Avaya Solution & Interoperability Test Lab

Configuring Extreme Networks Summit WM200/WM2000 WLAN Switch to support Avaya Wireless IP Telephones – Issue 1.0

Abstract

These Application Notes describe the steps for configuring the Extreme Networks Summit WM200/WM2000 WLAN Switch to support an Avaya Wireless IP Telephone solution consisting of Avaya 3616, 3631, 3641 and 3645 Wireless IP Telephones. Information in these Application Notes has been obtained through Developer*Connection* 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 configuring the Extreme Networks Summit WM200/WM2000 WLAN Switch to support an Avaya wireless mobility solution consisting of Avaya 3616, 3631, 3641 and 3645 Wireless IP Telephones.

The Extreme Networks wireless solution is a centrally managed wireless solution that consists of a WM200 or WM2000 controller, and an Altitude 350 Access Point (AP). All wireless configuration such enabling a, b, or g radio, channel selection, and wireless client management is performed from the WM200/WM2000.

The Extreme Networks wireless solution supports the concept of "WM Access Domain" (WM-AD), which is defined by a unique SSID. There are two bridged modes and one routed mode that a WM-AD can be configured as. In the case of "Routed" and "Bridged travel Locally at SWM" mode, a virtual tunnel is established between the WM200/WM2000 and each Altitude 350 AP. An Altitude 350 AP sends any network traffic it receives from any wireless client associated to it through the virtual tunnel to the WM200/WM2000. After the tunneled network traffic reaches the WM200/WM2000, the traffic is then routed by the WM200/WM2000 out again to its original intended destination. In order to maintain Quality of Service, DiffServ Code Point (DSCP) information from the original packet is re-written into the envelope Layer-3 header, and is preserved after the traffic exits the virtual tunnel.

The sample configuration defined two WM-AD, voice and data. Both the "voice" and "data" WM-AD are defined to use the "Routed" mode option. The "voice" WM-AD is defined with SSID of "acm" with IP network 192.168.100.1/24 and the "data" WM-AD is defined with SSID of "data" with IP network 192.168.99.1/24. Both WM-AD are applied to all three Altitude 350 APs and are enabled to use WiFi Protected Access – Pre-Shared Key (WPA-PSK) as their encryption mechanism. A single static route was defined in the WM200/WM2000 to send all traffic to the core IP network for routing.

The compliance test verified that the following features were supported by the Extreme Networks Wireless LAN Solutions with Avaya wireless mobility solutions:

- IEEE 802.11 a, b and g radio support
- Dynamic IP Addressing using DHCP relay
- Layer-2 and Layer-3 Seamless Roaming
- Wired Equivalent Privacy (WEP) and WPA-PSK Encryption
- 802.1x Security
- SpectraLink Voice Protocol (SVP) support
- Wireless Multimedia (WMM) support
- DSCP preservation of wireless client's data

2. Configuration

Figure 1 illustrates the configuration used in these Application Notes. All wireless clients shown are associated with SSID "acm". The sample configuration uses the WM200 WLAN Switch. The configuration described in these Application Notes also applies to the WM2000 WLAN Switch.

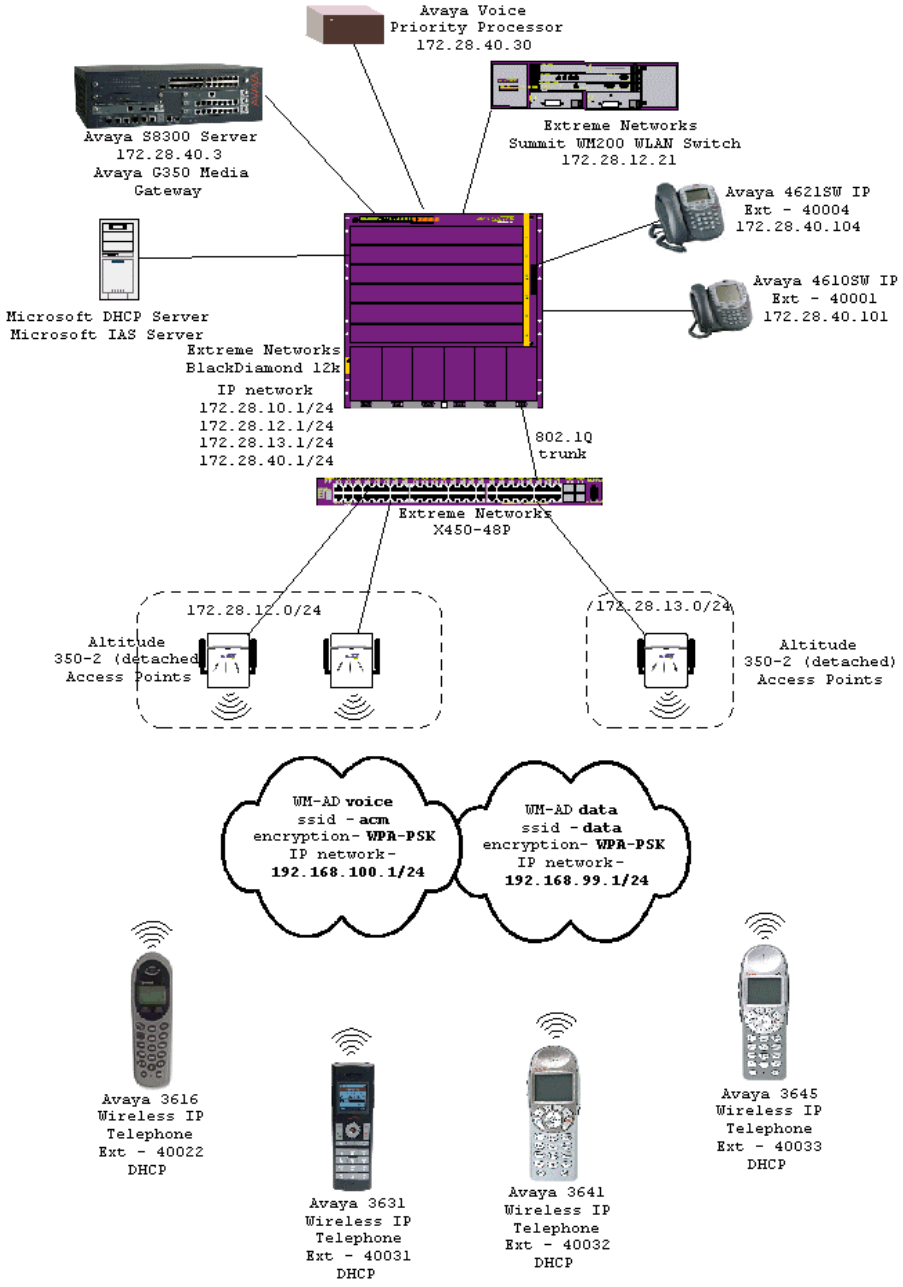


Figure 1: Sample Network Configuration

3. Equipment and Software Validated

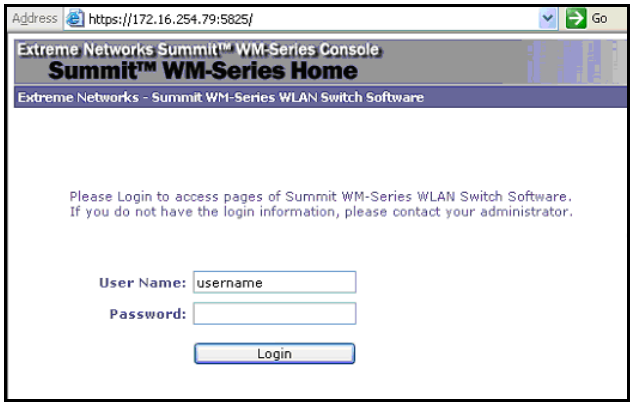
The following equipment and software/firmware were used for the sample configuration:

DEVICE DESCRIPTION	VERSION TESTED
Avaya S8300 Server with G350 Media Gateway	Avaya Communication Manager R4.0 (R014.0.730.5)
Avaya 4621SW IP Telephone	R 2.8
Avaya 4610SW IP Telephone	R 2.8
Avaya 3616 Wireless IP Telephone	96.048
Avaya 3631 Wireless IP Telephone	1.3.0
Avaya 3641/3645 Wireless IP Telephone	117.013
Extreme Networks WM200 WLAN Switch	V4 R1.3.14
Extreme Networks Altitude 350-2 Access Point	N/A
Extreme Networks BlackDiamond 12k	ExtremeXOS 11.4.3.4
Extreme Networks Summit X450-48p	ExtremeXOS 11.6.1.9
Microsoft Windows running	2003 Server Enterprise Edition
Active Directory Users and Computers	5.2.3790.1830
Internet Authentication Service	5.2.3790.1830
DHCP Server	5.2.3790.1830

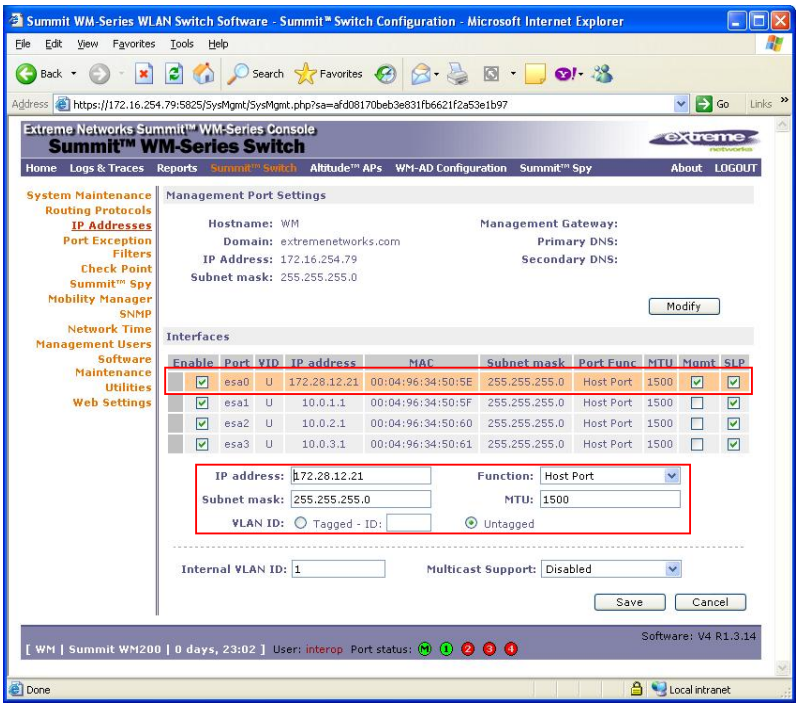
4. Configure Extreme Networks WM200

This section describes the configuration for Extreme Networks Summit WM200 WLAN Switch used in the sample as shown in **Figure 1**. The installation and configuration of any other Ethernet switches and router is beyond the scope of these Application Notes. Please refer to **[5]**, **[6],** and **[7]** in **Section 11** for additional information on how to install, configure, and administer the Extreme Networks Summit WM200 WLAN Switch.

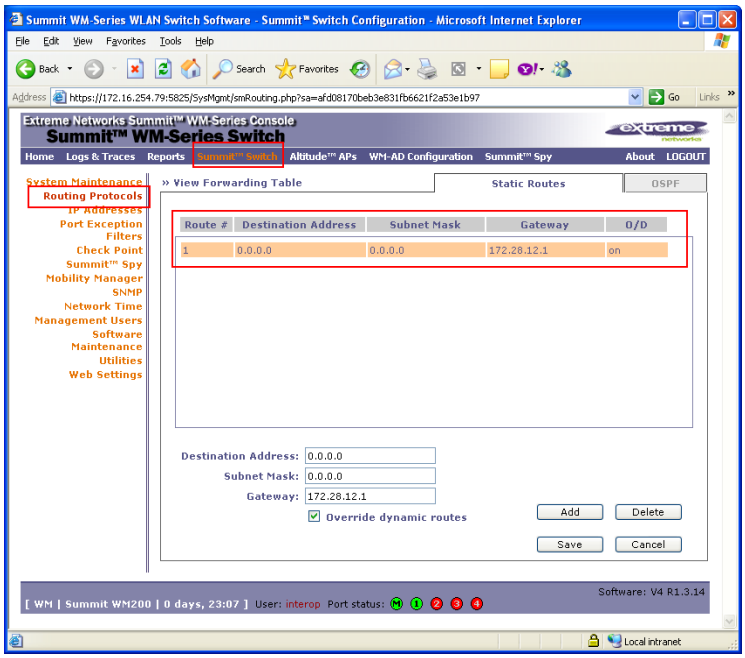
1. The WM200 configuration is performed using a web browser interface. Log in to the WM200 by entering the URL **https://<*IP address of WM200*>:5825** into a web browser. Enter appropriate credentials to gain access to the WM200. The IP address 172.16.254.79 shown in the sample configuration is the IP address of the WM200 Management port.



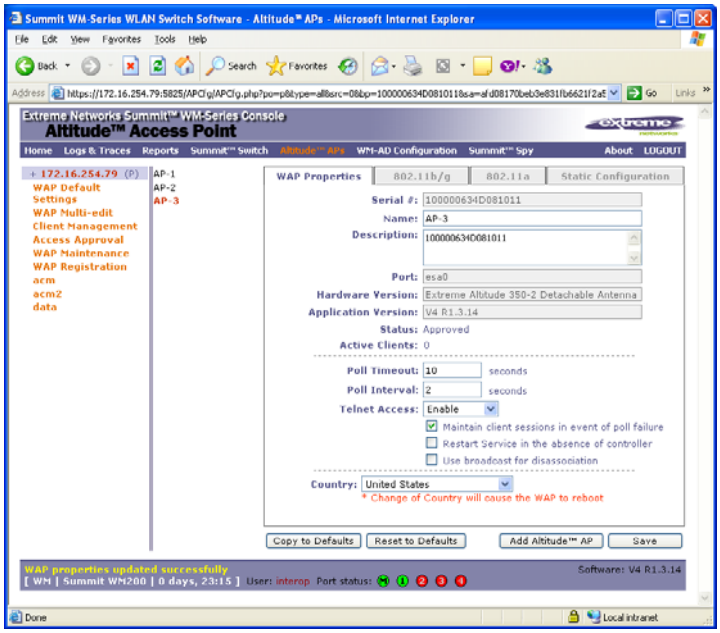
2. The esa0 interface is used for all network traffic between the WM200 and the Altitude 350 APs. This includes the tunnel traffic between the WM200 and the Altitude 350 APs, as well as traffic to and from the WM200 before entering and after exiting the tunnel. This is the interface used for the connection shown in **Figure 1**. The screen capture below shows the settings used for this esa0 interface.



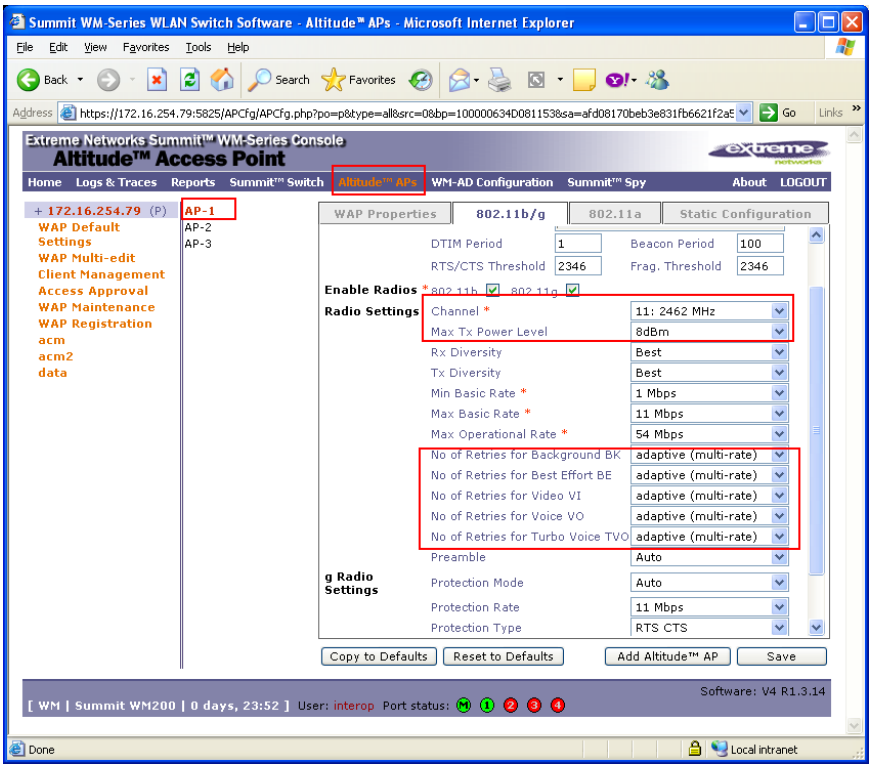
3. The WM200 is configured with one static route to send all traffic to the default gateway address of 172.28.12.1.

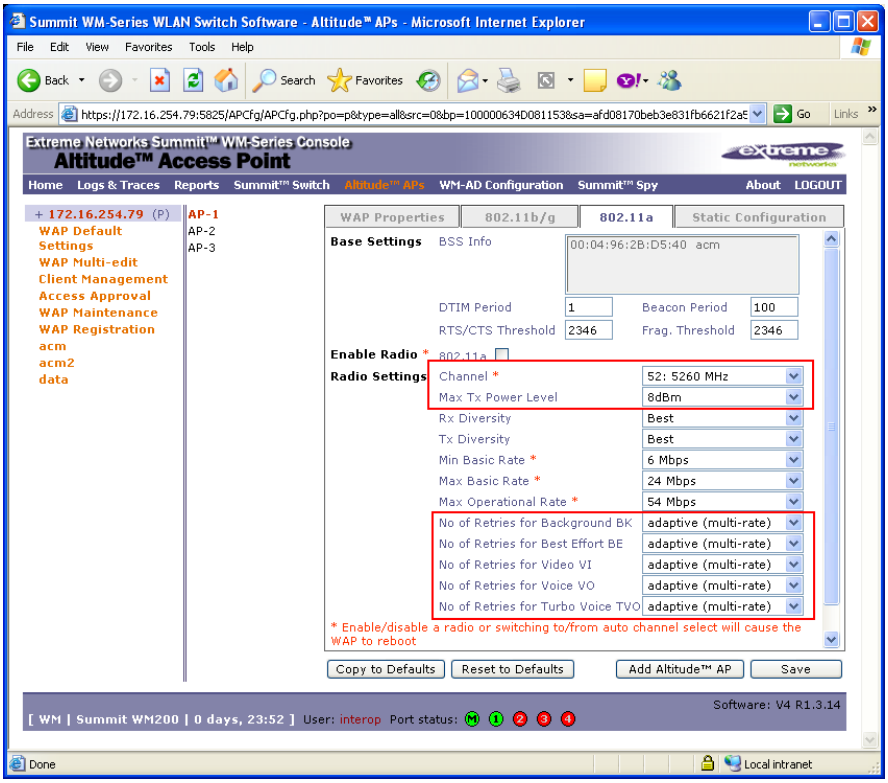


4. Three Altitude 350 APs named AP-1, AP-2, and AP-3 are used in the sample network. These APs self registered with the WM200 using the Services Location Protocol (SLP) option 78 of the DHCP Server. Newly registered APs use their serial number as their name. Although not necessary, a network administrator can elect to modify the Name for better identification and referencing.

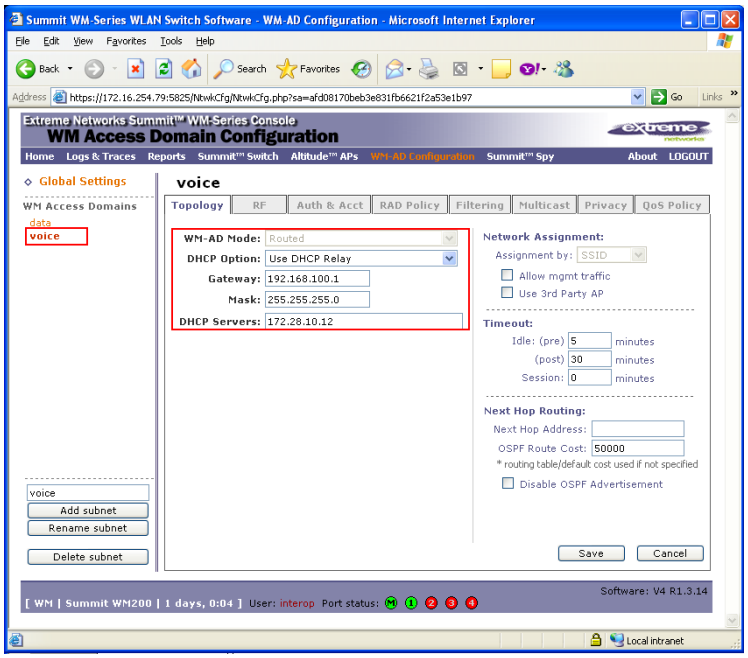


5. All three Altitude 350 APs are set to use “adaptive (multi-rate)” for the 5 different “No of Retries” types. This allows the APs to automatically adjust to allow different retry counts based on changing wireless environments. Due to the physical constraint of the test lab, channel selection was manually set based on site survey results to minimize cross channel interference. The Max Tx Power Level was also lowered to 8 dbm to decrease the coverage area and minimize interference. A site survey is recommended prior to any wireless network deployment to determine optimal configuration settings. Below are two screen captures showing the settings used in the sample network for both 802.11 b/g and 802.11 a.

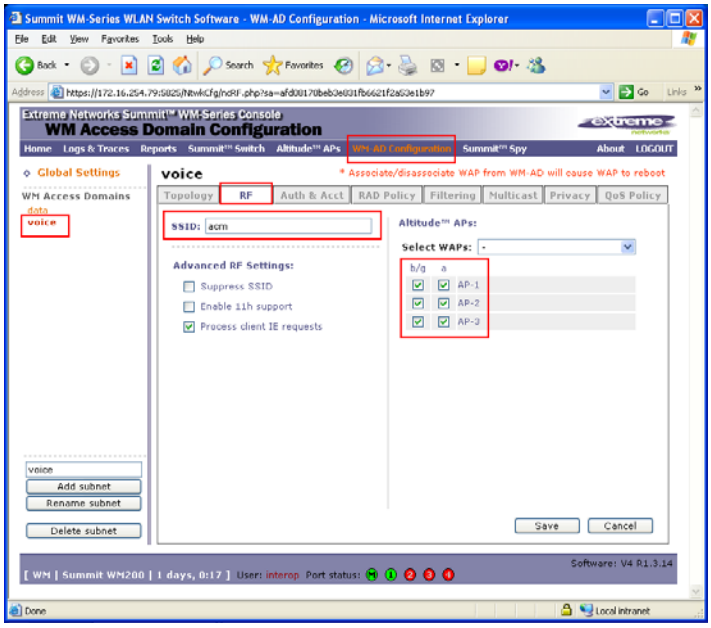




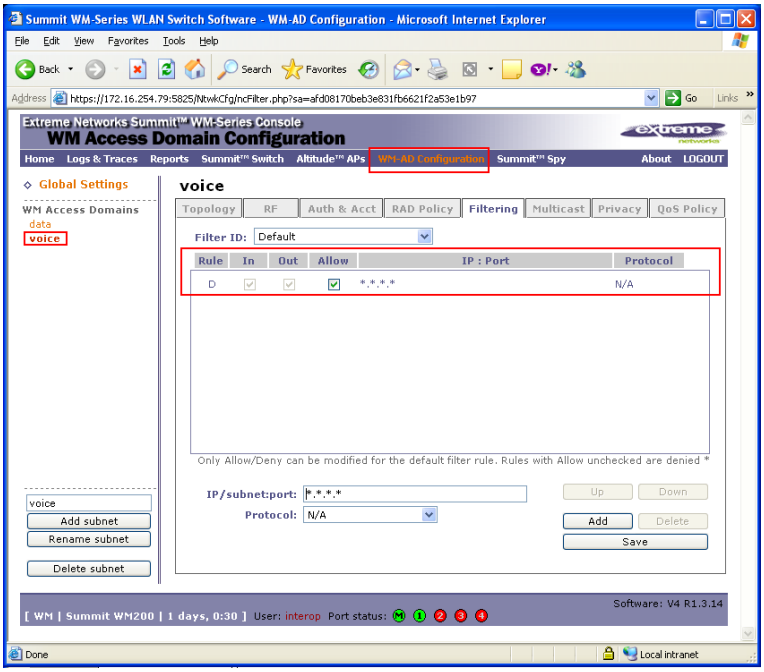
6. Two WM Access Domains, voice and data, were used in the sample network. Both voice and data WM-AD are configured as “Routed” with DHCP Relay option enabled. The voice WM-AD is configured with IP network 192.168.100.1/24 and the data WM-AD is configured with IP network 192.168.99.1/24 (not shown).



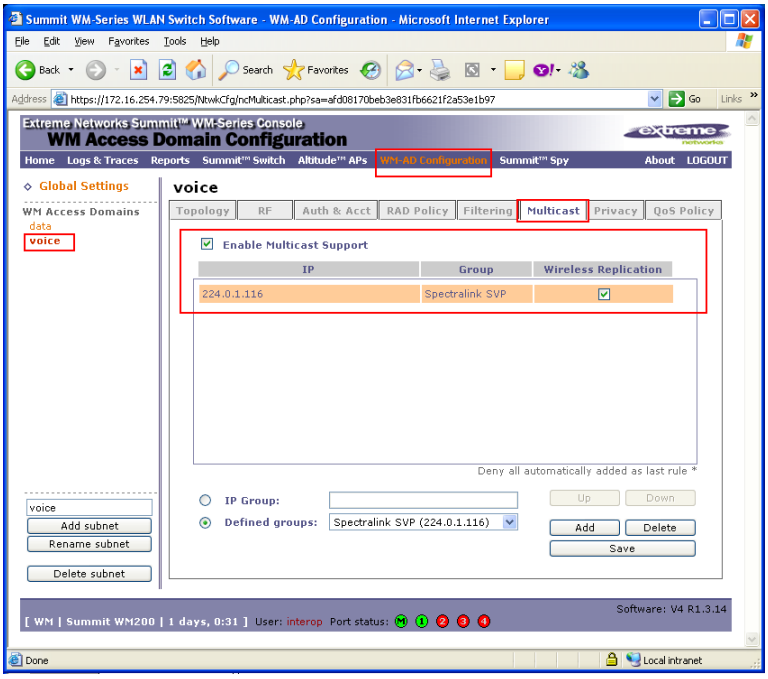
7. The voice WM-AD is configured to use SSID “acm” and is applied to all APs for both “b/g” and “a” radios. The data WM-AD is configured to use SSID ‘data” and is also applied to all APs for both “b/g” and “a” radios (not shown).



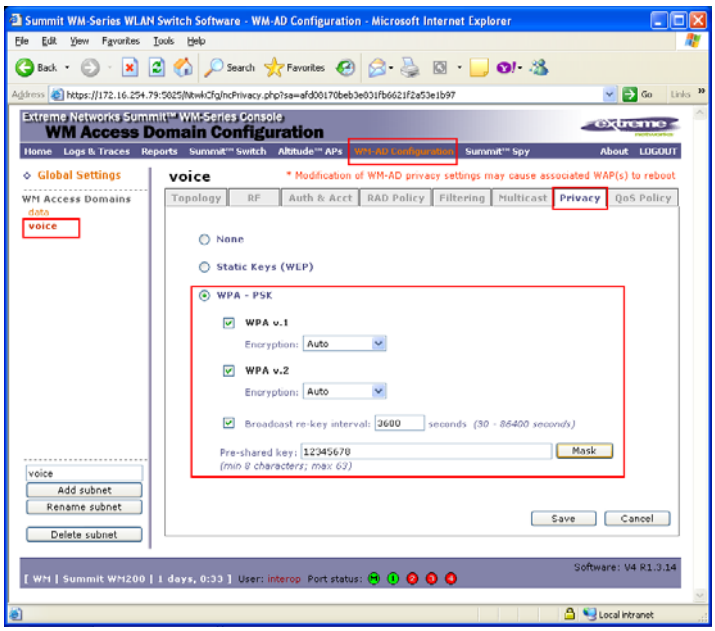
8. By default, all newly created WM-AD has a filtering rule that blocks all network traffic. Make sure to check the “Allow” check box to enable the WM-AD to pass network traffic.



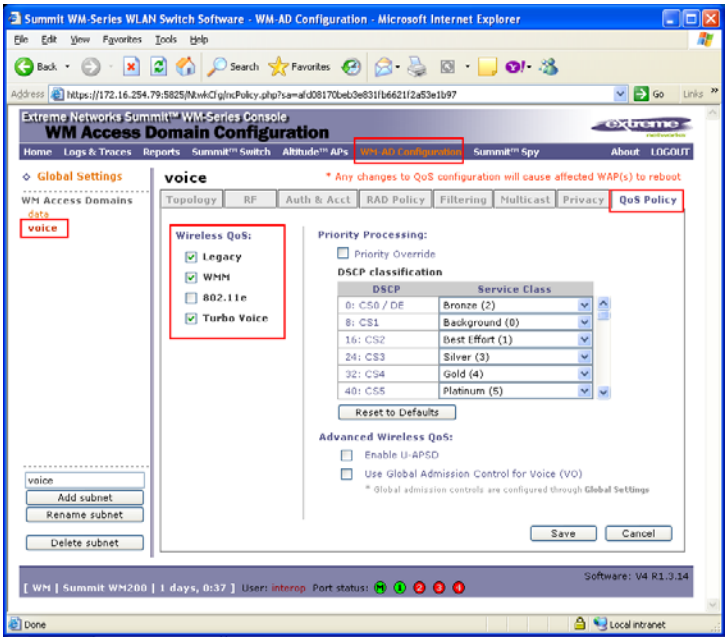
9. Multicast is enabled for the voice WM-AD to specifically allow for the Spectralink SVP group. This option is needed to allow for the Push-to-Talk features in the Avaya 3645 Wireless IP Telephone to work.



10. Both the voice and data WM-AD use **WPA-PSK** for encryption. The same pre-shared key must be entered into the Avaya Wireless IP Telephones in order for the wireless client to successfully associate with an AP.



11. For the voice WM-AD, the **Legacy**, **WMM**, and **Turbo Voice** options are selected under the Wireless QoS setting. Since the data WM-AD is designed for best effort data traffic, its QoS policy (not shown) is left as the default.



12. Make sure to save the configuration upon completion. This will cause the Access Points to reset.

5. Configure DHCP Server

Four DHCP Server scopes are defined on the DHCP server in the sample network. Two scopes are designed for allocating IP addresses to the Altitude 350 AP and two additional scopes are designed for wireless clients. The table below shows the options used in these four DHCP scopes.

Scope name	DHCP options
WiFi-1	**003** - Router = 172.28.12.1 **078** - SLP = 172.28.12.21
WiFi-2	**003** - Router = 172.28.13.1 **078** - SLP = 172.28.12.21
Voice	**003** - Router = 192.168.100.1 **151** - AVPP = 172.28.40.30 **176** - Avaya = MCIPADD=172.28.40.5, MCPORT=1719, TFTPSRVR=172.28.10.12
Data	**003** - Router = 192.168.99.1

- DHCP option 078 is used by the Altitude 350 AP to locate the WM200.
- DHCP option 151 is used by Avaya 3616, 3641, and 3645 Wireless IP Telephones to locate the Avaya Voice Priority Processor (AVPP).
- DHCP option 176 is used by Avaya 3616, 3631, 3641, and 3645 Wireless IP Telephones to register with Avaya Communication Manager and TFTP Server for configuration information.

6. Configure Stations in Avaya Communication Manager

The table and screen capture shown below illustrate the station types defined associated with the different models of the Avaya 36xx Wireless IP Telephone. Each Avaya 36xx Wireless IP Telephone type must be defined with the appropriate station type in Avaya Communication Manager in order to work properly. Use the "**add station <station #>**" command to create a new station extension. Refer to **[1]** and **[2]** in **Section 11** for other additional information related to the Avaya Communication Manager.

Avaya Wireless IP Telephone model	Station type
Avaya 3616	4606
Avaya 3631	4620
Avaya 3641 and 3645	4612

```
display station 40032                                        Page   1 of   5
                                    STATION

Extension: 40032                        Lock Messages? n               BCC: 0
     Type: 4612                         Security Code: 123456           TN: 1
     Port: S00007                     Coverage Path 1:                 COR: 1
     Name: Model-3641                 Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
             Loss Group: 19          Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 40032
           Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal               Media Complex Ext:
   Survivable Trunk Dest? y                           IP SoftPhone? n
```

7. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the Extreme Networks WM200 wireless solution to support an Avaya wireless IP mobility solution consisting of Avaya 3616, 3631, 3641, and 3645 Wireless IP Telephones registered with Avaya Communication Manager.

7.1. General Test Approach

Individual 802.11 radio support was verified by individually enabling the wireless client that supports that radio type and confirms that the wireless client is working appropriately. WMM and DSCP preservation support was verified by examining packets captured in both wireless and wired sniffers.

The following was verified on the WM200 with Avaya Wireless IP Telephones for this solution as depicted in **Figure 1**:

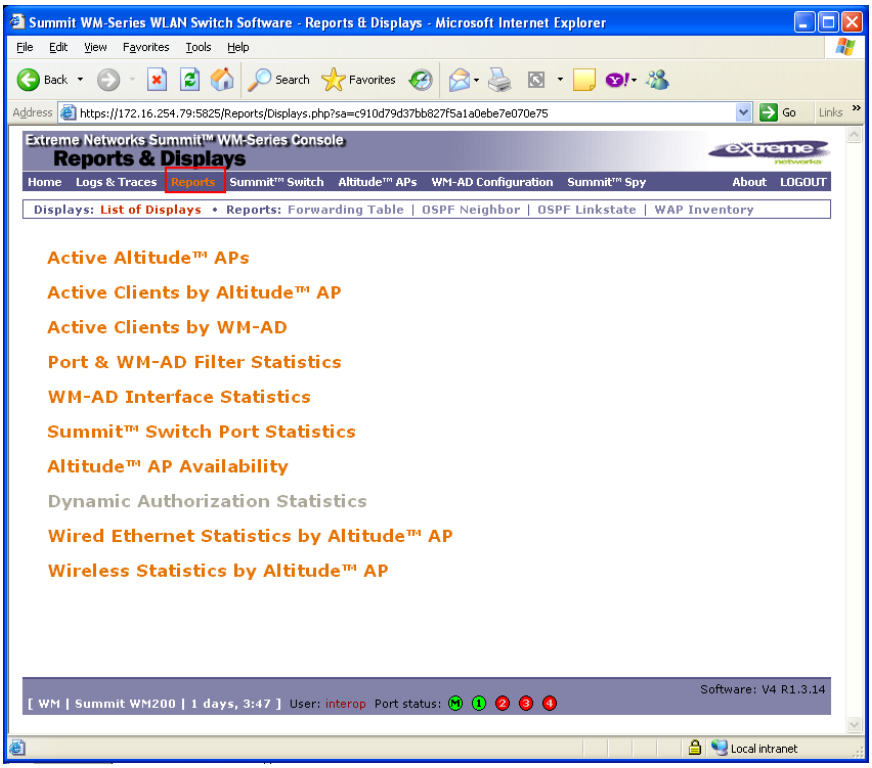
- IEEE 802.11 a, b and g radio support
- Dynamic IP Addressing using DHCP relay
- Layer-2 and Layer-3 Seamless Roaming
- WEP and WPA-PSK Encryption
- 802.1x Security
- SpectraLink Voice Protocol (SVP) support
- Wireless Multimedia (WMM) support
- DSCP preservation of wireless client's data

7.2. Test Results

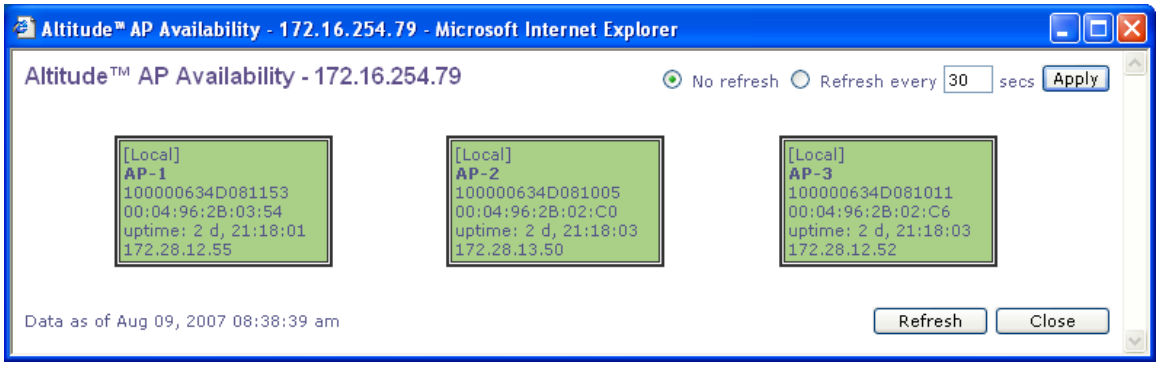
The Extreme Networks Summit WM200 WLAN Switches achieved the above objectives and completed compliance testing. Avaya 36xx Wireless IP Telephone successfully established and maintained VoIP calls while roaming throughout the area covered by Extreme Networks Altitude 350 APs.

8. Verification Steps

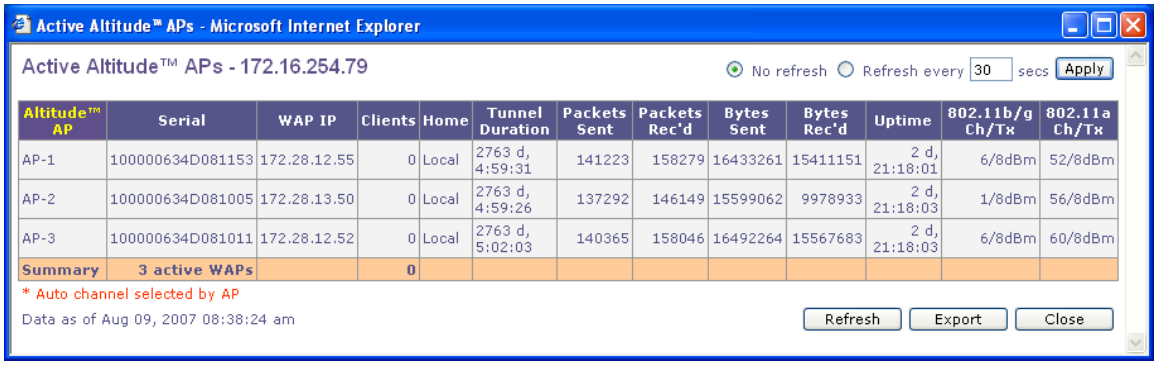
The following screen capture shows the different options available under “Reports” in the main menu bar of the WM200 management console.



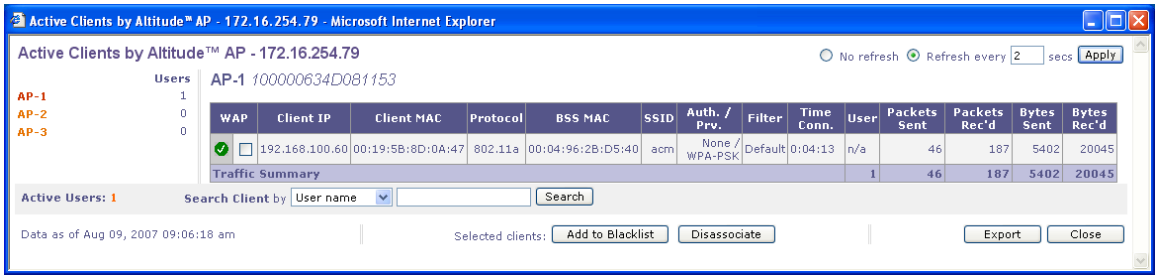
Select “Altitude™ AP Availability” from the main reports menu to verify whether the APs are available. All available APs are shown in green.



Select “Active Altitude™ APs” from the main reports menu to verify the channel selection and transmission power level of each AP. This screen will also show whether the 802.11 radio is turn on or off.



Select “Active Clients by Altitude™ APs” from the main reports menu to verify whether a wireless client has successfully associated with an AP. The wireless client’s IP address, and MAC address, protocol used (whether 802.11b/g/a), associated SSID and the authentication and encryption used is also listed. This window also allows the administrator to either blacklist or disassociate a wireless client from the wireless network.



9. Support

For technical support on the Extreme Networks product, contact Extreme Networks at (800) 998-2408, or refer to http://www.extremenetworks.com.

10. Conclusion

These Application Notes describe the administration steps required to configure the Extreme Networks Summit WM200/2000 WLAN Switch to support an Avaya wireless mobility solution as depicted in **Figure 1**.

11. Additional References

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

[1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 3.1, February 2007
[2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 3, February 2007
[3] *Administration for Network Connectivity for Avaya Communication Manager*, Doc # 555-233-504, Issue 12, February 2007
[4] *Avaya IP Telephony Implementation Guide*, May 1, 2006

Product documentation for Extreme Networks products may be found at http://www.extremenetworks.com

[5] *Summit WM Series WLAN Switch and Altitude Access Point Software Version 4.1 User Guide*, Part number: 120386-00 Rev. 01
[6] *Summit WM Series WLAN Switch and Altitude Access Point Software Version 4.1 Technical Reference Guide*, Part number: 120387-00 Rev. 01
[7] Summit WM-Series Switches, Altitude 350, and Summit WM-Series WLAN Switch Software Quick Start Guide, Part number: 100197-00 Rev. 01

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.