

Dell PowerConnect W- AirWave 7.5 Best Practices Guide



Copyright

© 2012 Aruba Networks, Inc. Aruba Networks trademarks include  airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, and Aruba Mobility Management System®. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

All rights reserved. Specifications in this manual are subject to change without notice.

Originated in the USA. All other trademarks are the property of their respective owners.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011

Infoblox, Inc. All rights reserved. [This product includes software developed by Lars Fenneberg, et al.](#) The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Contents

Preface.....	1	
Document Organization.....	1	
Note, Caution, and Warning Icons	2	
Contacting Support	2	
Chapter 1	Overview	3
	Understanding Dell PowerConnect W-Series Topology	3
	Prerequisites for Integrating Dell PowerConnect W-Series Infrastructure.....	4
Chapter 2	Configuring AirWave for Global Dell PowerConnect W-Series Infrastructure	5
	Disabling Rate Limiting in AMP Setup > General.....	5
	Entering Credentials in Device Setup > Communication	5
	Setting Up Recommended Timeout and Retries	6
	Setting Up Time Synchronization.....	7
	Setting up NTP on AirWave	7
	Manually Setting the Clock on a Controller	7
	Enabling Support for Channel Utilization And Statistics.....	7
	AirWave Setup.....	8
	Controller Setup (Master And Local)	8
Chapter 3	Configuring a Dell PowerConnect W Group in AirWave	9
	Basic Monitoring Configuration.....	9
	Advanced Configuration.....	10
Chapter 4	Discovering Dell PowerConnect W-Series Infrastructure.....	11
	Discovering Master Controllers.....	11
	Local Controller Discovery.....	13
	Thin AP Discovery	13
Chapter 5	AirWave and Dell PowerConnect W-Series Integration Strategies	15
	Integration Goals	15
	Example Use Cases	16
	When to Use Enable Stats	16
	When to Use WMS Offload.....	16
	When to Use RTLS.....	16
	When to Define AirWave as a Trap Host	16
	When to use Channel Utilization.....	16
	Prerequisites for Integration	17
	Enable Stats Utilizing AirWave.....	17
	WMS Offload with AirWave	18
	Define AirWave as a Trap Host using ArubaOS CLI.....	18
	ArubaOS Traps Utilized by AirWave	19
	Auth Traps	19
	IDS Traps	19

	ARM Traps.....	20
	Ensuring That IDS And Auth Traps Display in AirWave.....	20
	Understanding WMS Offload Impact on Dell PowerConnect W-Series Infrastructure.....	22
Chapter 6	Dell PowerConnect W-Series Specific Capabilities in AirWave	23
	Dell PowerConnect W-Series Traps for RADIUS Auth and IDS Tracking	23
	Remote AP Monitoring	24
	ARM and Channel Utilization Information	24
	VisualRF and Channel Utilization	25
	Configuring Channel Utilization Triggers.....	25
	Viewing Channel Utilization Alerts	26
	View Channel Utilization in RF Health Reports	26
	Viewing Controller License Information	27
	Rogue Device Classification.....	27
	Rules-Based Controller Classification	29
	Using RAPIDS Defaults for Controller Classification.....	29
	Changing RAPIDS based on Controller Classification	29
Appendix A	ArubaOS and AirWave CLI Commands	31
	Enable Channel Utilization Events	31
	Enable Stats With the ArubaOS CLI	31
	Offload WMS Using the ArubaOS or AirWave CLI	31
	ArubaOS CLI	31
	AirWave SNMP.....	32
	Pushing Configs from Master to Local Controllers.....	32
	Disable Debugging Utilizing ArubaOS CLI.....	32
	Restart WMS on Local Controllers.....	33
	Configure ArubaOS CLI when not Offloading WMS	33
	Copy and Paste to Enable Proper Traps with the ArubaOS CLI	33
Appendix B	AirWave Data Acquisition Methods	35
Appendix C	WMS Offload Details	37
	State Correlation Process.....	37
	Using AirWave as Master Device State Manager	38
Appendix D	Increasing Location Accuracy.....	39
	Understand Band Steering's Impact on Location.....	39
	Leveraging RTLS to Increase Accuracy.....	39
	Deployment Topology.....	39
	Prerequisites	40
	Enable RTLS service on the AirWave server.....	40
	Enable RTLS on the Controller.....	41
	Troubleshooting RTLS.....	41
	Using the WebUI	41
	Using the CLI	41
	Wi-Fi Tag Setup Guidelines	43

The preface provides an overview of the best practices guide and contact information for Dell PowerConnect W, and includes the following sections:

- [“Document Organization” on page 1](#)
- [“Note, Caution, and Warning Icons” on page 2](#)
- [“Contacting Support” on page 2](#)

Document Organization

This best practices guide includes instructions and examples of optimal ways to use and integrate the Dell PowerConnect W-AirWave Management Platform (AirWave) with Dell PowerConnect W-Series devices and infrastructure.

Table 1 *Document Organization and Purposes*

Chapter	Description
Chapter 1, “Overview” on page 3	This chapter explains the minimum requirements, prerequisites, topology of a Dell PowerConnect W-Series infrastructure integrated with AirWave.
Chapter 2, “Configuring AirWave for Global Dell PowerConnect W-Series Infrastructure” on page 5	This chapter explains global configuration options in AirWave.
Chapter 3, “Configuring a Dell PowerConnect W Group in AirWave” on page 9	This chapter explains how to create and monitor a Dell PowerConnect W group in AirWave.
Chapter 4, “Discovering Dell PowerConnect W-Series Infrastructure” on page 11	This chapter explains how to discover and manage your Dell PowerConnect W-Series infrastructure.
Chapter 5, “AirWave and Dell PowerConnect W-Series Integration Strategies” on page 15	This chapter highlights recommended integration strategies.
Chapter 6, “Dell PowerConnect W-Series Specific Capabilities in AirWave” on page 23	This chapter highlights AirWave capabilities that are specific to Dell PowerConnect W-Series devices.
Appendix A, “ArubaOS and AirWave CLI Commands”	This appendix explains command line interface (CLI) commands.
Appendix B, “AirWave Data Acquisition Methods”	This appendix provides a table that explains how AirWave acquires data from Dell PowerConnect W-Series devices.
Appendix C, “WMS Offload Details”	This appendix explains WMS Offload in further detail.
Appendix D, “Increasing Location Accuracy”	This appendix explains ways to increase location accuracy in AirWave.

Note, Caution, and Warning Icons

This document uses the following notice icons to emphasize advisories for certain actions, configurations, or concepts:



NOTE: Indicates helpful suggestions, pertinent information, and important things to remember.



CAUTION: Indicates a risk of damage to your hardware or loss of data.



WARNING: Indicates a risk of personal injury or death.

Contacting Support

Web Site Support	
Main Website	dell.com
Support Website	support.dell.com
Documentation Website	support.dell.com/manuals

This document provides best practices for leveraging AirWave to monitor and manage your Dell PowerConnect W-Series infrastructure. Dell PowerConnect W-Series wireless infrastructure provides a wealth of functionality such as firewall, VPN, remote AP, IDS, IPS, and ARM, as well as an abundance of statistical information.

Follow the simple guidelines in this document to garner the full benefit of your Dell PowerConnect W-Series infrastructure.

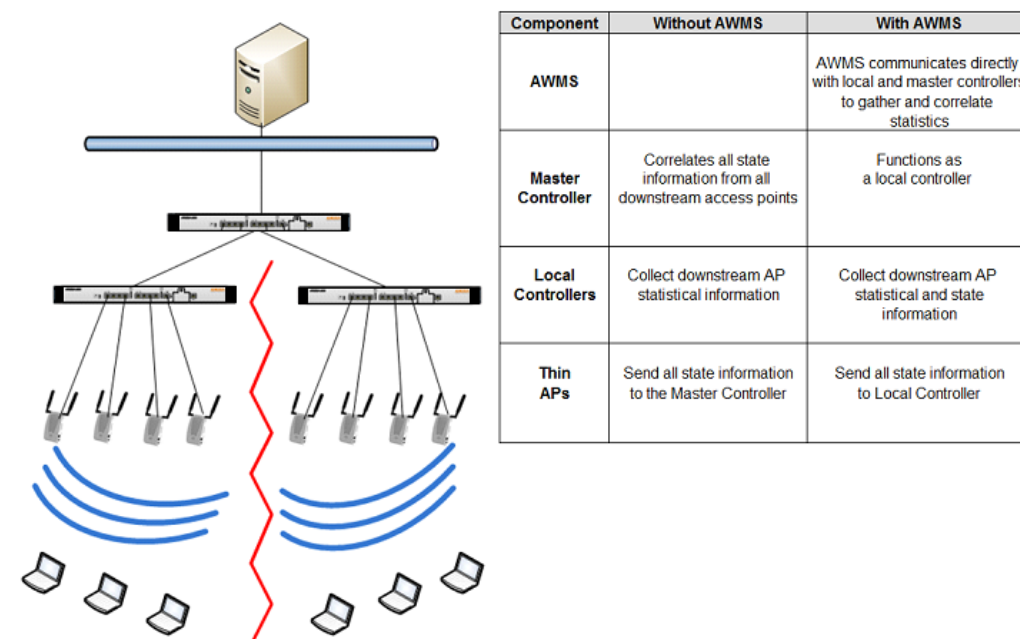
This overview chapter contains the following topics:

- “Understanding Dell PowerConnect W-Series Topology” on page 3
- “Prerequisites for Integrating Dell PowerConnect W-Series Infrastructure” on page 4

Understanding Dell PowerConnect W-Series Topology

Figure 1 depicts typical master-local deployment for the Dell PowerConnect W-AirWave Wireless Management System (AWMS):

Figure 1 Typical Dell PowerConnect W-Series Deployment



NOTE: There should never be a local controller managed by an AirWave server whose master controller is also not under management.

Prerequisites for Integrating Dell PowerConnect W-Series Infrastructure

You will need the following information to monitor and manage your Dell PowerConnect W-Series infrastructure:

- SNMP community string (monitoring and discovery)
- Telnet/SSH credentials (configuration only)
- Enable password (configuration only)



NOTE: Without proper Telnet/SSH credentials AirWave will not be able to acquire license and serial information from controllers.

- SNMPv3 credentials are required for WMS Offload:
 - Username
 - Auth password
 - Privacy password
 - Auth protocol

This chapter explains how to optimally configure Dell PowerConnect W-AirWave to globally manage your global Dell PowerConnect W-Series infrastructure, and contains the following topics:

- “Disabling Rate Limiting in AMP Setup > General” on page 5
- “Entering Credentials in Device Setup > Communication” on page 5
- “Setting Up Recommended Timeout and Retries” on page 6
- “Setting Up Time Synchronization” on page 7
- “Enabling Support for Channel Utilization And Statistics” on page 7

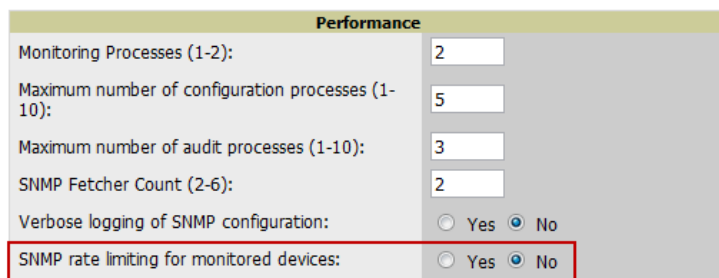
Disabling Rate Limiting in AMP Setup > General

The SNMP Rate Limiting for Monitored Devices option adds a small delay between each SNMP GET request, thus the actual polling intervals will be longer than what is configured. For example, setting a 10-minute polling interval will result in an actual 12-minute polling interval. Disabling rate limiting is recommended in most cases.

To disable rate limiting in AirWave, follow these steps:

1. Navigate to AMP Setup > General.
2. Locate the Performance section on this page.
3. In the SNMP Rate Limiting for Monitored Devices field, select No, as shown in [Figure 2](#).
4. Select Save.

Figure 2 SNMP Rate Limiting in AMP Setup > General



Performance	
Monitoring Processes (1-2):	2
Maximum number of configuration processes (1-10):	5
Maximum number of audit processes (1-10):	3
SNMP Fetcher Count (2-6):	2
Verbose logging of SNMP configuration:	<input type="radio"/> Yes <input checked="" type="radio"/> No
SNMP rate limiting for monitored devices:	<input type="radio"/> Yes <input checked="" type="radio"/> No

Entering Credentials in Device Setup > Communication

AirWave requires several credentials to properly interface with Dell PowerConnect W-Series devices. To enter these credentials, follow these steps:

1. Navigate to Device Setup > Communication.
2. In the Default Credentials section, select the Edit link next to Dell. The page illustrated in [Figure 3](#) appears.
3. Enter the SNMP Community String.



NOTE: Be sure to note the community string because it must match the SNMP trap community string, which is configured later in this document.

Figure 3 Credentials in Device Setup > Communication

4. Enter the required fields for configuration and basic monitoring:
 - Telnet/SSH Username
 - Telnet/SSH Password
 - “enable” Password
5. Enter the required fields for WMS Offload:
 - SNMPv3 Auth Protocol
 - SNMPv3 Privacy Protocol
 - SNMPv3 Username
 - Auth Password
 - Privacy Password



NOTE: The protocols should be SHA and DES in order for WMS Offload to work.

6. Select Save when you are finished.

Setting Up Recommended Timeout and Retries

To set recommended timeout and retries settings, follow these steps:

1. In the Device Setup > Communication page, locate the SNMP Setting section.
2. Change SNMP Timeout setting to a value of either 3, 4, or 5. This is the number of seconds that the AirWave will wait for a response from a device after sending an SNMP request, so a smaller number is more ideal.
3. Change SNMP Retries to 10. This value represents the number of times AirWave tries to poll a device when it does not receive a response within the SNMP Timeout Period or the Group’s Missed SNMP Poll Threshold setting (1-100).



NOTE: Although the upper limit for this value is 40, some SNMP libraries still have a hard limit of 20 retries. In these cases, any retry value that is set above 20 will still stop at 20.

Figure 4 Timeout settings in Device Setup > Communication

SNMP Settings	
SNMP Timeout (3-60 sec):	10
SNMP Retries (1-40):	3

4. Select Save.

Setting Up Time Synchronization

Setting up NTP on AirWave

On the AMP Setup > Network page, locate the Network Time Protocol (NTP) section. The Network Time Protocol is used to synchronize the time between AirWave and your network reference NTP server. NTP servers synchronize with external reference time sources, such as satellites, radios, or modems.



NOTE: Specifying NTP servers is optional. NTP servers synchronize the time on the AirWave server, not on individual access points.

To disable NTP services, clear both the Primary and Secondary NTP server fields. Any problem related to communication between AirWave and the NTP servers creates an entry in the event log. For more information on ensuring that AirWave servers have the correct time, please see <http://support.ntp.org/bin/view/Servers/NTPPoolServers>.

Table 2 AMP Setup > Network > Secondary Network Fields and Default Values

Setting	Default	Description
Primary	ntp1.yourdomain.com	Sets the IP address or DNS name for the primary NTP server.
Secondary	ntp2.yourdomain.com	Sets the IP address or DNS name for the secondary NTP server.

You can set the clock on a controller manually or by configuring the controller to use a Network Time Protocol (NTP) server to synchronize its system clock with a central time source.

Manually Setting the Clock on a Controller

You can use either the WebUI or CLI to manually set the time on the controller's clock.

1. Navigate to the Configuration > Management > Clock page.
2. Under Controller Date/Time, set the date and time for the clock.
3. Under Time Zone, enter the name of the time zone and the offset from Greenwich Mean Time (GMT).
4. To adjust the clock for daylight savings time, click Enabled under Summer Time. Additional fields appear that allow you to set the offset from UTC, and the start and end recurrences.
5. Click Apply.

Enabling Support for Channel Utilization And Statistics

In order to enable support for channel utilization statistics, you must have the following:

- AirWave 7.2 or later

- Dell PowerConnect W-ArubaOS 6.0.1 or later



NOTE: ArubaOS 6.0.1 can report RF utilization metrics, while ArubaOS 6.1 is necessary to also obtain classified interferer information.

- Access points - Dell PowerConnect W AP-105, AP-92, AP-93, AP-125, AP-124, AP-134, AP-135
- Controllers - Dell PowerConnect W 600 Series or 3000 Series

AirWave Setup

Follow these steps in AirWave:

1. Navigate to AMP Setup > General.
2. In the Additional AMP Services section, set Enable AMON Data Collection to Yes, as shown in [Figure 5](#):

Figure 5 AMON Data Collection setting in AMP Setup> General

Additional AMP Services	
Enable FTP server: required to manage Cisco WLC APs; optional for FTP upgrades on supported devices.	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable RTLS collector: Aruba only	<input type="radio"/> Yes <input checked="" type="radio"/> No
Use embedded mail server:	<input checked="" type="radio"/> Yes <input type="radio"/> No
<input type="button" value="Send Test Email"/>	
Process user roaming traps from Cisco WLC:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable AMON Data Collection:	<input checked="" type="radio"/> Yes <input type="radio"/> No

3. Select Save.

Controller Setup (Master And Local)



CAUTION: Enabling these commands on ArubaOS versions prior to 6.0.1.0 can result in performance issues on the controller. If you are running previous firmware versions such as ArubaOS 6.0.0.0, you should upgrade to ArubaOS 6.0.1 (to obtain RF utilization metrics) or 6.1 (to obtain RF utilization *and* classified interferer information) before you enter this command.

Use SSH to access the controller's command-line interface, enter enable mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(Controller-Name) (config) # mgmt-server type amp primary-server <AMP-IP>
(Controller-Name) (config) # write mem
```

It is prudent to establish one or more Dell PowerConnect W Groups within AirWave. During the discovery process you will move new discovered controllers into this group.

This chapter contains the following topics:

- “Basic Monitoring Configuration” on page 9
- “Advanced Configuration” on page 10

Basic Monitoring Configuration

1. Navigate to Groups > List.
2. Select Add.
3. Enter a Name that represents the Dell PowerConnect W-Series device infrastructure from a security, geographical, or departmental perspective and select Add.
4. You will be redirected to the Groups > Basic page for the Group you just created. On this page you will need to tweak a few Dell-specific settings.
5. Find the SNMP Polling Periods section of the page, as illustrated in [Figure 6](#).
6. Change Override Polling Period for Other Services to Yes.
7. Ensure User Data Polling Period is set to 10 minutes. Do not configure this interval lower than 5 minutes.



NOTE: Enabling the SNMP Rate Limiting for Monitored Devices option in the previous chapter adds a small delay between each SNMP Get request, thus the actual polling interval is 12 minutes for 10 minute polling interval.

8. Change Device-to-Device Link Polling Period to 30 minutes.
9. Change Rogue AP and Device Location Data Polling Period to 30 minutes.

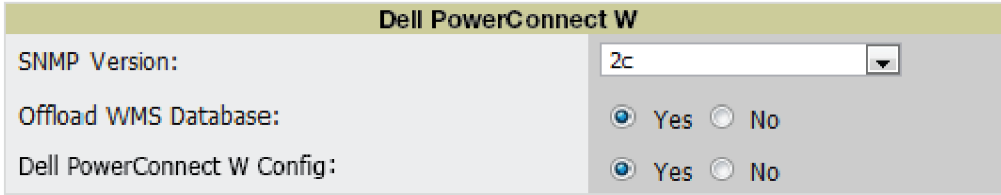
Figure 6 SNMP Polling Periods section of Groups > Basic

SNMP Polling Periods	
Up/Down Status Polling Period:	5 minutes
Override Polling Period for Other Services:	<input checked="" type="radio"/> Yes <input type="radio"/> No
AP Interface Polling Period:	10 minutes
User Data Polling Period:	10 minutes
Thin AP Discovery Polling Period:	15 minutes
Device-to-Device Link Polling Period:	30 minutes
802.11 Counters Polling Period:	15 minutes
Rogue AP and Device Location Data Polling Period:	30 minutes
CDP Neighbor Data Polling Period:	30 minutes

10. Locate the Dell PowerConnect W section of this page, as illustrated in [Figure 7](#).

11. Configure the proper SNMP Version for monitoring the Dell PowerConnect W-Series infrastructure.

Figure 7 Group SNMP Version for Monitoring



The screenshot shows a configuration window titled "Dell PowerConnect W". It contains three settings:

- SNMP Version:** A dropdown menu is set to "2c".
- Offload WMS Database:** A radio button group with "Yes" selected and "No" unselected.
- Dell PowerConnect W Config:** A radio button group with "Yes" selected and "No" unselected.

12. Select Save and Apply.

Advanced Configuration

Refer to the *Dell PowerConnect W-AirWave 7.5 Configuration Guide* located at **Home > Documentation** for detailed instructions.

AirWave utilizes Dell PowerConnect W-Series topology to efficiently discover downstream infrastructure. This chapter guides you through the process of discovering and managing your Dell PowerConnect W-Series device infrastructure.

Refer to the following earlier chapters in this book before attempting discovery:

- Chapter 2, “Configuring AirWave for Global Dell PowerConnect W-Series Infrastructure” on page 5
- Chapter 3, “Configuring a Dell PowerConnect W Group in AirWave” on page 9

The following topics in this chapter walk through the basic procedure for discovering and managing Dell PowerConnect W-Series Infrastructure:

- “Discovering Master Controllers” on page 11
- “Local Controller Discovery” on page 13
- “Thin AP Discovery” on page 13



NOTE: Always add one controller and its affiliated Thin APs into management or monitoring mode in a serial fashion, one at a time. Adding new devices is a very CPU intensive process for AirWave and can quickly overwhelm all of the processing power of the server if hundreds of Thin APs are added (migrated from New to Managed or Monitoring) simultaneously.

Discovering Master Controllers

Scan networks containing Dell PowerConnect W-Series master controllers from Device Setup > Discover.

- or -

Manually enter the master controller by following these steps in the Device Setup > Add page:

1. Select the Dell Controller type and select Add. The page illustrated on [Figure 8](#) appears.
2. Enter the Name and the IP Address for the controller.
3. Enter SNMP Community String, which is required field for device discovery.



NOTE: Be sure to note the community string because it must match the SNMP trap community string, which is configured later in this document.

Figure 8 Dell PowerConnect W Credentials in Device Setup > Add

Configure default credentials on the [Communication](#) page.

Device Communications

Name: Leave name blank to read it from device

IP Address:

SNMP Port: 161

Community String:

Confirm Community String:

SNMPv3 Username:

Auth Password:

Confirm Auth Password:

SNMPv3 Auth Protocol: MD5

Privacy Password:

Confirm Privacy Password:

SNMPv3 Privacy Protocol: DES

Telnet/SSH Username: admin

Telnet/SSH Password:

Confirm Telnet/SSH Password:

"enable" Password:

Confirm "enable" Password:

Location

Group: East

Folder: Top

Monitor Only (no changes will be made to device)

Manage read/write (group settings will be applied to device)

Add Cancel

4. Enter the required fields for configuration and basic monitoring:
 - Telnet/SSH Username
 - Telnet/SSH password
 - “enable” password
5. Enter the required fields for WMS Offload
 - SNMPv3 Auth Protocol
 - SNMPv3 Privacy Protocol
 - SNMPv3 Username
 - Auth Password
 - Privacy Password



NOTE: The protocols should be SHA and DES in order for WMS Offload to work.



CAUTION: If you are using SNMPv3 and the controller's date/time is incorrect, the SNMP agent will not respond to SNMP requests from AirWave SNMP manager. This will result in the controller and all of its downstream access points showing as Down in AirWave.

6. Assign controller to a Group and Folder.
7. Ensure Monitor Only option is selected.
8. Select Add.
9. Navigate to APs/Devices > New page.
10. Select the Dell PowerConnect W-Series master controller you just added from the list of new devices.
11. Ensure Monitor Only option is selected.
12. Select Add.

Local Controller Discovery

Local controllers are added to AirWave via the master controller, by a discovery scan, or manually added in Device Setup > Add. After waiting for the Thin AP Polling Period interval or executing a Poll Now command from the APs/Devices > Monitor page, the local controllers will appear on the APs/Devices > New page.

Add the local controller to the Group defined previously. Within AirWave, local controllers can be split away from the master controller's Group.



NOTE: Local Controller Discovery/monitoring may not work as expected if AirWave is unable to communicate directly with the target device. Be sure and update any ACL/Firewall rules to allow AirWave to communicate with your network equipment.

Thin AP Discovery

Thin APs are discovered via the local controller. After waiting for the Thin AP Polling Period or executing a Poll Now command from the APs/Devices > Monitor page, thin APs will appear on the APs/Devices > New page.

Add the thin APs to the Group defined previously. Within AirWave, thin APs can be split away from the controller's Group. You can split thin APs into multiple Groups if required.

This chapter describes strategies for integrating AirWave and Dell PowerConnect W-Series devices and contains the following topics:

- [“Integration Goals” on page 15](#)
- [“Example Use Cases” on page 16](#)
- [“Prerequisites for Integration” on page 17](#)
- [“Enable Stats Utilizing AirWave” on page 17](#)
- [“WMS Offload with AirWave” on page 18](#)
- [“Define AirWave as a Trap Host using ArubaOS CLI” on page 18](#)
- [“Understanding WMS Offload Impact on Dell PowerConnect W-Series Infrastructure” on page 22](#)

Integration Goals

The following table summarizes the types of integration goals and strategies for meeting them in certain architectural contexts:

Table 3 *Integration Goals in All Masters or Master/Local Architectures*

Integration Goals	All Masters Architecture	Master/Local Architecture
Rogue And Client Info		enable stats
Rogue containment only	ssh access to controllers	ssh access to controllers
Rogue And Client containment	WMS Offload	WMS Offload
Reduce Master Controller Load		WMS Offload debugging off
IDS And Auth Tracking	Define AirWave as trap host	Define AirWave as trap host
Track Tag Location	enable RTLS WMS Offload	enable RTLS WMS Offload
Channel Utilization	enable AMON	enable AMON
Spectrum	enable AMON	enable AMON

Key integration points to consider include the following:

- IDS Tracking does not require WMS Offload in an all-master or master/local environment.
- IDS Tracking does require enable stats in a master/local environment.
- WMS Offload will hide the Security Summary tab on master controller’s web interface.
- WMS Offload encompasses enable stats or enable stats is a subset of WMS Offload.
- Unless you enable stats on the local controllers in a master/local environment, the local controllers do not populate their MIBs with any information about clients or rogue devices discovered/associated with their APs. Instead the information is sent upstream to master controller.

Example Use Cases

The following are example use cases of integration strategies:

When to Use Enable Stats

You want to pilot AMWS and doesn't want to make major configuration changes to their infrastructure or manage configuration from AirWave.



NOTE: Enable Stats still pushes a small subset of commands to the controllers via SSH.

See [“Enable Stats Utilizing AirWave”](#) on page 17.

When to Use WMS Offload

- You have older Dell PowerConnect W-Series infrastructure in a master/local environment and their master controller is fully taxed. Offloading WMS will increase the capacity of the master controller by offloading statistic gathering requirements and device classification coordination to AirWave.
- You want to use AirWave to distribute client and rogue device classification amongst multiple master controllers in a master/local environment or in an All-Masters environment.
- See the following topics:
 - [“WMS Offload with AirWave”](#) on page 18
 - [“Understanding WMS Offload Impact on Dell PowerConnect W-Series Infrastructure”](#) on page 22
 - [“WMS Offload Details”](#) on page 37

When to Use RTLS

- A hospital wants to achieve very precise location accuracy (5 -15 feet) for their medical devices which are associating to the WLAN.
- You want to locate items utilizing WiFi Tags.



NOTE: RTLS can negatively impact your AirWave server's performance.

- See [“Leveraging RTLS to Increase Accuracy”](#) on page 39.

When to Define AirWave as a Trap Host

- You want to track IDS events within the AirWave UI.
- You are in the process of converting their older third-party WLAN devices to Dell PowerConnect W-Series devices and want a unified IDS dashboard for all WLAN infrastructure.
- You want to relate Auth failures to a client device, AP, Group of APs, and controller. AirWave provides this unique correlation capability.
- See [“Define AirWave as a Trap Host using ArubaOS CLI”](#) on page 18.

When to use Channel Utilization

- You have a minimum version of ArubaOS 6.1.0.0 and AP-105 or AP-135.

Prerequisites for Integration

If you have not discovered the Dell infrastructure or configured credentials, refer to the previous chapters of this book:

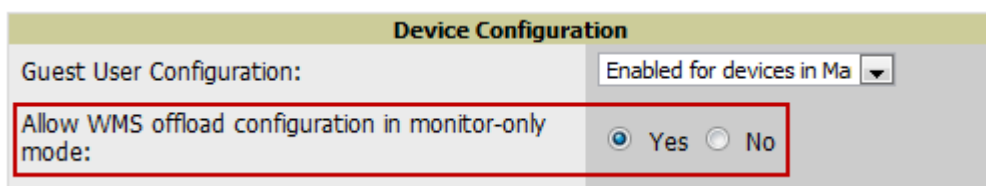
- Chapter 2, “Configuring AirWave for Global Dell PowerConnect W-Series Infrastructure” on page 5
- Chapter 3, “Configuring a Dell PowerConnect W Group in AirWave” on page 9
- Chapter 4, “Discovering Dell PowerConnect W-Series Infrastructure” on page 11

Enable Stats Utilizing AirWave

To enable stats on the Dell PowerConnect W-Series controllers, follow these steps:

1. Navigate to AMP Setup > General and locate the Device Configuration section.
2. Set the Allow WMS Offload Configuration in Monitor-Only Mode field to Yes, as shown in [Figure 9](#):

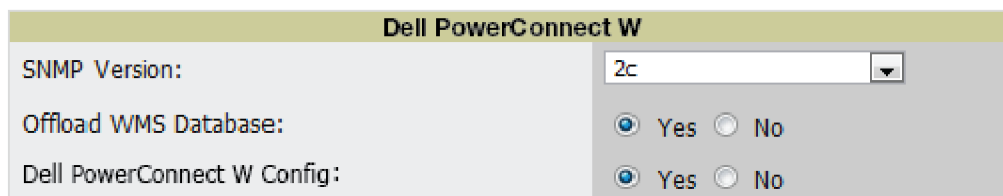
Figure 9 WMS Offload Configuration in AMP Setup > General



The screenshot shows the 'Device Configuration' section. Under 'Guest User Configuration', there is a dropdown menu set to 'Enabled for devices in Ma'. Below this, the 'Allow WMS offload configuration in monitor-only mode:' field is highlighted with a red box. It has two radio buttons: 'Yes' (which is selected) and 'No'.

3. Navigate to Groups > Basic for the group that contains your Dell PowerConnect W-Series controllers.
4. Locate the Dell PowerConnect W section on the page.
5. Set the Offload WMS Database field to No, as shown in [Figure 10](#):

Figure 10 Offload WMS Database field in Groups > Basic



The screenshot shows the 'Dell PowerConnect W' section. It includes a dropdown menu for 'SNMP Version:' set to '2c'. Below that, the 'Offload WMS Database:' field has two radio buttons: 'Yes' and 'No', with 'No' selected. The 'Dell PowerConnect W Config:' field also has two radio buttons: 'Yes' and 'No', with 'Yes' selected.

6. Select Save and Apply.
7. Select Save.

This will push a set of commands via SSH to all Dell PowerConnect W-Series local controllers. AirWave must have read/write access to the controllers in order to push these commands.



NOTE: This process will not reboot your controllers.



CAUTION: If you don't follow the above steps, local controllers will not be configured to populate statistics. This decreases AirWave's capability to trend client signal information and to properly locate devices. See [Appendix A, “ArubaOS and AirWave CLI Commands”](#) on how to utilize the ArubaOS CLI to enable stats on Dell PowerConnect W-Series infrastructure.

If your credentials are invalid or the changes are not applied to the controller, error messages will display on the controller's APs/Devices > Monitor page under the Recent Events section. If the change fails, AirWave does not

audit these setting (display mismatches) and you will need to apply to the controller by hand. See [Appendix A, “ArubaOS and AirWave CLI Commands”](#) for detailed instructions.

These are the commands pushed by AirWave while enabling WMS Offload (do not enter these commands):

```
configure terminal
no mobility-manager <Active WMS IP Address>
wms
general collect-stats enable
stats-update-interval 120
show wms general
write mem
```

WMS Offload with AirWave

To offload WMS on the Dell PowerConnect W-Series controllers using AirWave:

1. In AMP Setup > General, locate the Device Configuration section and enable or disable Allow WMS Offload Configuration in Monitor-Only Mode.
2. Select Save and Apply. This will push a set of commands via SSH to all Dell PowerConnect W-Series master controllers. If the controller does not have an SNMPv3 user that matches the AirWave database it will automatically create a new SNMPv3 user. AirWave must have read/write access to the controllers in order to push these commands
3. Navigate to Groups > Basic and locate the Dell PowerConnect W section.
4. Set the Offload WMS Database field to Yes, as shown in [Figure 10](#).



NOTE: This process will not reboot your controllers. See [Appendix A, “ArubaOS and AirWave CLI Commands”](#) on how to utilize the ArubaOS CLI to enable stats or WMS Offload.



CAUTION: The SNMPv3 user's Auth Password and Privacy Password must be the same.

Do not enter these commands; these are pushed by AirWave while enabling WMS Offload.

```
configure terminal
mobility-manager <AMP IP> user <AMP SNMPv3 User Name> <AMP Auth/Priv PW>
stats-update-interval 120
write mem
```



NOTE: AirWave will configure SNMPv2 traps with the mobile manager command.

Define AirWave as a Trap Host using ArubaOS CLI

To ensure the AirWave server is defined a trap host, access the command line interface of each controller (master and local), enter “enable” mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
```

```
(Controller-Name) (config) # snmp-server host <AMP IP ADDR> version 2c <SNMP Community String of Controller>
```



NOTE: Ensure the SNMP community matches those that were configured in [Chapter 2, “Configuring AirWave for Global Dell PowerConnect W-Series Infrastructure”](#) .

```
(Controller-Name) (config) # snmp-server trap source <Controller-IP>
(Controller-Name) (config) # write mem
```



NOTE: AirWave supports SNMP v2 traps and SNMP v3 informs in ArubaOS 3.4 and higher. SNMP v3 traps are not supported.

ArubaOS Traps Utilized by AirWave

The following are Auth, IDS, and ARM traps utilized by AirWave:

- “Auth Traps” on page 19
- “IDS Traps” on page 19
- “ARM Traps” on page 20

Auth Traps

- wlsxNUserAuthenticationFailed
- wlsxNAuthServerReqTimedOut

IDS Traps

- wlsxwlsxSignatureMatchAP
- wlsxSignatureMatchSta
- wlsxSignAPNetstumbler
- wlsxSignStaNetstumbler
- wlsxSignAPAsleap
- wlsxSignStaAsleap
- wlsxSignAPAirjack
- wlsxSignStaAirjack
- wlsxSignAPNullProbeResp
- wlsxSignStaNullProbeResp
- wlsxSignAPDeauthBcast
- wlsxSignStaDeauthBcastwlsxChannelFrameErrorRateExceeded
- wlsxChannelFrameFragmentationRateExceeded
- wlsxChannelFrameRetryRateExceeded
- wlsxNIPspoofingDetected
- wlsxStaImpersonation
- wlsxReservedChannelViolation
- wlsxValidSSIDViolation
- wlsxStaPolicyViolation
- wlsxRepeatWEPIVViolation
- wlsxWeakWEPIVViolation

- wlsxFrameRetryRateExceeded
- wlsxFrameReceiveErrorRateExceeded
- wlsxFrameFragmentationRateExceeded
- wlsxFrameBandWidthRateExceeded
- wlsxFrameLowSpeedRateExceeded
- wlsxFrameNonUnicastRateExceeded
- wlsxChannelRateAnomaly
- wlsxNodeRateAnomalyAP
- wlsxNodeRateAnomalySta
- wlsxEAPRateAnomaly
- wlsxSignalAnomaly
- wlsxSequenceNumberAnomalyAP
- wlsxSequenceNumberAnomalySta
- wlsxApFloodAttack
- wlsxInvalidMacOUIAP
- wlsxInvalidMacOUISta
- wlsxStaRepeatWEPIVViolation
- wlsxStaWeakWEPIVViolation
- wlsxStaAssociatedToUnsecureAP
- wlsxStaUnAssociatedFromUnsecureAP
- wlsxAPImpersonation
- wlsxDisconnectStationAttackAP
- wlsxDisconnectStationAttackSta

ARM Traps

- AP Power Change
- AP Mode Change
- AP Channel Change

Ensuring That IDS And Auth Traps Display in AirWave

Validate your ArubaOS configuration by exiting the configure terminal mode and issue the following command:

```
(Controller-Name) # show snmp trap-list
```

If any of the traps in the output of this command do not appear to be enabled enter `configure terminal` mode and issue the following command:

```
(Controller-Name) (config) # snmp-server trap enable <TRAPS FROM LIST ABOVE>
(Controller-Name) (config) # write mem
```



NOTE: See [Appendix A, "ArubaOS and AirWave CLI Commands"](#) for the full command that can be copied and pasted directly into the ArubaOS CLI.

Ensure the source IP of the traps match the IP that AirWave utilizes to manage the controller, as shown in [Figure 11](#). Navigate to `APs/Devices > Monitor` to validate the IP address in the Device Info section.

Figure 11 Verify IP Address on APs/Devices > Monitor Page

Status: Up (OK)	Configuration: Mismatched (The settings on the device do not match the desired configuration policy.)					
Firmware: 3.3.2.11	Licenses (3 Expired)					
Controller Role: Local	VRRP IP: 10.1.1.242					
Type: Aruba 3600	Last Contacted: 6/1/2009 1:50 PM	Uptime: 46 days 18 hrs 31 mins				
LAN MAC Address: 98:08:86:61:12:40	Serial: AC0000303	Location: 1344 Server Room	Contact: Aruba IT			
IP Address: 10.1.1.241	SSID: -	Total APs: 266	Total Users: 62	Bandwidth: 2435 kbps		
Notes:						

Verify that there is a SNMPv2 community string that matches the SNMP Trap community string on the controller.

```
(Controller-Name) # show snmp community
```

```
SNMP COMMUNITIES
```

```
-----
```

```
COMMUNITY ACCESS      VERSION
```

```
-----
```

```
public      READ_ONLY V1, V2c
```

```
(Controller-Name) # #show snmp trap-host
```

```
SNMP TRAP HOSTS
```

```
-----
```

```
HOST          VERSION      SECURITY NAME PORT      TYPE TIMEOUT RETRY
```

```
-----
```

```
10.2.32.4     SNMPv2c     public      162      Trap N/A      N/A
```

Verify that firewall port 162 (default) is open between AirWave and the controller.

Validate that traps are making it into AirWave by issuing the following commands from AirWave command line.

```
[root@AMP ~]# qlog enable snmp_traps
```

```
[root@AMP ~]# tail -f /var/log/amp_diag/snmp_traps
```

```
1241627740.392536 handle_trap|2009-05-06 09:35:40 UDP: [10.2.32.65]->[10.51.5.118]:-
32737 sends trap: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (127227800) 14 days,
17:24:38.00 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-
SMI::enterprises.14823.2.3.1.11.1.2.1106 SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.60
= Hex-STRING: 07 D9 05 06 09 16 0F 00 2D 08 00      SNMPv2-
SMI::enterprises.14823.2.3.1.11.1.1.5.0 = Hex-STRING: 00 1A 1E 6F 82 D0 SNMPv2-
SMI::enterprises.14823.2.3.1.11.1.1.6.0 = STRING: dell-apSNMPv2-
SMI::enterprises.14823.2.3.1.11.1.1.1.0 = Hex-STRING: 00 1A 1E C0 2B 32 SNMPv2-
SMI::enterprises.14823.2.3.1.11.1.1.56.0 = INTEGER: 2      SNMPv2-
SMI::enterprises.14823.2.3.1.11.1.1.17.0 = STRING: dell-124-c0:2b:32 SNMPv2-
SMI::enterprises.14823.2.3.1.11.1.1.18.0 = INTEGER: 11      SNMPv2-
SMI::enterprises.14823.2.3.1.11.1.1.58.0 = STRING: http://10.51.5.118/screens/wmsi/
reports.html?mode=ap&bssid=00:1a:1e:6f:82:d0
```



NOTE: You will see many IDS and Auth Traps from this command. AirWave only processes a small subset of these traps which display within AirWave. The traps that AirWave does process are listed above.

Ensure you disable qlogging after testing as it could negatively impact AirWave performance if left turned on:

```
[root@AMP ~]# qlog enable snmp_traps
```

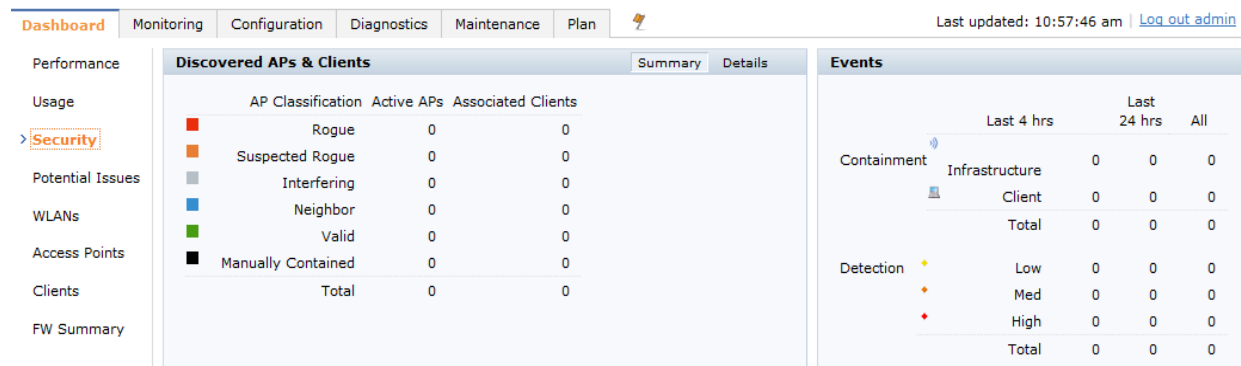
Understanding WMS Offload Impact on Dell PowerConnect W-Series Infrastructure

When offloading WMS, it is important to understand what functionality is migrated to AirWave and what functionality is deprecated.

The following ArubaOS tabs and sections are deprecated after offloading WMS:

- **Plan** - The tab where floor plans are stored and heatmaps are generated. Prior to offloading WMS, ensure that you have exported floor plans from ArubaOS and imported them into AirWave. All functionality within the Plan Tab is incorporated with the VisualRF module in AirWave.
- **Dashboard > Security Summary** - The Security Summary section ([Figure 12](#)) disappears after offloading WMS. The data is still being processed by the master controller, but the summary information is not available. You must use AirWave to view data for APs, clients and events in detail and summary from.
 - AirWave displays information on Rogue APs in the RAPIDS > Overview pages.
 - Information on Suspected Rogue, Interfering and known interfering APs is available in AirWave on each APs/Devices > Manage page.
 - IDS events data and reports appear on AirWave's Reports > Generated > IDS Events page.

Figure 12 Security Summary on Master Controller



See “[Rogue Device Classification](#)” on page 27 for more information on security, IDS, WIPS, WIDS, classification, and RAPIDS.

This chapter discusses Dell PowerConnect W-Series specific capabilities in AirWave and contains the following topics:

- “Dell PowerConnect W-Series Traps for RADIUS Auth and IDS Tracking” on page 23
- “Remote AP Monitoring” on page 24
- “ARM and Channel Utilization Information” on page 24
- “Viewing Controller License Information” on page 27
- “Rogue Device Classification” on page 27
- “Rules-Based Controller Classification” on page 29

Dell PowerConnect W-Series Traps for RADIUS Auth and IDS Tracking

The authentication failure traps are received by the AirWave server and correlated to the proper controller, AP, and user. See [Figure 13](#) showing all authentication failures related to a controller.

Figure 13 RADIUS Authentication Traps in AirWave

RADIUS Authentication Issues for HQ-Aruba-Controller in group Acme Corporation in folder Top > Acme Corporation > Corporate HQ | Return to AP/Device Monitor page

Event Type ▲	Last 2 Hours	Last 24 Hours	Total
Client authentication failed	0	4	1103

1-20 of 1103 RADIUS Authentication Issues Page 1 of 56 > >|

Event	Username	User MAC Address	AP	Radio	RADIUS Server	Time ▼
<input type="checkbox"/> Client authentication failed for 00:08:7D:0C:19:E9	-	00:08:7D:0C:19:E9	-	-	-	4/2/2008 5:24 PM
<input type="checkbox"/> Client authentication failed for 00:17:3F:20:99:6B	-	00:17:3F:20:99:6B	-	-	-	4/2/2008 4:21 PM

The IDS traps are received by the AirWave server and correlated to the proper controller, AP, and user. See [Figure 14](#) showing all IDS traps related to a controller.

Figure 14 IDS Traps in AirWave

IDS Events for HQ-Aruba-Controller in group Acme Corporation in folder Top > Acme Corporation > Corporate HQ | Return to AP/Device Monitor page

Attack ▲	Last 2 Hours	Last 24 Hours	Total
Deauth-Broadcast	0	0	47
Netstumbler Generic	13	122	1756
Null-Probe-Response	22	263	2776
3 Attack Types	35	385	4579

1-20 ▼ of 4579 IDS Events Page 1 ▼ of 229 > >|

Attack	Attacker	AP	Radio	Channel	SNR	Precedence	Time ▼
<input type="checkbox"/> Null-Probe-Response	00:20:A6:49:92:AE	HQ-Aruba-Boardroom	802.11a	-	13	-	7/17/2008 1:58 PM
<input type="checkbox"/> Null-Probe-Response	00:0D:97:00:81:6A	HQ-Northeast-Corner-b6b6	802.11bg	-	23	-	7/17/2008 1:56 PM
<input type="checkbox"/> Null-Probe-Response	00:20:A6:49:92:AE	HQ-Southwest-Corner-eb3e	802.11a	-	39	-	7/17/2008 1:41 PM

Remote AP Monitoring

To monitor remote APs, follow these steps:

1. From the APs/Devices > List page, filter on the Remote Device column to find remote devices.
2. To view detailed information on the remote device, select the device name. The page illustrated in [Figure 15](#) appears.

Figure 15 Remote AP Detail Page

Monitoring **ayre-rap2wg** in group **aruba corp** in folder **Top > cor'p > rap** Poll Controller Now
This device is in monitor-only-with-firmware-upgrades mode.

Device Info

Status: Up (OK)	Aruba AP Group: -	Upstream Device: -
Configuration: -	Remote Device: Yes	Last Contacted: 6/1/2011 1:38 PM
Controller: RAP-OPS-02	Serial: AH0000498	Upstream Port: -
Type: Aruba RAP-2WG	Total Users: 3	Uptime: 10 days 20 hrs 22 mins
LAN MAC Address: 00:08:86:C3:59:94	Bandwidth: 6.04 Kbps	
IP Address: 10.230.205.107		
Quick Links: Open controller web UI... Run a command...		

Notes:

Radios

Name	MAC Address	Users	BW (Kbps)	Channel	Tx Power	Radio Role	Active SSIDs
802.11bg	00:08:86:B5:99:40	2	6.04	6	19.5 dBm	-	-

Wired Interfaces

Name	MAC Address	Users	Admin Status	Operational Status	Type	Duplex	Aruba Port Mode	Input Capacity	Output Capacity
Enet0	00:08:86:C3:59:94	0	Up	Up	fastEther	Full	N/A	100 Mbps	100 Mbps
Enet1	00:08:86:C3:59:95	1	Up	Up	fastEther	Full	Split	100 Mbps	100 Mbps

3. You can also see if there are users plugged into the wired interfaces in the Connected Users list.



NOTE: This feature is only available when the remote APs are in split tunnel and tunnel modes.

ARM and Channel Utilization Information

ARM statistics and Channel utilization are very powerful tools for diagnosing capacity and other issues in your WLAN.

1. Navigate to an APs/Devices > Monitor page for any of the following Dell PowerConnect W-Series models: Dell PowerConnect W-AP-105, AP-92, AP-93, AP-124, AP-125, or AP-135.
2. In the Radios table, select a radio link under the Name column for a radio.

Figure 16 ARM and Channel Utilization Graphs

AP Monitoring | Radio Statistics
 Monitoring **802.11bgn** radio for AP **cheath-rap5d**
Run a command...

802.11 Radio Counters Summary (frames/sec)

	Current	Last Hour	Last Day	Last Week
Unacked	1	1	1	0
Retries	0	0	0	0
Failures	0	1	1	0
Dup Frames	0	0	0	0
FCS Errors	2	2	2	0

Channel | Last 1 hour

Maximum Average: 11 frames/sec

Channel

Utilization | Last 1 hour

Metric	Maximum	Average
Busy	22.8 %	14.6 %
Interference	3.9 %	2 %
Receiving	13.4 %	5.9 %
Transmitting	9.8 %	7.1 %

1 year ago now

No ARM Events

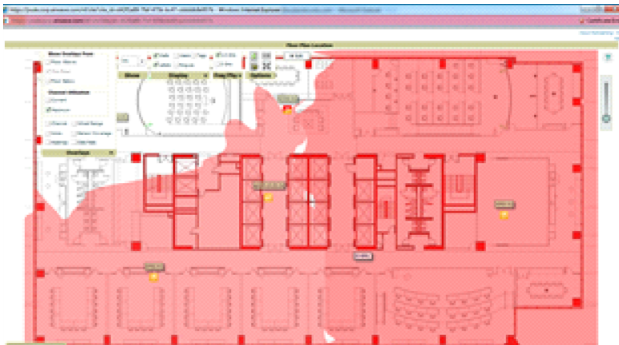
See the *Dell PowerConnect W-AirWave User Guide* in Home > Documentation for more information on the data displayed in the Radio Statistics page for these devices.

VisualRF and Channel Utilization

To view how channel utilization is impacting an area within a building, follow these steps:

1. Navigate to a floor plan by clicking on the thumbnail on a device's APs/Devices > Monitor page or navigating to VisualRF > Floor Plans page.
2. Select the Overlays menu.
3. Select Utilization overlay.
4. Select Current or Maximum (over last 24 hours).
5. Select total (default), receive, transmit, or interference (see [Figure 17](#)).

Figure 17 Channel Utilization in VisualRF (Interference)



Configuring Channel Utilization Triggers

1. Navigate to System > Triggers and select Add.
2. Select Channel Utilization from the Type drop-down menu as seen on [Figure 18](#):

Figure 18 Channel Utilization Trigger

3. Enter the duration evaluation period.
4. Select Add New Trigger Condition.
5. Create a trigger condition for Radio Type and select the frequency to evaluate.
6. Select total, receive, transmit, or interference trigger condition.
7. Set up any restrictions or notifications (refer to the *Dell PowerConnect W-AirWave 7.5 User Guide* in **Home > Documentation** for more details)
8. When finished, select Add.

Viewing Channel Utilization Alerts

1. Navigate to APs/Devices > Monitor or System > Alerts.
2. Sort the Trigger Type column and find Channel Utilization alerts.

View Channel Utilization in RF Health Reports

1. Navigate to Reports > Generated.
2. Find and select a Device Summary or RF Health report.

Figure 19 Channel Utilization in an RF Health Report

Most Utilized by Channel Usage (2.4 GHz)

Rank ▲	Device	Channel Busy (%)	Interference (%)	Number of Users	Bandwidth (bps)	Location	Controller
1	AP0018.19bd.b1d0	85.43	83.86	0	14.00	ap lab	wlc 5500
2	AP001d.a1fc.ca7a	85.04	83.86	0	32.00	default location	wlc 5500
3	Cisco-13:21:1E	67.72	59.45	0	4.00	default location	wlc 5500
4	AP10	64.57	63.39	0	24.00	Sales Office-helloX	Cisco4400

Viewing Controller License Information

Follow these steps to view your controller's license information in AirWave:

1. Navigate to the APs/Devices > Monitor page of a controller under AirWave management.
2. Select the License link in the Device Info section. A pop-up window appears listing all licenses.

Figure 20 License Popup from APs/Devices > Monitor

132: Oak Grove Guest Iss

License Table for alpha-local-1:

Service Type ▲	Installed	Expires	Flag	Key
Client Integrity Module	4/29/2005 12:36 PM		E	n9XQpMZN-kUMfht6z-j98lcV0J-TSikt4In-xA2LFT0-v58
External Services Interface	4/29/2005 12:35 PM		E	PIF8DrBV-nBXlkp75-+Z8TT2NS-aj4oa8/h-VVm+Cx86-zVU
External Services Interface	4/29/2005 12:34 PM		E	OMstNveDX-W3wEHSKx-TpXkQbHV-NyTb3HAN-OYA2zNY-\
Indoor Mesh Access Points: 256	10/19/2007 6:54 PM		E	lkwFlaJR-6y8p6rm+-CzOUh7tl-bMhkMA1v-1DV+2m+H-kZE
MMC AP	10/19/2007 6:54 PM		E	WP6JN8IS-y4AoaG9p-P2r7wV Tk-/PXV3JgR-C0fg3d4-LLk
Ortronics Access Points: 256	10/19/2007 6:54 PM		E	+jl6oDRK-PIRXv5nF-lDMwrDJ-oES1ydXR-4K7sFEHQ-SmU
Outdoor Mesh Access Points: 100	5/2/2007 2:51 PM	Expired		99CSOvul-jL4Z0YkS-Q8lov2BI-BS+Y0Vxi-YkC9TT0V-5js
Outdoor Mesh Access Points: 256	10/19/2007 6:54 PM		E	RKC/wjVj-fcRQGDH-K/F8vurv-oYRwgCuG-CsmY7wYh-w18
Outdoor Mesh Access Points: 64	8/1/2007 3:59 PM		E	C5j/bSfb-yVOxff0h-BWWWUVEVe-Glb2xz4A-LKcq440D-IXQ
Policy Enforcement Firewall	4/29/2005 12:30 PM		E	vDXRo7pz-Jo8asgU2-HG7w74l+-zzI3yGku-zz7w3rj+-/11
Remote Access Points: 256	10/19/2007 6:54 PM		E	QnR882W+-o1Kb2XcR-2vrePyl+-J++rWbxh-jtCqjH3h-LPU
Remote Access Points: 48	4/29/2005 12:38 PM		E	5zz7c0jO-LpDgDbLH-4bEnzNbg-pj/oEnS2a-nTtHaS8t-ms0
Voice Services Module	10/19/2007 6:54 PM		E	Lj/ByOfs-wMdJU3Xv-5djAkCDj-vJ9zRok3-sWZ4Z2bn-aH4
VPN Server	4/29/2005 12:32 PM		E	SOKR1Sa8-KKMjj/Gv-HlcJcwaK-uEZuPvcs-c/LIzjg0-2IE
Wireless Intrusion Protection	4/29/2005 12:33 PM		E	xVc/lqw-Os1ei+yL-b1CqzoTr-UwGp2OAI-LD6wHOW2-qSw
xSec Module	4/29/2005 12:37 PM		E	ukxUwAcB-PE+GeyB9-7u7IMtQ1-CaibELI2-LuqdRsqA-fac

Rogue Device Classification

Complete this section if you have completed WMS Offload procedure above. After offloading WMS, AirWave maintains the primary ARM, WIPS, and WIDS state classification for all devices discovered over-the-air.

Table 4 WIPS/WIDS to AirWave Controller Classification Matrix

AirWave Controller Classification	ArubaOS (WIPS/WIDS)
Unclassified (default state)	Unknown
Valid	Valid
Suspected Neighbor	Interfering
Neighbor	Known Interfering
Suspected Rogue	Suspected Rogue
Rogue	Rogue
Contained Rogue	DOS

To check and reclassify rogue devices, follow these steps:

1. Navigate to the Rogue > Detail page for the rogue device, as shown in .

Figure 21 Rogue Detail Page Illustration

Name:	Aruba-83:43:01	Model:	-	First Discovered:	
Acknowledge:	<input type="radio"/> Yes <input checked="" type="radio"/> No	IP Address:	-	First Discovery M:	
Controller Classification:	Suspected Neighbor	Confidence:	0		
WMS Classification Override:	Unclassified	First Discovery Agent:	00:24:6c:c8:6e:e7		
SSID:	qa-dp-vw-c3-2	Channel:	149	Last Discovered:	
RAPIDS Classification:	Unclassified	WEP:	No	Last Discovery M:	
Classification Rule:	-	WPA:	Yes	Last Discovery A:	
RAPIDS Classification Override:	- No Override -	Network Type:	AP		
Threat Level:	- No Override -				
Threat Level Override:	Valid				
Radio MAC Address:	Suspected Valid				
Radio Vendor:	Neighbor				
LAN MAC Address:	Suspected Neighbor				
LAN Vendor:	Suspected Rogue				
OUI Score:	Rogue				
Operating System:					

2. Select the proper classification from the RAPIDS Classification Override drop-down menu.



CAUTION: Changing the controller's classification within the AirWave UI will push a reclassification message to all controllers managed by the AirWave server that are in Groups with Offloading the WMS database set to Yes. To reset the controller classification of a rogue device on AirWave, change the controller classification on the AirWave UI to unclassified.

Controller classification can also be updated from RAPIDS > List via the Modify Devices link.

All rogue devices will be set to a default controller classification of unclassified when WMS is first offloaded except for devices classified as valid. Rogue devices classified in ArubaOS as valid will also be classified within AirWave as valid for their controller classification as well. As APs report subsequent classification information about rogues, this classification will be reflected within AirWave UI and propagated to controllers that AirWave manages. The device classification reflected in the controller's UI and in the AirWave UI will probably not match, because the controller/APs do not reclassify rogue devices frequently.

To update a group of devices' controller classification to match the ArubaOS device classification, navigate to RAPIDS > List and utilize the Modify Devices checkbox combined with the multiple sorting a filtering features.

Table 5 ARM to AMP Classification Matrix

AMP	AOS (ARM)
Unclassified (default state)	Unknown
Valid	Valid
Contained	DOS

1. Navigate to the Users > User Detail page for the user.
2. Select the proper classification from the Classification drop-down menu as seen in [Figure 22](#):

Figure 22 User Classification

Device Information	
Username:	madisonl
Vendor:	Apple
First Seen:	1/8/2009 10:29 AM on <Deleted> for 50 mins
Last Seen:	4/11/2011 1:22 PM on 78C for 5 hrs 25 mins
Classification:	Unclassified
Automatically populate device information:	Valid
Device Description:	Unclassified
	Contained



CAUTION: Changing User Classification within the AirWave UI will push a user reclassification message to all controllers managed by the AirWave server that are in Groups with Offloading the WMS database set to Yes.

All users will be set to a default classification of unclassified when WMS is first offloaded. As APs report subsequent classification information about users, this classification will be reflected within AirWave UI and propagated to controllers that AirWave manages. It is probable that the user's classification reflected in the controller's UI and in the AirWave UI will not match, because the controller/APs do not reclassify users frequently.

There is no method in the AirWave UI to update user classification on mass to match the controller's classification. Each client must be updated individually within the AirWave UI.

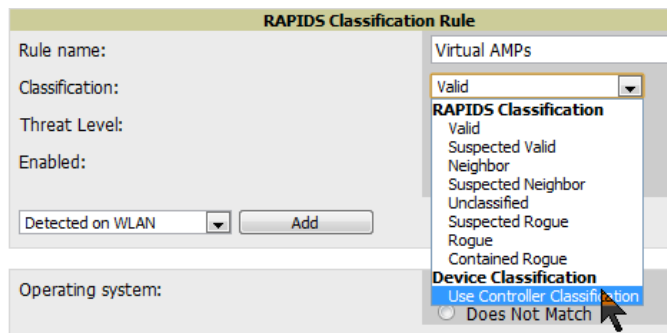
Rules-Based Controller Classification

Using RAPIDS Defaults for Controller Classification

To use the controller's classification as RAPIDS classification, follow these steps:

1. Navigate to RAPIDS > Rules and select the pencil icon for a rule.
2. In the Classification drop-down menu, select Use Controllers Classification as seen in [Figure 23](#).
3. Select Save.

Figure 23 *Using Controller Classification*



Changing RAPIDS based on Controller Classification

1. Navigate to RAPIDS > Rules.
2. In the Classification drop-down menu, select desired RAPIDS classification.
3. Select Controller Classification from drop-down menu, as shown in [Figure 24](#).

Figure 24 Configure Rules for Classification

RAPIDS Classification Rule

Rule name: KVMs

Classification: Suspected Neighbor

Threat Level: 1

Enabled: Yes No

Controller Classification

Wireless Properties
Detected on WLAN
Detecting AP count
Encryption
Network type
Signal strength
SSID

Wireline Properties
Detected on LAN
Fingerprint scan
IP address
OUI score
Operating system

Wireless/Wireline Properties
Manufacturer
MAC Address

Aruba Controller Properties
Controller Classification
Confidence

Matches
 Does Not Match

manufacturers, one
d. Matching is case-
e and non-

(remove condition)
Unclassified
(remove condition)

4. Select Add.
5. Select desired controller classification to use as an evaluation in RAPIDS.
6. Select Save.

Enable Channel Utilization Events



CAUTION: Enabling these commands on ArubaOS versions prior to 6.1 can result in performance issues on the controller.

To enable channel utilization events utilizing the Dell PowerConnect W-Series ArubaOS CLI, use SSH to access a local or master controller's command-line interface, enter enable mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(Controller-Name) (config) # mgmt-server type amp primary-server <AMP IP>
(Controller-Name) (config) # write mem
```

Enable Stats With the ArubaOS CLI

The following commands enable collection of statistics (up to 25,000 entries) on the master controller for monitored APs and clients.



NOTE: Do not use these commands if you use the AirWave GUI to monitor APs and Clients. Enabling these commands on ArubaOS versions prior to 6.1 can result in performance issues on the controller.

Use SSH to access the master controller's command-line interface, enter enable mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(Controller-Name) (config) # wms general collect-stats enable
(Controller-Name) (config) # write mem
```

Offload WMS Using the ArubaOS or AirWave CLI



NOTE: Do not use these commands if you use the AirWave GUI to monitor APs and clients.

Use the following commands to offload WMS using the ArubaOS command-line interface or the AirWave SNMP Walk.

ArubaOS CLI

SSH into all controllers (local and master), and enter "enable" mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(Controller-Name) (config) # mobility-manager <AMP IP> user <MMS-USER> <MMS-SNMP-
PASSWORD> trap-version 2c
```

```
(Controller-Name) (config) # write mem
```

This command creates the AirWave server as an SNMPv3 Trap Host in the controller's running configuration. This command also creates an SNMPv3 user on the controller with authentication protocol configured to SHA and privacy protocol DES. The user and password must be at least eight characters, because the Net-SNMP package in AirWave adheres to this IETF recommendation. ArubaOS automatically creates Auth and Privacy passwords from this single password. If mobility-manager is already using a preconfigured SNMPv3 user, ensure the privacy and authentication passwords are the same.

Example:

```
mobility-manager 10.2.32.1 user airwave123 airwave123
```

AirWave SNMP

Log in into the AirWave server with proper administrative access and issue the following command for all controllers (master and locals):

```
[root@AMP ~]# snmpwalk -v3 -a SHA -l AuthPriv -u <MMS-USER> -A <MMS-SNMP-PASSWORD> -X <MMS-SNMP-PASSWORD> <Controller-IP> wlsxSystemExtGroup
```

```
WLSX-SYSTEMEXT-MIB::wlsxSysExtSwitchIp.0 = IPAddress: 10.51.5.222
```

```
WLSX-SYSTEMEXT-MIB::wlsxSysExtHostname.0 = STRING: dell-3600-2
```

```
.
```

```
..
```

```
WLSX-SYSTEMEXT-MIB::wlsxSysExtSwitchLastReload.0 = STRING: User reboot.
```

```
WLSX-SYSTEMEXT-MIB::wlsxSysExtLastStatsReset.0 = Timeticks: (0) 0:00:00.00 response
```

```
[root@AMP ~]#
```

Unless this SNMP walk command is issued properly on all of the controllers, they will not properly populate client and rogue statistics. Ensure the user and passwords match exactly to those entered in above sections.

Example:

```
snmpwalk -v3 -a SHA -l AuthPriv -u airwave123 -A airwave123 -X airwave123 10.51.3.222 wlsxSystemExtGroup
```

If you do not use the AirWave WebUI to offload WMS, you must add a cronjob on the AirWave server to ensure continued statistical population. Because the MIB walk/touch does not persist through a controller reboot, a cronjob is required to continually walk and touch the MIB.

Pushing Configs from Master to Local Controllers

Use the following ArubaOS CLI commands to ensure that the master controller is properly pushing configuration settings from the master controller to local controllers. This command ensures configuration changes made on the master controller will propagate to all local controllers.



NOTE: Do not use these commands if you use the AirWave GUI to monitor APs and clients.

```
(Controller-Name) (config) # cfgm mms config disable
```

```
(Controller-Name) (config) # write mem
```

Disable Debugging Utilizing ArubaOS CLI

If you are experiencing performance issues on the master controller, ensure that debugging is disabled. It should be disabled by default. Debugging coupled with gathering the enhanced statistics can put a strain on the controllers CPU, so it is highly recommended to disable debugging.

To disable debugging, SSH into the controller, enter “enable” mode, and issue the following commands:

```
(Controller-Name) # show running-config | include logging level debugging
```

If there is output, then use the following commands to remove the debugging:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(Controller-Name) (config) # no logging level debugging <module from above>
(Controller-Name) (config) # write mem
```

Restart WMS on Local Controllers

To ensure local controllers are populating rogue information properly, use SSH to access the command-line interface of each local controller, enter enable mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(Controller-Name) (config) # process restart wms
```

After executing the restart WMS command in ArubaOS, you will need to wait until the next Rogue Poll Period on the AirWave and execute a Poll Now operation for each local controller on the APs/Devices > List page before rogue devices begin to appear in AirWave.

Configure ArubaOS CLI when not Offloading WMS

To ensure proper event correlation for IDS events when WMS is not offloaded to AirWave, access the command line interface of each controller (master and local), enter “enable” mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(Controller-Name) (config) # ids management-profile
(Controller-Name) (config) # ids general-profile <name>
(Controller-Name) (config) # ids-events logs-and-traps
(Controller-Name) (config) # write mem
```

Copy and Paste to Enable Proper Traps with the ArubaOS CLI

To ensure the proper traps are configured on Dell PowerConnect W-Series controllers, copy and paste the following command in config mode:

```
snmp-server trap enable wlsxNUserAuthenticationFailed
snmp-server trap enable wlsxUserAuthenticationFailed
snmp-server trap enable wlsxNAuthServerReqTimedOut
snmp-server trap enable wlsxSignatureMatchAP
snmp-server trap enable wlsxSignatureMatchSta
snmp-server trap enable wlsxSignAPNetstumbler
snmp-server trap enable wlsxSignStaNetstumbler
snmp-server trap enable wlsxSignAPAsleap
snmp-server trap enable wlsxSignStaAsleap
snmp-server trap enable wlsxSignAPAirjack
snmp-server trap enable wlsxSignStaAirjack
snmp-server trap enable wlsxSignAPNullProbeResp
snmp-server trap enable wlsxSignStaNullProbeResp
snmp-server trap enable wlsxSignAPDeauthBcast
snmp-server trap enable wlsxSignStaDeauthBcastwlsxChannelFrameErrorRateExceeded
snmp-server trap enable wlsxChannelFrameFragmentationRateExceeded
```

```
snmp-server trap enable wlsxChannelFrameRetryRateExceeded
snmp-server trap enable wlsxNIPspoofingDetected
snmp-server trap enable wlsxStaImpersonation
snmp-server trap enable wlsxReservedChannelViolation
snmp-server trap enable wlsxValidSSIDViolation
snmp-server trap enable wlsxStaPolicyViolation
snmp-server trap enable wlsxRepeatWEPIVViolation
snmp-server trap enable wlsxWeakWEPIVViolation
snmp-server trap enable wlsxFrameRetryRateExceeded
snmp-server trap enable wlsxFrameReceiveErrorRateExceeded
snmp-server trap enable wlsxFrameFragmentationRateExceeded
snmp-server trap enable wlsxFrameBandwidthRateExceeded
snmp-server trap enable wlsxFrameLowSpeedRateExceeded
snmp-server trap enable wlsxFrameNonUnicastRateExceeded
snmp-server trap enable wlsxChannelRateAnomaly
snmp-server trap enable wlsxNodeRateAnomalyAP
snmp-server trap enable wlsxNodeRateAnomalySta
snmp-server trap enable wlsxEAPRateAnomaly
snmp-server trap enable wlsxSignalAnomaly
snmp-server trap enable wlsxSequenceNumberAnomalyAP
snmp-server trap enable wlsxSequenceNumberAnomalySta
snmp-server trap enable wlsxApFloodAttack
snmp-server trap enable wlsxInvalidMacOUIAP
snmp-server trap enable wlsxInvalidMacOUISta
snmp-server trap enable wlsxStaRepeatWEPIVViolation
snmp-server trap enable wlsxStaWeakWEPIVViolation
snmp-server trap enable wlsxStaAssociatedToUnsecureAP
snmp-server trap enable wlsxStaUnAssociatedFromUnsecureAP
snmp-server trap enable wlsxAPImpersonation
snmp-server trap enable wlsxDisconnectStationAttackAP
snmp-server trap enable wlsxDisconnectStationAttackSta
```



NOTE: You will need to issue the `write mem` command.

Appendix B

AirWave Data Acquisition Methods

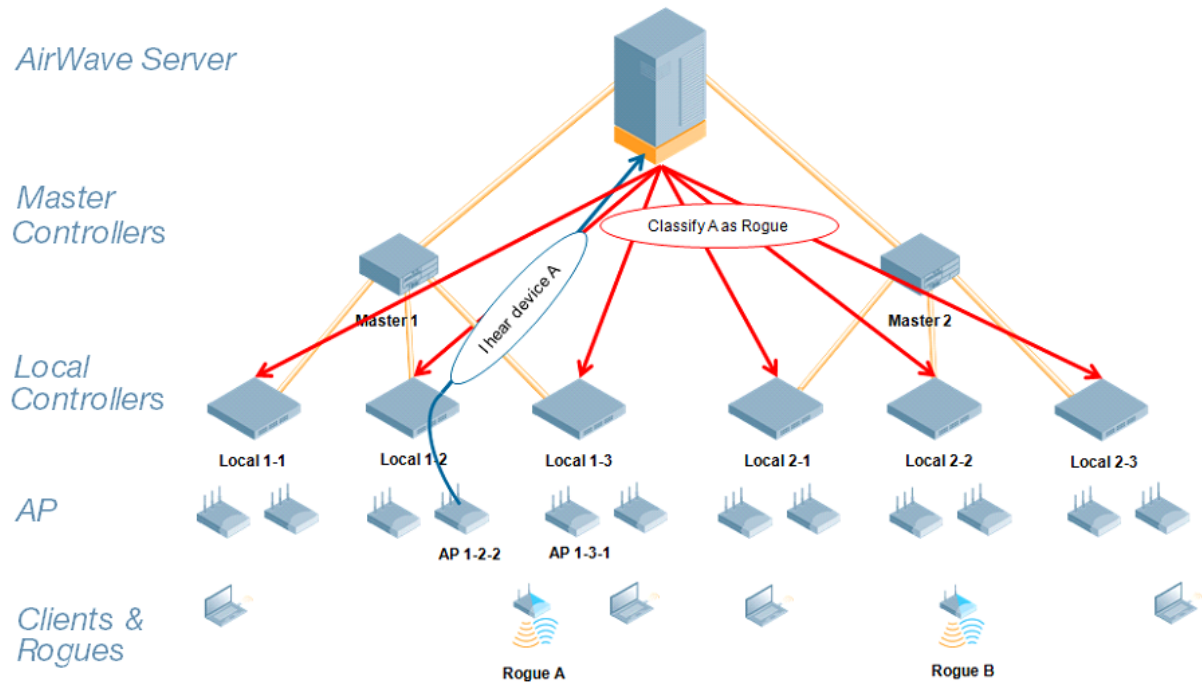
The following table describes the different methods through which AirWave acquires data from Dell PowerConnect W-Series devices on the network.

Table 6 Methods by which AirWave Acquires Data from Dell PowerConnect W-Series Devices

Data Elements	Controller/Thin AP						Dell PowerConnect W-Instant	
	SNMP MIB	SNMP Traps	AMON	CLI/SSH	WMS Offload	RTLS	HTTPS	
Configuration interface								
Device configuration/audit				X			X	
User and client interfaces								
Assoc/auth/roam	X	X					X	
Bandwidth	X						X	
Signal quality	X					X	X	
Auth failures		X					N/A	
AP/radio interfaces								
CPU And memory utilization	<-----N/A----->							X
Bandwidth	X						X	
Transmit Power	X						X	
Channel utilization			X				X	
Noise floor	X						X	
Frame rates	X						X	
Error counters	X						X	
Channel summary				X			N/A	
ARM events		X					N/A	
Active interferers			X				N/A	
Active BSSIDs/SSIDs	X						X	
Security								
IDS events		X					N/A	
Neighbors/rogues	X				X		X	
Neighbor re-classification				X	X		N/A	
Client classification					X		N/A	
User deauthorization				X			N/A	

WMS Offload instructs the master controller to stop correlating ARM, WIPS, and WIDS state information amongst its local controllers because AirWave will assume this responsibility. Figure 25 depicts how AirWave communicates state information with local controllers.

Figure 25 ARM/WIPS/WIDS Classification Message Workflow



State Correlation Process

1. AP-1-3-1 hears rogue device A.
2. Local controller 1-3 evaluates devices and does initial classification and sends a classification request to the AirWave.
3. AirWave receives message and re-classifies the device if necessary and reflects this within AirWave GUI and via SNMP traps, if configured.
4. AirWave sends a classification message back to all local controllers managed by master controller 1, (1-1, 1-2, and 1-3).
5. AirWave sends a classification message back to all additional local controllers managed by the AirWave server. In this example all local controllers under master controller 2, (2-1, 2-2, and 2-3) would receive the classification messages.
6. If an administrative AirWave user manually overrides the classification, then AirWave will send a re-classification message to all applicable local controllers.

7. AirWave periodically polls each local controller's MIB to ensure state parity with the AirWave database. If the local controller's device state does not comply with the AirWave database, AirWave will send a re-classification message to bring it back into compliance.



NOTE: The Rogue Detail page displays a BSSID table for each rogue that displays the desired classification and the classification on the device.

Using AirWave as Master Device State Manager

AirWave offers the following benefits as a master device state manager:

- Ability to correlate state among multiple master controllers. This will reduce delays in containing a rogue device or authorizing a valid device when devices roam across a large campus.
- Ability to correlate state of third party access points with ARM. This will ensure Dell PowerConnect W-Series infrastructure interoperates more efficiently in a mixed infrastructure environment.
- Ability to better classify devices based on AirWave wire-line information not currently available in ArubaOS.
- AirWave provides a near real-time event notification and classification of new devices entering air space.
- RAPIDS gains additional wire-line discovery data from Dell PowerConnect W-Series controllers.

Understand Band Steering's Impact on Location

Band steering can negatively impact location accuracy when testing in highly mobile environment. The biggest hurdle is scanning times in 5 GHz frequency.

Table 7 Location accuracy impact

Operating Frequency	Total Channels	Scanning Frequency	Scanning Time	Total Time One Pass
2.4 GHz	11 (US)	10 seconds	110 milliseconds	121.21 seconds
5 GHz	24 (US)	10 seconds	110 milliseconds	242.64 seconds

Leveraging RTLS to Increase Accuracy

This section provides instructions for integrating the AirWave, Dell PowerConnect W-Series WLAN infrastructure and Dell PowerConnect W's RTLS feed to more accurately locate wireless clients and Wi-Fi Tags.

Deployment Topology

Figure 26 Typical Client Location

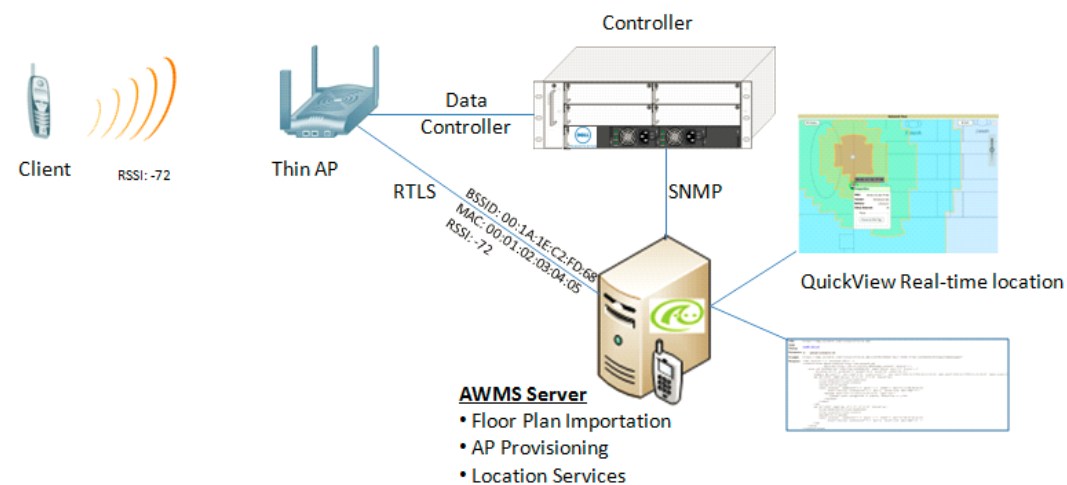
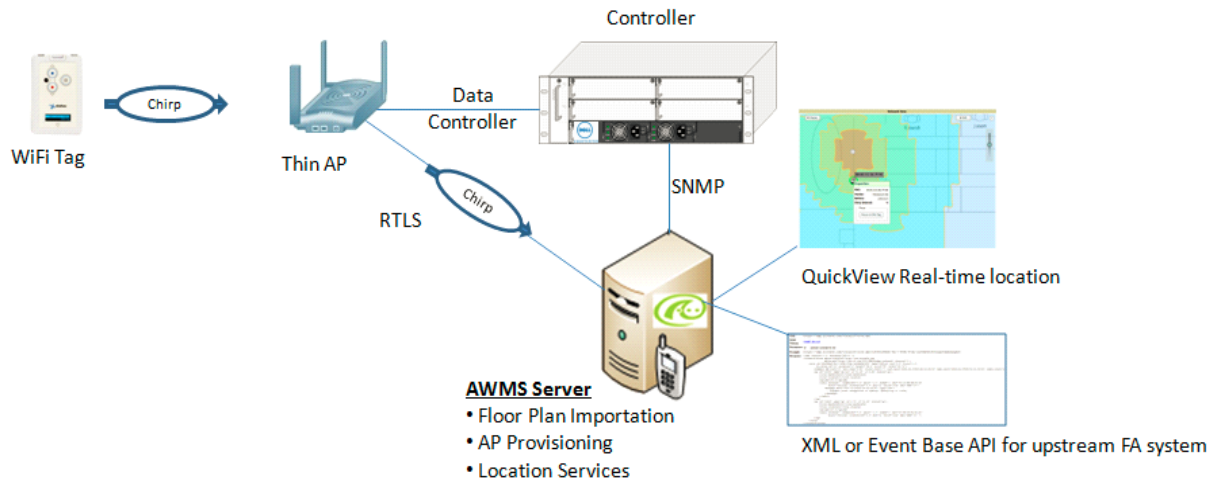


Figure 27 Typical Tag Deployment



Prerequisites

You will need the following information to monitor and manage your Dell PowerConnect W-Series infrastructure.

- Ensure AirWave server is already monitoring Dell PowerConnect W-Series infrastructure
- Ensure WMS Offload process is complete
- Ensure firewall configuration for port 5050 (default port) supports bidirectional UDP communication between the AirWave server's IP address and each access point's IP address

Enable RTLS service on the AirWave server

To enable RTLS service on the AirWave server, follow these steps:

1. Navigate to AMP Setup > General and locate the AMP Additional Services section
2. Select Yes for the Enable RTLS Collector option.
3. A new section will automatically appear with the following settings:
 - RTLS Port - the match controller default is 5050
 - RTLS Username - match the SNMPv3 MMS username configured on controller
 - RTLS Password - match the SNMPv3 MMS password configured on controller

Figure 28 RTLS Fields in AMP Setup > General

Additional AMP Services	
Enable FTP server: required to manage Cisco WLC APs; optional for FTP upgrades on supported devices.	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable RTLS collector: Dell PowerConnect W only	<input checked="" type="radio"/> Yes <input type="radio"/> No
RTLS Port:	<input type="text" value="5050"/>
RTLS Username:	<input type="text" value="admin"/>
RTLS Password:	<input type="password" value="••••••••"/>
Confirm RTLS Password:	<input type="password" value="••••••••"/>
Use embedded mail server:	<input checked="" type="radio"/> Yes <input type="radio"/> No
	<input type="button" value="Send Test Email"/>
Process user roaming traps from Cisco WLC:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable AMON Data Collection:	<input checked="" type="radio"/> Yes <input type="radio"/> No

4. Select Save at the bottom of the page.

Enable RTLS on the Controller



NOTE: RTLS can only be enabled on the master controller and it will automatically propagate to all local controllers.

SSH into master controller, enter enable mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(Controller-Name) (config) # ap system-profile <Thin-AP-Profile-Name>

(Controller-Name) (AP system profile default) # rtls-server ip-addr <IP of AMP Server>
port 5050 key <Controller-SNMPv3-MMS-Password>

(Controller-Name) (AP system profile default) # write mem
```

To validate exit configuration mode:

```
(Controller-Name) # show ap monitor debug status ip-addr <AP-IP-Address>
...
RTLS configuration
-----
Type          Server IP    Port Frequency Active
-----
MMS           10.51.2.45  5070 120
Aeroscout    N/A          N/A   N/A
RTLS          10.51.2.45  5050 60          *
```

Troubleshooting RTLS

You can use either the WebUI or CLI to ensure the RTLS service is running on your AirWave server.

Using the WebUI

Access the AirWave WebUI and navigate to System > Status.

Scroll down Services list and look for the RTLS service, as shown below

Figure 29 RTLS System Status

Home	Groups	APs/Devices	Clients	Reports	System	Device Setup
Status	Syslog & Traps	Event Log	Triggers	Alerts	Backups	Configuration Change
RADIUS Accounting Server			OK	/var/log/radius/radius.log		
Report Runner			OK	/var/log/amp_report_runner		
Rogue Filter			OK	/var/log/rogue_filter		
RRD Write Cache			OK	-		
RTLS Collector			OK	/var/log/rtls		
SNMP Enabler			OK	/var/log/snmp_enabler		
SNMP Fetcher			OK	/var/log/snmp_fetcher		
SNMP V2 Fetcher			OK	/var/log/snmp_v2_fetcher		

Using the CLI

Use SSH to access the command-line interface of your AirWave server, and issue the following commands:

```
[root@AMPServer]# daemons | grep RTLS
root          17859 12809 0 10:35 ?          00:00:00 Daemon::RTLS
```

Issue the logs and tail rtls commands to check the RTLS log file and verify that Tag chirps are making it to the AirWave server.

```
[root@AMPServer]# logs
```

```
[root@AMPServer]# tail rtls
```

```
payload:
00147aaf01000020001a1ec02b320000001000000137aae0100000c001a1ec02b32000001a1e82b322
590006ddff02
1224534900.588245 - got 96 bytes from 10.51.1.39 on port 5050
Mon Oct 20 13:35:00 2008: 1224534900.588338 - got 96 bytes from 10.51.1.39 on port
5050
payload:
0014c9c90100003c001a1ec05078000000200000013c9c70100000c001a1ec050780000000d54a7a280
540001ddff020013c9c80100000c001a1ec050780000000cdb8ae9a9000006c4ff02
1224534900.588245 - got 96 bytes from 10.51.1.39 on port 5050
Mon Oct 20 13:35:00 2008: 1224534900.588338 - got 96 bytes from 10.51.1.39 on port
5050
payload:
0014c9c90100003c001a1ec05078000000200000013c9c70100000c001a1ec050780000000d54a7a280
540001ddff020013c9c80100000c001a1ec050780000000cdb8ae9a9000006c4ff02
```

Ensure chirps are published to Airbus by snooping on RTLS tag reports.

```
[root@AMPserver]# airbus_snoop rtls_tag_report
```

```
Snooping on rtls_tag_report:
```

```
Mon Oct 20 13:49:03 2008 (1224535743.54077)
```

```
%
```

```
ap_mac => 00:1A:1E:C0:50:78
battery => 0
bssid => 00:1A:1E:85:07:80
channel => 1
data_rate => 2
noise_floor => 85
payload =>
rssi => -64
tag_mac => 00:14:7E:00:4C:E4
timestamp => 303139810
tx_power => 19
```

Verify external applications can see WiFi Tag information by exercising the Tag XML API:

```
https://<AMP-Server-IP>/visualrf/rfid.xml
```

You should see the following XML output:

```
<visualrf:ruids version=1>
<rfid battery-level=0 chirp-interval= radio-mac=00:14:7E:00:4C:E0
vendor=>
<radio phy=g xmit-dbm=10.0/>
<discovering-radio ap=SC-MB-03-AP10 dBm=-91 id=811 index=1
timestamp=2008-10-21T12:23:30-04:00/>
<discovering-radio ap=SC-MB-03-AP06 dBm=-81 id=769 index=1
timestamp=2008-10-21T12:23:31-04:00/>
<discovering-radio ap=SC-MB-01-AP06 dBm=-63 id=708 index=1
timestamp=2008-10-21T12:23:31-04:00/>
<discovering-radio ap=SC-MB-02-AP04 dBm=-88 id=806 index=1
timestamp=2008-10-21T12:22:34-04:00/>
</rfid>
<rfid battery-level=0 chirp-interval= radio-mac=00:14:7E:00:4B:5C
vendor=>
<radio phy=g xmit-dbm=10.0/>
```

```
<discovering-radio ap=SC-MB-03-AP06 dBm=-74 id=769 index=1
  timestamp=2008-10-21T12:23:20-04:00/>
<discovering-radio ap=SC-MB-01-AP06 dBm=-58 id=708 index=1
  timestamp=2008-10-21T12:23:20-04:00/>
<discovering-radio ap=SC-MB-03-AP02 dBm=-91 id=734 index=1
  timestamp=2008-10-21T12:23:20-04:00/>
</rfid>
<rfid battery-level=0 chirp-interval= radio-mac=00:14:7E:00:4D:06
  vendor=>
  <radio phy=g xmit-dbm=10.0/>
  <discovering-radio ap=SC-SB-GR-AP04 dBm=-91 id=837 index=1
    timestamp=2008-10-21T12:21:08-04:00/>
  <discovering-radio ap=SC-MB-03-AP06 dBm=-79 id=769 index=1
    timestamp=2008-10-21T12:22:08-04:00/>
  <discovering-radio ap=SC-MB-01-AP06 dBm=-59 id=708 index=1
    timestamp=2008-10-21T12:23:08-04:00/>
  <discovering-radio ap=SC-MB-02-AP04 dBm=-90 id=806 index=1
    timestamp=2008-10-21T12:22:08-04:00/>
</rfid>
</visualrf:rfids>
```

Wi-Fi Tag Setup Guidelines

- Ensure that the tags can be heard by at least three (3) access points from any given location. The recommended value is 4 APs.
- Ensure that the tags chirp on all regulatory channels.

