

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

Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved.

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. The WM200 configuration is performed using a web browser interface. Log in to the WM200 by entering the URL <u>https://<IP address of WM200>:5825</u> 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.

Address 🛃 https://172.16.25	4.79:5825/	💙 🄁 Go
Extreme Networks Sum Summit™ W	mit [™] WM-Series Console W-Series Home	
Extreme Networks - Sumn	iit WM-Series WLAN Switch Softw	are
Please Login to ac If you do not have User Name: Password:	cess pages of Summit WM-Serie the login information, please of username Login	is WLAN Switch Software. antact your administrator.

 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.

		1	Search	Favorites	🖌 🔁 🖓	🖾 - 📄 🛛	1			
ess 🕘 https://172.16.254.3	9:5825/5	/sMgmt/:	5ysMgm	t.php?sa=afd08:	170beb3e831fb6621f2a5	3e1b97		~	🖌 🔁 Go	
ktreme Networks Sum	nit™ W	M-Serie	as Co	nsole					drem	e :
Summit"" WN	1-ser	les 3	WIE	CN Altitude III	ADc WM AD Copfigu	nation Europaiti	1 6011	0.h	note	COUT
	pores		Strift C		ni si tri i no coningu	ruuun summe	- 9 99	ALC:	Jour Lo	
Routing Protocols	nanage	menti	orts	ettings						
IP Addresses	F	lostna	me: V	VM		Management 0	iateway:			
Port Exception Filters		Dom	ain: e	xtremenetwor	ks.com	Prim	ary DNS:			
Check Point	IF	Addre	ss: 1	.72.16.254.79		Second	ary DNS:			
Summit™ Spy	Sub	net ma	ISK: 2	55.255.255.0						
Mobility Manager								Mo	dify	
Network Time										
Management Users	interiat	.es								
Maintenance	Enable	Port	VID	IP address	MAC	Subnet mask	Port Func	MTU	Mamt S	LP
Utilities		esa0	U	172.28.12.21	00:04:96:34:50:5E	255.255.255.0	Host Port	1500		
Web Settings	V	esa1	U	10.0.1.1	00:04:96:34:50:5F	255.255.255.0	Host Port	1500		~
	V	esa2	U	10.0.2.1	00:04:96:34:50:60	255.255.255.0	Host Port	1500		~
	V	esa3	U	10.0.3.1	00:04:96:34:50:61	255.255.255.0	Host Port	1500		~
		IP add	ress:	172.28.12.21		Function: Host	: Port	~		
	Su	ibnet r	nask:	255.255.255	.0	MTU: 1500	E.			
		VI A	N ID.	O Tanged		Untagged				
		T CI		- ragged		, ontaggod	an ana an	eo perco ne		
				i.						
	Inter	nal ¥L/	AN ID:	1	Multicas	t Support: Disa	ibled	×		
							Sav	•	Cancel	

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

Summit WM-Series WLAN	Switch Softv Lools Help	vare - Summit [®] Switch Co	nfiguration - Microso	ft Internet Explorer		
😋 Back 🔹 🐑 🖌 🚺	3 🏠 🔎	Search 🫧 Favorites 🧔) 🔗 🌺 🖸	• 📙 191- 🖓		
Address 🕘 https://172.16.254.7	9:5825/SysMgmt	t/smRouting.php?sa=afd08170b	eb3e831fb6621f2a53e1b97	7	💌 🄁 Go	Links *
Extreme Networks Sumn Summit™ WM	nit™ WM-Ser I-Series	ries Console <mark>Switch</mark>			extreme	
Home Logs & Traces Re	ports Summ	it™ Switch Altitude™ APs	WM-AD Configuration	Summit™ Spy	About LOGO	л
System Maintenance Routing Protocols	» View Forw	arding Table		Static Routes	OSPF	
IP Addresses						
Port Exception Filters	Route #	Destination Address	Subnet Mask	Gateway	0/D	
Check Point	1	0.0.0.0	0.0.0.0	172.28.12.1	on	
Summit" Spy Mobility Manager						
SNMP						
Management Users						
Software Maintenance						
Utilities						
Web Settings						
	Destinat	ion Address: 0.0.0.0				
	Sestinat	iubnet Mask: 0.0.0.0				
		Gateway: 172.28.12.				
		V Overri	de dynamic routes	Add	Delete	
		_				
				Save	Cancel	
						_
[WM Summit WM200	0 days, 23:0	07] User: interop Port sta	itus: 🕅 🕦 🙆 🙆)	Software: V4 R1.3.	14

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.

Summit WM-Series WLA	N Switch Software - A Tools Help	ltitude® APs - Microsoft Int	iternet Explorer
🌀 Back 🝷 🕥 - 💌	🗟 🏠 🔎 Search	👷 Favorites 🕢 🔗	· 🎍 🛛 • 🔜 Ø!• 🍇
ddress 🗃 https://172.16.254	79:5825/APClg/APClg.php	po=p&type=all&src=0&bp=1000	000634D0810118sa=afd08170beb3e831fb6621f2a5 🛩 🛃 Go 🛛 Lini
Extreme Networks Sum Altitude™ Ac Home Logs & Traces R	mit™ WM-Series Con CESS Point leports Summit™ Swite	tsole ch attrade ^{re} APa WM-AD (Configuration Summit ^{re} Spy About LOGOUT
+ 172.16.254.79 (P)	AP-1	WAP Properties 8	802.11b/g 802.11a Static Configuration
WAP Default Settings	AP-2	Seria	al d: 100000634D081011
WAP Multi-edit	MF-0	Na	ame: 40-2
Client Management		Descript	
WAP Maintenance			100000530001011
WAP Registration			Boots accel
acm		Handmann Pour	Fort: esau
data		Application Vers	sion: V4 P1 3.14
		Sta	atus: Approved
		Active Clie	ents: 0
		Poll Time	eout: 10 seconds
		Poll Inter	rual: 2 seconds
		Telpet Acc	cars: Enable
		Temec Acc	Maintain client sessions in event of poll failure
			Restart Service in the absence of controller
			Use broadcast for disassociation
		Country: United	1 States
		* Chan	sge of Country will cause the WAP to reboot
		Copy to Defaults Rese	et to Defaults Add Altitude" AP Save
WAP properties update [WH Summit Wh200	d successfully 0 days, 23:15] Us	er: interop Port status: 🔫 (0 0 0 0

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.



Back - 🕥 - 💌	😰 🏠 🔎 Se 79:5825/APCfg/APCf	earch 🤆 Favorites 🥝	🔗 • 🌺 🔯 • 🗾 🔇	70beb3e831fb6621f2a5 🗸	Go Links	
Inspan in the second management of the se						
+ 172.16.254.79 (P)	AP-1	WAP Properties	802.11b/g 802.	11a Static Config	uration	
WAP Default	AP-2	Base Settings	SS Info	00.05.40		
WAP Multi-edit Client Management Access Approval WAP Maintenance WAP Registration acm	nr-U	C	TIM Period 1 TS/CTS Threshold 2346	Beacon Period 100 Frag. Threshold 234	6	
acm2		Enable Radio *	02.11a			
data		Radio Settings	Channel *	52: 5260 MHz	~	
		P	lax Tx Power Level	8dBm	*	
		F	× Diversity	Best	×	
		1	× Diversity	Best	~	
		1	lin Basic Rate *	6 Mbps	*	
		1	lax Basic Rate *	24 Mbps	*	
		1	1ax Operational Rate *	54 Mbps	*	
		9	lo of Retries for Background Bł	< adaptive (multi-rate)	~	
		1	lo of Retries for Best Effort BE	adaptive (multi-rate)	~	
		P	lo of Retries for Video VI	adaptive (multi-rate)	~	
		1	lo of Retries for Voice VO	adaptive (multi-rate)	~	
		P	lo of Retries for Turbo Voice T\	/0 adaptive (multi-rate)	~	
		* Enable/disable a WAP to reboot	radio or switching to/from auto	channel select will cause	e the	
		Copy to Defaults	Reset to Defaults	Add Altitude™ AP	Save	
WM Summit WM200	0 days, 23:52	User: interop Port statu	is: M 1 0 0 0	Software:	V4 R1.3.14	

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).

Ele Edd yew Fayorites Tools Edd Back Image: Stream Production Stream Product Stream Product Stream Product Stream Product Stream Product Product Diddle Product Stream Product Produ	Summit WM-Series WLA	N Switch Software - WM-AD Configuration - Microsoft Inte	rnet Explorer 📃 🗖 🔀					
Seate Image: Seate interpretation Address Image: Seate interpretation Address Image: Seate interpretation Extreme: Networks: Stammittle WM4Series: Console: WM Access Domain Configuration WM Access Domain Configuration Image: Seate interpretation Itome: Logs & Traces Reports Summitting WM4Series: Console: WM Access Domain Configuration Image: Seate interpretation About LOGUT • Clobal Setting: Voice Summitting WM4Series: Summitting WM4Series: Seate interpretation About LOGUT • Clobal Setting: Voice WM-AD Mode: Routed Network Assignment: Assignment by: SSID Interpretation Assignment by: SSID Interpretation UP option: Use DHCP Relay Interpretation: Interpretation: Ide: (pre) 5 minutes Session: 0 minutes Ide: (pre) 5 minutes Session: 0 minutes Session: 0 Minutes Session: 0 minutes Voice Source Source Source Interpretation: Session: 0 Iter (pre) 5 minutes (pre) 5 minutes	Eile Edit View Favorites	Iools Help	📲 🖉 🖉					
Address	🈋 Back • 💿 • 🖹 📓 🏠 🔎 Search 👷 Favorites 🤣 🔗 • 🌺 🔯 • 🛄 🞯 • 🍇							
Extreme Networks Summit!** WMScries Console WM Access Domain Configuration Home Logs & Traces Report Summit** Swith Albude** APP WM Access Domains Voice WM-AD Node: Network Assignment: DHCP Option: Use DHCP Relay Gateway: 192.168.100.1 Network Assignment traffic Use CHCP Relay Gateway: 192.168.100.1 Network Assignment: Allow and Party AP Timeout: Idle: (port) Servers: 172.28.10.12 Net Hop Address: Net Hop Address: Option table/default cox used if not specified	ddress 🕘 https://172.16.254.79:5825/NtwkCfg/NtwkCfg.php?sa=afd08170beb3e831fb6621f2a53e1b97 🛛 🍷 Go 🛛 Links 🎽							
	Extreme Networks Sum WM Access I Home Logs & Traces R	mit™ WM-Series Console Domain Configuration eports Summit™ Switch Altitude™ APs WC1-AD / onfigurati	Summit [™] Spy About LOGOUT					
WM Access Domains data voice WN-AD Mode: Routed DHCP Option: Use DHCP Relay Gateway: 192.168.100.1 Mask: 255.255.255.0 DHCP Servers: 172.28.10.12 Timeout: Idle: (pre) 5 minutes Session: 0 Minutes Session: 0 minutes Session: 0 Mext Hop Address: OSPF Route Cost: Source OSPF Route Cost: Source 1000	♦ Global Settings	voice						
Odf0 WH-AD Mode: [Routed] Network Assignment: DHCP Option: Use DHCP Relay Assignment by: [SSID] Gateway: [92.168.00.1] Allow ngmt raffic Mask: 255.255.0 Use 3rd Party AP DHCP Servers: [72.28.10.12 Timeout: Ide: (pre) [5] minutes Session: [0] minutes Voice Session: [0] minutes Voice Next Hop Address: [] OSPF Route Cost: [5000] * routing table/idefaut cost used if not specified	WM Access Domains	Topology RF Auth & Acct RAD Policy F	iltering Multicast Privacy QoS Policy					
DHCP Option: Use DHCP Relay Allow mgmt raffic Gateway: 192.168.100.1 Use 3rd Party AP DHCP Servers: 172.28.10.12 Timeout: Idle: (prs) 5 minutes (prst) 30 minutes Session: Next Hop Routing: Next Hop Address: OSPF Route Cost: SOSP Route Cost: 50000 *routing tabl/default cost used if not specified	voice	WM-AD Mode: Routed	Network Assignment:					
Mask: 255.255.0 DHCP Servers: 172.28.10.12 Timeout: Idle: (post) 30 minutes Session: 0 minutes Vext Hop Address: OSPF Route Cost: 0 % routing table/default cost used if not specified		DHCP Option: Use DHCP Relay Gateway: 192.168.100.1	Assignment by: SSID					
DHCP Servers: 172.28.10.12 Timeout: Idle: (pre) 5 minutes (post) 30 minutes Session: 0 minutes Next Hop Roting: Next Hop Address: OSPF Route Cost: 50000 * routing table/default cost used if not specified		Mask: 255.255.255.0	Use 3rd Party AP					
OSPF Route Cost: [50000 * routing table/default cost used if not specified		DHCP Servers: 172.28.10.12	Timeout: Idle: (pret) (post) 30 minutes Session: minutes Next Hop Routing: Next Hop Address:					
Disable OSPE Advertisement			OSPF Route Cost: 50000 * routing table/default cost used if not specified Disable OSPF Advertisement					
Voice Add subnet Rename subnet	Voice Add subnet Rename subnet							
Delete subnet Cancel	Delete subnet		Save Cancel					
[WM Summit WM200 1 days, 0:04] User: interop Port status: 🕲 () 🧿 🌒 🌑	[WM Summit WM200	1 days, 0:04]User: interop Port status: 闽 🕕 2 🧿	Software: V4 R1.3.14					
A Storal interact	 <i>副</i>		A Stocal intrapet					

Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved. 8 of 17 EXTR_SWM_WLAN 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).

🗿 Back 🔹 🐑 - 💌 🛛	Search 9:5825/NewkCfg/ncRF.php	rsa-afd00120beb3e001fb6/	3• 🌺 🔯 • 🗾 🞯• 21f2a63a1b97	3 <mark>▼ ⊉</mark> ∞ ।
Extreme Networks Sumr WM Access D Home Logs & Traces Re	nit™ WM-Series Con Iomain Config ports Summit™ Swite	sole) Suration th Altitude™ APs WM	AD Configuration Summit ^{en} Spy	About LOGOL
© Clobal Settings WH Access Domains data voice	Voice Topology RF SSID: acm Advanced RF Sc Suppress S: Cnable 11h V Process client	4 Asso Auth B: Acct RA Auth B: Acct RA IRA INFORMATION SID SID SID SID SID SID SID SID SID SID	ide/disassoide WAP from WM Policy Filtering Multica Altitude [™] APs: Select WAPs: - b/g a v AP-1 v v AP-1 v v AP-2 v v AP-2 v v AP-2	AD will cause WAP to reboot ist Privacy QoS Policy
Voice Add subnet Rename subnet Delete subnet	1 days, 0:17] User	r: interop Port status: @	0000	Save Cancel Software: V4 R1.3.14

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.

Summit WM-Series WLAN S	witch Software - WM-AD Configuration - Microsoft Internet Explorer	
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> o	ols <u>H</u> elp	At 1
🌀 Back 🔹 🐑 🔺 💈	🟠 🔎 Search 🤺 Favorites 🤣 🙆 - 嫨 🔯 - 🛄 🎯 - 🎎	
Address 🕘 https://172.16.254.79:	5825/NtwkCfg/ncFilter.php?sa=afd08170beb3e831fb6621f2a53e1b97	💙 🋃 Go 🛛 Links 🎽
Extreme Networks Summi WM Access Do Home Logs & Traces Repo	1 th WM-Series Console main Configuration rts Summit ^{er} Switch Altitude ^{re} APs Wit AD Configuration Summit ^{ere} Soy	
♦ Global Settings	voice	
WM Access Domains	Topology RF Auth & Acct RAD Policy Filtering Multicast P	rivacy QoS Policy
data Voice	Filter ID: Default	
VOICE	Rule To Out Allow IP : Port	Protocol
		N/A
	Only Allow/Deny can be modified for the default filter rule. Rules with Allow unc	hecked are denied *
		Dawa
voice	IP/subnet:port: *.*.*	DOWN
Add subnet	Add	Delete
Rename subnet		Save
Delete subnet		
		Software: V4 R1 3 14
[WM Summit WM200 1	days, 0:30]User: interop Port status: 🕅 🛈 🙆 🔕	00/01/01/01/04 N1/0/14
Ch.		· · ·
e Done		🗎 🤡 Local intranet 🔤

Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved. 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.

Summit WM-Series WLA	N Switch	Software - WM	N-AD Configuration	- interosoft internet explo	rer	
	Toos f	leth	A			
Back • 🕑 • 💌	2 🚺	>>> Search	📈 Favorites 😁	🛛 • 🎯 🔊 • 🛄		
dress 🕘 https://172.16.254.	.79:5825/N	twkCfg/ncMulticast	.php?sa=afd08170beb3	e831fb6621f2a53e1b97	Y → C	50 Links
Extreme Networks Sum	mit™ W Doma	M-Series Cons	ole uration		extre	ne <
lome Logs & Traces R	eports !	Summit™ Switch	Altitude™ APs W	M-AD Configuration Summ	it™Spy About L	.0GOUT
> Global Settings	void	`e				
/M Access Domains	Topo	logy RE	Auth & Arct	AD Policy Filtering	Aulticast Privacy DoS Pr	licy
data						
voice	[Enable Mul	ticast Support			
			IP	Group	Wireless Replication	
		224.0.1.116		Spectralink SVP	V	
		224.0.1.116		Spectralink SVP	V	*
		224.0.1.116		Spectralink SVP	utomatically added as last rule	*
voice) IP Group:		Spectralink SVP Deny all a	utomatically added as last rule	*
voice Add subnet Bename subnet) IP Group:) Defined gr	oups: Spectralink	Spectralink SVP Deny all ar SVP (224.0.1.116)	utomatically added as last rule	*
voice Add subnet Rename subnet) IP Group:) Defined gr	oups: Spectralink	Spectralink SVP Deny all an SVP (224.0.1.116)	Utomatically added as last rule Up Down Add Delete Save	*
voice Add subnet Rename subnet Delete subnet) IP Group:) Defined gr	oups: Spectralink	Spectralink SVP Deny all ar SVP (224.0.1.116)	Utomatically added as last rule Up Down Add Delete Save	*
voice Add subnet Rename subnet Delete subnet (WM Summit WM200	1 days) IP Group:) Defined gr , 0:31] User: 	oups: Spectralink	Spectralink SVP Deny all ar SVP (224.0.1.116) V	Utomatically added as last rule Up Down Add Delete Save Software: V4 P	*
voice Add subnet Renama subnet Delete subnet WM Summit WM200	1 days) IP Group:) Defined gr , 0:31] User: 	oups: Spectralink	Spectralink SVP Deny all ar SVP (224.0.1.116) V	utomatically added as last rule Up Down Add Delete Save	*

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



Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved. 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		Da	age 1 of	5
display station 40052		STATION	ige i Oi	5
Extension: 40032		Lock Messages? n Security Code: 123456	BCC: TN:	0 1
Port: S00007		Coverage Path 1:	COR:	1
Name: Model-3641		Coverage Path 2: Hunt-to Station:	COS:	1
STATION OPTIONS				
Loss Group:	19	Time of Day Lock Table Personalized Ringing Pattern Message Lamp Ext	: : 1 : 40032	
Speakerphone: Display Language: Survivable GK Node Name:	2-way english	Mute Button Enabled?	? У	
Survivable COR: Survivable Trunk Dest?	internal Y	Media Complex Ext 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.

🗿 Summit WM-Series WLAN Switch Software - Reports & Displays - Microsoft Internet Explorer		
Elle Edit View Favorites Iools Help		-
😋 Back • 🕞 · 🖹 🖻 🏠 🔎 Search 👷 Favorites 🤣 😒 • 🌉 🔯 • 🛄 🞯 • 🦓		
Address alphttps://172.16.254.79:5825/Reports/Displays.php?sa=c910d79d37bb827f5a1a0ebe7e070e75	🔽 🄁 Go 🛛 I	_inks »
Extreme Networks Summit ^{va} WM-Series Console Reports & Displays	extreme	<u>^</u>
Home Logs & Traces Reports Summit [™] Switch Altitude [™] APs WM-AD Configuration Summit [™] Spy	About LOGOU	T .
Displays: List of Displays • Reports: Forwarding Table OSPF Neighbor OSPF Linkstate WAP In-	ventory	
Active Altitude™ APs		
Active Clients by Altitude™ AP		
Active Clients by WM-AD		
Port & WM-AD Filter Statistics		
WM-AD Interface Statistics		
Summit [™] Switch Port Statistics		
Altitude™ AP Availability		
Dynamic Authorization Statistics		
Wired Ethernet Statistics by Altitude™ AP		
Wireless Statistics by Altitude™ AP		
[WM Summit WM200 1 days, 3:47] User: interop Port status: 🖲 🕕 📀 🔕 🔕	Software: V4 R1.3.14	4
		~
۵ ا ا ا	Secol intranet	.;

Select "AltitudeTM AP Availability" from the main reports menu to verify whether the APs are available. All available APs are shown in green.

🗿 Altitude 🖱 AP Availability - 172.16.254.7	9 - Microsoft Internet Exp	lorer		
Altitude™ AP Availability - 172.16.2	No refresh	O Refresh every 30	secs Apply	
[Local] AP-1 100000634D081153 00:04:96:28:03:54 uptime: 2 d, 21:18:01 172:28:12:55	[Local] AP-2 100000634D081005 00:04:96:2B:02:C0 uptime: 2 d, 21:18:03 172.28.13.50		[Local] AP-3 100000634D081011 00:04:96:28:02:C6 uptime: 2 d, 21:18:03 172.28.12.52	
Data as of Aug 09, 2007 08:38:39 am			Refresh	Close

Select "Active AltitudeTM 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.

🗿 Active Altitude" APs - Microsoft Internet Explorer													
Active Altitude™ APs - 172.16.254.79											S Apply		
Altitude™ AP	Serial	WAP IP	Clients	Home	Tunnel Duration	Packets Sent	Packets Rec'd	Bytes Sent	Bytes Rec'd	Uptime	802.11b/g Ch/Tx	802.11a Ch/Tx	
AP-1	100000634D081153	172.28.12.55	0	Local	2763 d, 4:59:31	141223	158279	16433261	15411151	2 d, 21:18:01	6/8dBm	52/8dBm	
AP-2	100000634D081005	172.28.13.50	0	Local	2763 d, 4:59:26	137292	146149	15599062	9978933	2 d, 21:18:03	1/8dBm	56/8dBm	
AP-3	100000634D081011	172.28.12.52	0	Local	2763 d, 5:02:03	140365	158046	16492264	15567683	2 d, 21:18:03	6/8dBm	60/8dBm	
Summary	3 active WAPs		0										
* Auto channel selected by AP													
Data as of Aug 09, 2007 08:38:24 am Refresh Export Close													

Select "Active Clients by AltitudeTM 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.

🗿 Active Clients by Altitude" AP - 172.16.254.79 - Microsoft Internet Explorer															
Active Clients by Altitude™ AP - 172.16.254.79 O No refresh @ Refresh every 2 secs Apply															
Users AP-1 100000634D081153															
AP-1 AP-2	1	WAP Client IP Client MAC Protocol BSS MAC SSID Auth. / Filter Time User Packets Packets Bytes By											Bytes Rec'd		
AF-J		0	192.168.100.60	00:19:5B:8D:0A:47	802.11a	00:04:96:2B:D5:40	acm	None / WPA-PSK	Default	0:04:13	n/a	46	187	5402	20045
		Traffic	Summary								1	46	187	5402	20045
Active Users: 1 Search Client by User name 💌 Search															
Data as of Aug 09, 2007 09:06:18 am Selected clients: Add to Blacklist Disassociate Export Close															

9. Support

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

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 <u>http://www.extremenetworks.com</u>

- [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

©2007 Avaya Inc. All Rights Reserved.

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.