AirWave 7.6 and RAPIDS

ARUBA networks

Best Practices

Copyright Information

Copyright

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.

Warranty

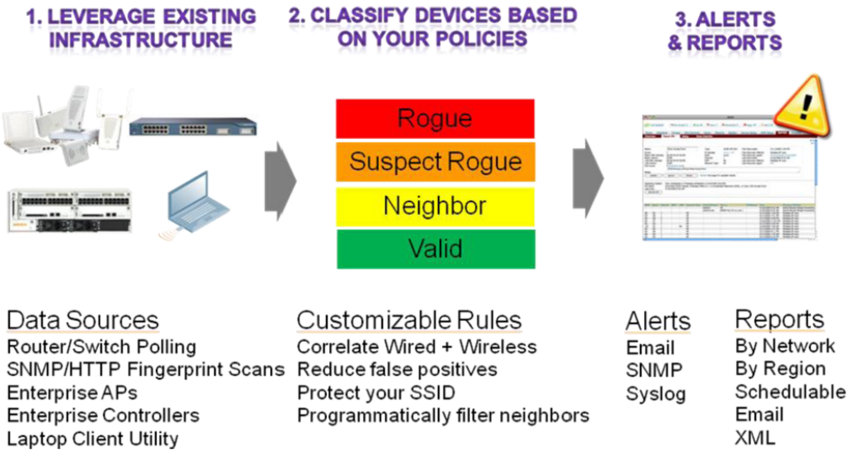
This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

Chapter 1
Overview

This document provides best practices for leveraging the Rogue Access Point Detection (RAPIDS) module of the AirWave Wireless Management Suite (AWMS) to secure your network. RAPIDS is designed to identify and locate wireless threats by leveraging all of the information available from your existing infrastructure. RAPIDS takes the information it collects and feeds it through a customizable set of classification rules, isolating the threat devices based on your security concerns. When a threatis identified, RAPIDS can be configured to alert administrators via email, SNMP traps, or syslog messages.

Figure 1 *RAPIDS Overview*



Determining Your Organization’s Security Needs

The first step to securing your network is determining what constitutes a security threat worth investigating. Every company and organization has a different set of security needs. There are a number of factors to consider when determining what is a security risk. Some of the most common factors are:

- Compliance requirements (PCI, HIPAA, SOX, etc)
- Deployed environments
- Cost of removing threats

The next step is to determine what the appropriate response actions are.

- How quickly should the rogue be removed from the network?
- Should the user who placed the rogue be educated about the dangers of rogue devices?
- Should the device be confiscated?
- How does your organization feel about wireless containment?
- How long should Rogue discovery information be stored?

Many organizations feel wireless containment constitutes a breach of FCC regulations and is illegal, while others feel that it is within their rights to contain any wireless network within their facility. Please consult with your legal department to determine your enterprise guidelines.

Common Security Threat Red Flags

Wired and Wireless

Any unmanaged device plugged into the wired network and broadcasting a signal is worth investigating. Good solution for dense environments like cities or large office buildings.

Wireless Above > -75 Signal

Any device broadcasting with a signal quality that is sufficiently strong will be investigated. A strong signal often indicates that a device is inside your organizations walls. Good for campuses that are fairly remote and will not see a lot of legitimate neighbor devices.

Wireless with a Managed SSID

Your enterprise’s SSIDs are managed by your IT department. No unauthorized access points should be using it. AirWave strongly recommends that any device using the enterprise SSIDs should be classified as a rogue and investigated immediately. Attackers will often deploy Honey Pot APs using managed SSIDs in an attempt to lure valid clients to associate with them and attempt to login. It is very easy for well meaning users to accidentally attempt to login to the foreign system using their corporate credentials. Once the attacker has those credentials they can easily access the wireless network.

Wireless with More than Three Detecting APs

The number of detecting APs is another method for determining if a rogue is inside your premises. If only a few APs detect the device it is very likely on the outside of the network and a neighboring AP. If it is heard by a large number of APs there is a much higher chance that the device is inside the building. Good for campuses with single tenants.

Shared office buildings may have neighbor APs on the floors above or below them that will be detected by a number of core APs.

RAPIDS has a number of configurable options. The sections referenced below outline a number of the recommended settings that will help you get the most out of RAPIDS. These are general recommendations that may not apply to all customers.

- "Wired-to-Wireless MAC Address Correlation (0-8 bits)" on page 5
- "Wireless-to-Wireless BSSID Correlation (0-8 bits) " on page 5
- "Delete Rogues not heard for: (Number of Days)" on page 5
- "Automatically OS Scan Rogue Devices" on page 5
- "Filter Rogues Discovered by Remote APs" on page 6
- "Wired-to-Wireless Time Correlation Window" on page 6
- "Triggers" on page 6

Wired-to-Wireless MAC Address Correlation (0-8 bits)

8 recommended

The Rogue MAC Address Correlation setting is used to correlated wireless discovery events with wired MAC addresses. If the two addresses are within the bit mask, they will be combined into one device record in RAPIDS. A setting of 8 bits will match addresses that have the same first 8 characters (00:11:22:33:44:XX). 4 bits will match addresses that have the same first 9 characters. Newer SOHO device LAN MAC addresses tend to be fairly far from the radio addresses. A setting of 8 will combine more devices. The higher you set this value, the more likely you will see an incorrect correlation.

Wireless-to-Wireless BSSID Correlation (0-8 bits)

4 recommended

The wireless BSSID correlation is used to correlate BSSIDs from a single physical radio into one record. Generally, BSSIDs increment by 1 on a radio and will be very close together. Because of this, we recommend 4 instead of 8 for wired-to-wireless correlation.

Delete Rogues not heard for: (Number of Days)

14 recommended

If a rogue device has not been detected for the specified number of days, it is likely gone. Removing it from RAPIDS automatically will decrease the number of devices that need to be investigated/tracked. If the device is detected again, it will be recreated, and any alerts that have been defined will fire again.

Automatically OS Scan Rogue Devices

Yes recommended

When enabled, RAPIDS will automatically perform an OS scan of devices with an IP address. The scans take about a minute per IP address. Do not enable this option if your wired security team has concerns about running port scans on clients.

Filter Rogues Discovered by Remote APs

Yes recommended

This is an Aruba specific feature designed to ignore devices heard by Remote APs. Remote APs are often installed at employees homes. The corporate security team has no ability to make any changes to neighboring devices and there are no corporate wired ports that need to be monitored.

Wired-to-Wireless Time Correlation Window

240 recommended

This option allows you to specify a time frame for wired and wireless correlation. RAPIDS discovery events detected wirelessly and on LAN will only match if the wireless and LAN discovery events occur during this timeframe.

We recommend that this value match the polling period for bridge forwarding, which is four hours by default. With this configuration, any rogues seen on the wired and wireless network will be classified as such if the discovery event is within four hours. Users who are concerned about events where a rogue is on both the wired and wireless network may consider increasing this value. Note that increasing this value might yield more classifications of wired/wireless than expected. Similarly, some users may consider setting this value to match the Rogue AP Polling interval, which is 30 minutes by default.

Triggers

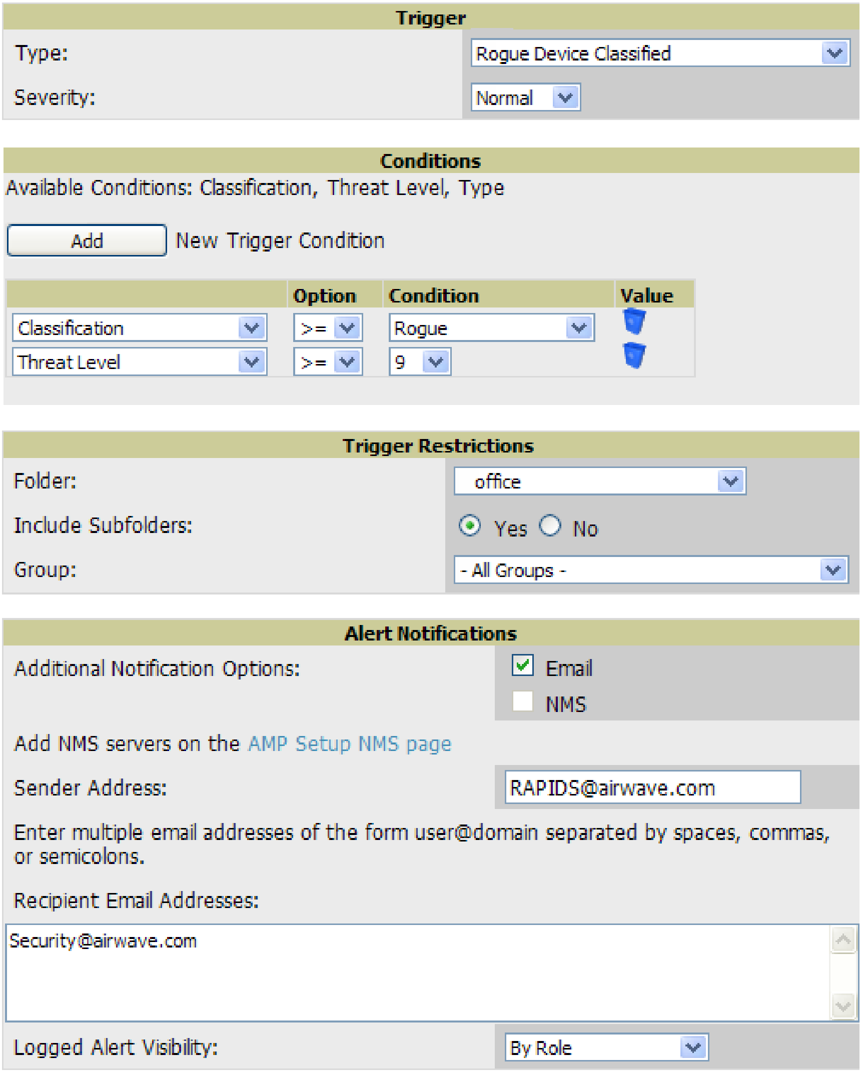
Triggers are an important, and often overlooked, part of RAPIDS. Detecting rogue devices does not mean much if the security team is not notified about them. Triggers are defined on the **System > Triggers** page. Add a Rogue Device Classified trigger type to ensure that you are notified of any rogues that are detected by the system. Multiple Rogue Device Classified types can be defined on one server based on classification and threat level. The trigger will only fire an alert when a rogue device is classified to meet the conditions. The alert will not continuously fire every time the rogue device is detected.

AirWave recommends emailing the appropriate individuals when any Rogue devices are classified so that the appropriate action can be taken.

NOTE

Triggers must be enabled in order to meet PCI compliance requirements.

Figure 2 ***System > Triggers > Add*** *page*



Trigger

Type:	Rogue Device Classified
Severity:	Normal

Conditions

Available Conditions: Classification, Threat Level, Type

New Trigger Condition

	Option	Condition	Value
Classification	>=	Rogue	
Threat Level	>=	9	

Trigger Restrictions

Folder:	office
Include Subfolders:	● Yes ○ No
Group:	- All Groups -

Alert Notifications

Additional Notification Options:	☑ Email ☐ NMS

Add NMS servers on the AMP Setup NMS page

Sender Address: RAPIDS@airwave.com

Enter multiple email addresses of the form user@domain separated by spaces, commas, or semicolons.

Recipient Email Addresses:

Security@airwave.com

Logged Alert Visibility: By Role

This section describes how to best configure Rogue scans (i.e, making sure RAPIDS is getting all of the data that it can).

RAPIDS has four main detection mechanisms:

- Wireless
  - AMC scans
  - Enterprise AP scans
- Wired
  - HTTP/SNMP fingerprint scans
  - Router/switch scans

Wireless Scans

Enterprise AP scans

The first step to getting wireless discovery information is adding your supported controllers and APs into AWMS. AWMS will automatically start polling the controllers and APs via SNMP for rogue discovery information once they are monitored. The rogue data polling interval is configured on the **Groups** > **Basic** page under the **SNMP Polling Periods**.

Most enterprise APs support wireless scanning but there is one notable exception, IOS APs. IOS APs use a proprietary protocol to transfer the rogue discovery data. AWMS can be configured to poll WLSE servers for rogue discovery. Please see the *AirWave User Guide* for WLSE polling setup instructions.

AMC Scans

The AirWave Management Client (AMC) provides another option for customers with APs that do not report wireless discovery data or do not have full AP coverage. The AMC is a client application that runs in Windows XP. It passively listens for beaconing APs and reports them back to the RAPIDS engine via an XML interface.

Wired Scans

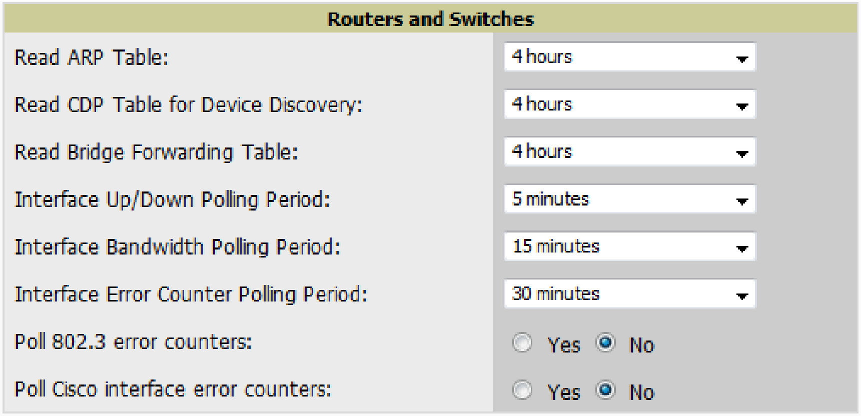
Fingerprint Scans

The **Device Setup** > **Discover** page defines the network scans that are run. AirWave recommends running daily device discovery scans on any networks likely to have APs or Rogues. The scans look at the credential challenges and rejections from the device to determine the model. The HTTP rogue scans should not have the correct rogue credentials. The HTTP scan requires that the rogue have an HTTP interface available on the scanned IP address. Similarly, the SNMP scan requires a SNMP interface on the scanned IP address. HTTP/SNMP fingerprint scans provide another valuable data point to RAPIDS. There are a number of ways a hacker can circumvent these scans but what is found is certainly a rogue worth investigating.

Router/Switch Polling

Router/Switch polling is configured by adding routers/switches to groups as monitored devices. The group has configurable wired polling periods on the **Groups** > **Basic** page as seen in the following figure.

Figure 3 *Routers and Switches*

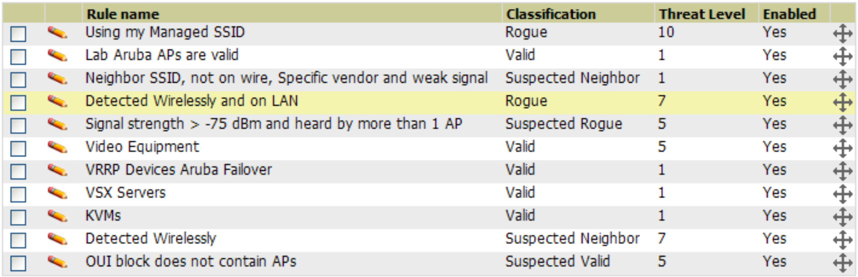


Routers and Switches	
Read ARP Table:	4 hours
Read CDP Table for Device Discovery:	4 hours
Read Bridge Forwarding Table:	4 hours
Interface Up/Down Polling Period:	5 minutes
Interface Bandwidth Polling Period:	15 minutes
Interface Error Counter Polling Period:	30 minutes
Poll 802.3 error counters:	○ Yes ● No
Poll Cisco interface error counters:	○ Yes ● No

The **Read ARP Table** and the **Read Bridge Forwarding Table** are used by RAPIDS. Depending on the data returned by the router/switch, RAPIDS is able to gather IP addresses, LAN MAC addresses, OUI scores, LAN vendor, and switch ports. After RAPIDS has an IP address for a device, it can perform an operating system scan and discover the likely operating system of a device. Operating system scans can be run on demand from the **RAPIDS > Rogue APs** page using **Modify Devices** or on the Rogue detail page.

The specific rules that will work best in your environment are going to vary heavily based on your security requirements, but there are some general best practices to keep in mind.

Figure 4 ***RAPIDS > Rules***



		Rule name	Classification	Threat Level	Enabled	
□	✎	Using my Managed SSID	Rogue	10	Yes	✥
□	✎	Lab Aruba APs are valid	Valid	1	Yes	✥
□	✎	Neighbor SSID, not on wire, Specific vendor and weak signal	Suspected Neighbor	1	Yes	✥
□	✎	Detected Wirelessly and on LAN	Rogue	7	Yes	✥
□	✎	Signal strength > -75 dBm and heard by more than 1 AP	Suspected Rogue	5	Yes	✥
□	✎	Video Equipment	Valid	5	Yes	✥
□	✎	VRRP Devices Aruba Failover	Valid	1	Yes	✥
□	✎	VSX Servers	Valid	1	Yes	✥
□	✎	KVMs	Valid	1	Yes	✥
□	✎	Detected Wirelessly	Suspected Neighbor	7	Yes	✥
□	✎	OUI block does not contain APs	Suspected Valid	5	Yes	✥

Rule Guidelines

Order is Important

The first rule in the list that matches (from the top down) will determine the devices' classification. Make sure that the most detailed rules are at the top of the list. If new information comes in and updates the device, it will be classified up the list of rules but not down.

Name the Rules Intuitively

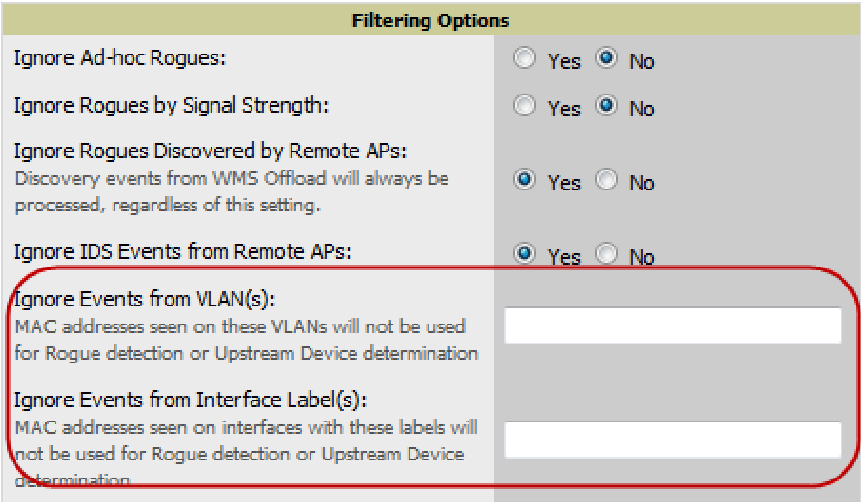
Detailed names that outline the criteria of a rule are very helpful in the rogue list and rogue detail pages. There are a number of places where you can see the name of a classifying rule but can't see the detailed criteria.

Don't Forget Neighbor and Valid Rules

Valid rules are often forgotten or overlooked but are just as important as Rogue rules. Valid rules help filter out a large number of devices that are not threats. Review the list of detected devices. Create suspect neighbor or neighbor rules based on the neighboring SSID, manufacturer, and the fact that it is not connected to the wired network.

AirWave allows you to specify VLANs and Interfaces that can be ignored in wired Rogue Discovery events and in upstream device determination. These settings, configured on the **RAPIDS > Setup** page, are particularly useful to customers who have switches in AMP. The ports on those switches contain either special interface labels or multiple VLANs. In the case of multiple VLANs, imagine that the user has two VLANs: one acting as the corporate, and the other acting as a guest. Use the "Ignore Events from VLAN(s)" setting so that the guest VLAN wired Rogue Discovery Events can be ignored because they are not critical.

Figure 5 *Ignore Events*



Filtering Options	
Ignore Ad-hoc Rogues:	○ Yes ● No
Ignore Rogues by Signal Strength:	○ Yes ● No
Ignore Rogues Discovered by Remote APs: Discovery events from WMS Offload will always be processed, regardless of this setting.	● Yes ○ No
Ignore IDS Events from Remote APs:	● Yes ○ No
Ignore Events from VLAN(s): MAC addresses seen on these VLANs will not be used for Rogue detection or Upstream Device determination	
Ignore Events from Interface Label(s): MAC addresses seen on interfaces with these labels will not be used for Rogue detection or Upstream Device determination	

Protect Your SSID

Only your managed devices should be broadcasting your enterprise's SSID. Unauthorized devices broadcasting your SSID pose a significant security risk. Hackers will frequently put up rogue APs broadcasting an official SSID in an attempt to trick an unsuspecting user into associating to it. Once associated, the hacker will attempt to obtain the users valid network credentials.

After RAPIDS has identified a rogue device, the next step is to investigate it and remove it from the network. The exact steps and workflow will depend on your organization's security standards. Some common workflows are listed below.

NOTE

The last step in the examples below is to delete the rogue from RAPIDS. If the rogue is rediscovered, then it will be recreated and reclassified in RAPIDS.

Occasionally the rogue device turns out to be an approved AP that is not managed by the IT team. When that happens, update the **Notes** field with appropriate information about the rogue, and reclassify it as a valid device.

Common Rogue Response Scenarios

Rogue Connected to the Wired Network

RAPIDS will report the switch and port number for devices that are discovered on the wire. Review the list of switches and determine the edge switch. Login to the switch and disable the port. Physically trace the cable and remove the rogue device. If the rogue device can be related to an employee, educate them on the dangers of rogue devices. Delete the rogue from RAPIDS.

Rogue Detected Wirelessly Only

Wirelessly detected devices are a little harder to track down than wired rogues.

If your organization is comfortable with wireless containment, and you have devices capable of wireless containment, the first step is to configure it.

Wireless Rogue Detection with VisualRF

If VisualRF is installed, locate the rogue in VisualRF.

If you are not running VisualRF or it is not up to date, navigate to the rogue detail page and investigate the list of discovering devices. Using that list of devices and discovered signal strengths, you should be able to determine the general location of the rogue device. Physically inspect the area where VisualRF has placed the rogues or where you estimate it to be.

If the rogue device can be related to an employee, educate them on the dangers of rogue devices, and then delete the rogue from RAPIDS. If the rogue turns out to be a valid neighboring device, update the classification to Neighbor, acknowledge the device, and then update the Notes field with investigation information, including who located the device, when it was located, and the neighboring company that the device belongs to.

Ad-Hoc Rogues

Ad-Hoc rogues are notoriously hard to track down. They are highly mobile, temporary devices that are often the result of well meaning but misconfigured laptops. Some wireless drivers will use the radio MAC address when in ad-hoc mode. It is recommended to search historical clients on AMP for the ad-hoc MAC address. If the ad-hoc rogue is found as a client, you will know the historical users of the laptop and can contact them to properly configure the laptop. Follow the "Rogue Detected Wirelessly Only" on page 13 process above if the MAC address is not found as a user.