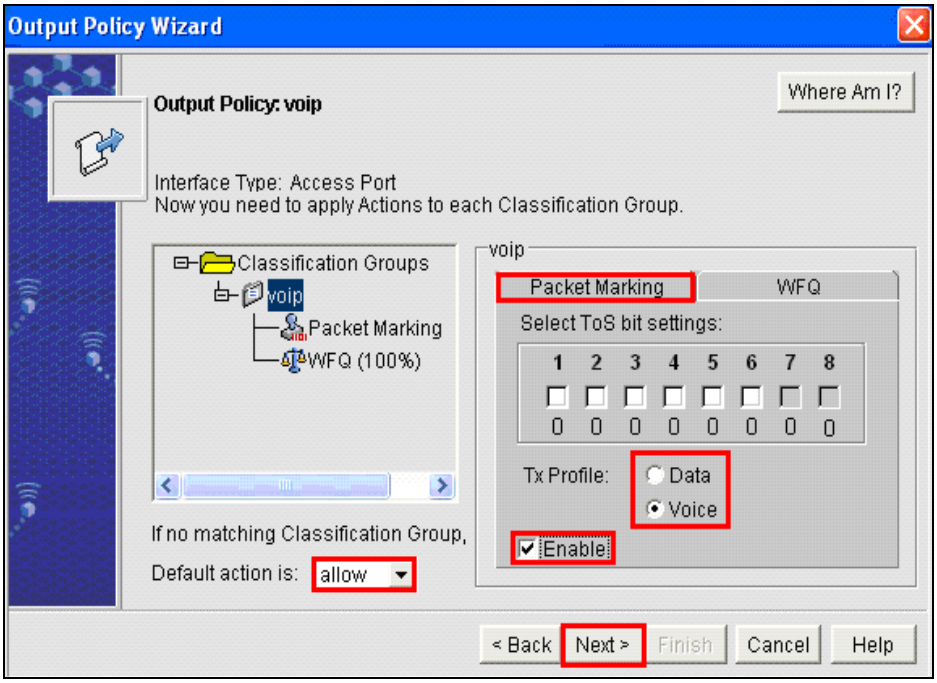
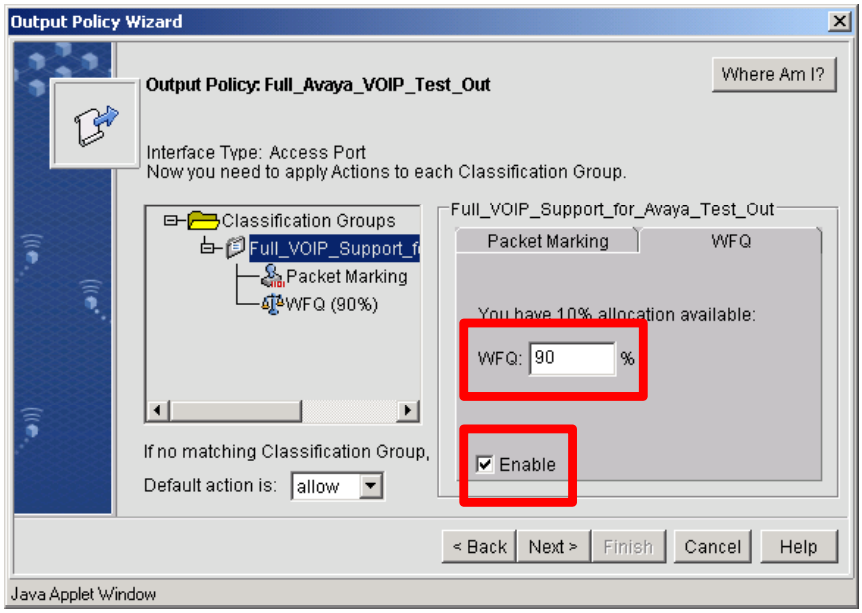
Step	Description
3.	Select **Create** and follow the wizard's direction to create a new Classification Group for downstream VoIP traffic. The sample configuration uses **"Full_VOIP_Support_for_Avaya_Test_Out"** as the name for this Classification Group. Make sure to select all the Classifiers listed below. • VoIP_Ras_Out • VoIP_Call_Setup_Out • VoIP_Ext_Services_Out • RTP_Data • Spectra_Link_Phone • VIP_UDP_Range_For RTP_Port 2048_OUT • avaya_test_out The Classifier "avaya_test_out" was created in section 3.2.1. 

3.2.3. Creating In/Out Policy

Create an In/Out Policy, The sample used the name "**Full_Avaya_VOIP_Test_In**" for the Input Policy and "**Full_Avaya_VOIP_Test_Out**" for the Output Policy. These policies govern the QoS aspect of this sample configuration.

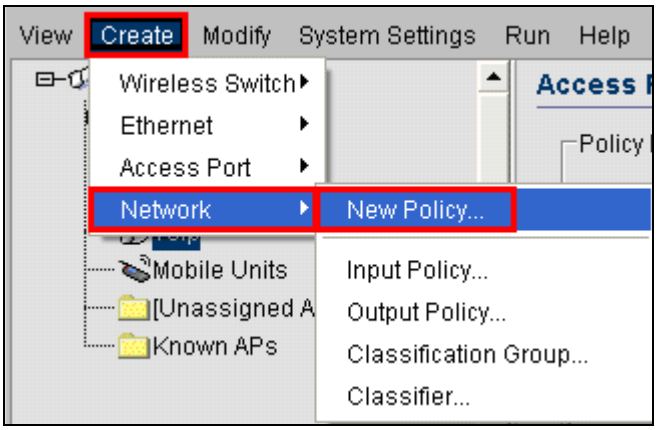
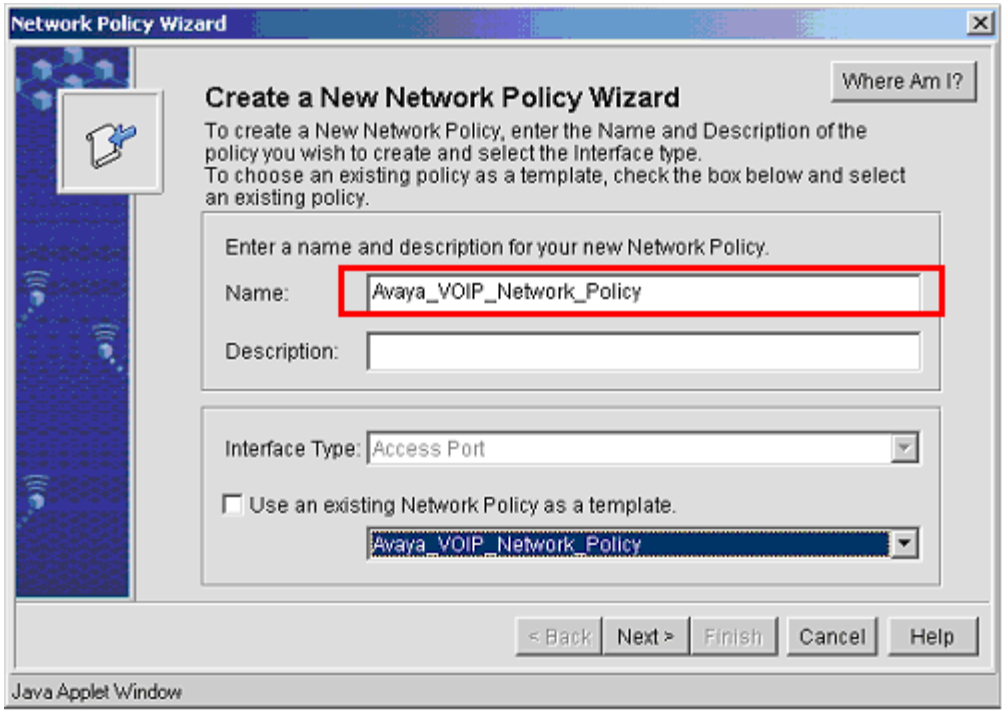
Step	Description
1.	Begin configuration of the In/Out Policy by selecting **Modify → Network → In/Out Policy**. This displays the In/Out Policy Manager. 
2.	Create a New Input Policy "**Full_Avaya_VOIP_Test_In**" by clicking **Create** from the Wizard. Click **Next** to continue. 

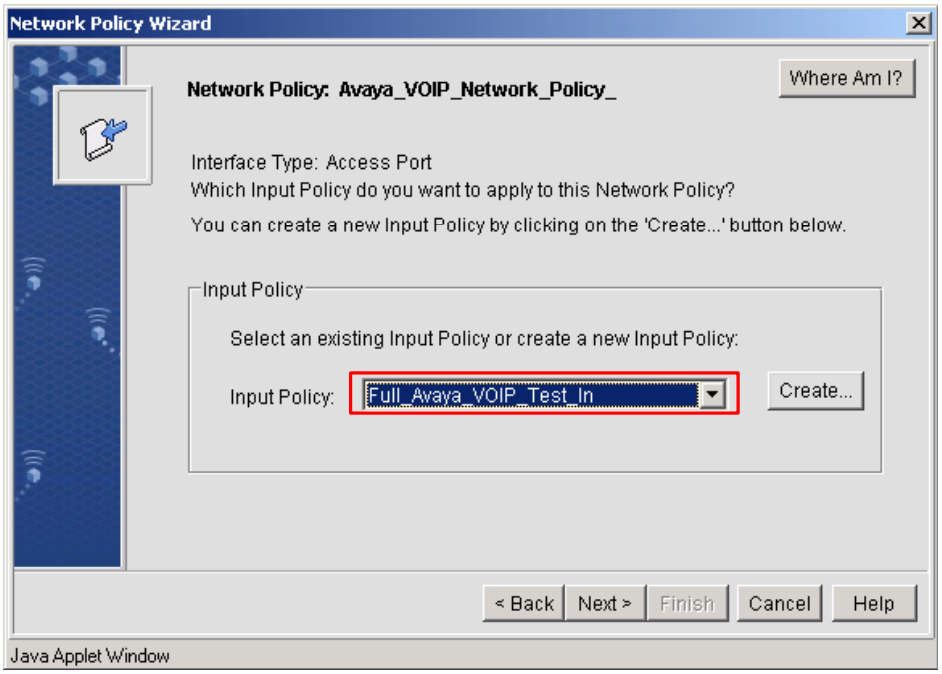
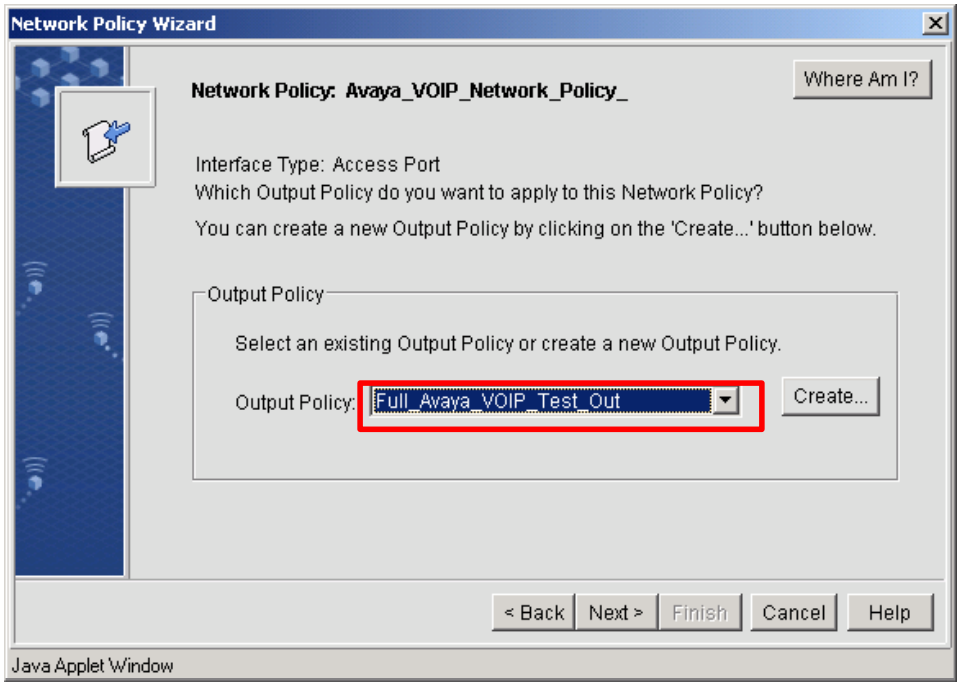
Step	Description
3.	From the "Available:" window on the left, select an appropriate Input Policy, an example is "**Full_VOIP_Support_for Avaya_Test_In**" and click">>**"** on an Input Policy that was created in section 3.2.2-Creating a New Classification Group. Click **Next** to continue. 
4.	From the "Available:" windows on the left, select an appropriate Output Policy, an example is "**Full_VOIP_Support_for Avaya_Test_Out**" and click ">>**"** or an output policy that was created in section 3.2.2-Creating a New Classification Group. Click **Next** to continue. 

Step	Description
5.	Set the Packet Marking tab as shown below to enable QoS. Since Symbol Technologies wireless solution has support for the Spectralink Voice Priority protocol, there is no need to change the ToS bit mapping other than what's shown in the following screen. 
6.	Select the **WFQ** tab as shown below for queuing priority. The sample configuration has WFQ parameter set for 90%. This is a tunable parameter, but Symbol Technologies recommends at least a WFQ setting of at least 70%. 

3.2.4. Creating Network Policy

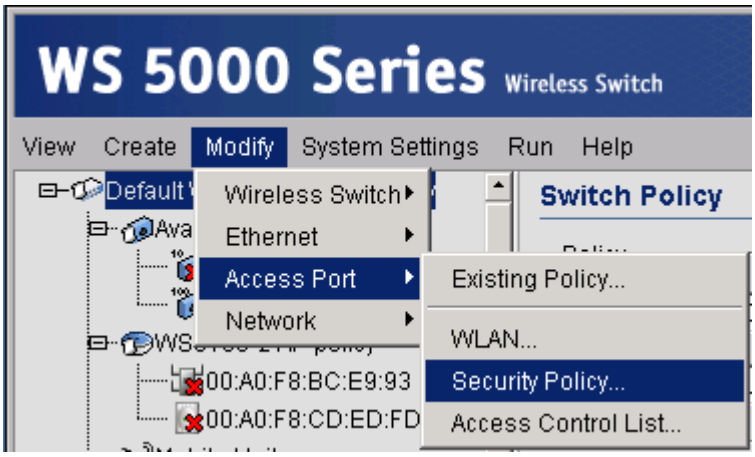
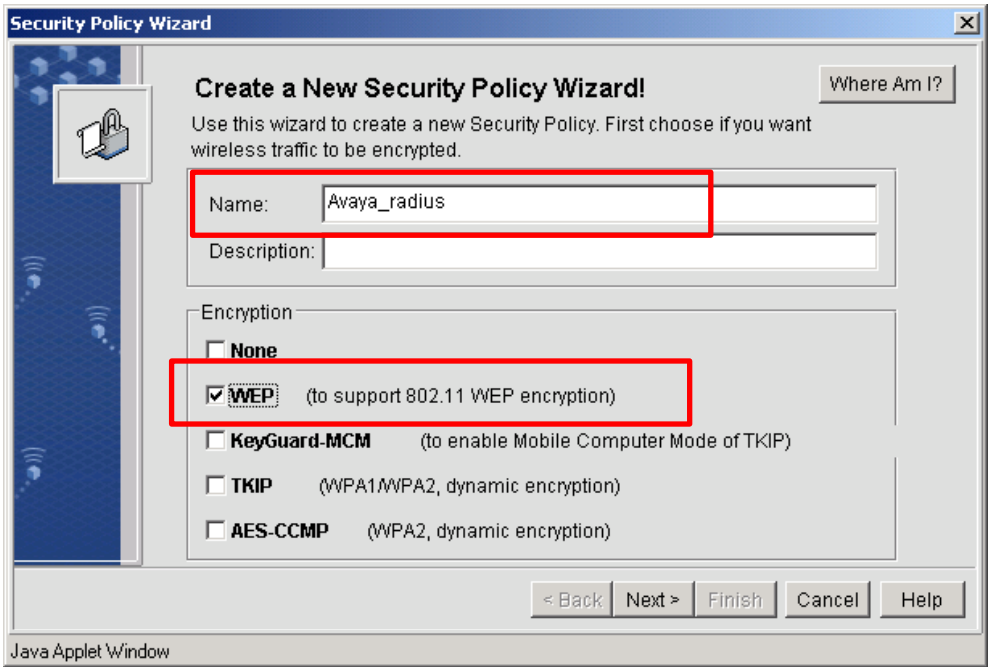
Select **New Policy** to bring up the "Create a New Policy Wizard". Follow the wizard through all the necessary steps to create a policy.

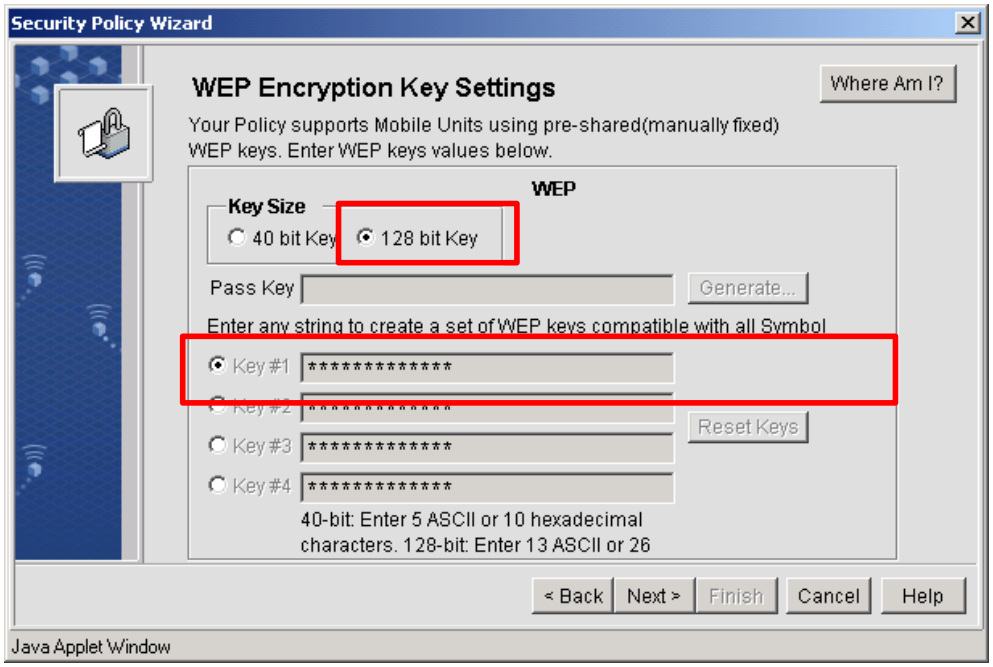
Step	Description
1.	From the main menu bar select **Create → Network → New Policy** 
2.	This will bring up the "Create a New Network Policy Wizard" window. Enter a **Name** and **Description** for the New Policy. Leave all other fields as default. Click **Next** to continue. 

Step	Description
3.	Select the **Input Policy** "**Full_Avaya_VOIP_Test_In**" that was created in section 3.2.3. Click **Next** to continue. 
4.	Select the **Output Policy** "**Full_Avaya_VOIP_Test_Out**" that was created in section 3.2.3. Click **Next** to continue. 

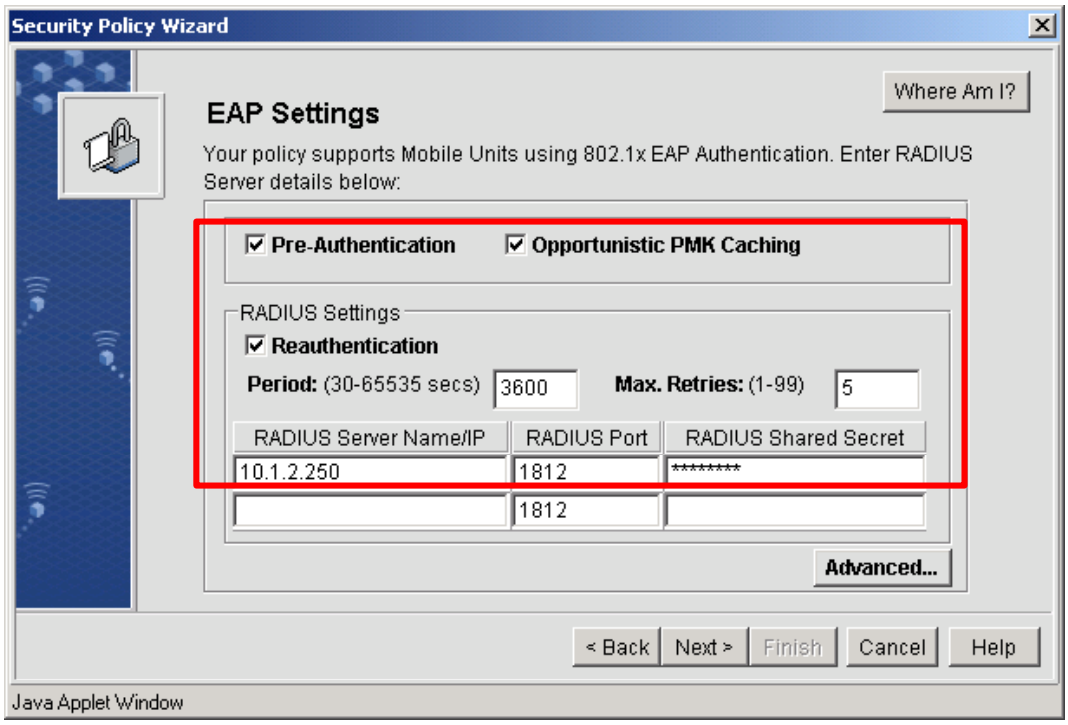
3.2.5. Creating a Security Policy

The Security Policy configures what type of authentication is required from the wireless client to gain access to the wireless network.

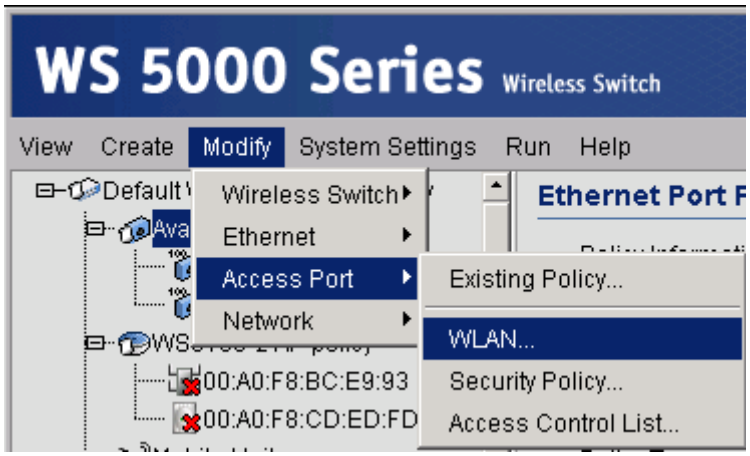
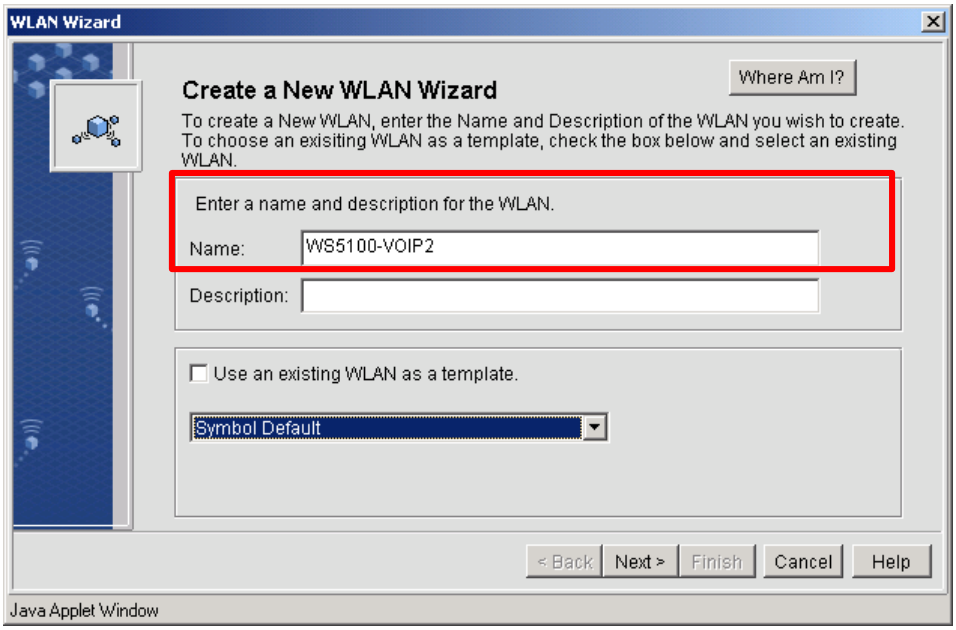
Step	Description
1.	Begin configuration of the Security Policy by selecting **Modify → Access Port → Security Policy**. This displays the Security Policy Wizard. Select **Create** in the Security Policy Wizard to begin configuration. 
2.	Enter a name for the new Security Policy, this example uses "**Avaya_radius**". Check **WEP** encryption for this policy. Click **Next** to continue. 

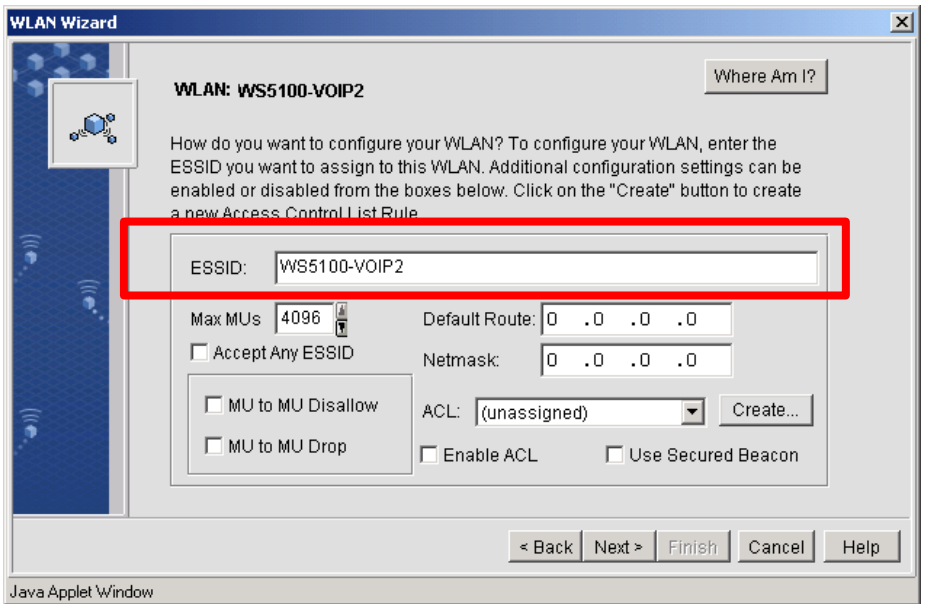
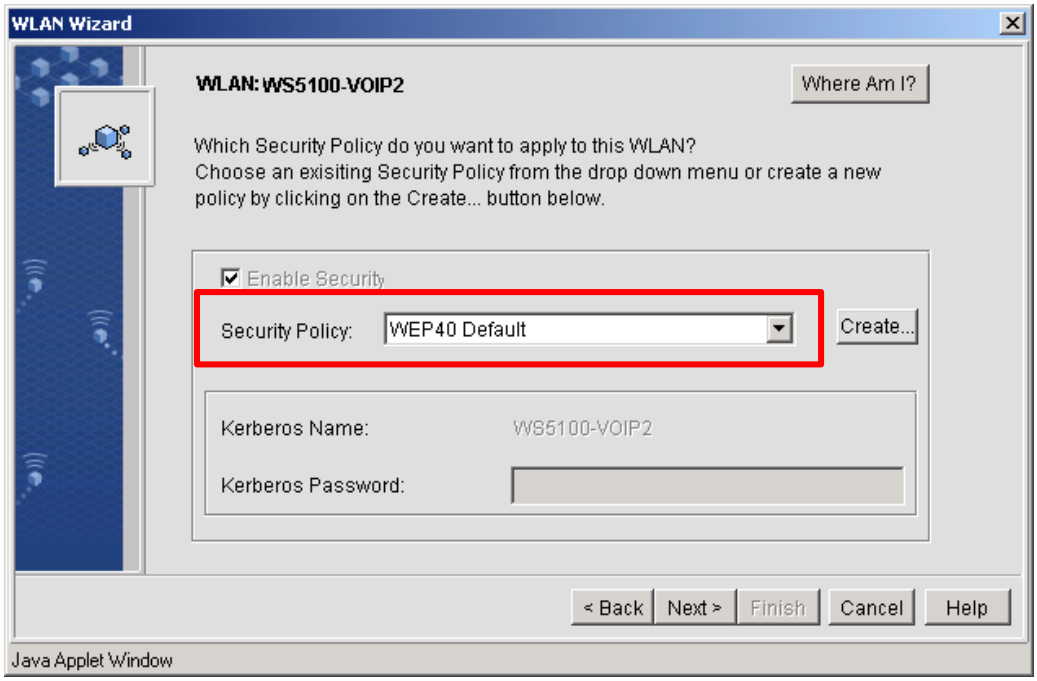
Step	Description
3.	Select "**802.1x EAP**" for authentication. Click **Next** to continue. 
4.	Enter the shared key for the WEP Encryption. Any wireless client accessing this wireless network will need to have this same key entered. Click **Next** to continue. 

Step	Description
5.	Enter the ***IP address*** for the **RADIUS Server Name/IP** that will be performing the authentication, the **RADIUS port** and **RADIUS Shared Secret**. Click **Next** to continue, and **Finish** on the next Window.



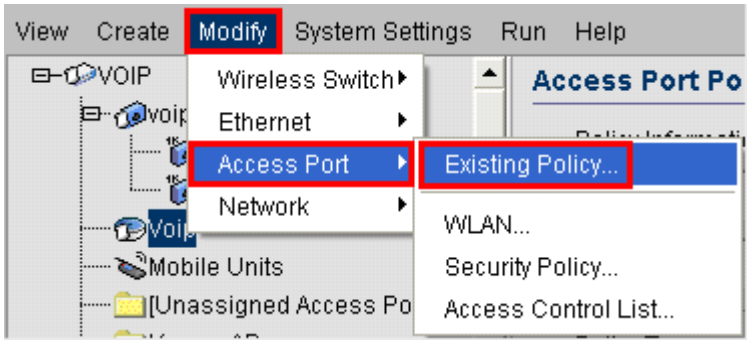
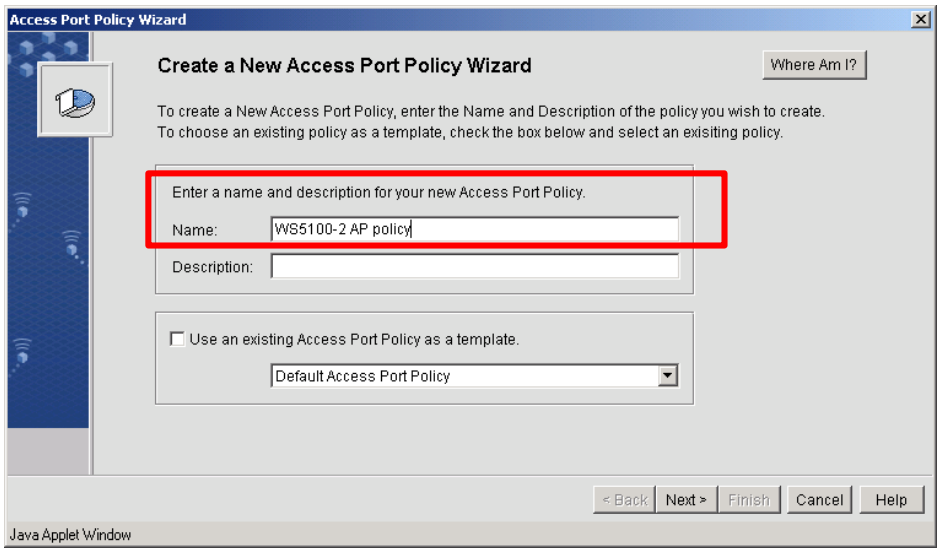
3.2.6. Creating the WLAN

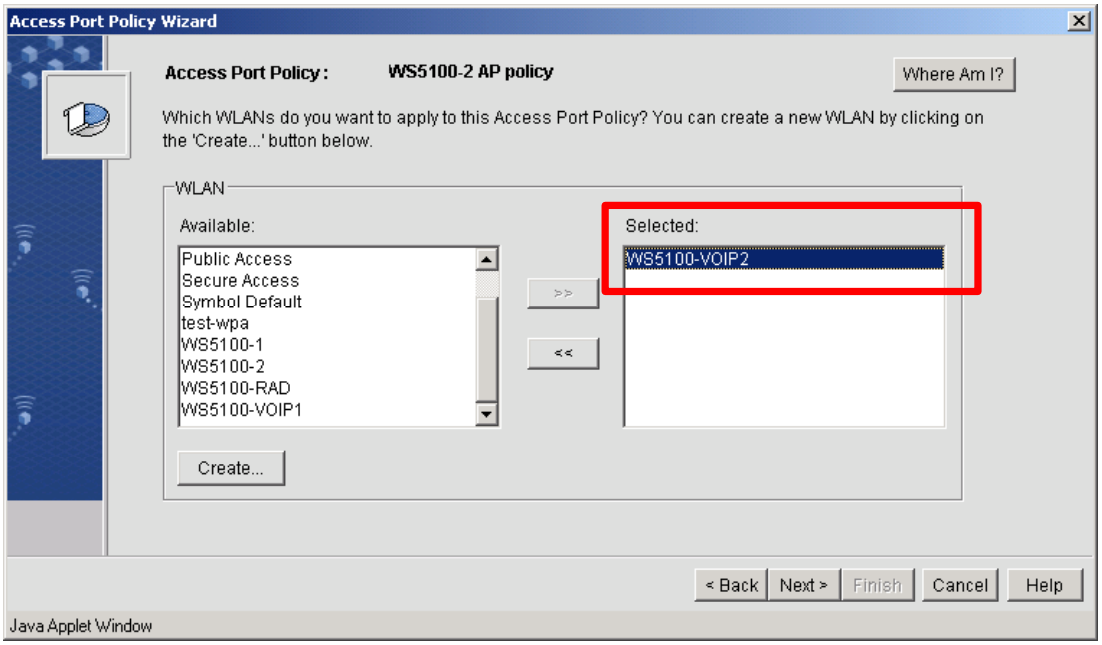
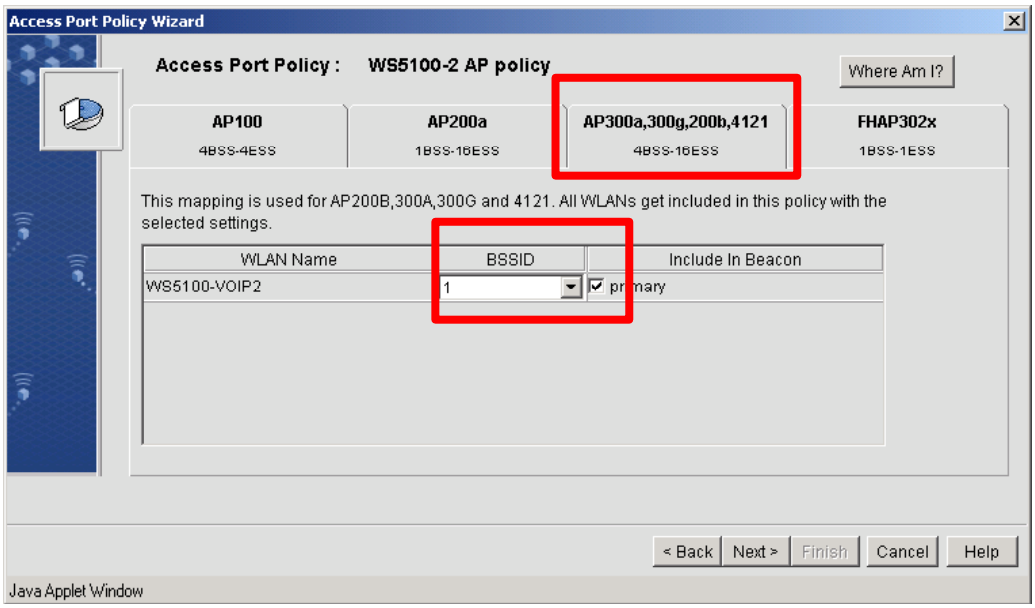
Step	Description
1.	Begin configuration of the WLAN by selecting **Modify → Access Port → WLAN**. This will display the WLAN Manager. 
2.	Follow the WLAN wizard's direction and enter a **Name** for the WLAN. Click **Next** to continue. 

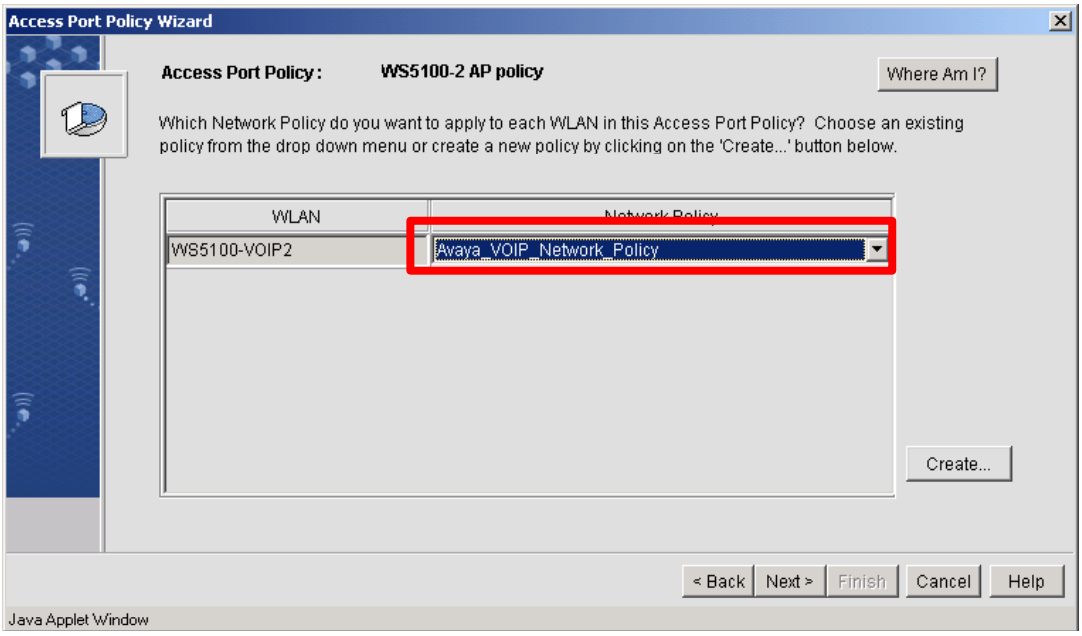
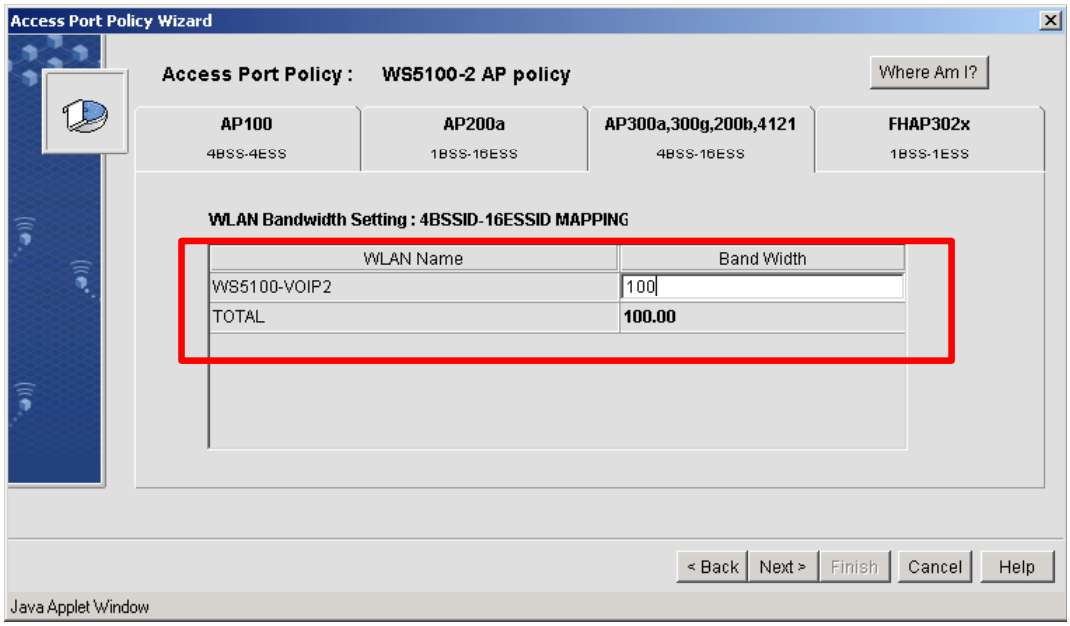
Step	Description
3.	This sample network uses the name "**WS5100-VOIP2**" as the ESSID for this WLAN. Since the sample network does not use any access control list, leave all other fields as default. Click **Next** to continue. 
4.	Select the Security Policy called "***Avaya_radius***" that was created in section 3.2.5 (the default Security Policy shows "WEP40 Default"). Click **Next** to continue, and **Finish** at the next window. 

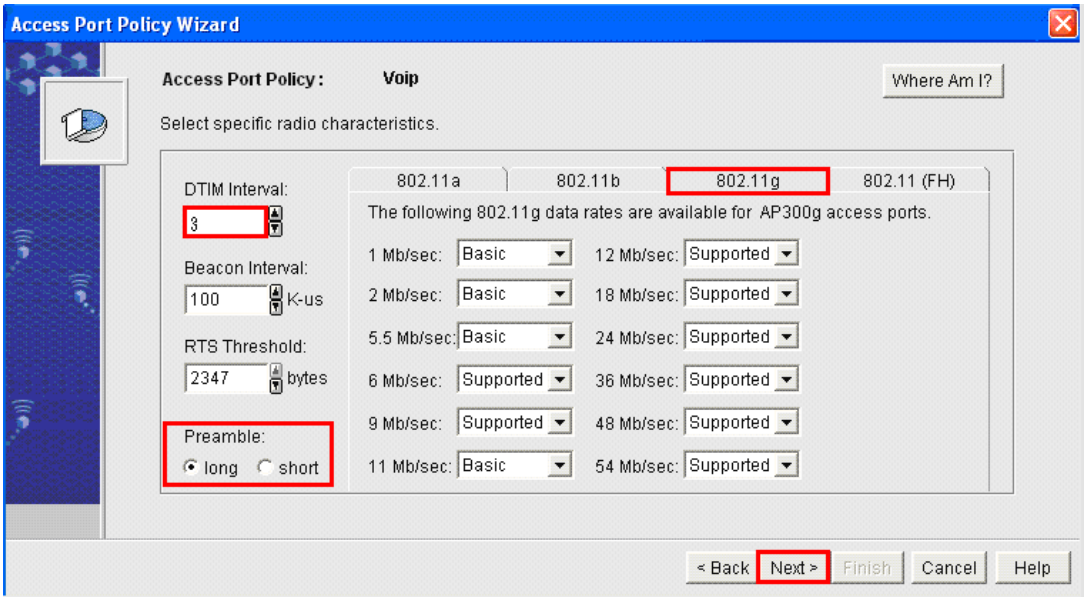
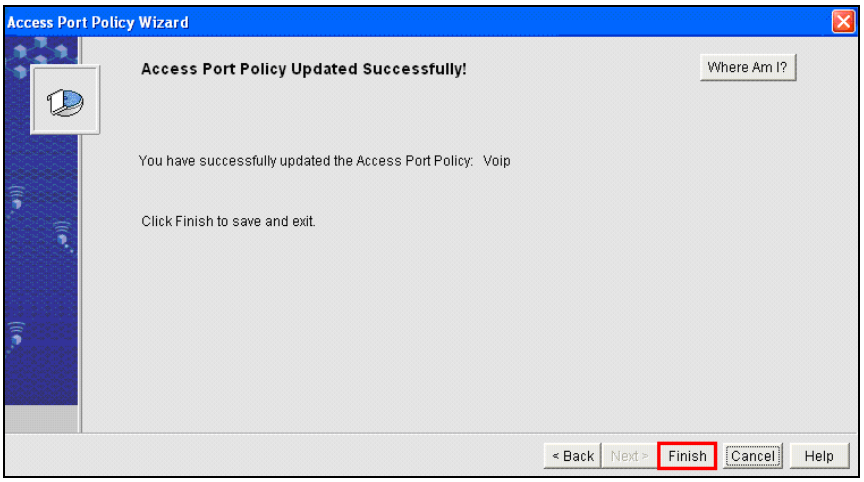
3.2.7. Setting Access Port Policy

This will configure the admission policy for the Symbol Technologies AP300 Access Ports.

Step	Description
1.	Begin configuration of the Access Port Policy by selecting **Modify → Access Port → Existing Policy**. This displays the Access Port Policy Manager. 
2.	Select **Create** to display the Access Port Policy Wizard. Enter a name for the Access Port Policy. The sample network uses the name "**WS5100-2 AP policy**". Click **Next** to continue. 

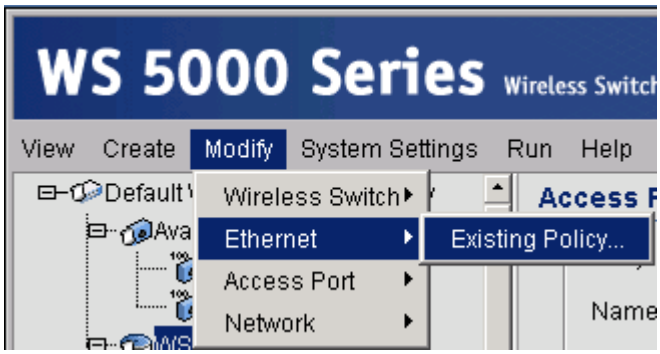
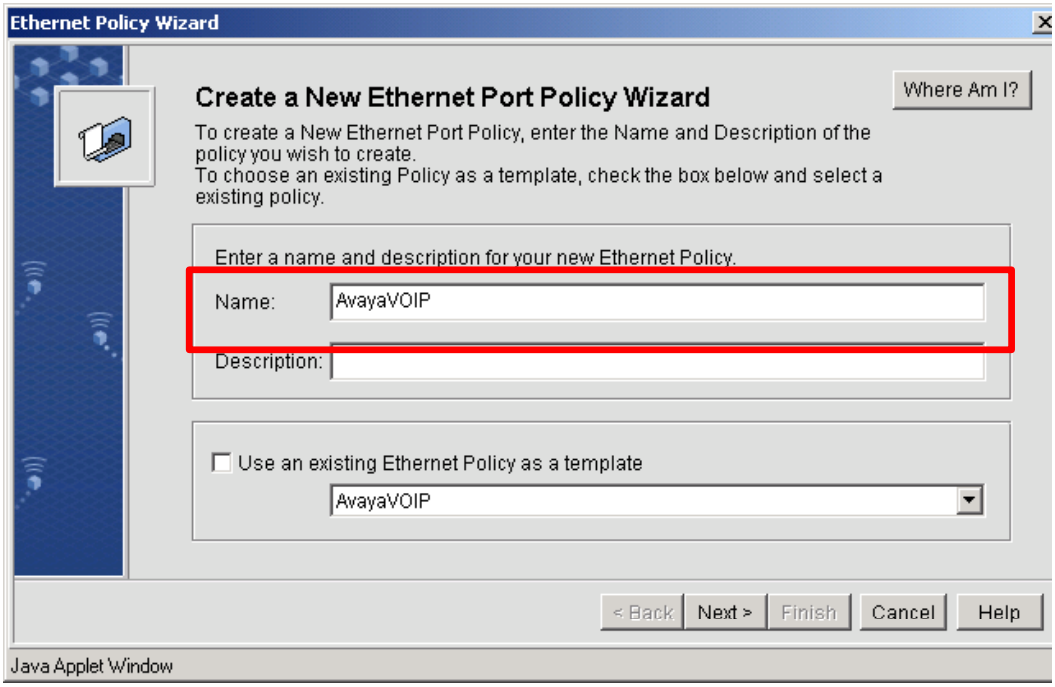
Step	Description
3.	Select the WLAN that will be assigned to the Access Point. Use "**WS5100_VOIP2**" that was created in section 3.2.6. Click **Next** to continue. 
4.	Select the "**AP300a,300g,200b,4121**" tab. Verify the correct WLAN name and BSSID is on this list. The sample network only has one BSSID. Click **Next** to continue. 

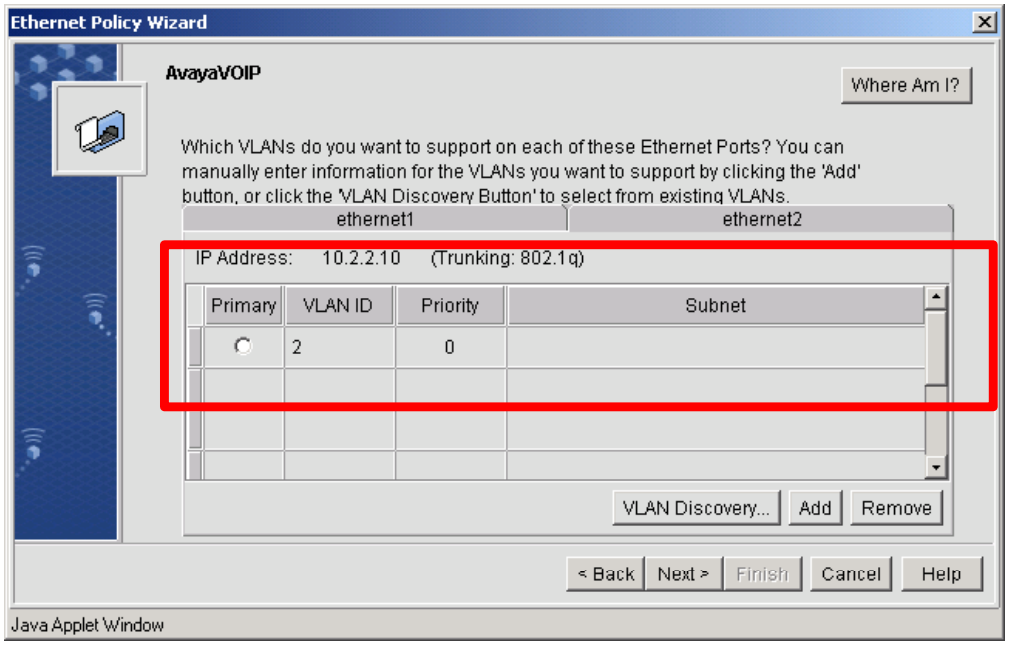
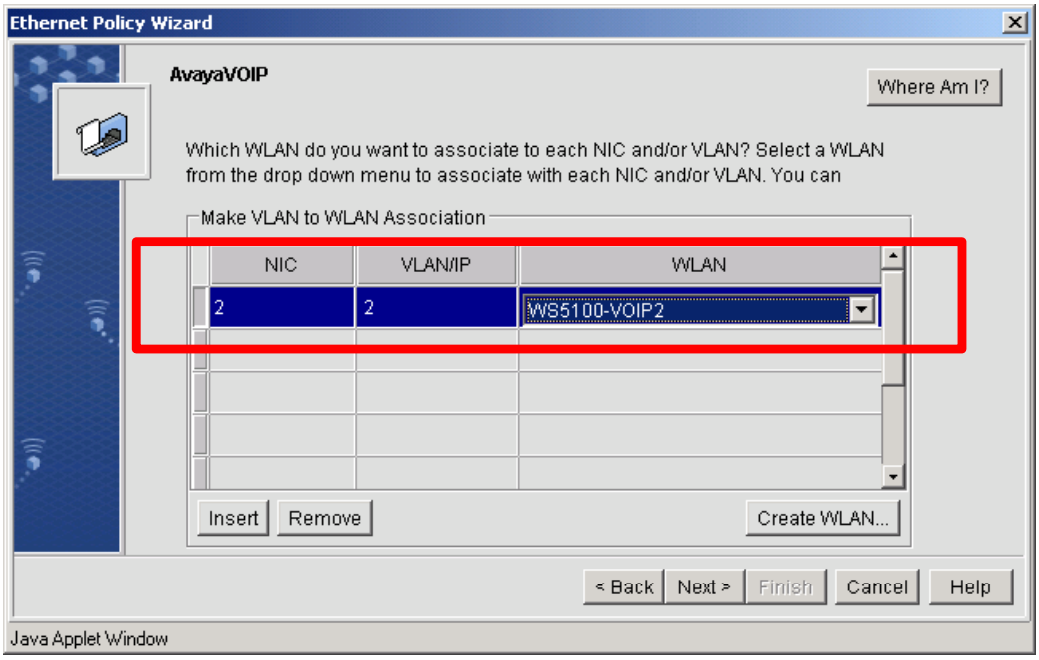
Step	Description
5.	Assign the Network Policy "**Avaya_VOIP_Network_Policy**" that was created in section 3.2.4. Click **Next** to continue. 
6.	Make sure that the appropriate Bandwidth allocation is assigned to this WLAN. Since the sample network only has one WLAN, 100 is assigned. Click **Next** to continue. 

Step	Description
7.	Verify that **DTIM** is set to ***3*** and **Preamble** is ***long***. Leave all other settings at default values. These are Symbol Technologies recommended settings. Click **Next** to continue. 
8.	Click **Finish** to complete the Access Port Policy setting. 

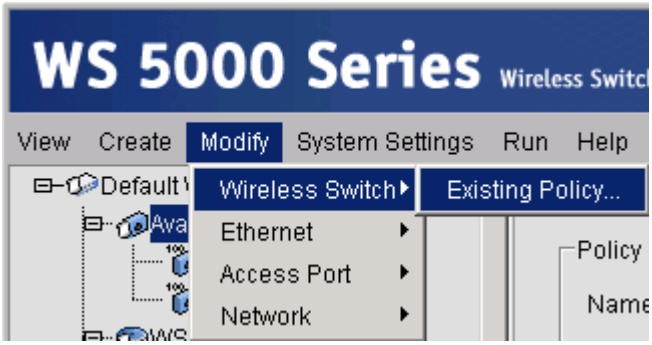
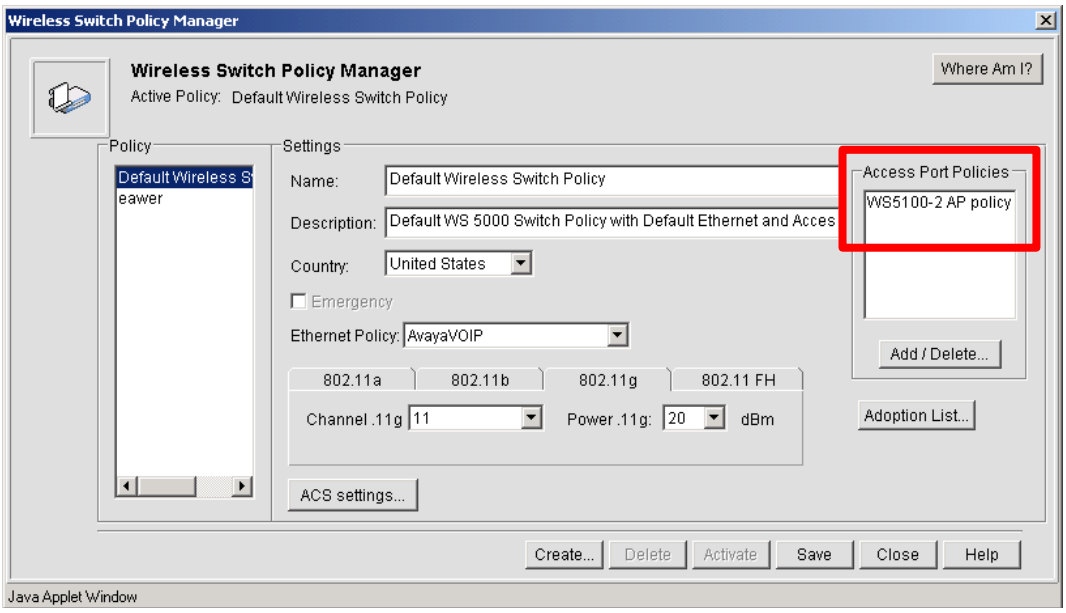
3.3. Setting the Ethernet Policy

This determines the mapping between wireless network and VLAN.

Step	Description
1.	Begin configuration of the Ethernet Policy by selecting **Modify → Ethernet → Existing Policy**. This will display the Ethernet Policy Manager. 
2.	Select **Create** to display the Ethernet Port Policy Wizard. Enter the **Name** for the new Ethernet Policy. Click **Next** to continue. 

Step	Description
3.	Add VLAN 2 to the Ethernet port. This determines what VLAN is supported by the WS5100 Wireless Switch. Click **Next** to continue. 
4.	Select the WLAN for the VLAN. In the sample network, WLAN WS5100-VOIP2's traffic is mapped to VLAN 2 on the wired network. Click **Next** to continue, and **Finish** in the next Window. 

3.4. Setting the Wireless Switch Policy

Step	Description
1.	Begin configuration of the Wireless Switch Policy by selecting **Modify → Wireless Switch → Existing Policy**. This will bring up the Wireless Switch Policy Manager. 
2.	Select the "**Default Wireless Switch Policy**" and add the "**WS5100-2 AP policy**" that was created in section 3.2.7 - Access Port Policy on the right side. Click **Save** to complete Wireless Switch Policy setup. 

4. Configure Avaya Communication Manager

This section highlights the important commands for defining QoS parameter on Avaya Communication Manager. For complete documentation, see Reference[1][2]. Use the Avaya System Access Terminal (SAT) interface to perform these steps. Log in with the appropriate permission.

4.1. Configure VoIP Attributes and QoS

To configure the VoIP attributes for each IP network region, enter **change ip-network-region r**, where **r** is the number of the region.

On Page 1 of the change ip-network-region form, configure the following:

- **Codec Set** – Enter the number of the codec set that will be used in this region.
- **UDP Port Min** – Enter the minimum UDP port for audio portion of the calls.
- **UDP Port Max** – Enter the maximum UDP port for audio portion of the calls.
- **DiffServ/ToS Parameters and 802.1P/Q Parameters** – Enter DSCP and 802.1p values for call control and audio RTP packets originating from the region.
- **Intra-region IP-IP Direct Audio** –***yes***, RTP audio paths may be established directly between IP telephones within the region.
- **Inter-region IP-IP Direct Audio** –***yes***, RTP audio paths may be established directly between an IP telephone within this region and another IP telephone in another region that also has this parameter set to yes. These are also called the **shuffled paths**.

```
change ip-network-region 1                                      Page   1 of  19
                              IP NETWORK REGION

Location:         Authoritative Domain:
                                Intra-region IP-IP Direct Audio: yes
MEDIA PARAMETERS                Inter-region IP-IP Direct Audio: yes
      Codec Set: 1                        IP Audio Hairpinning? y
   UDP Port Min: 2048
   UDP Port Max: 3027                   RTCP Reporting Enabled? y
DIFFSERV/TOS PARAMETERS          RTCP MONITOR SERVER PARAMETERS
 Call Control PHB Value: 34       Use Default Server Parameters? y
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        Audio 802.1p Priority: 6      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                   RSVP Enabled? n
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5. Configure the Avaya C360T-PWR Converged Stackable Switch

The Avaya C360T-PWR Ethernet Switch was configured with 2 Virtual LANs (VLAN), VLAN 2 and VLAN 200. Both of the Symbol Technologies AP300 Access Ports connect to ports belonging to VLAN 200. Port 1/1 on the Avaya C360T-PWR Converged Stackable Switch was configured as an 802.1Q trunk port. Traffic from the Symbol access point travel into the Avaya C360T-PWR Converged Stackable Switch via VLAN 200 and is sent to the WS5100 Wireless Switch via port 1/13. After the WS5100 Wireless Switch applies the appropriate QoS policy, the traffic is then sent back to port 1/2 on the Avaya C360T-PWR Converged Stackable Switch and out through trunk port 1/1 to the Extreme Alpine 3804 switch in the Core Network.

```
C360-1(super)# show trunk
Port   Mode  Binding mode               Native vlan
------ ----- -------------------------- -----------
 1/1   dot1q bound to all vlans            2
 1/2   off   statically bound              2
 1/3   off   statically bound              2
 1/4   off   statically bound              2
 1/5   off   statically bound              2
 1/6   off   statically bound              2
 1/7   off   statically bound              2
 1/8   off   statically bound              2
 1/9   off   statically bound              2
 1/10  off   statically bound              2
 1/11  off   statically bound              2
 1/12  off   statically bound              2
 1/13  off   statically bound              200
 1/14  off   statically bound              200
 1/15  off   statically bound              200
 1/16  off   statically bound              200
 1/17  off   statically bound              200
 1/18  off   statically bound              200
 1/19  off   statically bound              200
 1/20  off   statically bound              200
 1/21  off   statically bound              200
 1/22  off   statically bound              200
 1/23  off   statically bound              200
 1/24  off   statically bound              200
```

5.1. General Test Approach

The general approach was to place calls between the Wired and Wireless telephones registered with Avaya Communication Manager and Avaya IP Office.

- Calls between pairs of Avaya telephones (3616/3626 wireless IP phone – IP Softphone, 3616/3626 wireless IP phone – IP phone, IP Softphone – Phone Manager Pro, IP Softphone – IP phone, Phone Manager Pro – IP phone) can be established through Symbol Technologies wireless solution.
- The solution is valid for different voice codecs (G.711 and G.729).
- Call Shuffling was validated for both the Avaya Communication Manager and the Avaya IP Office.
- Both Wired Equivalent Privacy (WEP) and 802.1x RADIUS for IP Softphone running on a Windows based machine and Symbol Technologies MC50 Pocket PC was tested.
- Voice traffic was tested in the presence of data traffic.

5.2. Test Results

All test cases completed successfully. With the appropriate Network Policy set, Symbol Technologies was able to guarantee bandwidth for all calls up to the amount allocated on the wireless link, regardless of the amount of competing traffic sharing the wireless network. For a congested wireless network, the call quality was noticeably better with the Network Policy enable on the Symbol Technologies Access Point. In addition, the solution was successfully tested with G.711 and G.729 codec and with both call Shuffling enabled and disabled. WEP encryption was successfully tested against the Avaya 3616/3626 wireless IP telephones, Avaya IP Softphone, and Symbol Technologies MC50 Pocket PC. Separately, 802.1x EAP and RADIUS authentication were also successfully tested against the Symbol Technologies MC50 Pocket PC and Avaya IP Softphone.

6. Verification Steps

The following steps may be used to verify the configuration:

- Verify that calls can be completed across the wireless network with acceptable voice quality.
- On the Symbol Technologies Web User Interface, verify the appropriate Network Policy is implemented with the correct Output Policy and Weighted Fair Queue information. It may be necessary to exit from the web browser and log into the Symbol Technologies WS5100 Wireless Switch again to verify all the policies were implemented.
- Verify correct port setting is implemented for VLAN and 802.1 Q Trunking support.

7. Support

For technical support on the Symbol Technologies product line, consult
http://www.symbol.com/services/online_support/online_support.html

United States and Canada: 631 738 6213 or 1 800 653 5350
For international callers outside the US: 001 631 738 6213
South America: +55 11 4133 3180
Europe, the Middle East and Africa: +420 533 336 123
Australia: +613 986 270 79 or 1 800 672 906
Asia Pacific: +65 679 69 500

8. Conclusion

These Application Notes illustrated the steps necessary for configuring the Symbol Technologies WS5100 Wireless Switch to guarantee wireless network access for VoIP traffic generated by Avaya Media Servers, Avaya Media Gateways, Avaya wireless IP telephones and Avaya IP Softphone. With the appropriate QoS setting on the Symbol Technologies Wireless Switch WS5100 solution, quality and access for VoIP telephone calls from wireless end-point were ensured regardless of the amount of non-VoIP traffic sharing the network.

9. Additional References

[1] Administrator Guide for Avaya Communication Manager, Doc # 03-300509, Issue 1, June 2005
[2] Avaya Communication Manager Advanced Administration Quick Reference, Doc # 03-300364, Issue 2, June 2005 Release 3.0

Product documentation for Avaya products may be found at
http://support.avaya.com

Product documentation for Symbol products may be found at
http://www.symbol.com/products/wireless/wireless.html

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 Developer*Connection* Program at devconnect@avaya.com.