Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Extreme Networks Wireless LAN Solutions for Avaya IP Telephony Infrastructure - Issue 1.0

Abstract

These Application Notes describe a solution for supporting wireless voice traffic over an Avaya IP Telephony infrastructure using Extreme Networks Wireless LAN Solutions consisting of a WLAN Switch managing multiple Extreme Networks' Access Points. Avaya Wireless IP Telephones, IP Softphone, and Phone Manager Pro gained network access through the Extreme Networks Access Points 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 3616/3626 Wireless IP Telephones. An Extreme Networks BlackDiamond 8810 Switch, and Extreme Networks 300-48 Unified Access Switch interconnected all of the network devices. Emphasis 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 Extreme Networks Wireless LAN System consisting of the Summit WM100 WLAN Switch or Summit WM1000 WLAN Switch managing multiple Altitude 350-2 Access Points. The Extreme Networks Summit WM100 WLAN Switch, Summit WM1000 WLAN Switch and the Altitude 350-2 (Detachable) Access Point were used for the testing. The Extreme Networks Altitude 350-2 (Detachable) Access Points connected the Avaya 3616/3626 Wireless IP Telephones and the Avaya IP Softphone and Phone Manager Pro running on wireless laptops to the wired network and allowed these applications to register with either Avaya Communication Manager or 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 Extreme Networks Altitude 350-2 Access Points. An Extreme Networks BlackDiamond 8810 Switch and Summit 300-48 Unified Access Switch were 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.

All Extreme Networks Altitude 350-2 (Detachable) Access Points used in the sample configuration obtain their IP address via a DHCP Server. Using Service Location Profile (DHCP Scope option 78), the Extreme Networks Altitude 350-2 (Detachable) Access Points registered with the Extreme Networks WM100/WM1000 WLAN Switch automatically upon power up. The Extreme Networks WM100/WM1000 WLAN Switch serves as the focal point in bridging the wireless and the wired network's traffic and in managing the Extreme Networks Altitude 350-2 (Detachable) Access Points.

The Extreme Networks wireless solution supports the concept of "WM Access Domain". A unique SSID and a wireless IP network define each WM Access Domain. This WM Access Domain is different than and in addition to the IP Networks that exist in the wired network. The sample configuration has three WM Access Domains: Avaya-ACM, Avaya-Data, and Avaya-RAD. Wireless clients register to a wireless IP network based on the WM Access Domain and receive IP address information from the DHCP server. The Extreme Networks Altitude 350-2 (Detachable) Access Points can be configured to give priority to any of the WM Access Domains. Traffic from different WM Access Domains is tunneled through the wired network established between the Extreme Networks Altitude 350-2 (Detachable) Access Points and the Extreme Networks WM100/WM1000 WLAN Switch. DiffServ information in the encapsulating envelope preserves the priority of the tunneled traffic. The Extreme Networks WM100/WM1000 WLAN Switch serves as the default gateway for all WM Access Domains and forwards wireless clients' traffic.

Traffic flow in the reverse direction is conducted in a similar manner. Static routes in the router direct traffic destined to a wireless client to the Extreme Networks WM100/WM1000 WLAN Switch. Traffic enters the tunnel that terminates at the Access Point where the wireless client is associated. The Access Point then sends the traffic to the wireless client based on predefined priority.

The compliance test verified the following features supported by the Extreme Networks Wireless LAN Solutions:

- Layer-2 and Layer-3 Connectivity
- 802.1x Security
- WEP and WPA-PSK Encryption
- Quality of Service (QoS) based on Priority Queuing
- VLANs and 802.1Q Trunking
- Layer-2 and Layer-3 Seamless Roaming
- SpectraLink Voice Protocol (SVP)
- IEEE 802.11b and g
- Dynamic IP Addressing using DHCP

Figure 1 illustrates the wireless LAN (WLAN) configuration used to verify the Extreme Networks Wireless Solutions. All of the wireless IP devices depicted in the configuration roamed among the Extreme Networks Altitude 350-2 (Detachable) Access Points for full mobility. The wireless clients and the Extreme Networks Altitude 350-2 (Detachable) Access Points obtained their IP address from the DHCP Server. Telephones with extension 2xxxx are registered with the Avaya IP Office and Telephones with extension 5xxxx are registered with the Avaya Communication Manager.

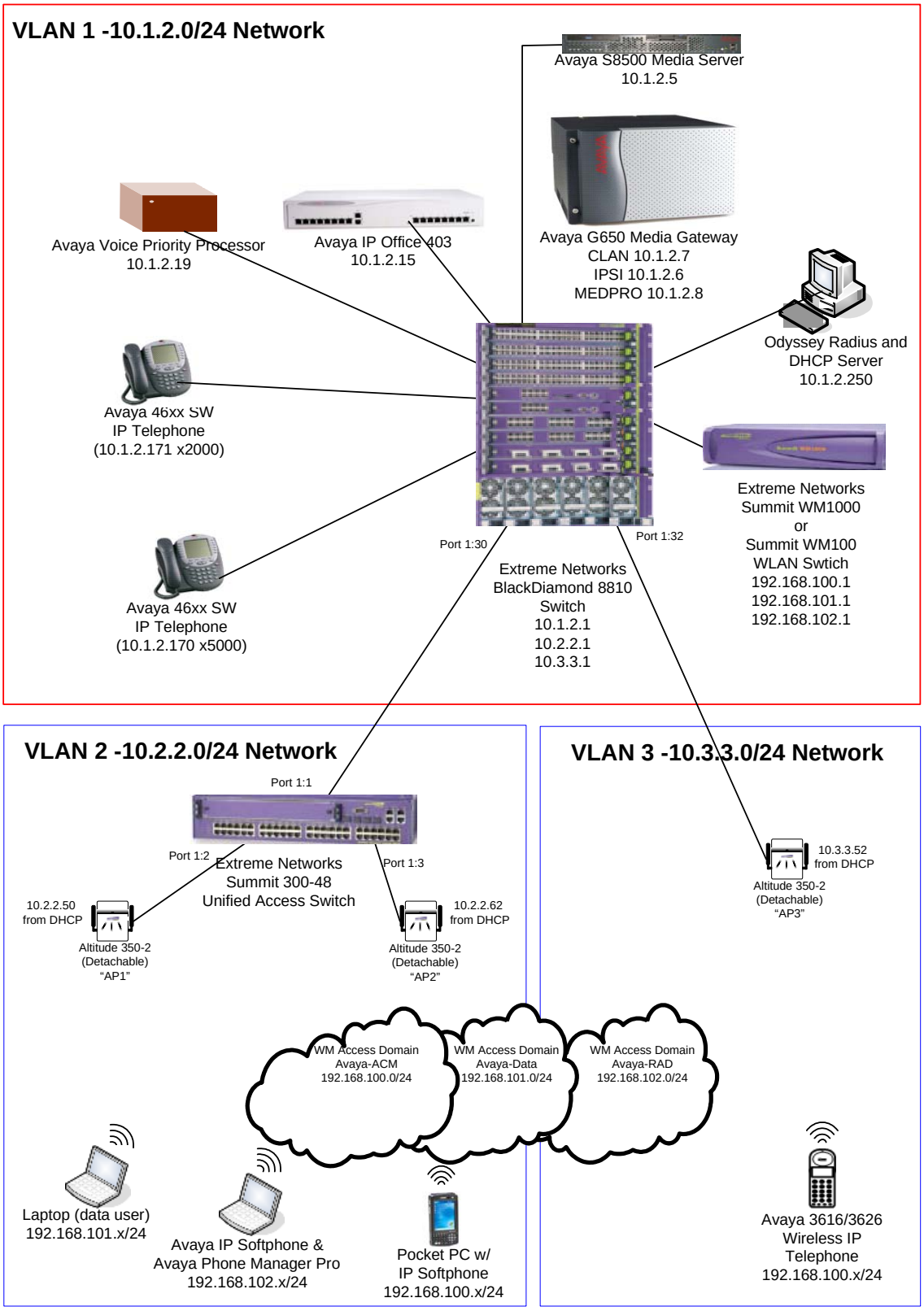


Figure 1: Avaya and Extreme Networks Wireless LAN Configuration

2. Equipment and Software Validated

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

Equipment	Software
Avaya S8500 Media Server with Avaya G650 Media Gateway	Avaya Communication Manager 3.0 (R013x.00.0.340.3)
Avaya IP Office 403	3.1(29)
Avaya Voice Priority Processor	33/02
Avaya 4602SW IP Telephones	2.100
Avaya 3616/3626 IP Wireless Telephones	96.040
Avaya IP Softphone	5.2
Avaya IP Softphone for Pocket PC	2.3
Avaya Phone Manager Pro	3.0.12
Extreme Networks BlackDiamond 8810 Switch	XOS version 11.2.2.3 v1122b3
Extreme Networks Summit 300-48 Unified Access Switch	7.4e.1.5
Extreme Networks Summit WM100 WLAN Switch	Rel1.0 (1.0.2.01.03)
Extreme Networks Summit WM1000 WLAN Switch	Rel1.0 (1.0.2.01.03)
Extreme Networks Altitude 350-2 Detachable	N/A
Funk Odyssey Radius Server	2.01.00.653
Funk Odyssey Client	3.03.0.119

3. Configure the Avaya Voice Priority Processor

The Avaya Voice Priority Processor utilizes SpectraLink Voice Priority (SVP) as the Quality of Service (QoS) mechanism supported by the Avaya 3616/3626 Wireless IP Telephones to reduce jitter and delay for voice traffic over the wireless network.

The Avaya Voice Priority Processor is required to serve as a “gateway” between the Avaya 3616/3626 Wireless IP Telephones and the Avaya IP Telephony infrastructure. Voice traffic from Avaya wireless telephones are directed to the Avaya Voice Priority Processor so that the SVP header information can be removed before the packets are forwarded to Avaya Communication Manager.

All Avaya 3616/3626 Wireless IP Telephones in the sample configuration were associated with WM Access Domain “Avaya-ACM” to ensure the highest priority was given to the voice traffic.

To configure the Avaya Voice Priority Processor, connect a PC or laptop to the serial port of the Avaya Voice Priority Processor. Run a terminal emulation program with the following configuration:

- Bits per second: 9600
- Data bits: 8

- Parity: None
- Stop bits: 1
- Flow control: None

Once connected, the Avaya Voice Priority Processor login screen is presented. Log in as *admin*. The **NetLink SVP-II System Menu** is displayed as shown in **Figure 2**.

```
                              NetLink SVP-II System
                   Hostname: [slnk-000006], Address: 10.1.2.19

                         System Status
                         SVP-II Configuration
                         Network Configuration
                         Change Password
                         Exit

      Enter=Select            ESC=Exit     Use Arrow Keys to Move Cursor
```

Figure 2: NetLink SVP-II System Menu

From the **NetLink SVP-II System Menu**, select **Network Configuration** to configure the IP address, subnet mask, and default gateway of the Avaya Voice Priority Processor.

```
                              Network Configuration
                   Hostname: [slnk-000006], Address: 10.1.2.19

     Ethernet Address (fixed):      00:90:7A:00:00:06
     IP Address:                    10.1.2.19
     Hostname:                      slnk-000006
     Subnet Mask:                   255.255.255.0
     Default Gateway:               10.1.2.1
     SVP-II TFTP Download Master:   NONE
     Primary DNS Server:            NONE
     Secondary DNS Server:          NONE
     DNS Domain:                    NONE
     WINS Server:                   NONE
     Workgroup:                     WORKGROUP
     Syslog Server:                 NONE
     Maintenance Lock:              N

       Enter=Change      Esc=Exit              Use Arrow Keys to Move Cursor
```

Figure 3: Network Configuration

From the **NetLink SVP-II System Menu** shown in **figure 2**, select **SVPP-II Configuration** to configure the **Phones per Access Point** and the **802.11 Rate** fields. In this configuration, the **802.11 Rate** was configured to *Automatic*, as shown **Figure 4**, to allow the wireless telephones to determine its rate (up to 11Mbps), as opposed to the Avaya Voice Priority Processor limiting the transmission rate of the wireless telephones to 1/2 Mbps. The sample network has a **Phones per Access Point** setting of *10***.** As mentioned in the introduction, the Extreme Networks wireless solution utilized the concept of WM Access Domain to treat the wireless domain as a separate network regardless of what wired network each Access Point belongs to. Therefore, the

Phones per Access Point field should specify the maximum number of calls supported by the entire system of Access Points.

```
                              SVP-II Configuration
                   Hostname: [slnk-000006], Address: 10.1.2.19

     Phones per Access Point:       10
     802.11 Rate:                   Automatic
     SVP-II Master:                 10.1.2.19
     SVP-II Mode:                   Netlink IP
     Ethernet link:                 100mbps/full duplex
     System Locked:                 N
     Maintenance Lock:              N
     Reset System

       Enter=Change      Esc=Exit              Use Arrow Keys to Move Cursor
```

Figure 4: SVP-II Configuration

4. Configure the Extreme Networks BlackDiamond 8810 Switch

This section covers the relevant configuration of the Extreme Networks BlackDiamond 8810 Switch. Specifically, the configuration related to VLANs 2 and 3 and the Ethernet ports used by the Extreme Summit WM100/WM1000 WLAN Switch and the Altitude 350-2(Detachable) Access Points are covered below. Except where noted, configuration applies to both the Extreme Wireless WM100 and WM1000 WLAN Switch.

Step	Description
1.	Log in to the Extreme Networks BlackDiamond 8810 Switch as *admin*. It is assumed that a basic configuration and IP address has already been assigned to the BlackDiamond 8810.
2.	Clear all ports on the Extreme Networks BlackDiamond from the default VLAN. By default, all ports on the Extreme Networks BlackDiamond 8810 Switch belong to the default VLAN "**default**". `Aspen-8810.33 # configure vlan default delete port all`

3.	Create VLANs 2 and 3 on the Extreme Networks BlackDiamond 8810.
	Note: The "**default**" VLAN is used as VLAN 1. Therefore, the creation of VLAN 1 is not shown.
	`Aspen-8810.29 # create vlan vlan2`
	`Aspen-8810.29 # create vlan vlan3`

4.	Assign a tag to VLAN2 and VLAN3.
	Note: By default, the "**default**" VLAN already has a tag value of 1.
	`Aspen-8810.33 # configure vlan vlan2 tag 2`
	`Aspen-8810.33 # configure vlan vlan3 tag 3`

5.	Enable IP Forwarding on the VLAN interfaces to allow the Extreme Networks BlackDiamond 8810 Switch to route between VLANs "**default**", 2, and 3.
	`Aspen-8810.33 # enable ipforwarding vlan default`
	`Aspen-8810.33 # enable ipforwarding vlan vlan2`
	`Aspen-8810.33 # enable ipforwarding vlan vlan3`

6.	Configure an IP address and subnet mask for each VLAN interface.
	`Aspen-8810.33 # configure vlan default ipaddr 10.1.2.1 255.255.255.0`
	`Aspen-8810.33 # configure vlan vlan2 ipaddr 10.2.2.1 255.255.255.0`
	`Aspen-8810.33 # configure vlan vlan3 ipaddr 10.3.3.1 255.255.255.0`

7.	Configure the Ethernet port (port 1:30) for the link from the Extreme Networks BlackDiamond 8810 Switch to the Extreme Networks 300-48 Unified Access Switch.
	`Aspen-8810.26 # configure vlan default add port 1:30 tag`
	`Aspen-8810.26 # configure vlan vlan2 add port 1:30 tag`
	`Aspen-8810.26 # configure vlan vlan3 add port 1:30 tag`

8.	Configure the Ethernet port (port 6:1) to connect to the Extreme Networks **WM1000 WLAN Switch**. This is a 1-Gigabit fiber port. For the Extreme Networks **WM100 WLAN Switch** which has 100Mb Ethernet ports, leave the Ethernet port to auto-sensing (default). `Aspen-8810.25 # configure port 6:1 auto off speed 1000 duplex full`
9.	Enable DiffServ examination on the Extreme Networks BlackDiamond 8810 Switch for ports connecting to the Extreme Networks WM100/WM1000 WLAN Switch, the Altitude 350-2 (Detachable) Access Points, and 802.1Q trunk to the Extreme Summit 300-48 Unified Access Switch. Port 1:30 connects is the inter-switch trunk port Port 1:32 connects to Extreme Networks Altitude 350-2(Detachable) Access Points Port 6:1 connects to the Extreme Networks WM 1000 WLAN Switch. `Aspen-8810.25 # enable diffserv examination ports 1:30,1:32,6:1`

10.	Configure the qosprofile to give proper priority for voice traffic.
	`Aspen-8810.26 # configure diffserv examination code-point 34 qosprofile qp8`
	`Aspen-8810.26 # configure diffserv examination code-point 46 qosprofile qp8`

11.	Configure static routes that redirect wireless LAN traffic to the Summit WM100/WM1000 WLAN switch. 10.1.2.100 is the IP address of the WM100/WM1000 WLAN Switch.
	`Aspen-8810.24 # configure iproute add 192.168.100.0/24 10.1.2.100`
	`Aspen-8810.24 # configure iproute add 192.168.101.0/24 10.1.2.100`
	`Aspen-8810.24 # configure iproute add 192.168.102.0/24 10.1.2.100`

12.	Enable DHCP Relay and specify the IP address of the DHCP server. The Avaya wireless IP endpoints and the Extreme Networks APs request their IP configuration from the DHCP server.
	`Aspen-8810.26 # enable bootprelay`
	`Aspen-8810.26 # configure bootprelay add 10.1.2.250`

13.	Save the configuration changes using the following command: `Aspen-8810.26 # SAVE`

5. Configure the Extreme Networks Summit 300-48 Unified Access Switch

This section covers the relevant configuration of the Extreme Networks Summit 300-48 Unified Access Switch. Two Extreme Networks Altitude 350-2 (Detachable) Access Points are connected to this switch.

Step	Description
1.	Clear all ports on the Extreme Networks Summit 300-48 Unified Access Switch off the default VLAN. By default, all ports on the Extreme Networks Summit 300-48 Unified Access Switch belong to the default VLAN "**default**". `Summit300-48:3 # configure vlan default delete port all`

2.	Create VLANs 2 and 3 on the Extreme Networks Summit 300-48 Unified Access Switch.
	Note: The "**default**" VLAN is used as VLAN 1. Therefore, the creation of VLAN 1 is not shown.
	`Summit300-48:4 # create vlan vlan2`
	`Summit300-48:5 # create vlan vlan3`

3.	Configure the newly created VLANs with the appropriate VLAN tag.
	Note: The "**default**" VLAN has a VLAN tag of 1 by default. Therefore, the configuration of VLAN 1 is not shown.
	`Summit300-48:3 # configure vlan vlan2 tag 2`
	`Summit300-48:3 # configure vlan vlan3 tag 3`

4.	Configure the Ethernet port (port 1:1) for the link from the Extreme Networks 300-48 Unified Access Switch to the Extreme Networks BlackDiamond 8810 Switch. Port 1:2 and 1:3 connect to the Extreme Networks Altitude 350-2 (Detachable) Access Points.
	`Summit300-48:3 # configure vlan default add port 1:1 tag`
	`Summit300-48:3 # configure vlan vlan2 add port 1:1 tag`
	`Summit300-48:3 # configure vlan vlan3 add port 1:1 tag`
	`Summit300-48:3 # configure vlan vlan2 add port 1:2,1:3 untag`

5.	Enable DiffServ examination on the Extreme Networks 300-48 Unified Access Switch for ports connecting to the Extreme Networks Altitude 350-2 (Detachable) Access Points, and the 802.1Q trunk to the Extreme Networks BlackDiamond 8810 Switch. `Summit300-48:3 # enable diffserv examination ports 1:1-1:3`

6.	Configure the qosprofile to give proper priority for voice.
	`Summit300-48:3 # configure diffserv examination code-point 34 qosprofile qp8`
	`Summit300-48:3 # configure diffserv examination code-point 46 qosprofile qp8`

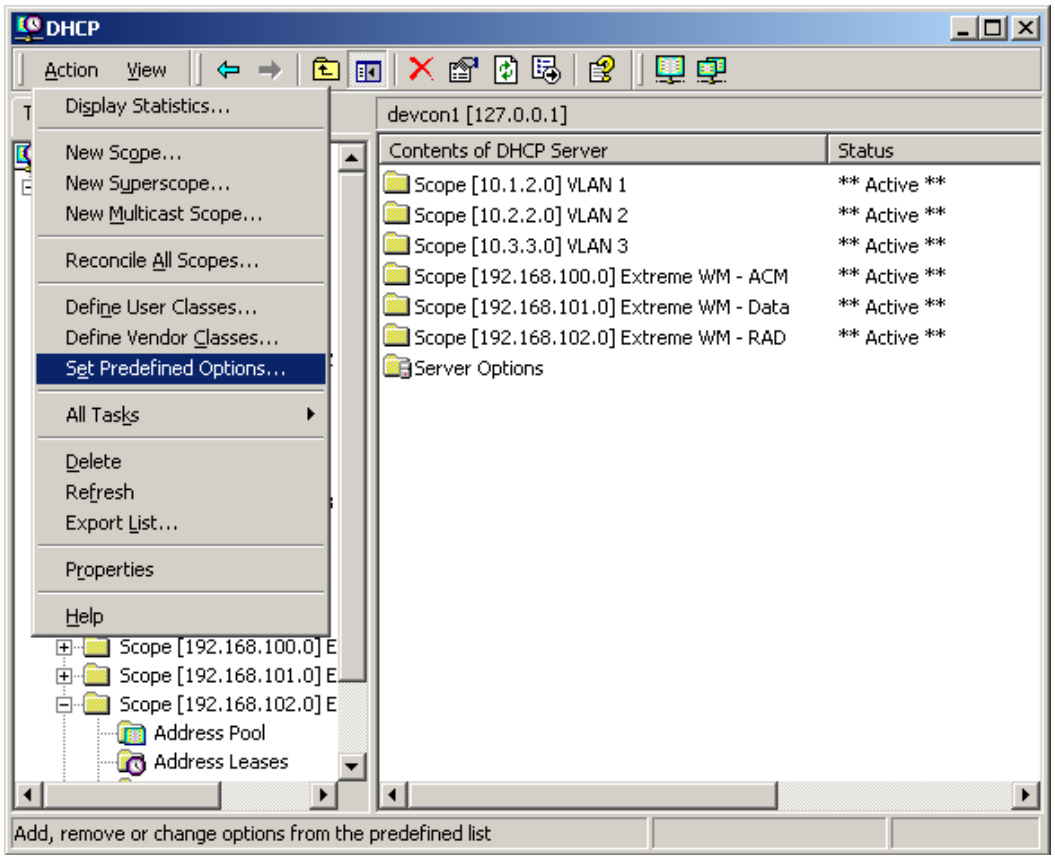
7.	Save the configuration changes using the following command: `Summit300-48:3 # SAVE`

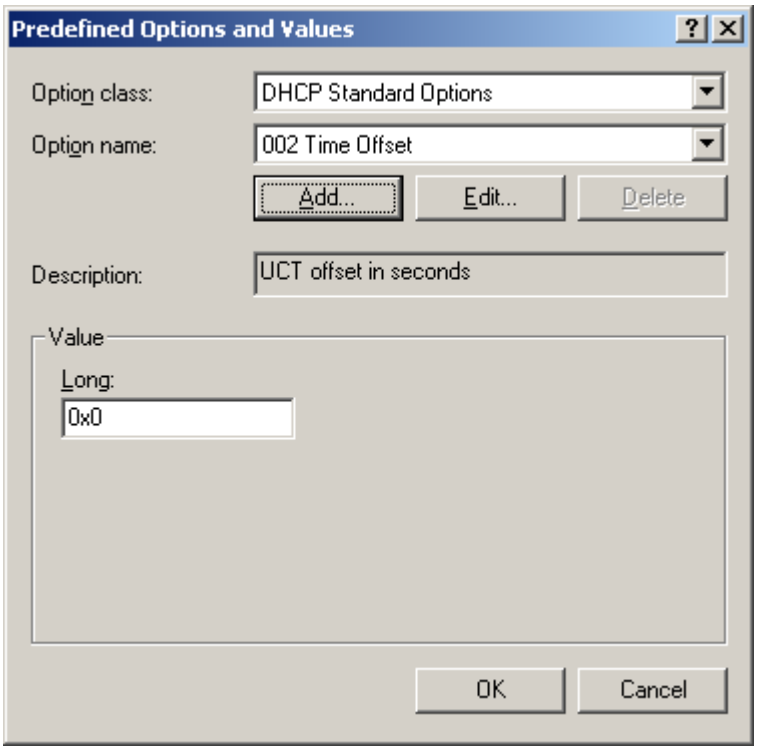
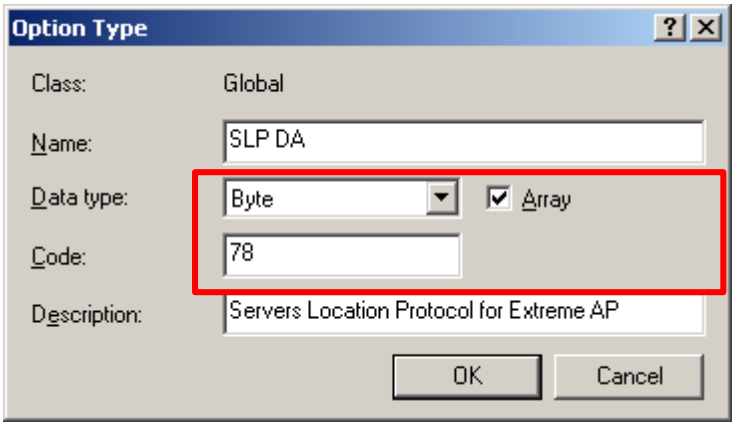
6. Configure the DHCP Server

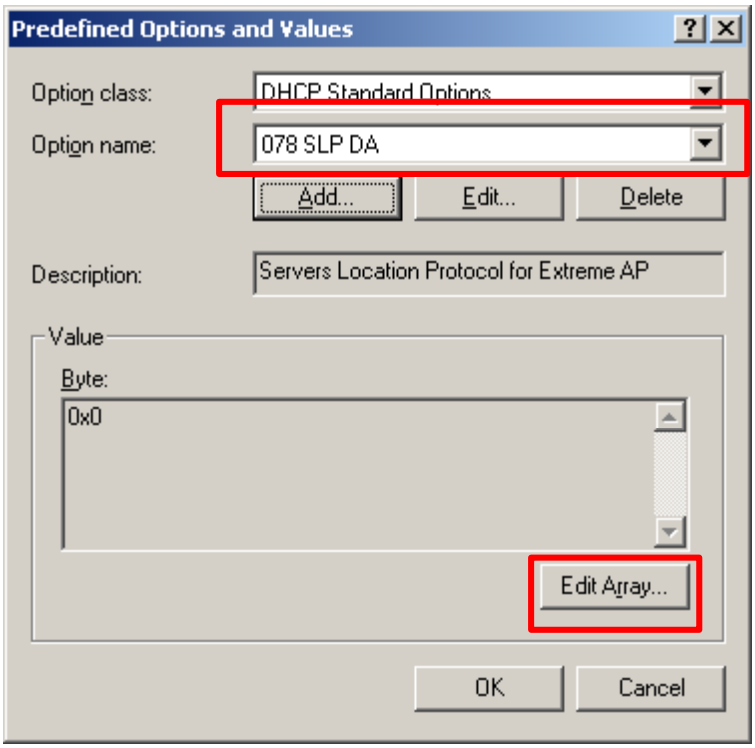
The Avaya Wireless IP Telephones, the laptops running IP Softphone and Phone Manager Pro, and the Extreme Networks Access Points obtained their IP configuration, Avaya Voice Priority Processor IP address, and Option 176 settings from a DHCP server. The DHCP server was configured with five scopes that served wireless IP endpoints. Two DHCP scopes, VLAN 2 and VLAN 3, serve clients in the wired network including the Extreme Networks Altitude 350-2 (Detachable) Access Points. Three additional DHCP scopes serve the wireless clients belonging to different WM Access Domains.

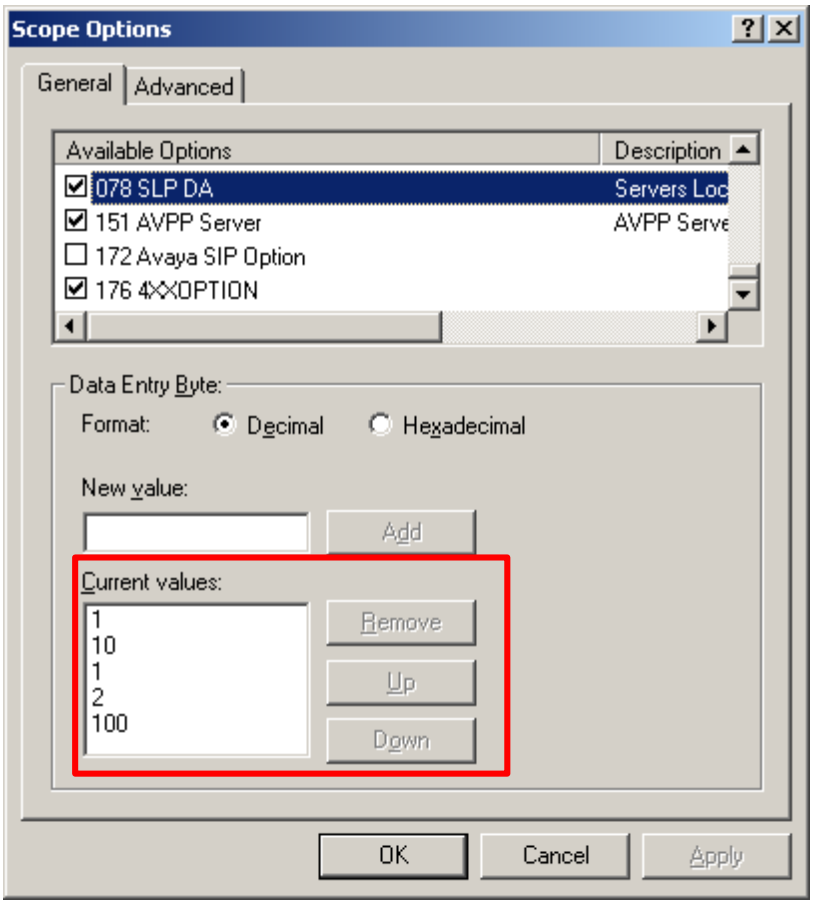
6.1. Define Service Location Profile-option 078

Define "option 078", Service Location Profile on the DHCP Server. This option is used by the Extreme Networks Altitude 350-2 (Detachable) Access Points to locate and register to the Extreme Networks WM100/WM1000 WLAN Switch.

Step	Description
1.	From the DHCP main menu, highlight the DHCP Server. Select **Action** from the main menu, and "**Set Predefined Options…**" 

2.	Click **Add** to create a new DHCP option. 
3.	Enter a new name and description for the option. The sample configuration uses the **Name** "***SLP DA***". The highlighted fields must be entered as shown below. 

4.	After adding the option, select **Edit Array** to modify the information. 

5.	Enter the information as shown in the highlighted area. This is the IP address of the Extreme Networks WM100/WM1000 WLAN Switch listed vertically and with a "1" on top. The IP address for the Extreme Networks WM100/WM1000 WLAN Switch is 10.1.2.100. To enter the IP address information, enter the value in the **New value** field and click on **Add**. Repeat for each value entered. Make sure that the order is listed correctly. Click **OK** after completing. 

6.	After creating option 078, Service Location Profile, add this option to VLAN2 and VLAN3. This option is required for the Extreme Networks Altitude 350-2 (Detachable) Access Points to locate and register with the Extreme Networks WM100/WM1000 WLAN Switch. Scopes for VLAN2 and VLAN3 must have at minimum the following two scopes associated with them.
	
	`Scope [10.2.2.0] VLAN2`
	`Address Pool`
	`  Start IP Address = 10.2.2.50`
	`  End IP Address = 10.2.2.70`
	`Option 003 Router = 10.2.2.1`
	`Option 078 SLP DA = 0x1, 0xa, 0x1, 0x2, 0x64`
	
	`Scope [10.3.3.0] VLAN3`
	`Address Pool`
	`  Start IP Address = 10.3.3.50`
	`  End IP Address = 10.3.3.70`
	`Option 003 Router = 10.3.3.1`
	`Option 078 SLP DA = 0x1, 0xa, 0x1, 0x2, 0x64`

6.2. Configure DHCP scope for the Wireless Client.

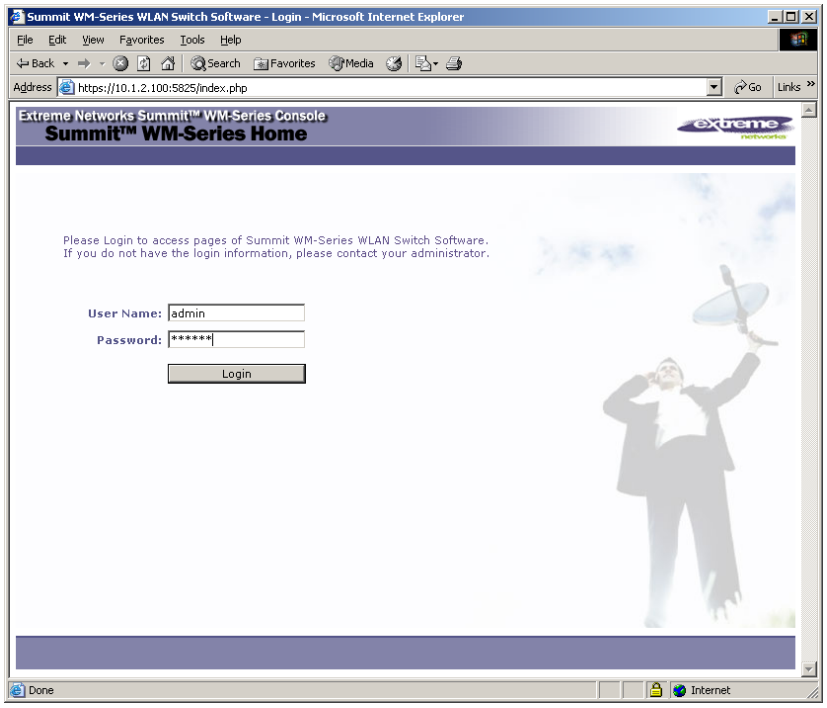
Extreme Networks Wireless Solutions utilizes a concept of WM Access Domain within the wireless network. Each of the WM Access Domains is a separate IP Network. The sample network uses the same central DHCP Server to service the WM Access Domains. Therefore, three additional scopes need to be added to the DHCP Server, one for each WM Access Domain. Configuration for each scope is shown below.

```
Scope [192.168.100.0] Avaya Communication Manager with WPA
Address Pool
  Start IP Address = 192.168.100.50
  End IP Address = 192.168.100.99
Option 003 Router = 192.168.100.1
Option 151 AVPP = 10.1.2.19
Option 176 IP Telephone = MCIPADD=10.1.2.7,MCPORT=1719,TFTPSRVR=10.1.2.250

Scope [192.168.101.0] Avaya Data
Address Pool
  Start IP Address = 192.168.101.50
  End IP Address = 192.168.101.99
Option 003 Router = 192.168.101.1

Scope [192.168.102.0] Avaya Communication Manager with RADIUS
Address Pool
  Start IP Address = 192.168.102.50
  End IP Address = 192.168.102.99
Option 003 Router = 192.168.102.1
Option 151 AVPP = 10.1.2.19
Option 176 IP Telephone = MCIPADD=10.1.2.7,MCPORT=1719,TFTPSRVR=10.1.2.250
```

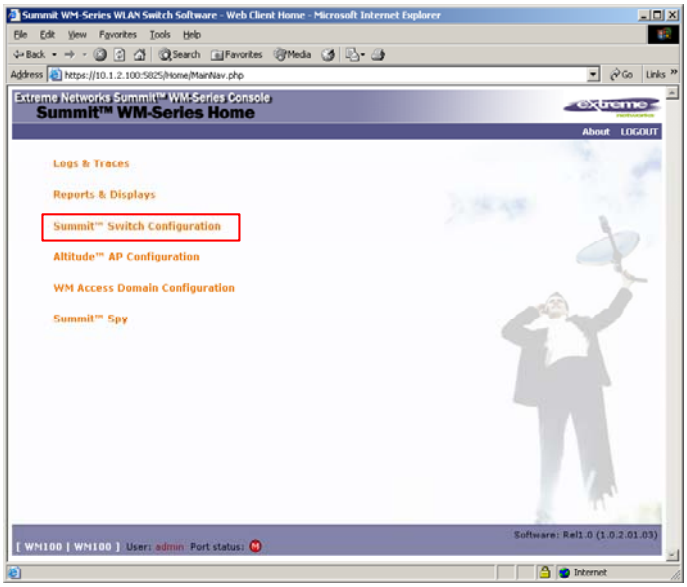
7. Configure the Summit WM100/WM1000 Switch and Altitude 350-2 (Detachable) Access Points

This section covers the configuration of the Extreme Networks WM100/WM1000 WLAN Switch and Altitude 350-2 Access Points. Configuration was performed on the Extreme Networks WM100/WM1000 WLAN Switch, which serves as the central control point for the Access Points.

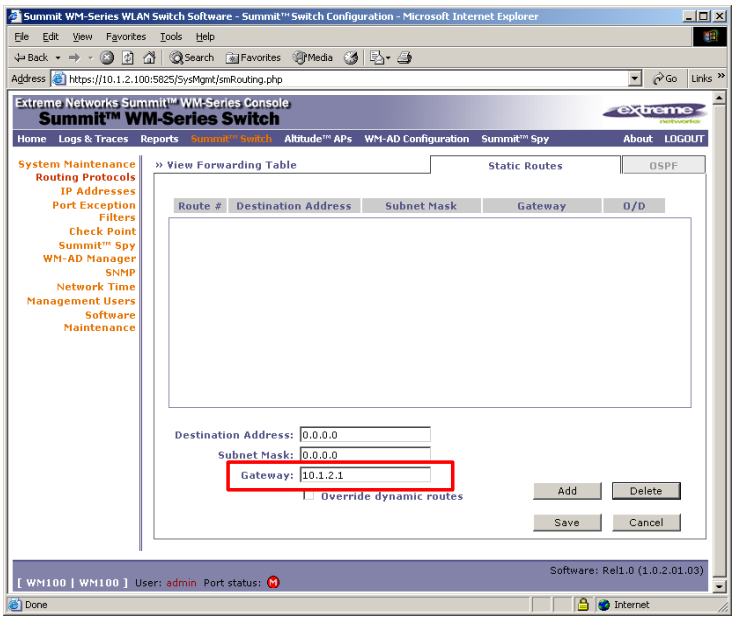
7.1. Basic configuration for the Extreme Networks Summit WM100/WM1000 WLAN Switch

Step	Description
1.	Log into the Extreme Networks Summit WM100/WM1000 WLAN Switch by pointing the Web browser to the IP address of the management port. The Extreme Networks Summit WM100/WM1000 WLAN Switch uses SSL to access the interface on port 5825 (i.e. **https://10.1.2.100:5825**). Default user name is "**admin**" and default password is "**abc123**". 

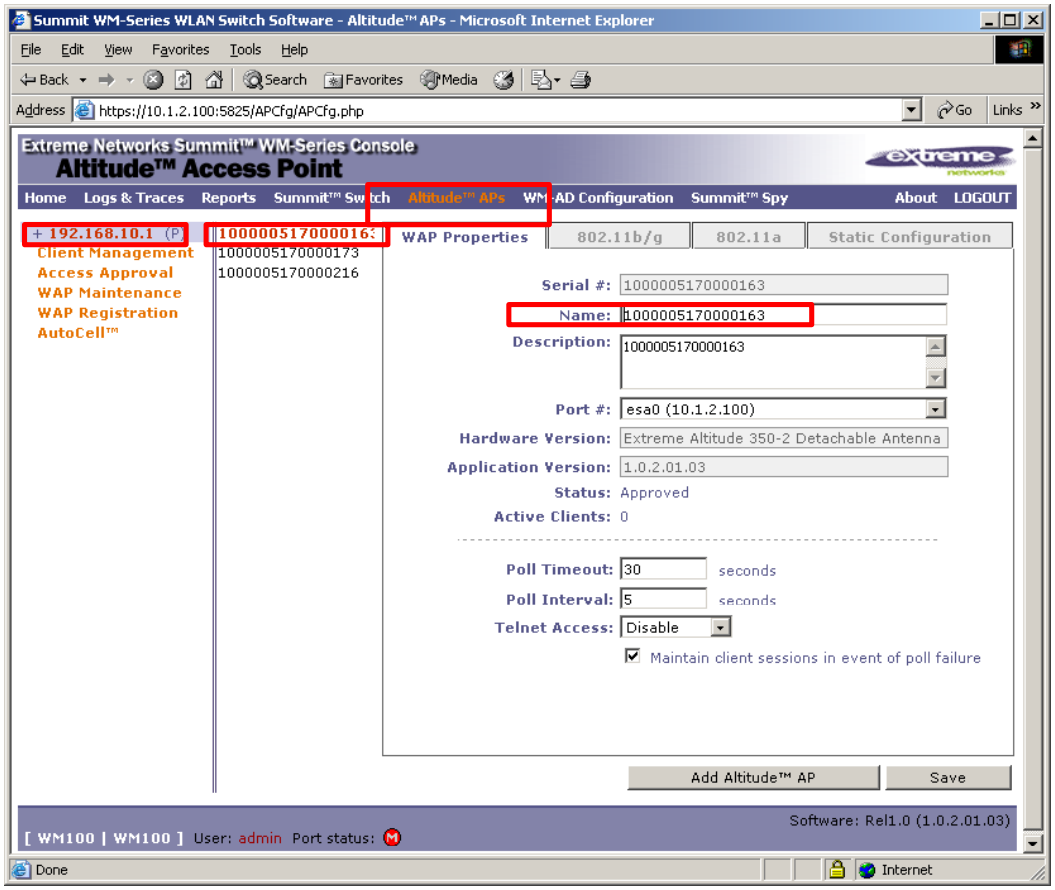
2. Select **Summit Switch Configuration** to begin configuration of the Extreme Networks WM100/WM1000 WLAN Switch.



3. Select **Routing Protocols** on the left menu and enter the **Gateway** IP address. After entering the correct information for your network, click **Add**, then **Save** to complete.



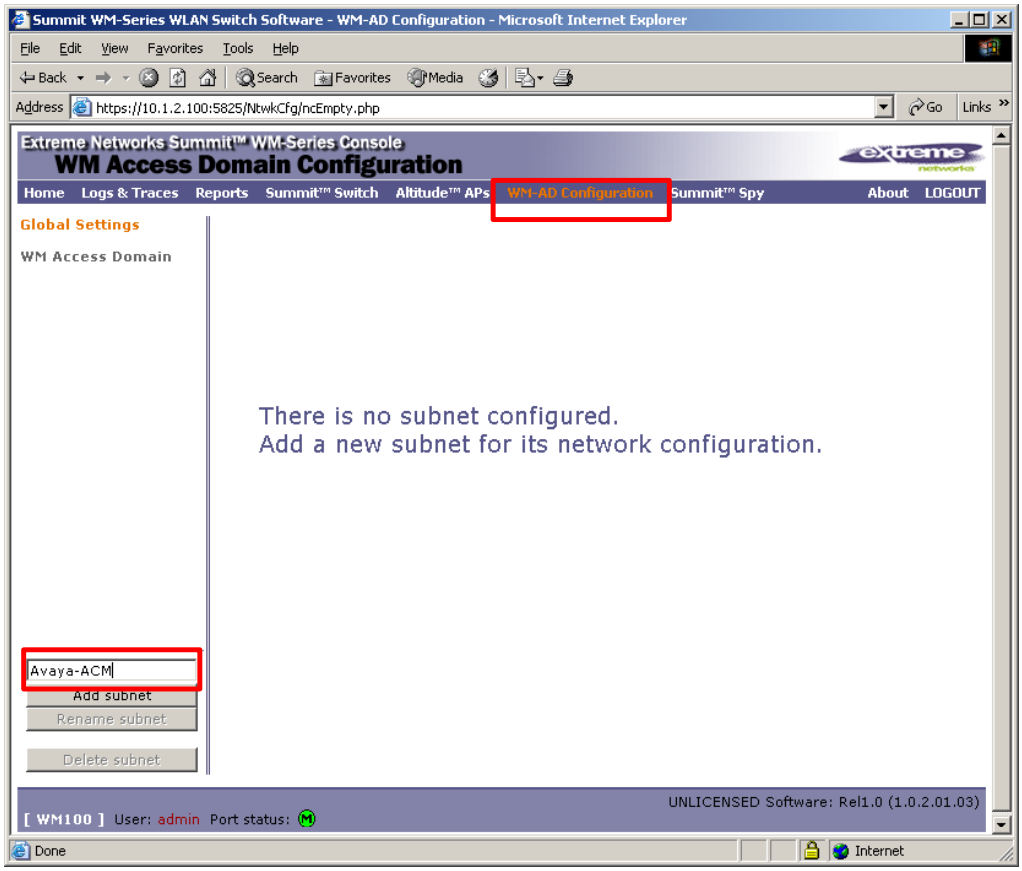
4. By default, the Extreme Networks WM100/WM1000 WLAN Switch will automatically discover all the Altitude 350-2 (Detachable) Access Points. Each newly discovered Altitude 350-2 (Detachable) Access Point is listed by its serial number. Rename the newly discovered Altitude 350-2 (Detachable) APs by selecting **Altitude APs** on the top menu and the ***serial number*** of an Altitude 350-2 (Detachable) Access Point. Enter an appropriate name in the **Name:** field. The sample configuration uses ***AP1***, ***AP2*** and ***AP3***. Click **Save** to complete.



7.2. Configure Wireless Network by SSID

In the sample configuration, there are three WM Access Domains each associated with a different SSID. The configuration is as follows:

WM Access Domain	SSID	IP Network	Encryption/Authentication
Avaya-ACM	acm	192.168.100.0/24	WPA-PSK
Avaya-Data	data	192.168.101.0/24	None
Avaya-Rad	rad	192.168.102.0/24	RADIUS

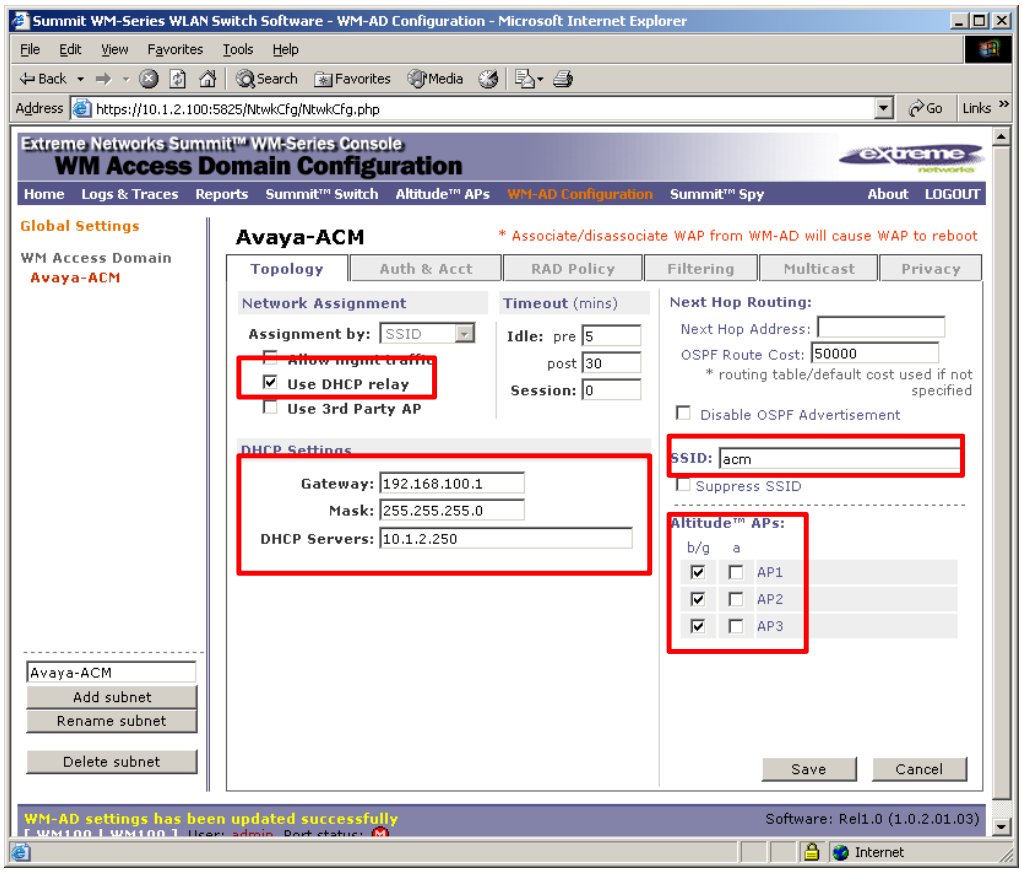
Step	Description
1.	Click on **WM-AD Configuration** from the top menu to begin configuration of the new SSID. Enter a name for this new wireless network. The sample configuration below uses ***Avaya-ACM***. Click **Add subnet** to continue. 

2. Click on the **Topology** tab and configure the following fields.

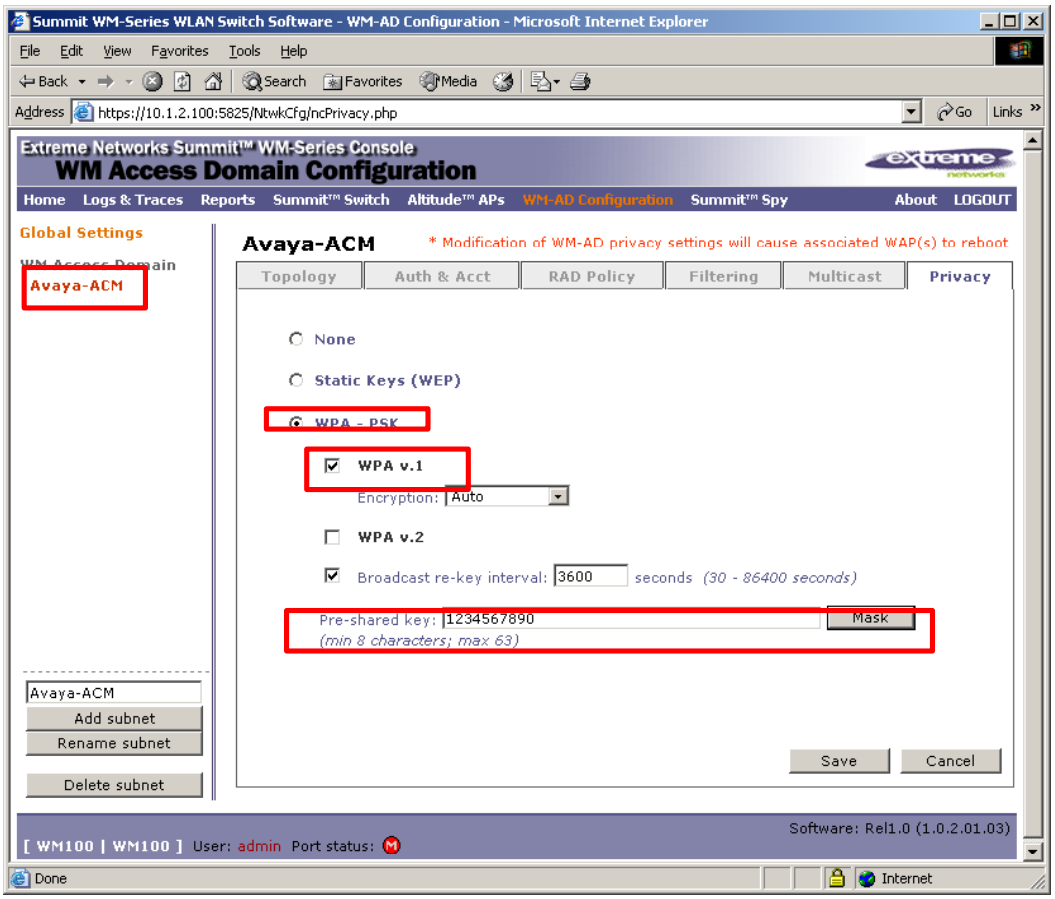
Use DHCP relay – Check to enable DHCP relay to a DHCP Server.
DHCP Settings – Specify the IP network information associated with this wireless network

Gateway	192.168.100.1
Mask	255.255.255.0
DHCP Servers	10.1.2.250

SSID – Enter the SSID for this wireless network. The sample network uses ssid ***acm***.
Altitude APs – Enable the radio for each of the listed APs by checking the check box. The sample network has three APs: AP1, AP2, and AP3.

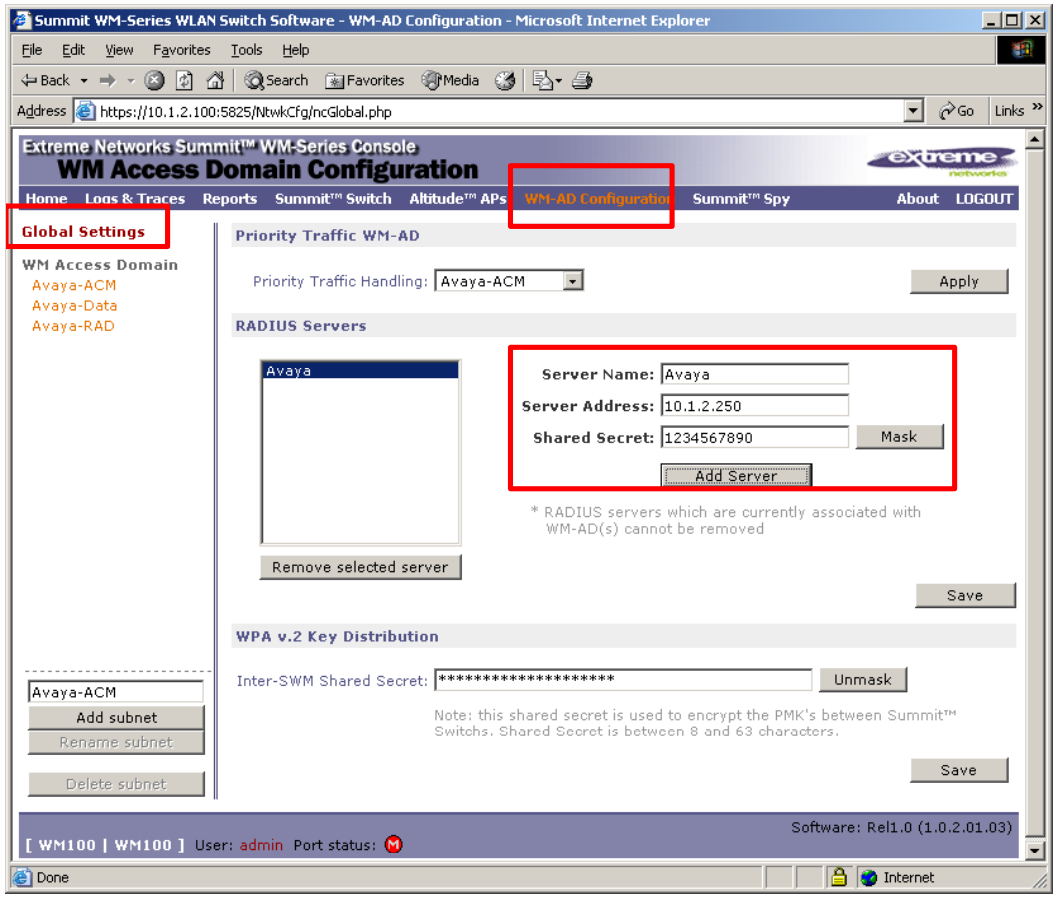


3.	To enable WPA-PSK encryption for WM Access Domain "Avaya-ACM", select the **Privacy** tab. Select **WPA-PSK** and **WPA v.1** for encryption. Entered the **Pre-shared key** that will be used by wireless clients. The sample network uses "***1234567890***" as the pre-shared key.

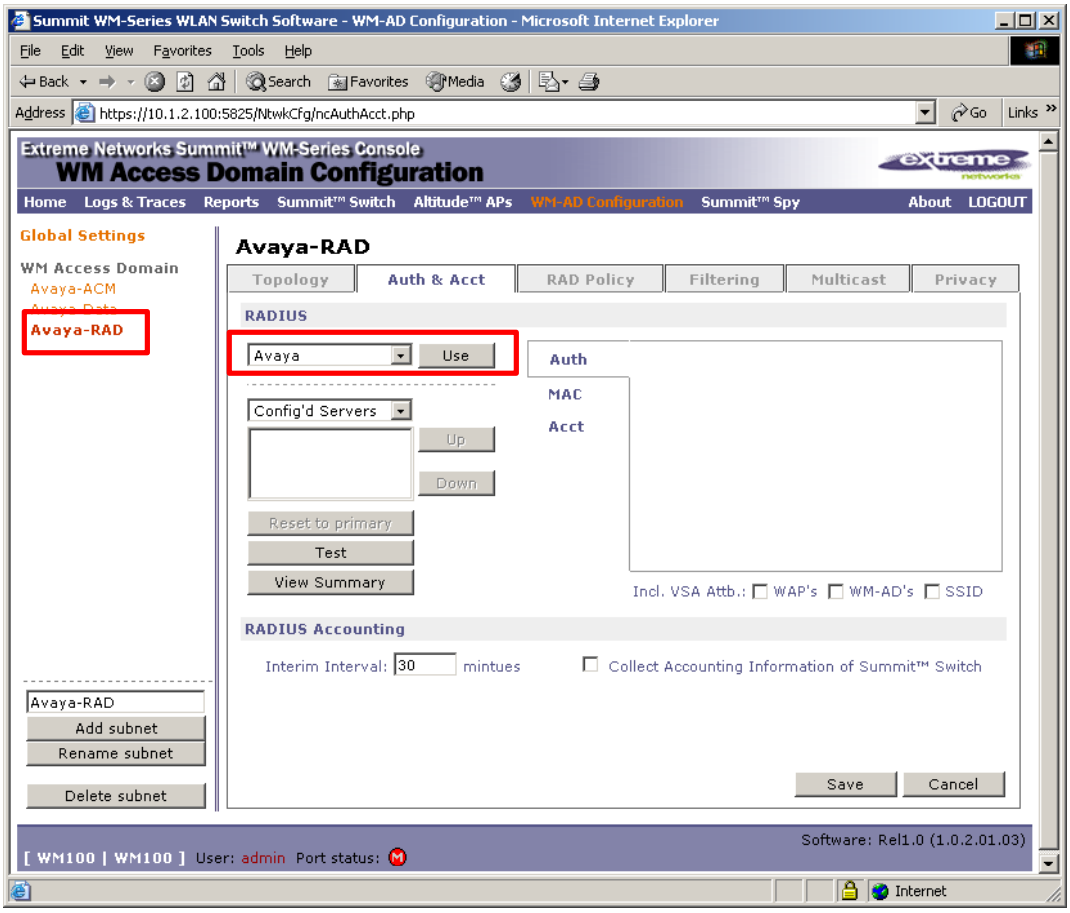


4.	Repeat Step 2 to create additional WM Access Domains. The sample network has a total of three WM Access Domains. The settings are as follows: **WM Access Domain** **Avaya-ACM** Use DHCP relay Gateway: 192.168.100.1 Mask: 255.255.255.0 DHCP Server: 10.1.2.250 SSID: acm **Avaya-Data** Use DHCP relay Gateway: 192.168.101.1 Mask: 255.255.255.0 DHCP Server: 10.1.2.250 SSID: data **Avaya-RAD** Use DHCP relay Gateway: 192.168.102.1 Mask: 255.255.255.0 DHCP Server: 10.1.2.250 SSID: rad

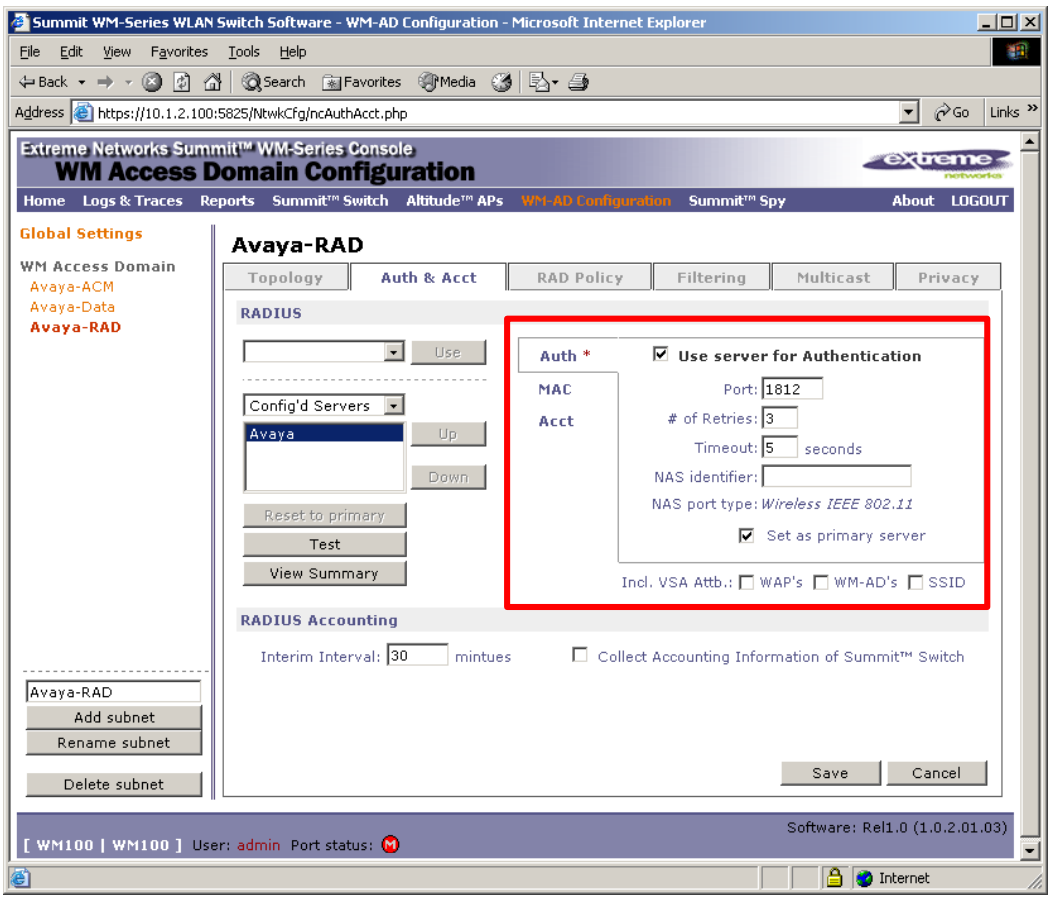
5.	To enable RADIUS authentication for the Avaya-RAD WM Access Domain, select **WM-AD Configuration** from the top menu and **Global Settings** from the left. Enter a **Server Name** for the RADIUS Server that will perform the authentication, its **Server Address** and the **Shared Secret**. Click **Add Server** then **Save** to complete.



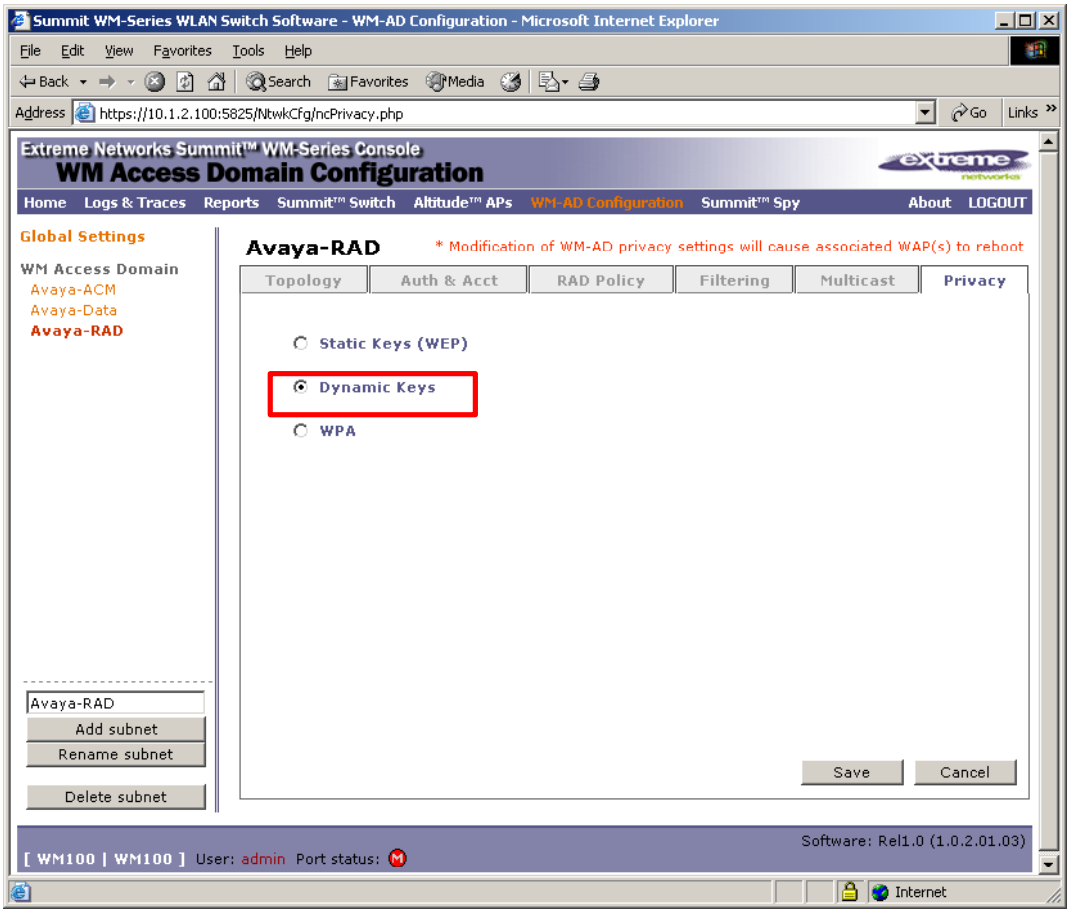
6.	Apply RADIUS authentication to WM Access Domain Avaya-RAD by selecting **Avaya-RAD** on the left and select the **Auth & Acct** tab. Select "***Avaya***" from the RADIUS drop down selection (or the RADIUS Server name defined in the previous step). Click **Use** to continue.

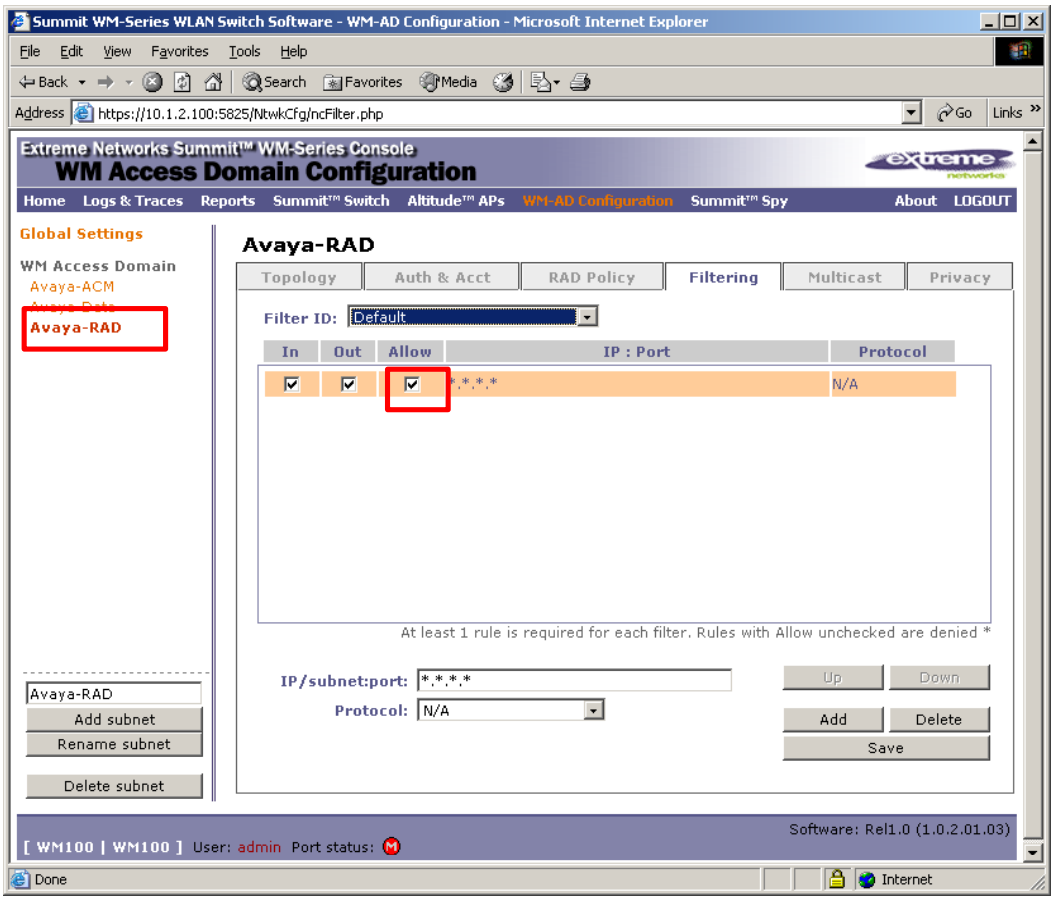


7.	Configure the **Auth** information as shown. The sample network uses Port: ***1812*** for RADIUS authentication.

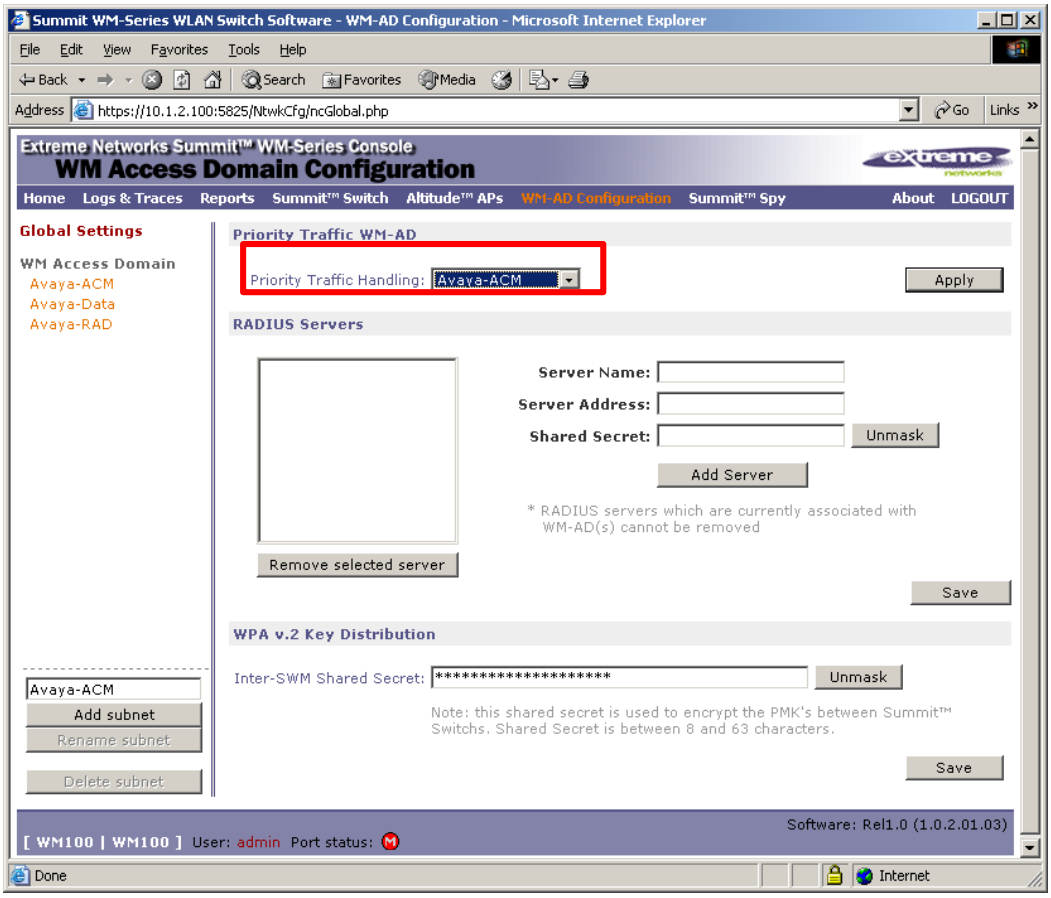


8.	Click on the **Privacy** tab, and select the desired encryption. The sample network uses **Dynamic Keys**. Click **Save** to complete.



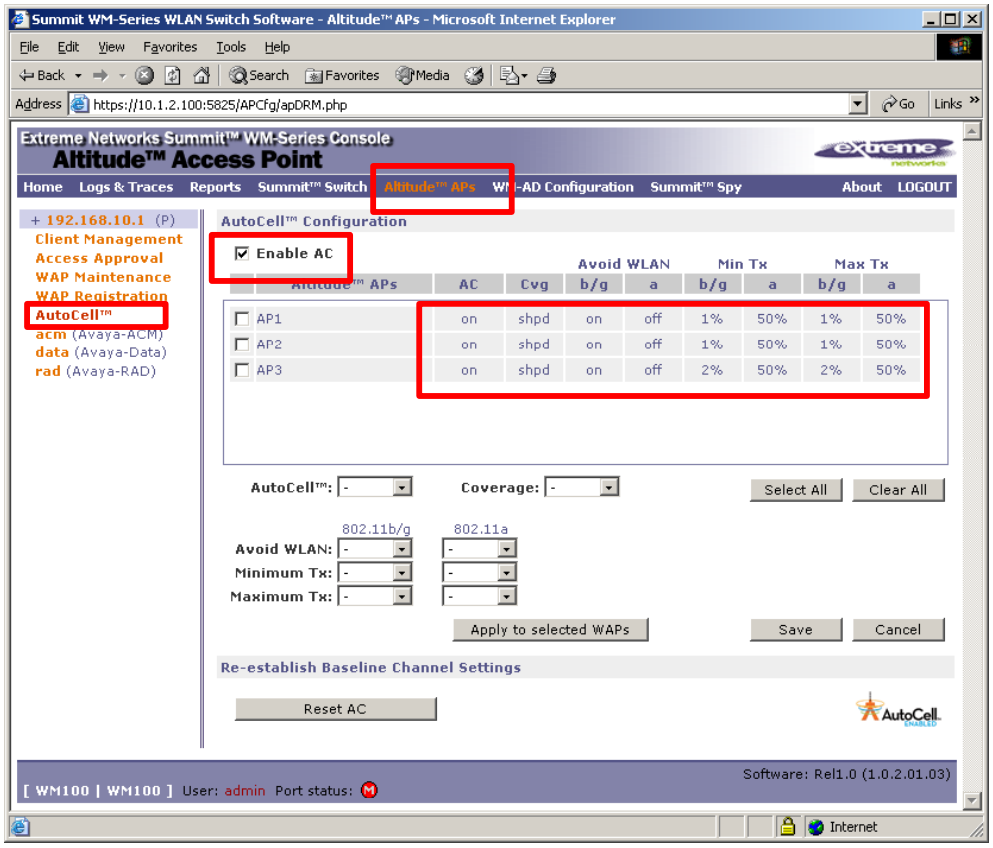
9.	By default, newly created access domains deny all traffic. To enable traffic on a WM Access Domain, select the **Filtering** tab. Check the **Allow** check box to allow traffic on the WM Access Domain. Click **Save** to complete. Select each of the WM Access Domains listed on the left (Avaya-ACM, Avaya-Data, Avaya-RAD) and perform this step to enable client access to the wireless network. 

7.1. Configure Priority on the Wireless Network.

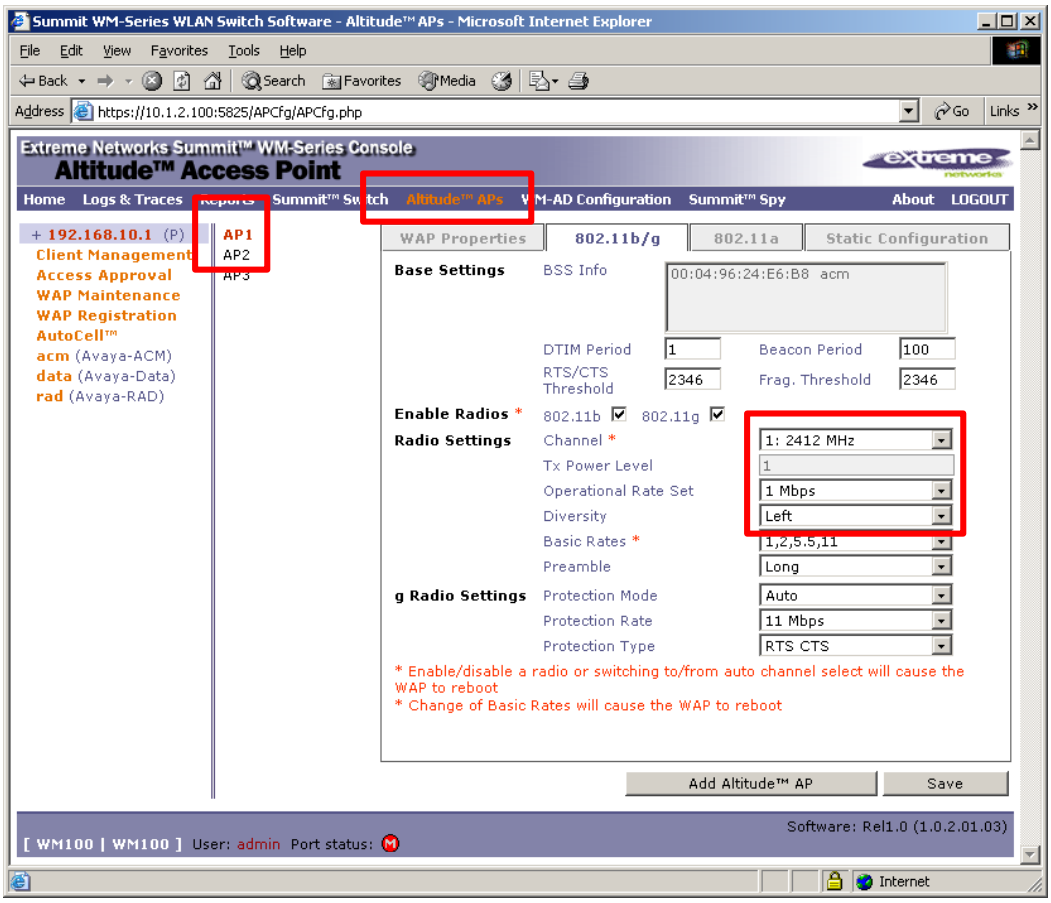
Step	Description
1.	Select **WM-AD Configuration** from the top menu and click on **Global Settings** on the left side of the screen. From the **Priority Traffic Handling** drop down box, select ***Avaya-ACM***. This will give traffic on the Avaya-ACM Access Domain priority in accessing the wireless network. 

7.2. Fine Tuning of Access Points

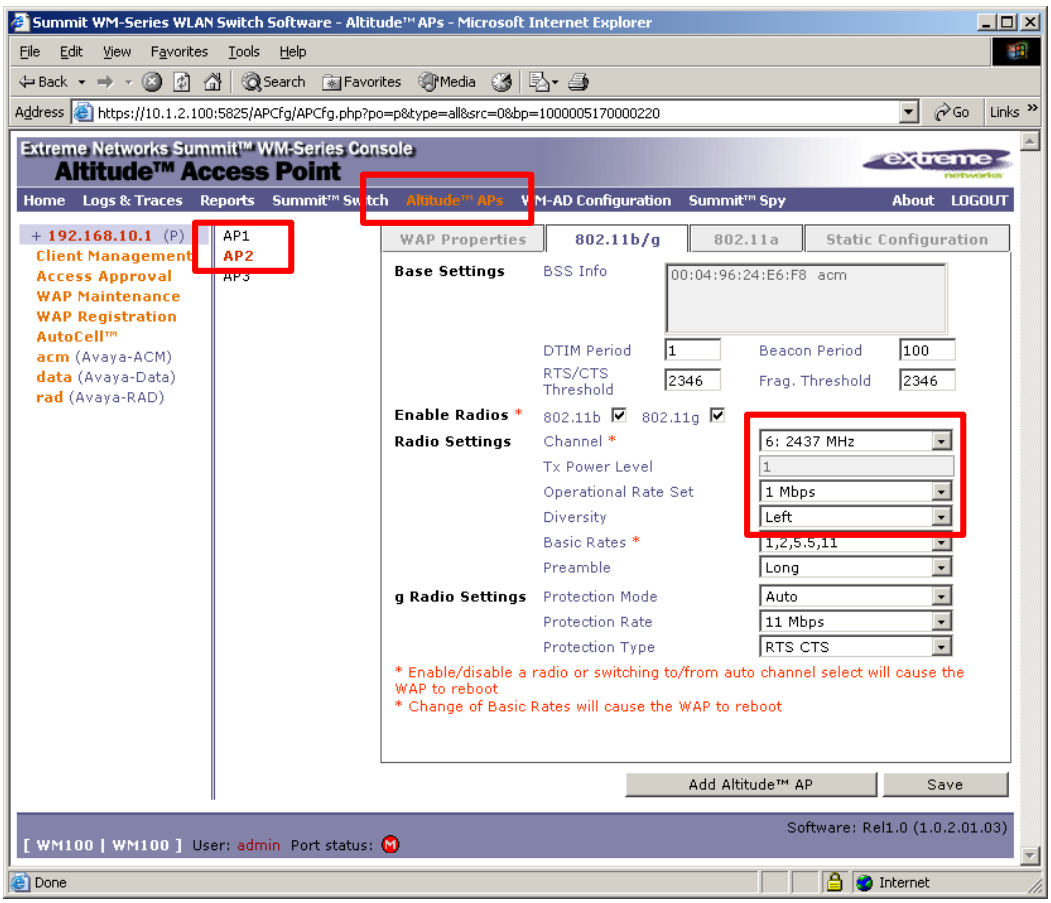
To obtain best coverage, it may be necessary to adjust both the channel assignment and transmitted power for each Access Point. This section highlights the parameters that were used in the sample configuration.

Step	Description
1.	Select **Altitude APs** from the top menu, and **AutoCell** on the left side of the screen. The sample configuration has **Enable AC** ***checked*** (enabled). AutoCell is enabled by default. AutoCell is an Extreme Networks solution to perform dynamic RF management to optimize wireless coverage utilizing inter-AP communication. To configure, select the drop down menu next to the field name. Select the desired settings for all the fields such as **AutoCell**, **Avoid WLAN**, **Minimum Tx** and **Maximum Tx** then click on **Apply to selected WAPs**. The highlighted box on the right side represents the settings used during compliance testing. 

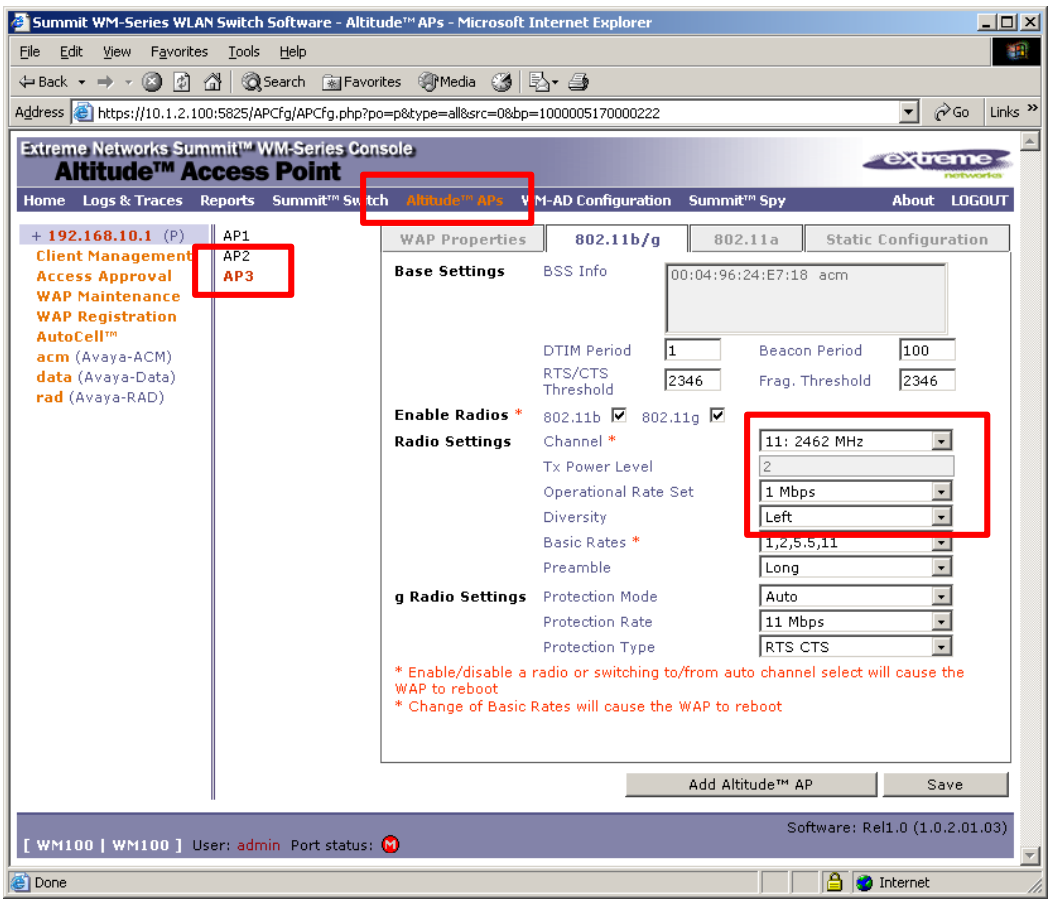
2. To adjust channel settings and transmitter power level, select **Altitude APs** from the top menu and select the desired Access Points on the left. The screen below shows the setting for "AP1".



3.	Follow Step 2 above to change the configuration for other Access Points. The screen below shows the setting for "AP2".



4.	Follow step 2 above to change the configuration for other Access Points. The screen below shows the setting for "AP3".



8. Interoperability Compliance Testing

Interoperability compliance testing covered feature functionality, serviceability, and performance testing. Feature functionality testing verified the ability of the Extreme Networks Wireless LAN Solution to provide network access to the Avaya 3616/3626 Wireless IP Telephones, Avaya IP Softphone, Avaya Phone Manager Pro, and other wireless clients. The emphasis of testing was on the QoS implementation to achieve good voice quality, Radius authentication, WEP and WPA encryption, and seamless roaming at layer-2 and layer-3.

8.1. General Test Approach

All feature functionality test cases were performed manually. The following features and functionality were verified:

- Layer-2 and Layer-3 Connectivity
- 802.1x Security
- WEP and WPA-PSK Encryption
- Quality of Service (QoS) based on Priority Queuing
- VLANs and 802.1Q Trunking
- Layer-2 and Layer-3 Seamless Roaming
- SpectraLink Voice Protocol (SVP)
- IEEE 802.11b and g
- Dynamic IP Addressing using DHCP

Performance testing was accomplished by running a *VoIP Test* on a traffic generator. The *VoIP Test* generated audio (RTP) packets between two wireless clients and calculated a MOS score to quantify the voice quality. In addition, low-priority traffic was generated while empirically verifying the voice quality on an active wireless call.

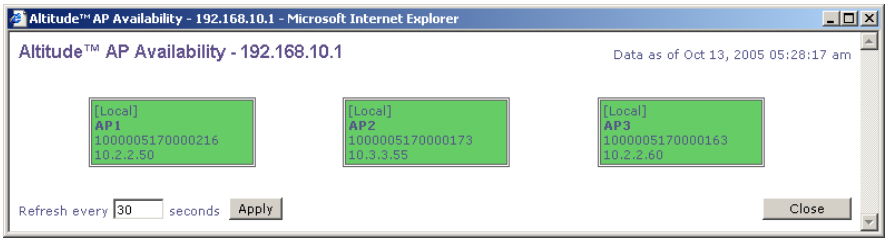
8.2. Test Results

All feature functionality, serviceability, and performance test cases passed. The Extreme Networks WM100/WM1000 WLAN Switch and Altitude 350-2 (Detachable) Access Points provide network access using 802.1x Security, WEP and WPA Encryption. Good voice quality was achieved on wireless voice calls through the use of DiffServ examination on the Extreme Networks BlackDiamond 8810 Switch, Summit 300-48 Unified Access Switch, and the prioritization of WM Access Domain.

9. Verification Steps

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

1. Check if the Extreme Networks Altitude 350-2 (Detachable) Access Points are communicating with the WM100/WM1000 WLAN Switch by logging into the Extreme Networks WM100/WM1000 WLAN Switch via the web interface. Select **Reports & Displays** then **Altitude AP Availability** from the menu selection. All Altitude 350-2 (Detachable) Access Points should be listed and highlighted in green. Below is a sample of what the **Altitude AP Availability** display looks like. The IP address information display below may be different from the sample configuration.



2. Log into the Extreme Networks BlackDiamond 8810 Switch and the Summit 300-48 Unified Access Switch and issue the command "**show diffserv examination**". Make sure the appropriate DiffServ code point values are set to QP8, the highest priority.

```
Aspen-8810.26 # show diffserv examination
CodePoint->QOSProfile mapping:
00->QP1 01->QP1 02->QP1 03->QP1 04->QP1 05->QP1 06->QP1 07->QP1
08->QP1 09->QP1 10->QP1 11->QP1 12->QP1 13->QP1 14->QP1 15->QP1
16->QP1 17->QP1 18->QP1 19->QP1 20->QP1 21->QP1 22->QP1 23->QP1
24->QP1 25->QP1 26->QP1 27->QP1 28->QP1 29->QP1 30->QP1 31->QP1
32->QP1 33->QP1 34*>QP8 35->QP1 36->QP1 37->QP1 38->QP1 39->QP1
40->QP1 41->QP1 42->QP1 43->QP1 44->QP1 45->QP1 46*>QP8 47->QP1
48->QP1 49->QP1 50->QP1 51->QP1 52->QP1 53->QP1 54->QP1 55->QP1
56->QP8 57->QP8 58->QP8 59->QP8 60->QP8 61->QP8 62->QP8 63->QP8
```

3. Log into the Extreme Networks BlackDiamond 8810 Switch and verify the correct static routes have been entered into the switch by using the **show iproute** command.

```
Aspen-8810.28 # show iproute
Ori Destination        Gateway         Mtr  Flags       VLAN       Duration
#d  10.1.2.0/24        10.1.2.1        1    U------um-- Default    0d:16h:26m:29s
#d  10.2.2.0/24        10.2.2.1        1    U------um-- vlan2      0d:16h:26m:29s
#d  10.3.3.0/24        10.3.3.1        1    U------um-- vlan3      0d:16h:26m:29s
#s  192.168.100.0/24   10.1.2.100      1    UG---S-um-- Default    0d:16h:26m:27s
#s  192.168.101.0/24   10.1.2.100      1    UG---S-um-- Default    0d:16h:26m:27s
#s  192.168.102.0/24   10.1.2.100      1    UG---S-um-- Default    0d:16h:26m:27s
```

10. Support

For technical support on the Extreme Networks Wireless LAN Solution, contact Extreme Networks Technical Assistance Center at http://ww.extremenetworks.com/services or the Extreme Networks Worldwide TAC at:

- Toll free: 800-998-2408
- Phone: 408-579-2826
- E-mail: support@extremenetworks.com

11. Conclusion

These Application Notes describe the configuration steps required for integrating the Extreme Networks Wireless LAN Solutions with an Avaya IP Telephony infrastructure. The Extreme Networks WM100/WM1000 WLAN Switch and Altitude 350-2 (Detachable) Access Points interoperated successfully with Avaya Communication Manager, Avaya IP Office, Avaya Voice Priority Processor, Avaya Wireless IP Telephones, and Avaya IP Softphone/Phone Manager Pro. The Extreme Networks WM100/WM1000 WLAN Switch and Altitude 350-2 (Detachable) Access Points supported DiffServ, and 802.1x Security as well as WEP and WPA Encryption. Seamless roaming at Layer-2 and Layer-3 was also verified. The Extreme Networks Wireless Solutions yielded good voice quality on the wireless IP endpoints.

12. References

This section references the Avaya and Extreme Networks product documentation that are relevant to these Application Notes.

Avaya product documentation can be found at http://support.avaya.com.
Extreme Networks product documentation can be found at http://www.extremenetworks.com.

[1] *Administration for Network Connectivity for Avaya Communication Manager*, Issue 10, June 2005, Document Number 555-233-504.
[2] *Administrator's Guide for Avaya Communication Manager*, Issue 1, June 2005, Document Number 03-300509.
[3] *Avaya Voice Priority Processor for SRP*, Issue 1, July 2005, Document Number 21-300637.
[4] *IP Office Manager 3.0*, Issue 16f, February 2005.
[5] *Phone Manager 2.1 Installation & Maintenance*, Issue 1, April 2004.
[6] Extreme Wireless LAN System Configuration Guide for Release 2.0.1
[7] Extreme Wireless LAN System Command Reference for Release 2.0.1
[8] Summit WM-Series Switch, Altitude 350, and Summit WM-Series WLAN Switch Software Quick Start Guide, part number:100197-00 Rev 01, May 2005
[9] Summit WM-Series WLAN Switch and Altitude Access Point Software Version 1.0 User Guide, part number: 100198-00 Rev 02, August 2005

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.