Dell PowerEdge VRTX Networking Deployment Guide: for Microsoft Lync and Dell Mobility

Tracy Alonzo

Network Solutions Engineering



This document is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

© 2013 Dell Inc. All rights reserved. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell, the Dell logo, and PowerEdge are trademarks of Dell Inc. Intel and Xeon are registered trademarks of Intel Corporation in the U.S. and other countries. Microsoft, Windows, and Windows Server are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others.

June 2013 | Rev 1.0

Contents

Executive Summary
Introduction
Networking for Dell PowerEdge VRTX Chassis7
Deployment Scenarios8
Small Office Deployment Components8
Intermediate Office Deployment Components9
Initial CMC Network Configuration 10
Logging into Chassis Management Controller (CMC) Using WEB Interface
Initial Blade Server Status 11
Accessing Blade Servers 12
Accessing the VRTX 1GbE Switch Module 15
Logging into the VRTX 1GbE Switch Module15
Setting Up Dell Mobility Controller 17
Dell Mobility Controller Login
AOS Version
Licenses
Virtual AP Employee Profile
Dynamic Multicast Optimization (DMO) 19
Band Steering
Access Control List (ACL) with Classify Media
Employee User Role
SSID Profile
Delivery Traffic Indication Message (DTIM) 22
Wireless Multimedia (WMM)
Differential Services Code Point (DSCP) 22
Local Probe Request Threshold (dB) 23
Broadcast/Multicast Rate Optimization (BC/MC)
Adaptive RADIO Management (ARM) Profile 24
VOIP Aware Scan
Power Save Aware Scan 24
Quality of Service (QoS) Profile
Airtime Fairness
Guest WLAN
Assigning the Guest VLAN Static IP address and Source NAT

Dell PowerEdge VRTX Networking Deployment Guide: for Microsoft Lync and Dell Mobility

	Adding DHCP Guest Pool	. 27
	Display Guest Pool	. 28
	Guest Role Network Policies	. 28
	Guest Role Time Range	. 29
	Create Guest Role	. 30
	Guest Virtual AP	. 30
	Guest Wireless Client Connection	. 32
	Mobility Controller Guest VLAN Interface now "UP"	. 32
A	dditional Resources	. 33
	Dell PowerEdge VRTX Product Page	. 33

Figures

Figure 1.	Dell PowerEdge VRTX Chassis
Figure 2.	Small Office Deployment8
Figure 3.	Intermediate Office Deployment9
Figure 4.	CMC Login 10
Figure 5.	Chassis Server Overview 11
Figure 6.	Powering On Blade Server 11
Figure 7.	Launch iDRAC GUI 12
Figure 8.	Accessing blade server
Figure 9.	Opening Viewer 13
Figure 10.	Starting Application
Figure 11.	Blade server Access
Figure 12.	I/O Module Status
Figure 13.	1GbE Switch Module Login 16
Figure 14.	VRTX 1GbE Switch Module Home Page 16
Figure 15.	Mobility Controller Login 17
Figure 16.	Mobility Controller Dashboard 17
Figure 17.	AOS Version
Figure 18.	Licenses
Figure 19.	VAP Employee
Figure 20.	Virtual AP Employee Profile 19
Figure 21.	Employee_Lync User Role
Figure 22.	Employee_Lync Policy Rules
Figure 23.	Employee_Lync Policies

Dell PowerEdge VRTX Networking Deployment Guide: for Microsoft Lync and Dell Mobility

Figure 24.	Creating Employee SSID 2	1
Figure 25.	Employee SSID Profile Settings 2	2
Figure 26.	Local Probe Request Threshold 2	23
Figure 27.	Adaptive RADIO Management (ARM) Profile 2	24
Figure 28.	Traffic Management Profile 2	25
Figure 29.	Create Guest VLAN 2	25
Figure 30.	Assign VLAN Static IP Address with Source NAT 2	.6
Figure 31.	Show VLANS 2	.6
Figure 32.	Enable DHCP and add Guest Pool 2	27
Figure 33.	Guest DHCP Settings 2	27
Figure 34.	DHCP Guest Pool 2	.8
Figure 35.	Guest Role 2	.8
Figure 36.	Guest Role Policies 2	.9
Figure 37.	Time Range 2	.9
Figure 38.	Create Guest Role 3	0
Figure 39.	Guest VAP 3	0
Figure 40.	Virtual AP Guest	51
Figure 41.	Guest SSID Profile 3	51
Figure 42.	Client's Connection	2
Figure 43.	Mobility Controller Guest VLAN Operational "Up" Status	32

Executive Summary

Dell PowerEdge VRTX is a new shared infrastructure product focused on remote, branch, and small office needs. It combines Dell PowerEdge M520 and M620 server blades, shared storage, and IO in the form of PCIe and one IOM slot. These elements are combined into a 5U rackable tower, providing a simpler model for Remote Office/Branch Office (ROBO) and Small and Medium Business (SMB) customers to deploy and manage. The Dell 1GbE switch I/O Module (IOM) includes eight external Gigabit Ethernet ports providing network connectivity to the Dell PowerEdge Blade servers within the Dell PowerEdge VRTX chassis.

Introduction

This deployment guide outlines the steps of connecting the VRTX to a SMB network including integration options for Dell W-Series WLAN Mobility controller. Dell PowerEdge VRTX is designed to empower ROBO's and SMB's with the connectivity, along with its optimized storage and compute power to deliver an end -to- end solution optimized for providing for time sensitive applications like Microsoft Lync.

ROBO's can now take advantage of running media collaborative applications like Microsoft Lync providing voice, video, and instant messaging (IM). With the flexibility of Dell's PowerEdge VRTX chassis, a virtualized Microsoft Lync Server can be hosted right on premise.

Networking for Dell PowerEdge VRTX Chassis

Dell PowerEdge VRTX can be configured with an integrated 1Gb pass-through switch module or an integrated 1GbE switch module, simplifying network connectivity and reducing costs for small business budgets. The 1GbE switch module is recommended for most applications. The diagrams below show the physical architecture and some representative logical network topologies for small and intermediate office deployments.



Deployment Scenarios



Figure 2. Small Office Deployment

Wired Desktop User

Small Office Deployment Components

Number of Users	1-5
Chassis Platform	Dell PowerEdge VRTX
Servers	Dell PowerEdge M520 or M620 Blade installed in slots 1-4
Operating System	1x Windows 2012 Server
Network	Integrated 1GbE switch module with 8 external RJ45 ports



Figure 3. Intermediate Office Deployment

Intermediate Office Deployment Components

Number of Users	25-50
Chassis Platform	Dell PowerEdge VRTX
Servers	Dell PowerEdge M520 or M620 Blade installed in slots 1-4
Operating System	1x Windows 2012 Server
Applications	1x Microsoft Lync Standard Edition Server
Network	Integrated 1GbE switch module with 8 external RJ45 ports 1x Dell Networking 5524P
Wireless Network	Access Point - Dell Networking W-AP105 Mobility Controller - 1x Dell Networking W-620

NOTE: Each Remote Office/Branch Office may have unique RF environments. A wireless Site Survey is highly recommended to ensure best results.

Initial CMC Network Configuration

By default, the Chassis Management Controller (CMC) is set to obtain IP address from an external DHCP server. By connecting the CMC network cable to the network, an IP address will be assigned to the CMC. This can be verified by using the VRTX LCD configuration wizard.

From the LCD panel on the front of the chassis, select IP summary from the main menu screen. (Use up and down arrow button to navigate pressing the center button to select) The CMC IP address is displayed along with iDRAC1 and iDRAC2.

For a detailed description on configuring the CMC settings, please see the Dell PowerEdge VRTX User's Guide <u>Dell PowerEdge VRTX User's Guide</u>

Logging into Chassis Management Controller (CMC) Using WEB Interface

Open a WEB browser, in the address field, enter the CMC IP address. Figure 4 shows the Login screen to the Dell PowerEdge VRTX Chassis Management Controller. Enter the default Username: *root* and Password: *calvin*, *and click* Submit.

NOTE: Dell recommends customers set unique username and password.



Figure 4. CMC Login

Initial Blade Server Status

Figure 5 shows two M-Series blade servers. Note the Power state field.

Figure 5. Chassis Server Overview

VRTX Chassis Man	agement Control	ler Express				8
CMC-002 PowerEdge VRTX root, Administrator	Properties Status WW	Setup Power	Troubleshooting			
Chassis Overview Chassis Controller Server Overview	Servers	Status				
1 SLOT-01	Slot	Name	Model	Health	Power State	Service Tag
2 SLOT-02		SLOT-01	PowerEdge M520		Off	7GCFQV1
3 SLOT-03 4 SLOT-04	1					Launch: IDRAC
I/O Module Overview		SLOT-02	PowerEdge M620			34YJQV1
A Gigabit Ethernet	2					Launch: IDRAC

In figure 6, enable the Blade Server slot.

NOTE: Each Dell PowerEdge M-Series blade server can be powered on by pressing the power button on the front bezel.

Properties	Setup	Power	Troubleshooting					
Control	Priority							
Power	Power Control							
Informa	ition							
	Setting change	s on this	page may not be refle	cted immediately. Refreshi	ing the page after an appro;	priate delay will display the new values.		
-								ļ
						Operation Accients all covers		
Slot	Name		Model	Priority	Power State	No Operation		
1	SLOT-01		PowerEdge M520	1	Off	Power On Server		
2	SLOT-02		PowerEdge M620	1				
						Cancel	pply	

Figure 6. Powering On Blade Server

Accessing Blade Servers

In figure 7, under Server Overview, highlight the Dell PowerEdge blade server slot then click Launch iDRAC GUI to open Integrated Dell Remote Access Controller

Figure 7. Launch iDRAC GUI

VRTX Chassis Manag	gement Controller Express	Sup				
CMC-002 PowerEdge VRTX root, Administrator	Properties Setup Power Status					
Chassis Overview	Server Status					
Server Overview SLOT-01 SLOT-02	Jump to: Properties I/O Fabric Interfaces iDRAC System Settings WWN/MAC Addresses	Event Log Common iDRAC Network Settings IPv4 iDRAC Network Settings IF				
SLOT-02 SLOT-03 SLOT-04 SLOT-04						
 I/O Module Overview A Gigabit Ethernet 	Attribute	Value				
PCle Overview	Slot	1				
-2 PCle Slot 2	Slot Name	SLOT-01				
-3 PCIe Slot 3	Present	Yes				
-4 PCle Slot 4 -5 PCle Slot 5 -6 PCle Slot 6 Server Model PowerEdge M520						
Front Panel	iDRAC Firmware	1.36.35 (Build 04)				

Figure 8 shows the Integrated Dell Remote Access Controller System Summary page. Under Virtual Console Preview, click Launch

Figure 8. Accessing blade server



Figure 9. Opening Viewer

Opening viewer.jnlp(172.25.106.232@0@idrac-BGCFQ¥1,+PowerE 🗙							
You have chosen to open:							
3854233@5T1=2a78a7b3c53db32def9400404444d01) which is a: JNLP File (3.6 KB) from: https://172.25.106.232							
What should Firefox do with this file?							
Open with Java(TM) Web Start Launcher (default)							
C Save File							
Do this automatically for files like this from now on.							
OK Cancel							

Figure 10. Starting Application

Starting applic	Starting application 🔀							
Verifying								
Name:								
Publisher:	Publisher: Dell Inc.							
Location:								
		Cancel						

Figure 11 shows the Integrated Dell Remote Access Controller connection to the Dell PowerEdge M-Series blade server. Network connectivity to the blade server can be setup.

Figure 11. Blade server Access

🖸 idrac-BGCF0	QV1, P	owerEd	ge M520,	Slot 1, l	Jser: cm	: root, 2.3 fp	s		
Virtual Media	File	View	Macros	Tools	Power	Next Boot	Chat	Performance	Help
Recycle Bin									
MS20_BIOS									
Data Center									
1505									

Accessing the VRTX 1GbE Switch Module

Figure 12 shows the I/O Module Overview. Launch IOM GUI.

NOTE: By default, the 1GbE switch module obtains its IP address from the local DHCP server. However, users can assign a static IP address by selecting the <Setup> entry from the I/O Module Overview page.

Figure 12. I/O Module Status

	NAGEMEN	T CONT	ROLLER Exp	ress	
CMC-PLSC001 PowerEdge VRTX	Properties	Setup	Power Tro	ubleshooting Update	
root, Administrator	Status				
Chassis Overview	I/O N	lodule	Status		
+ Server Overview					
I/O Module Overview	Slot	Health	Fabric	Name	Launch IOM GUI
A Gigabit Ethernet	А		Gigabit Ethernet	R1-2401 ROBO 1Gb Switch Module	Launch IOM GUI

Logging into the VRTX 1GbE Switch Module

Figure 13 shows the Login screen to the VRTX 1GbE Switch Module. Enter the default Username: *root* and Password: *calvin*, *and click* Submit.

NOTE: Dell recommends customers set unique username and password.



Figure 13. 1GbE Switch Module Login

Figure 14 shows the VRTX 1GbE Switch Module **Home** page. All Layer 2 switch configuration settings can be performed from this location.

Figure 14. VRTX 1GbE Switch Module Home Page



Setting Up Dell Mobility Controller

Dell Mobility Controller Login

Enter your User name and password created during the Console Configuration Setup.



then click Submit.				
ssword:				
	<i></i>			
	then click Submit. ssword:	then click Submit. ssword:	then click Submit. ssword:	then click Submit. ssword:

Figure 16 illustrates the initial Dell Mobility Controller Dashboard page.

Figure 16. Mobility Controller Dashboard

DØLI		мов	ILITY	CONTRC	LLER	P	owerCor	nect	W-620		Powered t Aruba Net	oy tworks	
Dashboard	Mon	itoring	Conf	iguration	Diagnos	stics	Maintena	ance	Plan	2			
> Performan	e												
Usage		Client	s										A
Security		Total:	0									Â	c
Potential Iss	ues	Client	PHY										
WLANs		a	0	aHT 0	a HT	40MH	lz 0						G
Access Point	s	b	0	gin o	giii	4011	12 0						Fr
Clients		SNR (d	dB)										Fr
		10 Speed) 1	5 20	25	30	35 4	0 4	45 5	D	55 60	E	
				<u> </u>	10.14		26.14						N

AOS Version

You can check the current version by selecting the **Maintenance** tab from the Dashboard, then choosing **About**, as shown in Figure 17.

Figure 17. AOS Version

D¢L	мс	BILITY CONTROL	LER PowerConnect W-620 Powered by Aruba Networks							
Dashboard	Monitoring	Configuration D	iagnostics Maintenance Plan 🦿							
CONTROLLER	2	Controller > Abou	ıt							
 About Image Mar Reboot Condition Clear Configure Synchroniz Boot Param 	nagement ntroller ïg re Database neters	Name: Model: Version: Compiled: WebSite: Legal:	Aruba Operating System Software. Dell PowerConnect W-620 Controller-US 6.1.3.6 2012-12-11 at 14:51:24 PST (build 36470) by p4build <u>http://www.dell.com</u> Copyright (c) 2002-2012, Aruba Networks, Inc.							
FILE Copy Files Copy Logs		AP-104 FCC ID: AP-105 FCC ID:	Q9DAP104 Q9DAP105SDR							
Copy Cras Backup Fla	h Files sh	AP-124 FCC ID: AP-125 FCC ID: AP-134 FCC ID:	Q9DAP124125SDR Q9DAP124125SDR Q9DAP134135							

Licenses

Figure 18 illustrates all licenses installed on the Dell mobility controller. Verify that the Access Point license and the Policy Enforcement Firewall Next Generation (PEFNG) license are installed. To verify, navigate to **Configuration** -> **Network** -> **Controller** -> **Licenses**.

Figure 18. Licenses

License Table				
Key	Installed	Expires	Flags	Service Type
4XCuVBqI-Y/xtJXn9-JHQrQ6lv-ADzbh/lu-iKyDMOY/-XPQ	2012-01-31 11:26:55	Never	E	Access Points: 4
cB9C8fJd-ZsSRdT/+-BLCH+GIA-lEJ3JmhB-2wuGyGQx-tns	2012-01-31 11:27:34	Never	E	RF Protect: 4
35X0deWk-CNqWUGew-WZXwCOEs-zlYP/WuE-eOk2mL4T-BT0	2012-01-31 11:27:56	Never	E	Next Generation Policy Enforcement Firewall Module: 4
FSkGZ3dP-/mwOY1TP-HVA1kB94-aNmh1ydb-c3RbnQ81-lhk	2012-01-31 12:42:09	Never	E	Power Over Ethernet
Flags: A - auto-generated; E - enabled; R - reboot required to activ	vate			

Virtual AP Employee Profile

Add Employee virtual AP to default AP group. Navigate to **Configuration** -> **All Profiles** -> **Wireless LAN** -> **Virtual AP**, as shown in Figure 19. Then choose to add a "New" profile, specify the name of the profile (for example, "employee") and click **Add**. Then click **Apply**.

Dell PowerEdge VRTX Networking Deployment Guide: for Microsoft Lync and Dell Mobility

			FI	gule 19.	VAP	Linploye	ee							
Dashboard	Monitoring	Configuration	Diagnostics	Maintenance F	Plan S.	ave Configuration) 🗶							
WIZARDS AP Wizard		Configuration >	AP Group > E	dit "default"										
Controller	Wizard		Prof	iles					Profile Details					
WLAN/LAN	Wizard	Wireless LAN				Virtual APs								
License Wi	zard	 Virtual AP 				none available								
WIP Wizard	d	🛨 RF Managem	ent			Add a profile	NEW	-	employee	Add				
NETWORK Controller VLANs Ports Uplink IP		 AP QOS IDS Mesh 												
SECURITY Authentical Access Cor WIRELESS > AP Config	tion ntrol juration													

Figure 19. VAP Employee

Dynamic Multicast Optimization (DMO)

Select the Dynamic Multicast Optimization (DMO) checkbox, as shown in Figure 20.

Figure 20. Virtual AP Employee Profile

Configuration > AP Group > Edit "default"

Profiles			Profile Details		
 Wireless LAN Virtual AP 		Virtual AP > employee		Show Reference	e Save As Re
 employee 		Virtual AP enable		Allowed band	all 🔻
AAA Profile	default	VLAN	1 ~ 1 •	Forward mode	tunnel 👻
802.11K Profile	default	Deny time range	NONE	Mobile IP	
 SSID Profile WMM Traffic Management Profile 	default	HA Discovery on- association		DoS Prevention	
 RF Management 		Station Blacklisting		Blacklist Time	3600 sec
 AP QOS IDS 		Dynamic Multicast Optimization (DMO)		Dynamic Multicast Optimization (DMO) Threshold	6
Mesh M ■ M ■ S 和 S 和 S 和 S 和 S 和 S 和 S 和 S 和 S 和 S 和 S 和 S 和 S 和 S 和 S 和 和 和 和 和 和 和 和 和		Authentication Failure Blacklist Time	3600 sec	Strict Compliance	
		VLAN Mobility		Preserve Client VLAN	
		Remote-AP Operation	standard 👻	Drop Broadcast and Multicast	
		Convert Broadcast ARP requests to unicast		Disable conversion multicast RA packets to unicast	
		Deny inter user traffic		Band Steering	
		Steering Mode	prefer-5ghz 🔻		

Band Steering

To enable this feature, click the **Band Steering** checkbox, as shown in Figure 20 above. **Steering Mode** defaults to **"Prefer 5ghz"**. Verify that it is selected. Click **Apply** to apply the changes. It is good practice to save the configuration.

With the Band Steering feature enabled, Dell access points will ignore 802.11 management Probe Requests from 2.5GHz RADIO client stations and will onl respond to Probe Requests from client stations in the 5GHz frequency band, effectively steering stations to the preferred spectrum.

Access Control List (ACL) with Classify Media

Employee User Role

Figure 21 illustrates how to configure employee user roles. Navigate to **Configuration** -> **Security** -> **Access Control** -> **Policies** -> **Firewall Policies.** Create six new rules. Add an IP access-list session named **Employee_Lync.**

Figure 21. Employee_Lync User Role

DØL	мс	DBILITY CONTRO	DLLER Pov	werConnec	W-620	Powered by Aruba Networks				5	Bupport	Log Out
Dashboard	Monitoring	Configuration	Diagnostics	Maintenance	Plan	Save Configuration	2					
WIZARDS		Security > Acce	ss Control > Use	er Roles								
AP Wizard	lined	User Roles S	System Roles	Policies T	ime Range	s Guest Access						
WI AN/I AN V	Nizard	Name			Firev	vall Policies		Bandwidth (Contract	Action	s	
License Wiza	ard	authenticated	allowall/,v6-allow	vall/				Up:Not Enforced D Enforced	own:Not	Show Reference	Edit	Delete
WIP Wizard		cpbase	Not Configured					Up:Not Enforced D Enforced	own:Not	Show Reference	Edit	Delete
Controller		default-via-role	allowall/					Up:Not Enforced E Enforced	own:Not	Show Reference	Edit	Delete
VLANs		default-vpn- role	allowall/,v6-allow	vall/				Up:Not Enforced E	own:Not	Show Reference	Edit	Delete
Uplink		denyall	Not Configured					Up:Not Enforced D	own:Not	Show Reference	Edit	Delete
IP		employee-lync	employee_lync/					Up:Not Enforced E	Down:Not	Show Reference	Edit	Delete
SECURITY Authenticatio	on	guest	http-acl/,https-ac icmp-acl/,v6-dns-	:l/,dhcp-acl/,io -acl/	:mp-acl/,dns	-acl/,v6-http-acl/,v6-h	https-acl/,v6-dhcp-acl/,v6-	Up:Not Enforced D Enforced	own:Not	Show Reference	Edit	Delete
Access Cor	ntrol	guest-logon	logon-control/,ca	ptiveportal/,v	6-logon-con	trol/,captiveportal6/		Up:Not Enforced E Enforced	own:Not	Show Reference	Edit	Delete
WIRELESS AP Configure	ation	logon	logon-control/,ca	ptiveportal/,v	pnlogon/,v6	-logon-control/,captive	eportal6/	Up:Not Enforced E Enforced	Down:Not	Show Reference	Edit	Delete
AP Installati	on	voice	sip-acl/,noe-acl/, acl/,icmp-acl/	svp-acl/,voce	ra-acl/,skinr	ny-acl/,h323-acl/,dhcp	-acl/,tftp-acl/,dns-	Up:Not Enforced D Enforced	own:Not	Show Reference	Edit	Delete
MANAGEMENT		Add										

Once Employee_Lync has been created, Figure 22 illustrates the six policies to be added.

Figure 22. Employee_Lync Policy Rules

Sec	urity > Firewall Policies > Edit Session (employee_lync)												
Us	er Roles	System R	oles Policie	s Time F	Ranges	Guest	Access						
R	ules												
	IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Pause ARM Scanning	BlackList	Classify Media	
I	Pv4	any	10.36.0.0 255.255.0.0	tcp 5223	permit			Low				Yes	
I	Pv4	Lync- servers	any	tcp 1024- 65535	permit			Low				Yes	
I	Pv4	any	any	tcp 5061	permit			Low				Yes	
I	Pv4	any	any	udp 5061	permit			Low				Yes	
I	Pv4	any	any	any	permit			Low					
I	Pv6	any	any	any	permit			Low					
1	Add												

Once all rules have been created and applied, Figure 23 displays Employee_Lync session.

	Control > Fi	rewall Po	licies					
r Roles Sys	stem Roles	Policies	Time Ranges	Guest A	Access			
olicies	All IPv4	Session	IPv6 Session	Ethernet	MAC	Standard	Extended	
N	ame		Туре		Rule	Count		Policy Usage
inny-acl		se	ssion	1			voice	
p-acl		se	ssion	1			voice	
logout		se	ssion	1				
cp-acl		se	ssion	1			voice gue	st
p-acl		se	ssion	1			guest	
-acl		se	ssion	6			ap-role	
p-acl		se	ssion	2			voice	
e-acl		se	ssion	1			voice	
23-acl		se	ssion	2			voice	
nployee_lync		se	ssion	6			employee	-lync

Figure 23. Employee_Lync Policies

SSID Profile

Configuring an SSID profile is shown in Figure 24. Navigate to Configuration -> Wireless -> AP Configuration -> Wireless LAN -> Virtual AP -> employee -> SSID Profile. Then select "New" from the SSID Profile pull-down menu. Type "dell-ap" is the default Network Name (SSID). This can be customized to each Branch Office location. The SSID can be up to 32 characters and is case sensitive. Under 802.11 Security, select WPA2 PSK as the Network Authentication and AES will automatically be selected as encryption. For format, select PSK Passphrase, then enter passphrase.

Figure 24. Creating Employee SSID

Dashboard Monitoring	Configuration	Diagnostics	Maintenance	Plan	Save Configuration	2			
WIZARDS AP Wizard	Configuration >	AP Group > E	dit "default"						
Controller Wizard		Prof	iles				Profil	e Details	
WLAN/LAN Wizard	Wireless LAN								
License Wizard	Virtual AP				SSID Profile >	 default 	•	Show Refer	ence Save As Reset
WIP Wizard	employee				Basic Adv	vanced			
NETWORK	AAA Pro	file		default					
Controller	802.11K F	Profile		default	Network Na	ame (SSID)		dell an	
Ports	 SSID Pro 	file		default	incenter ind			deir-dp	
Uplink	EDCA	Parameters Station	profile		802.11 Se	curity			
IP SECURITY	EDCA High-ti	Parameters AP prof	ile ofile	default	Network Au	uthentication	• None C 802.1x/WEP C Mixed	C WPA C WPA-PSK	C WPA2 C WPA2-PSK
Authentication Access Control	WMM Tr	affic Management P	rofile		Encryption		• Open O WEP		
WIRELESS > AP Configuration AP Installation	 RF Managem AP QOS IDS 	ent			Keys				

NOTE: Please consult your local Network Administrator for Pass-Phrase Security Settings.

Delivery Traffic Indication Message (DTIM)

Delivery Traffic Indication Message (DTIM) configuration is shown in Figure 25. Select **Configuration** -> Advanced Services -> All Profile Management -> SSID Profile -> employee ->Advanced. Then enter 3 into the DTIM Interval field.

DTIM Interval	3			bead perio	con ods	Sta	tion A	ge	out Tii	me		1(000			sec	2
902 11g Transmit Pater		1		2		5		•	6	V	9		~	11		\checkmark	12
002.11g Hansmit Rates	◄	18	~	24		36		•	48	v	5	4					
902 11e Racio Dates	~	1	•	2	Γ	5			6	Γ	9			11			12
ouz.rig basic Rates		18		24		36			48	Γ	5	4					
902 115 Transmit Dates	~	6		•	9			13	2		•	18			~	24	
602.11a Transmit Rates		36		•	48		•	54	4								
000 the Basis Bates	~	6			9			12	2			18			~	24	
602.11a basic Rates		36			48			54	4								
Max Transmit Attempts	8					RTS	6 Thre	esho	bld			23	333			byt	tes
Short Preamble						Max	(Asso	ocia	tions			64	ļ				
Wireless Multimedia (WMM)						Win APS Pow	eless SD (W versav	Mu /MM ve	ltimed I-UAP:	dia U- SD)		V					
WMM TSPEC Min Inactiv Interval	ity 0			mse	с	Ove for	erride WMM	DS clie	CP m ents	appir	ngs	Γ]				
DSCP mapping for WMI voice AC	46					DS0 vide	CP ma ao AC	app C	ing fo	or WM	м	40)				

Figure 25. Employee SSID Profile Settings

When setting DTIM to a value of 3, every third Management Beacon frame is a DTIM beacon for client stations to wake from a power management state to retrieve multicast traffic from Dell access points.

Wireless Multimedia (WMM)

Wireless Multimedia (WMM) is enabled by selecting the checkbox, as shown in Figure 25.

The Wi-Fi Alliance includes Wi-Fi Multimedia (WMM) as part of its Certification Program. Wi-Fi Multimedia defines Layer-2 MAC methods needed to meet the Quality of Service (QoS) requirements for time-sensitive applications.

Differential Services Code Point (DSCP)

Set **DSCP mapping for WMM voice AC** field to value of **46**, as shown in Figure 25. See RFC 3246 Section 2.7 Recommended Code Point for Expedited Forwarding, <u>http://datatracker.ietf.org/doc/rfc3246/</u>.

Dell PowerEdge VRTX Networking Deployment Guide: for Microsoft Lync and Dell Mobility

Local Probe Request Threshold (dB)

Set the Local Probe Request Threshold (dB) field to value of 25, as shown in See Figure 26.

Figure 26.	Local	Probe	Request	Threshold
inguic 20.	Locut	1 I ODC	ricquest	

Counters			
Deny_Broadcast Probes		Local Probe Request Threshold (dB)	25
Disable Probe Retry		Battery Boost	
WEP Key 1	Retype:	WEP Key 2	Retype:
WEP Key 3	Retype:	WEP Key 4	Retype:
WEP Transmit Key Index	1 -	WPA Hexkey	Retype:
WPA Passphrase	Retype:	Maximum Transmit Failures	0
BC/MC Rate Optimization		Rate Optimization for delivering EAPOL frames	
Strict Spectralink Voice Protocol (SVP)		802.11g Beacon Rate	default 👻
802.11a Beacon Rate	default 👻	Advertise QBSS Load IE	

Broadcast/Multicast Rate Optimization (BC/MC)

Select the BC/MC Rate Optimization checkbox to enable the feature, as shown in Figure 26.

This feature suppresses broadcast and multicast traffic on both wired and wireless networks.

Adaptive RADIO Management (ARM) Profile

VOIP Aware Scan

Navigate to Configuration -> All Profiles -> RF Management -> Adaptive RADIO Management ARM Profile -> <profile name>-> ARM Profile Details -> VOIP Aware Scan.

Adaptive Radio Manag default	ement (ARM) profile >	Show Reference Save As Reset			
Assignment	single-band 👻	Allowed bands for 40MHz channels	a-only 🔻		
Client Aware		Max Tx EIRP	127 👻		
Min Tx EIRP	9 🔻	Multi Band Scan			
Rogue AP Aware		Scan Interval	10 sec		
Active Scan		Scanning			
Scan Time	110 msec	VoIP Aware Scan			
Power Save Aware Scan		Video Aware Scan			

Figure 27. Adaptive RADIO Management (ARM) Profile

This feature prevents any single access point from becoming congested with voice calls. Dell access points will not attempt to scan different channels if one client has an active VOIP call.

Power Save Aware Scan

Select the Power Save Aware Scan checkbox to enable the feature, as shown in Figure 27.

With this feature enabled, if Dell access points detect one or more clients in power save mode the access point will not scan across other channels.

Quality of Service (QoS) Profile

Airtime Fairness

Figure 28 illustrates the Traffic Management Profile. Navigate to **Configuration** -> **All Profiles** -> **QOS** - > **Traffic Management Profile** -> **Profile Details**. Add Lync by selecting it. In the **Station Shaping Policy** field, select **fair-access**.

This feature allows each wireless client station equal access to the wireless medium.

Profiles	Profile Details					
AP RF Management Wireless LAN Gos QoS WMM Traffic management profile Traffic management profile	Traffic management pr Proportional BW Allocation	Delete Virtual AP default Share(%) 100 Add	Show Reference Report interval	Save As Reset		
 VoIP Call Admission Control profile default 	Station Shaping Policy	fair-access 🔻				

Figure 28. Traffic Management Profile

Guest WLAN

Figure 29 illustrates adding a guest VLAN. Configuration -> Network -> VLANS -> Add -> VLAN ID -> enter 900 -> Apply.

Figure 29. Create Guest VLAN

D¢LL M	OBILITY CONTROLLER Power	Connect W-620 Powered by Aruba Networks	Support Log Out
Dashboard Monitoring	Configuration Diagnostics Ma	ntenance Plan Save Configuration 🦿	
WIZARDS	Network > VLAN > Add New VLAN		« Back
AP Wizard	Configuration		
Controller Wizard	VLAN ID	900	
VLAN/LAN WIZard	Associate with	Port C Port-Channel	
WIP Wizard	Wired AAA Profile	N/A 🔻	
NETWORK			
Controller	Deat Calenting		
> VLANs	Port Selection		
Ports		4 5 6 7	
Uplink IP		0 1 2 3 8	
SECURITY			
Authentication			
Access Control			Apply

NOTE: Customers can set their own VLAN assignment. The VLAN specified here is only for explanatory purposes.

Assigning the Guest VLAN Static IP address and Source NAT

Figure 30 shows assigning the guest VLAN static IP address. Select **Configuration** -> **Network** -> **IP** -> **IP interfaces** -> **Use the following IP address**. Then set VLAN900 to IP address 192.168.200.1 and a Net Mask of 255.255.255.0. Under NAT, enable source NAT for the VLAN checkbox. Under Inter-VLAN Routing, deselect **Enable Inter-VLAN Routing** checkbox. Then click **Apply**.

NOTE: Customers can set their own Static IP VLAN and Net mask assignments. The Static VLAN IP address and Net mask are only for explanatory purposes.

Switch VLAN Configurat	ion		👌 🔹 🗟 🔹 🖃 🖶 💌 Page 🔹 Safety 💌 Tools 💌 🔞 💌
D¢LL M	DBILITY CONTROLLER PowerConnect W-620	wered by uba Networks	Support Log Out
Dashboard Monitoring	Configuration Diagnostics Maintenance Plan Save	Configuration 🦿	
WIZARDS	Network > IP > IP Interface > Edit VLAN (900)		« Back
AP Wizard	>		
Controller Wizard	IP version	IPv4 🔻	
WLAN/LAN Wizard	VLAN ID	900	
License Wizard	Details	DHCP Helper Addresses	
WIP Wizard	C Obtain an IP address from DHCP	No Helper Addresses Cd	
NETWORK	Client ID	Add	
Controller		Option 82	
VLANs	Obtain an IP address with PPPoE	Option-62	one 🗸
Ports	Service name	ICMP	
Uplink	Username		E
> IP	Password	Enable IGMP	
SECURITY	Confirm Password	Snooping	
Authentication	• Use the following IP address	Proxy	
WIDELESS	IP Address 192.168.200.1	Interface Gigabitetherne	et 1/8 👻 🔿 Port-Channel ID 🛛 👻
AP Configuration	Net Mask 255.255.255.0	NAT	
AP Installation	Uplink Priority	Enable source NAT for this VI	AN 🔽
MANAGEMENT	· · ·	Inter-VLAN Routing	
General		Enable Inter-VLAN Routing	

Figure 30. Assign VLAN Static IP Address with Source NAT

Figure 31 shows the Dell mobility controller VLANS. Select **Configuration** -> **Network** -> **VLANS**. Guest VLAN is now displayed including assigned IP address and Net Mask.

Figure 31. Show VLANS

DEEL MO	BILITY CONTRO	DLLER F	PowerConnect W	-620 Powere Aruba J	ed by Networks					Support	Log Out
Dashboard Monitoring	Configuration	Diagnostics	Maintenance	Plan Save Cor	figuration 🧳						
WIZARDS	Network > IP >	IP Interface									
AP Wizard	IP Interfaces	IP Routes	IPv6 Neighbors	GRE Tunnels	NAT Pools DHC	P Server OSP	F Multicast				
Controller Wizard			TDv4 Not Mack	TDue Addroce	Accordiated Post		Admin State	Operation State	Mada	Action	-
WLAN/LAN Wizard	1 17	2.16.0.254	255.255.255.0	fe80::b:8600: -	FE1/0-7,GE1/8,Pc0-	7 N/A	Enabled	Up	Regular	Disable	Edit
WIP Wizard	900 19	2.168.200.1	255.255.255.0		1	N/A	Enabled	Down	Regular	Disable	Edit
NETWORK	Operation Per	formed Success	fully								
Controller											
VLANs											
Ports											
> IP											

NOTE: Figure 31 shows VLAN900 operation state as "down". This will change to "Up" state once a guest user establishes a connection to the Guest WLAN.

Adding DHCP Guest Pool

Figure 32 shows adding DHCP guest pool. Select **Configuration -> Network ->IP -> DHCP Server**. Check the **Enable DHCP Server** checkbox, then click **Add**.

Figure 32. Enable DHCP and add Guest Pool

D¢¢ll M	OBILITY CONTROLLER	PowerConnect W-620 Powered by Aruba Netwo	orks		
Dashboard Monitoring	Configuration Diagnostic	Maintenance Plan Save Configur	ration 🦿		
WIZARDS	Network > IP > DHCP Serve	r			
AP Wizard	IP Interfaces IP Routes	IPv6 Neighbors GRE Tunnels NA	T Pools DHCP Server OSPF Multic	ast	
Controller Wizard			-		
WLAN/LAN Wizard	Enable DHCP Server				
License Wizard	Pool Configuration				
WIP Wizard	Name	Default Router	Network	Range	
NETWORK	Add				
Controller					
VLANs	Excluded Address Range				
Ports				Add	
Uplink	Excluded Address			Add	
> IP				Delete	

Figure 33 shows enabling DHCP and adding a guest pool. Enter "guestpool" into pool name field, then enter **192.168.200.1** as the default router. Enter the DNS Server address provided by your local network administrator, then enter **192.168.200.0** for Network IP address and **255.255.255.0** as the netmask. Finally, choose **Done -> Apply -> Save Configuration**.

Figure 33. Guest DHCP Settings

🙀 Favorites 🛛 🚔 🙋 Web Slice Gallery 🕶	events
Switch DHCP Configuration	📩 🔻 🗟 👻 🖃 👘 👻 Page 👻 Safety 💌 Tools 👻 🚷
	ROLLER PowerConnect W-620 Powered by Aruba Networks Support Log Out
Dashboard Monitoring Configurat	n Diagnostics Maintenance Plan Save Configuration 🦿
WIZARDS Network > 1 AP Wizard	> DHCP > Add DHCP Pool
Controller Wizard Pool Name WLAN/LAN Wizard Default Rou License Wizard DNS Server WIP Wizard DNS Server NETWORK Domain Nat	guestpool r 192.168.200.1 222.222 208.67.222.200 Import from DHCP/PPPoE (Multiple DNS Servers should be separated by spaces) a
Controller WINS Server VLANs Lease Ports Network Uplink > IP	s Import from DHCP/PPPGE (Multiple WINS Servers should be separated by spaces) Days Hrs Mins Secs IP Address[192.168.200.0] Netmask[255.255.255.0] Done Cancel
SECURITY	

Dell PowerEdge VRTX Networking Deployment Guide: for Microsoft Lync and Dell Mobility

Display Guest Pool

Figure 34 displays the DHCP Guestpool including default router, network address, and address range.

Figure 34. DHCP Guest Pool

D¢LL M	OBILITY CONTROL	LER PowerConnect W-	620 Powered by Aruba Networks			Support Log Out
Dashboard Monitoring	Configuration	Diagnostics Maintenance P	an Save Configuration	2		
WIZARDS	Network > IP > D	HCP Server				
AP Wizard Controller Wizard	IP Interfaces	IP Routes IPv6 Neighbors	GRE Tunnels NAT Pools	DHCP Server OSPF Multicast		
WLAN/LAN Wizard	Enable DHCP S	erver		\checkmark		
License Wizard	Pool Configura	tion				
WIP Wizard	Name	Default Router	Network	Range		Action
NETWORK	guestpool	192.168.200.1	192.168.200.0	192.168.200.2-192.168.200.254		Edit Delete
Controller	Add					
VLANs						
Ports	Excluded Addre	ss Range				
Uplink						
> IP	Excluded Addres	s			Add	

Guest Role Network Policies

Figure 35 illustrates setting policy role for guest users. Select **Policies**, then pick "guest network policy" under **Policy Name**. Choose Session under **Policy Type**. Then click **Add** -> **Http under services** -> **Permit** -> working hours -> **Add** -> **Https** -> **Permit** -> working hours -> **add** -> **Apply**.

Dashboard Monitorin	g Configuration	Diagnostics	Maintenance	Plan	ave Configuration	2	
WIZARDS	Security > Firewal	dd New Policy	/				
AP Wizard	User Roles Sys	stem Roles	Policies Tim	ne Ranges	Guest Access		
Controller Wizard							
WLAN/LAN Wizard							
License Wizard							
WIP Wizard	Policy Name				guest network	policy	
NETWORK	Policy Type				Session 👻		
Controller	Rules						
VLANs	IP Version Se	ource Destin	nation Servi	ce Action	Log Mirror	Queue	Time I
Ports	Add						
Uplink							
IP							
SECURITY	Commands						
Authentication	Communus						
Access Control							

Figure 35. Guest Role

			Figure 3	36. G	uest	Role	Polic	les		
Configuration	Diagno	ostics Mainte	nance Pla	an Sa	ave Con	tiguration	JZ			
Security > Fire	wall Polic	cies > Add Nev	v Policy							
User Roles	System R	oles Policie	5 Time F	Ranges	Guest	Access				
Deline Mana								1		
Policy Name					gues	sion -	policy			
Rules					000	SIGH .				
IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Pause ARM Scanning	BlackList
IPv4	any	any	svc-http	permit			low	working-hours	No	No
IPv4	any	any	svc-https	permit			low	working-hours	No	No
Add										
6 I										
Commands										

Figure 36 above illustrates HTTP and HTTPS services only allowed during work hours for guest users.

Guest Role Time Range

Figure 37 shows how to allow guest users WEB access only during business hours. Select Configuration -> Security -> Access Control -> Time Ranges -> Add -> guest work hours in "name" field -> Periodic -> Add -> Weekday -> 08:00 for start time -> 17:00 for end time -> Done -> Apply.

Figure 37. Time Range

WIZARDS	Security > Ac	cess Control > T	imeRange 3	> Add Time Ran	ge			
AP Wizard	User Roles	System Roles	Policies	Time Ranges	Guest Access			
Controller Wizard				-				
WLAN/LAN Wizard	Name			guest work hour	s			
License Wizard	Туре			C Absolute @ Periodic				
WIP Wizard		Start Day		Start Ti	ne	End Day	E	
NETWORK	Add							
Controller				Add Pe	riodic Rule			
VLANs	Start Day		O Daily	• Weekday C	Weekend C Day Sunday	/ 🔻		
Ports	Start Time((hh:mm)	08 :00					
IP	End Day		Sunday	Ŧ				
SECURITY	End Time(h	h:mm)	17 :00					
Authentication							Done Cancel	
> Access Control								

12

Create Guest Role

Figure 38 shows how to create guest user role. Select User Roles -> Add -> Guest role Name -> guest network policy from drop down list -> Done -> Apply.

Figure 38. Create Guest Role

er Roles	System Roles	Policies	Time Ranges	Guest Access		
Role Name	e			guest		
irewall P	olicies					
	Name		F	Rule Count	Location	Actio
Add						
• Cho	ose From Configure	ed Policies	guest network polic	cy (session) 🔻 Location		
C Crea	te New Policy Fron	n Existing Po	licy validuser (se	ssion) 👻 Create		
C Crea	te New Policy Cre	ate				
						r

Guest Virtual AP

Configuring guest virtual AP is shown in Figure 39. Select Configuration -> Wireless -> AP Configuration -> AP Specific -> select guest Ap's from the list -> Add -> select the guest AP -> Wireless LAN -> Virtual AP -> Add "new" profile named guest -> Apply.

Figure 39. Guest VAP

Dashboard Monitoring	Configuration Diagnostics Maintenance Plan	Save Configuration 🦿
WIZARDS AP Wizard	Configuration > AP Specific > Edit "00:24:6c:c0:23:3a"	n
Controller Wizard	Profiles ("default" group / AP specifc value)	Profile Details
WLAN/LAN Wizard	Wireless LAN	Virtual APs
License Wizard	 Virtual AP 	none available
WIP Wizard	Excluded Virtual AP	Add a profileNEW v guest Add
NETWORK	RF Management	
Controller	AP A	
VLANs		
Ports	IDS	
Uplink	Mesh	
IP		
SECURITY		
Authentication		
Access Control		
WIRELESS		
AP Configuration		

As shown in Figure 40, ensure Guest -> Virtual AP checkbox is enabled and VLAN is set, then select Apply. Select AAA Profile -> default-open -> Apply.

Profiles ("default" group / AP s	specifc value)	Profile Details						
Wireless LAN Virtual AP		Virtual AP > guest		Show Reference	e Save As			
 guest 		Virtual AP enable		Allowed band	all 🔻			
AAA Profile	default-open	VLAN	900 < 900 -	Forward mode	tunnel -			
802.11K Profile	default	Denv time range	NONE	Mobile IP				
 SSID Profile 	guest	HA Discovery on-						
EDCA Parameters Station profile		association		DoS Prevention				
EDCA Parameters AP profile		Station Blacklisting		Blacklist Time	3600 se			
High-throughput SSID Profile	default	Dynamic Multicast		Dynamic Multicast Optimization (DMO)	6			
WMM Traffic Management Profile		optimization (DHO)		Threshold				
Excluded Virtual AP		Authentication Failure Blacklist Time	3600 sec	Strict Compliance				
RF Management		VLAN Mobility		Preserve Client VLAN				
AP QOS		Remote-AP Operation	standard 👻	Drop Broadcast and Multicast				
 TDS IDS IDS 		Convert Broadcast ARP requests to unicast		Disable conversion multicast RA packets to unicast				
		Deny inter user traffic		Band Steering				
		Steering Mode	prefer-5ghz 👻					

Figure 40. Virtual AP Guest

As shown in Figure 41, select "New" SSID profile named "guest". Enter Network Name as guest. Choose "None" for Network Authentication and "Open" for Encryption. Then click Apply.

Figure 41. Guest SSID Profile

Profiles ("default" group / AP s	pecifc value)	Profile Details					
Wireless LAN		SSID Profile >					
Virtual AP		NEW 🔻 guest					
= guest		Pagic Advanced					
AAA Profile	default-open	basic Advanced					
802.11K Profile	default	Network					
 SSID Profile 	NEW	Network Name (SSID) guest					
EDCA Parameters Station profile	default	802.11 Security					
EDCA Parameters AP profile	default	€ None © 802.1x/WEP © WPA © WPA-PSK © WPA2 © WPA2-PSK					
High-throughput SSID Profile	default	Network Authentication C Mixed					
WMM Traffic Management Profile		Encryption Open C WEP					
Excluded Virtual AP		Vovs					
RF Management		1012					
AP							

Guest Wireless Client Connection

Figure 42 shows an established wireless client's connection status to the Guest SSID.

Figure 42. (Client's (Connection
--------------	------------	------------

n[] Wireless Network Connec	×						
Network Connection Detail:	Network Connection Details						
Network Connection Details:							
Property	Value						
Connection-specific DN Description Physical Address DHCP Enabled IPv4 Address IPv4 Subnet Mask Lease Obtained Lease Expires IPv4 Default Gateway IPv4 DHCP Server IPv4 DNS Servers	Intel(R) Centrino(R) Advanced-N 58-94-6B-94-8C-C0 Yes 192.168.200.254 255.255.255.0 Tuesday, May 07, 2013 12:24:3; Wednesday, May 08, 2013 12:24 192.168.200.1 192.168.200.1 208.67.222.220 209.67.202.220	6200 2 PM 4:32 , ≡					
IPv4 WINS Server NetBIOS over Tcpip En Link-local IPv6 Address IPv6 Default Gateway	Yes fe80::1cef:30d4:2d41:be2e%13	► lose					

Mobility Controller Guest VLAN Interface now "UP"

Figure 43 shows the Guest VLAN operational state as "Up". You can check the state by selecting Configuration -> IP -> IP Interfaces.

Figure 43.	Nobility (Controller	Guest '	VLAN O	perational	"Up"	Status
------------	------------	------------	---------	--------	------------	------	--------

MOBILITY CONTROLLER PowerConnect W-620 Powered by Aruba Networks									
Dashboard Monitoring	Configurati	Diagnostics	Maintenance	Plan Save Cor	figuration	7			
WIZARDS	Network > IF	> IP Interface							
AP Wizard	IP Interface	IP Routes	IPv6 Neighbors	GRE Tunnels	NAT Pools	DHCP Server	OSPF	Multicast	
Controller Wizard	VIAN TO	IDv4 Address	TDv4 Net Mack	TDV6 Address	Associated		Profile	Admin State	Operation State
WLAN/LAN WIZard	1	172.16.0.254	255.255.255.0	fe80::b:8600: -	FE1/0-7,GE1/	3,Pc0-7 N/A	Tome	Enabled	Up
WIP Wizard	900	192.168.200.1	255.255.255.0	fe80::b:8603: -	j	N/A	1	Enabled	Up
NETWORK									
Controller									
VLANs									
Ports									
Uplink									
> IP									

Additional Resources

Recommended Dell publications:

- Dell PowerEdge VRTX Product Page
- Dell Chassis Management Controller For PowerEdge VRTX
- Dell Networking W-Series Mobility
- Dell Networking W-Series Mobility Software
- Dell Networking W-Series Mobility Support
- <u>Microsoft Lync Server 2010 on Dell Systems</u>

Recommended Microsoft publications:

<u>Microsoft Lync Qualified Infrastructure</u>