Rogue Management in a Unified Wireless Network using v7.4

First Published: Aug 10, 2010
Last Updated: May 9, 2013

Contents

Cisco Systems, Inc.
www.cisco.com

Introduction

Wireless network is becoming new norm with the trend of BYOD in the enterprise environment. These new types of devices give flexibility on where and how they consume data and access network. For example, any personal smart device can be a WiFi Access Point or a Personal Hotspot. Such trends make Rogue device management a common practice for enterprise wireless security policy

Cisco's latest enhancement on Rogue management and base WIPS offers much enhanced rogue manageability and provides easy yet powerful wireless protection mechanism. This document will cover Base WIPS Rogue management service which can be done via AP and WLC only. License-based feature or PI/MSE-required feature is not a part or intention of this document. Also, New Security module in AP3600 is covered in a different document.

Prerequisites

Requirements

This document assumes you are familiar with basic controller configurations and WIPS configuration before 7.4 software versions.

Components Used

The information in this document is based on the following software and hardware versions:

- Cisco Unified Controllers (2500, 5500, WiSM2, 7500, 8500 and SRE for ISR G2 Series) running version 7.4
- Control and Provisioning of Wireless Access Point Protocol (CAPWAP)-based LAPs - 1130AG, 1140, 1240AG, 1250, 1260, 1600, 2600 and 3500, 3600 Series LAPs as well as WSSI module on 3600 Series AP

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Cisco WIPS Solution Overview

Cisco WIPS solution offers flexible and scalable, 24x7x365-based full time wireless security solution to different types of customer requirement. These Cisco WIPS solution are more comprehensive and sophisticated. This document primarily covers most of the fundamental WIPS security solutions that Cisco Unified Wireless Solution offer. Cisco's Adaptive Wireless Protection System, Cisco MSE (Mobility Solution Engine) as well as solution that leverages Cisco CleanAir® , Cisco's unique ASIC-based Spectrum Intelligence and intelligence across Wireless LAN Controller and Mobility Solution Engine enable hardware's security capability and provide protection from intrusive and harmful type of wireless threats.

Table 1 provides a summary of WIPS functionality that comes with WLC, WLC plus MSE, and WLC plus MSE plus CleanAir.

Table 1 Cisco WIPS Comparison

Feature	BaseWIPS (WLC)	Adaptive WIPS (WLC and MSE)	Adaptive WIPS (WLC plus MSE plus CleanAir)
Rogue access point and ad hoc rogue detection, classification, location tracking, and containment	Yes	Yes	Yes
Switchport tracing and disabling	Yes	Yes	Yes
Management frame impersonation detection	Yes	Yes	Yes
Rogue containment when WAN is down	Yes	Yes	Yes
Internal and external rogue access point detection and containment times	Yes	Yes	Yes
Smartphone tethering detection and containment	Yes	Yes	Yes
Location tracking and containment for DoS attacker and non authorized device that is trying to associate internal access point	Yes	Yes	Yes
Wired Equivalent Privacy (WEP) cracking detection	Yes	Yes	Yes
MAC spoofing rogue's detection and containment	Yes	Yes	Yes
Auto MAC learning and Internet connection sharing (ICS) detection	Yes	Yes	Yes
Internet connection sharing (ICS) detection	Yes	Yes	Yes
Enterprise-level alarm/event correlation	Yes	Yes	Yes
Attack signature threshold customization	Yes	Yes	Yes
Off-channel rogue detection and location, integrated into infrastructure	Yes	Yee	Yes
DoS signature updates	No	Yes	Yes
Wireless intrusion signature updates	No	Yes	Yes
Attack forensics (all signatures)	No	Yes	Yes
Non-Wi-Fi transmitter detection and location	No	No	Yes
Non-Wi-Fi bridge detection and location	No	No	Yes
Non-Wi-Fi access point detection and location	No	No	Yes
Layer 1 DoS attack location and detection	No	No	Yes

Cisco CleanAir® technology is an effective tool to monitor and manage your network's RF conditions. Cisco MSE extends those capabilities. Table 2 provides a summary of CleanAir plus MSE offers.

Table 2 CleanAir plus MSE Offers

	CleanAir Access Points-(2600, 3500, 3600) plus WLC	**CleanAir Access Points plus WLC plus MSE**
Rogue mitigation	Yes	Yes
Detect, classify, and mitigate interferers	Yes	Yes
Maintain air quality	Yes	Yes
Detect Layer 1 exploits	Yes	Yes
Track and trace rogues	No	Yes
Security penetration and DoS attack mitigation	No	Yes
System wide interferer details and event correlation	No	Yes
Zone of impact and interferer notification	No	Yes
Track and trace interferers and Layer 1 exploits	No	Yes

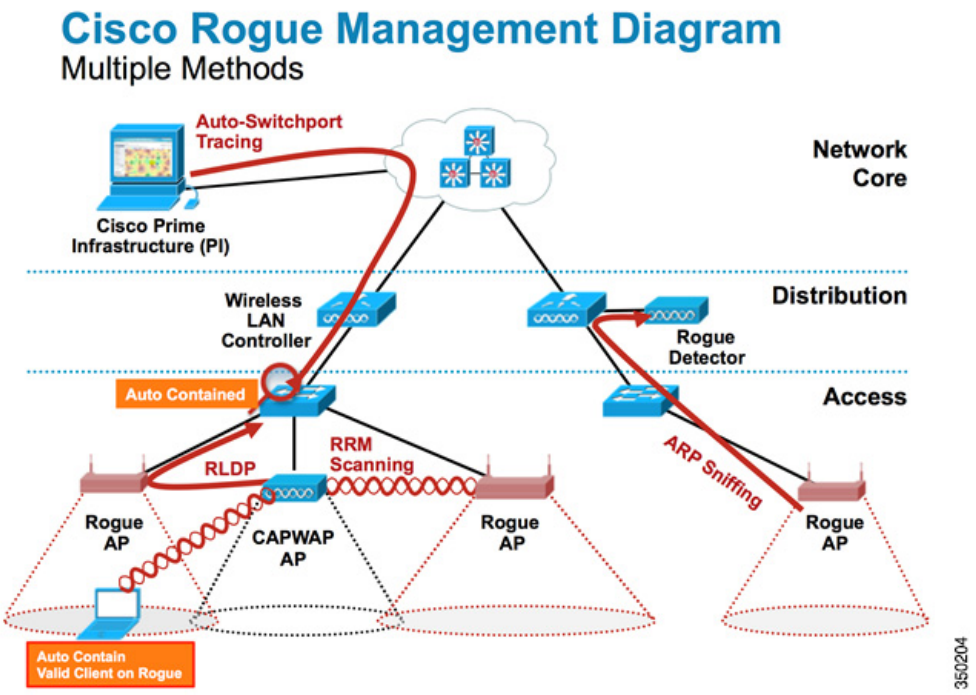
Rogue Overview

Any device that shares your spectrum and is not managed by you can be considered a rogue. A rogue becomes dangerous in the following scenarios:

- When the Rogue AP uses the same SSID as your network (honeypot).
- When the Rougue AP device is detected on wired network also.
- Ad-hoc rogues are also a big threat.
- Setup by an outsider with malicious intent.

There are three main phases of rogue device management in Cisco Unified Wireless Network (UWN) solution:

- Detection – Radio Resource Management (RRM) scanning is used to detect the presence of rogue devices.
- Classification – Rogue Location Discovery Protocol (RLDP), Rogue Detectors and switch port tracing are used to identify if the rogue device is connected to the wired network. Rogue classification rules also assist in filtering rogues into specific categories based on their characteristics.
- Mitigation – Switch port Trace and shutting down, rogue location, and rogue containment are used to track down physical location and nullify the threat of rogue devices.



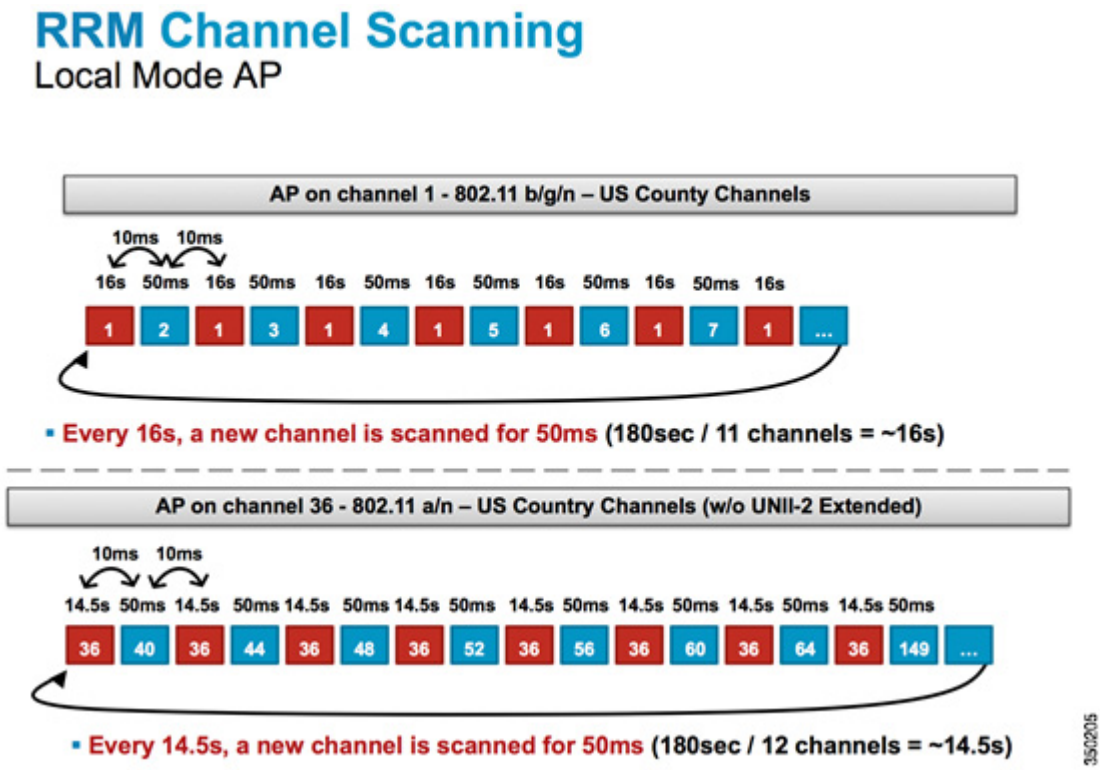
Rogue Management Theory of Operation

Rogue Detection

A rogue is essentially any device that is sharing your spectrum, but is not in your control. This includes rogue Access Points (APs), wireless router, rogue clients, and rogue ad-hoc networks. The Cisco UWN uses a number of methods to detect Wi-Fi-based rogue devices including off-channel scanning and dedicated monitor mode capabilities. Cisco Spectrum Expert can also be used to identify rogue devices not based on the 802.11 protocol, such as Bluetooth bridges.

Off-Channel Scanning

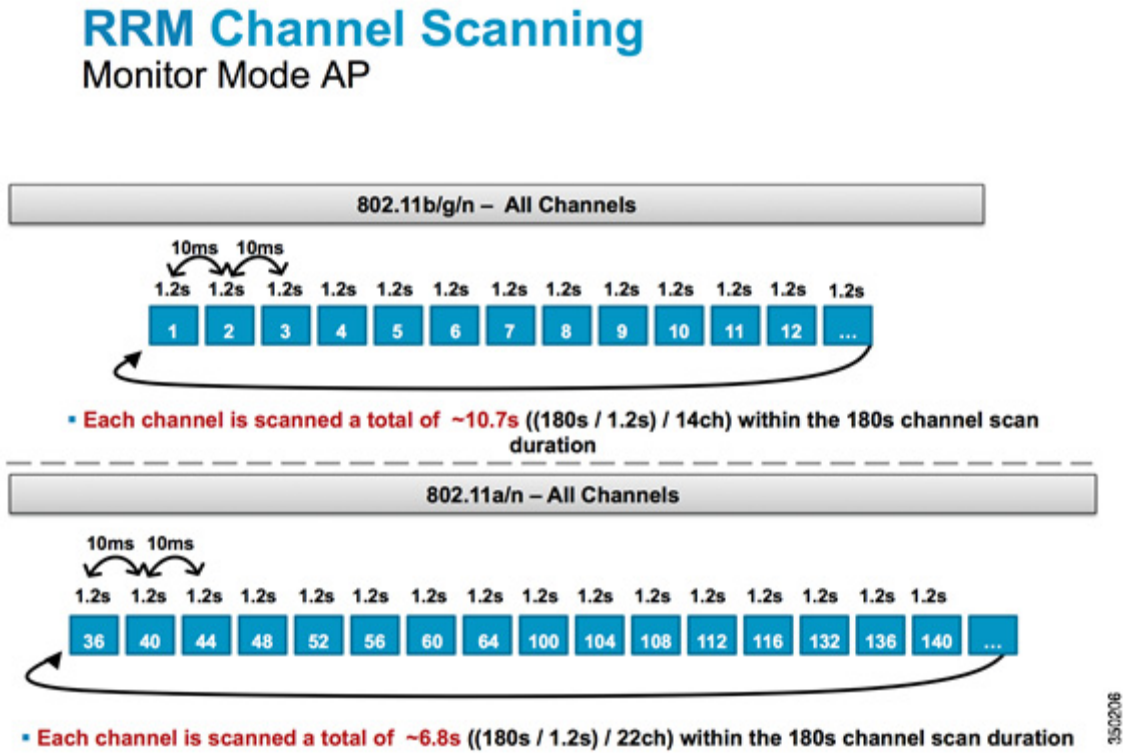
This operation is performed by Local mode and FlexConnect (in connected mode) APs and utilizes a time-slicing technique that allows client service and channel scanning using the same radio. By going off channel for a period of 50ms every 16 seconds, the AP, by default, only spends a small percentage of its time not serving clients. Also, note there is a 10ms channel change interval that will occur. In the default scan interval of 180 seconds, each 2.4Ghz FCC channel (1-11) is scanned at least once. For other regulatory domains, such as ETSI, the AP will be off channel for a slightly higher percentage of time. Both the list of channels and scan interval can be adjusted in the RRM configuration. This limits the performance impact to a maximum of 1.5% and intelligence is built into the algorithm to suspend scanning when high-priority QoS frames, such as voice, need to be delivered.



This above graphic is a depiction of the off-channel scanning algorithm for a local mode AP in the 2.4GHz & 5GHz frequency band. Each red square represents the time spent on the APs home channel, whereas each blue square represents time spent on adjacent channels for scanning purposes.

Monitor Mode Scanning

This operation is performed by Monitor Mode and Adaptive wIPS monitor mode APs which utilizes 100% of the radio's time for scanning all channels in each respective frequency band. This allows greater speed of detection and enables more time to be spent on each individual channel. Monitor mode APs are also far superior at detecting rogue clients as they have a more comprehensive view of the activity occurring in each channel.



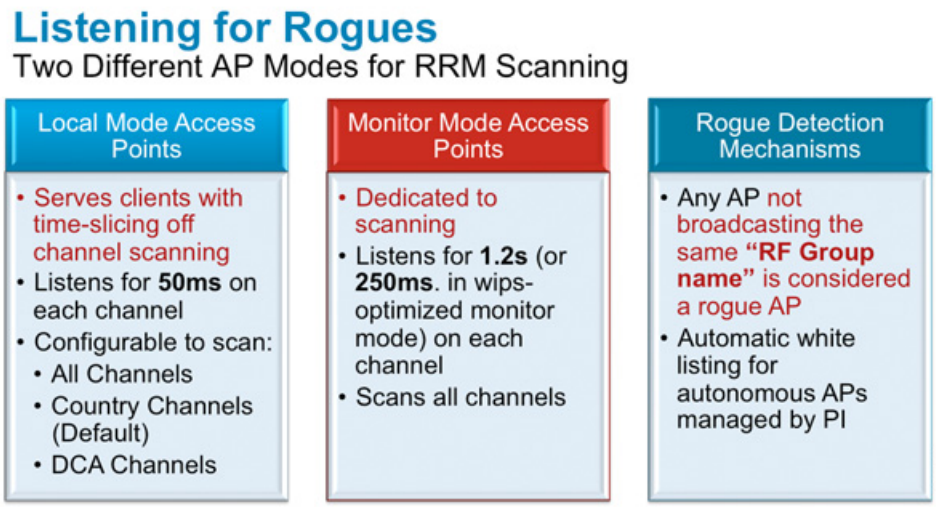
This graphic is a depiction of the off-channel scanning algorithm for a monitor mode AP in the 2.4GHz and 5Ghz frequency band.

By default, Monitor mode dwell on 1.1 sec. for each channel. If user' turn on (CLI: config ap monitor-mode wips-optimized) WIPS-optimized Monitor mode, AP changes dwell time of each channel on monitor mode from 1.1sec to 250msec. this will allow monitor AP to sweep channel quickly and the time to cycle entire channel scan becomes much faster for rogue detection and containment.

Local Mode and Monitor Mode Comparison

A local mode AP splits its cycles between serving WLAN clients and scanning channels for threats. As a result, it takes a local mode AP longer to cycle through all the channels, and it spends less time collecting data on any particular channel so that client operations are not disrupted. Consequently, rogue and attack detection times are longer (3 to 60 minutes) and a smaller range of over-the-air attacks can be detected than with a monitor mode AP. Furthermore, detection for bursty traffic, such as rogue clients, is much less deterministic because the AP has to be on the channel of the traffic at the same time the traffic is being transmitted or received. This becomes an exercise in probabilities. Local mode AP operations Wireless threats management from local mode AP can be extended by enabling Enhanced Local mode (ELM, WIPS-submode). ELM enables full adaptive WIPS signature detection while it leaves AP to serve data mode most of time. ELM and Adaptive WIPS solution will be described in separate WIPS Deployment Guide.

A monitor mode AP spends all of its cycles scanning channels looking for rogues and over-the-air attacks. A monitor mode AP can simultaneously be used for Adaptive wIPS, location (context-aware) services, and other monitor mode services. When monitor mode APs are deployed, the benefits are lower time-to-detection. When monitor mode APs are additionally configured with Adaptive wIPS, a broader range of over-the-air threats and attacks can be detected.



Rogue Identification

If probe response or beacons from a rogue device are heard by either local mode, FlexConnect mode, or monitor mode APs, then this information is communicated via CAPWAP to the Wireless LAN controller (WLC) for processing. Rogue device can be identified regardless of its SSID is broadcast or not. In order to prevent false positives, a number of methods are used to ensure that other managed Cisco-based APs are not identified as a rogue device. These methods include mobility group updates, RF neighbor packets, and white listing autonomous APs via Cisco Prime Infrastructure (PI).

Rogue Records

While the controller's database of rogue devices contains only the current set of detected rogues, the Cisco PI also includes an event history and logs rogues that are no longer seen.

Rogue Details

A CAPWAP AP goes off-channel for 50ms in order to listen for rogue clients, monitor for noise, and channel interference. Any detected rogue clients or APs are sent to the controller, which gathers the following information:

- The rogue AP's MAC address
- Name of the AP detected rogue
- The rogue connected client(s) MAC address
- Whether the frames are protected with WPA or WEP
- The preamble
- The Signal-to-Noise Ratio (SNR)
- The Receiver Signal Strength Indicator (RSSI)
- Channel of Rogue detection
- Radio in which rogue is detected
- Rogue SSID (if the rogue SSID is broadcasted)

- Rogue IP address
- First and last time the rogue is reported
- Channel width

Exporting Rogue Events

In order to export rogue events to a third-party Network Management System (NMS) for archival, the WLC permits additional SNMP trap receivers to be added. When a rogue is detected or cleared by the controller, a trap containing this information is communicated to all SNMP trap receivers. One caveat with exporting events via SNMP is that if multiple controllers detect the same rogue, duplicate events are seen by the NMS as correlation is only done at PI.

Rogue Record Timeout

Once a rogue AP has been added to the WLC's records, it will remain there until it is no longer seen. After a user configurable timeout (1200 seconds default, configurable from 120 to 3600 sec.), a rogue in the “Unclassified” category is aged out. Rogues in other states such as “Contained” and “Friendly” will persist so that the appropriate classification is applied to them if they reappear.

There is a maximum database size for rogue records that is variable across controller platforms:

	8500/7500	5760	WISM2	5508	vWLC	2504
Rogue AP	24000	12000	4000	2000	800	2000
Rogue Client	32000	12000	5000	2500	1500	2500

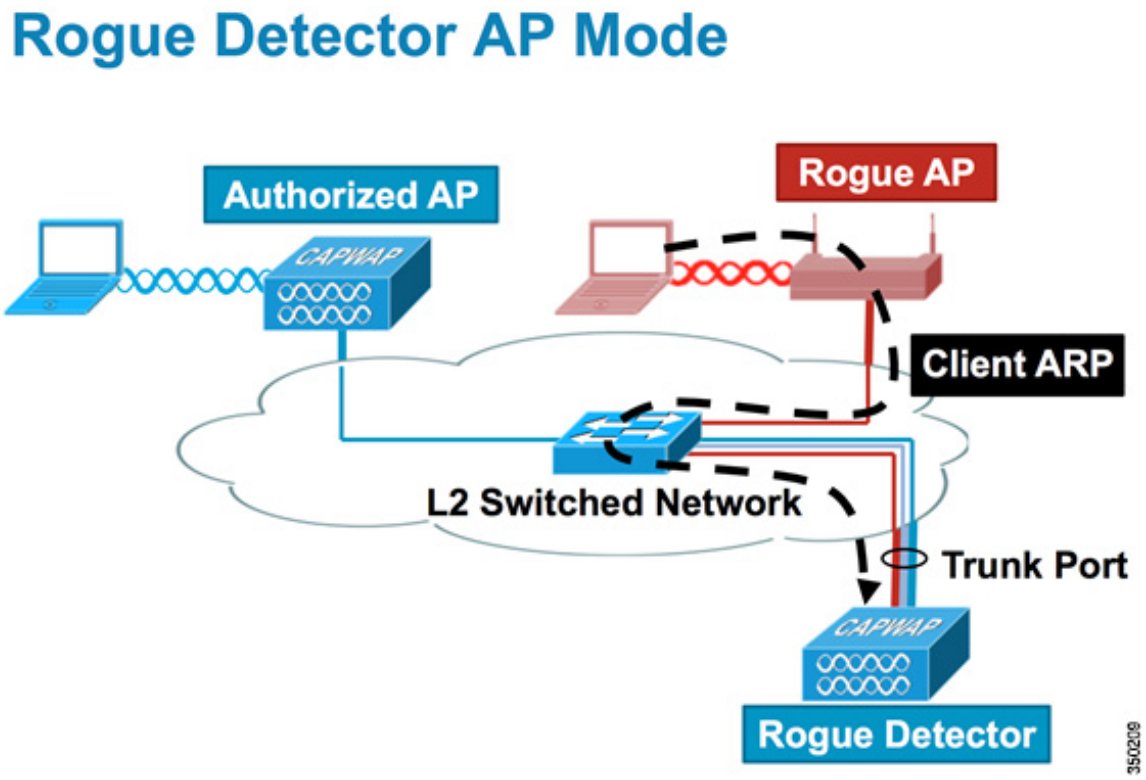
Number of Max Rogue Client per AP is increased to 256 from 16 from 7.4

Rogue Classification

By default, all rogues that are detected by the Cisco UWN are considered Unclassified. As depicted in this the below graphic, rogues can be classified on a number of criteria including RSSI, SSID, Duration, Security type, on/off network, and number of clients:

Rogue Detector AP

A rogue detector AP aims to correlate rogue information heard over the air with ARP information obtained from the wired network. A positive match is based on the wired and wireless MAC address with difference of +1/-1. If a MAC address is heard over the air as a rogue AP or client and is also heard on the wired network, then the rogue is determined to be on the wired network. If the rogue is detected to be on the wired network, then the alarm severity for that rogue AP is raised to “Critical”. It should be noted that a rogue detector AP is not successful at identifying rogue clients behind a device using NAT.

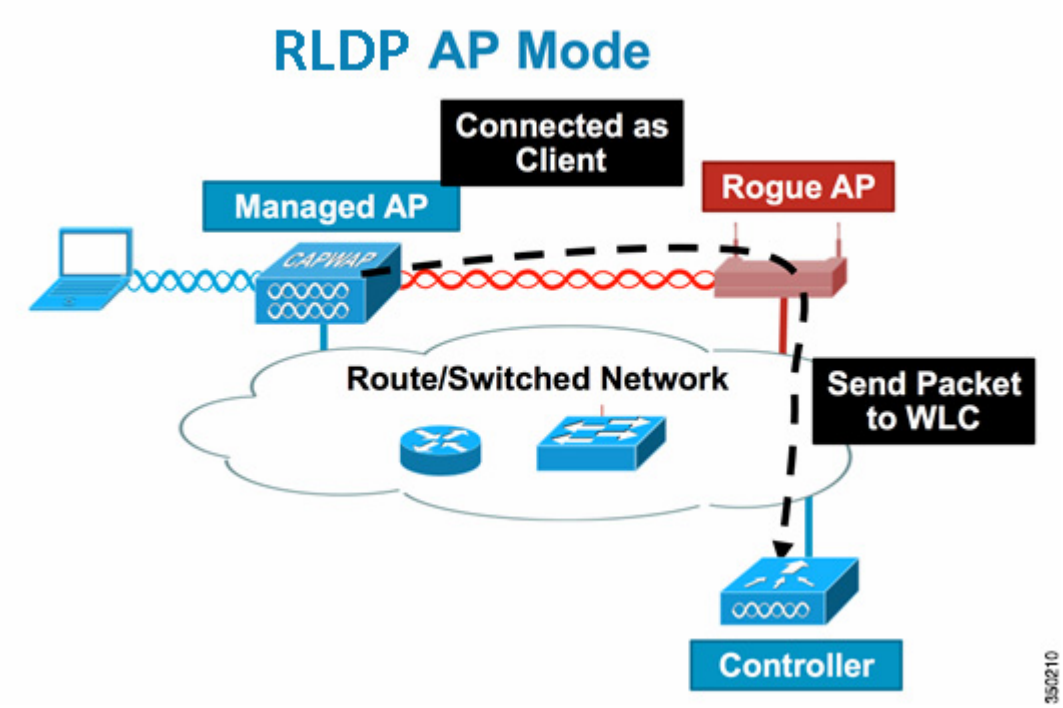


Scalability Considerations

A rogue detector AP can detect up to 500 rogues and 500 rogue clients. If the rogue detector is placed on a trunk with too many rogue devices, then these limits might be exceed, which causes issues. In order to prevent this from occurring, keep rogue detector APs at the distribution or access layer of your network.

RLDP

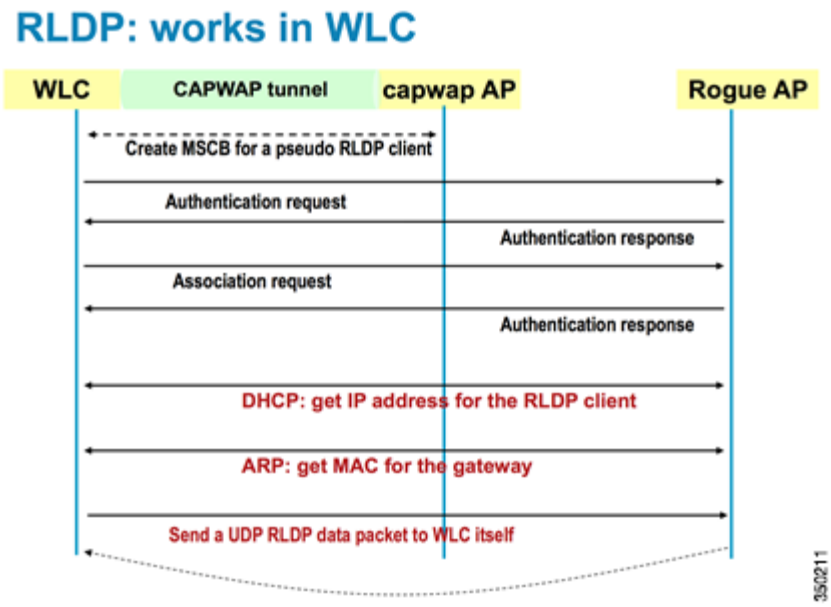
The aim of RLDP is to identify if a specific rogue AP is connected to the wired infrastructure. This feature essentially uses the closest Unified AP to connect to the rogue device as a wireless client. After connecting as a client, a packet is sent with the destination address of the WLC to assess if the AP is connected to the wired network. If the rogue is detected to be on the wired network, then the alarm severity for that rogue AP is raised to critical.



The algorithm of RLDP is listed here:

1. Identify the closest Unified AP to the rogue using signal strength values.
2. The AP then connects to the rogue as a WLAN client, attempting three associations before timing out.
3. If association is successful, the AP then uses DHCP to obtain an IP address.
4. If an IP address was obtained, the AP (acting as a WLAN client) sends a UDP packet to each of the controller's IP addresses.
5. If the controller receives even one of the RLDP packets from the client, that rogue is marked as on-wire with a severity of critical.

Note The RLDP packets will be unable to reach the controller if filtering rules are placed between the controller's network and the network where the rogue device is located.

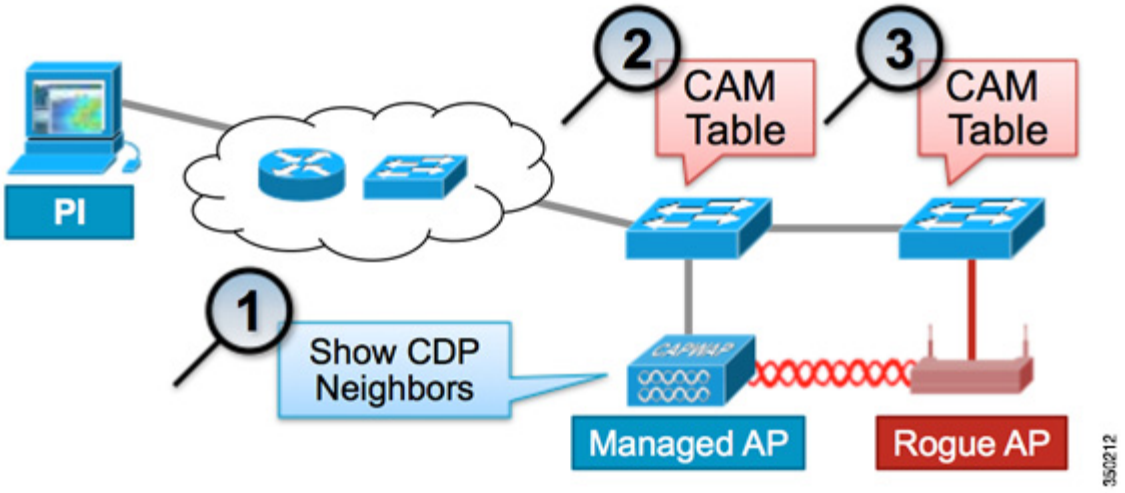


Caveats of RLDP

- RLDP only works with open rogue APs broadcasting their SSID with authentication and encryption disabled.
- RLDP requires that the Managed AP acting as a client is able to obtain an IP address via DHCP on the rogue network.
- Manual RLDP can be used to attempt an RLDP trace on a rogue multiple number of times.
- During RLDP process, the AP is unable to serve clients. This will negatively impact performance and connectivity for local mode APs. To avoid this case, RLDP can be selectively enabled for Monitor Mode AP only.
- RLDP does not attempt to connect to a rogue AP operating in a 5GHz DFS channel.

Switch Port Tracing

Switch port tracing is a rogue AP mitigation technique first implemented in the 5.1 release and later with MSE 7.3 and PI 1.2, evolved into Auto Switch Port Tracing. Although switch port tracing is initiated at the PI, it utilizes both CDP and SNMP information to track a rogue down to a specific port in the network. In order for switch port tracing to run, all switches in the network must be added to the PI with SNMP credentials. Although read-only credentials work for identifying the port the rogue is on, read-write credentials allow the PI to also shut the port down, thus containing the threat. At this time, this feature works only with Cisco switches that run IOS with CDP enabled, and CDP must also be enabled on the Managed APs.



The algorithm for switch port tracing is listed here:

- The PI finds the closest AP, which detects the rogue AP over-the-air, and retrieves its CDP neighbors.
- The PI then uses SNMP to examine the CAM table within the neighboring switch, looking for a positive match to identify the rogue location.
- A positive match is based on the exact rogue MAC address, +1/-1 & +2/-2 the rogue MAC address, any rogue client MAC addresses, or an OUI match based on the vendor information inherent in a MAC address.
- If a positive match is not found on the closest switch, the PI continues searching neighboring switches up to two hops away (by default).

Wired-Side Tracing Techniques

	How it Works	What It Detects	Accuracy
Switchport Tracing	1. AP hears rogue over air 2. Detecting AP advises of nearby switches 3. Trace starts on nearby switches 4. Results reported in order of probability 5. Administrator may disable port	▪Secured APs ▪Open APs ▪NAT APs	▪Moderate
RLDP	1. AP hears rogue over air 2. Detecting AP connects as client to rogue AP 3. Detecting AP sends RLDP packet 4. If RLDP packet seen at WLC, then on wire	▪Open APs ▪NAT APs	▪100%
Rogue Detector	1. Place detector AP on trunk 2. Detector receives all rogue MACs from WLC 3. Detector AP matches rogue MACs from wired-side ARPs	▪Secured APs ▪Open APs ▪NAT APs	▪High

350213

Rogue Classification Rules

Rogue classification rules, introduced in the 5.0 release, allow you to define a set of conditions that mark a rogue as either malicious or friendly. This feature is revamped on 7.4 by adding Custom, Policy-based Rogue Classification Rule. This allow WLC to create custom-defined Rogue list, with custom severity level, ranging from 1 to 100. Hence, in addition to Malicious and Friendly rule, Administrator can add Custom Rogue Rule that custom defines Rogue's character such as Internal/External/Alert/Contain. Among these four classifications, Contain type defines auto containment action, based on this rogue filter rule. Once certain Rogue device is classified as "contain" as its notification type, neighboring APs immediately contains such Rogue devices. These rules are configured at the PI or the WLC, but they are always performed on the controller as new rogues are discovered.

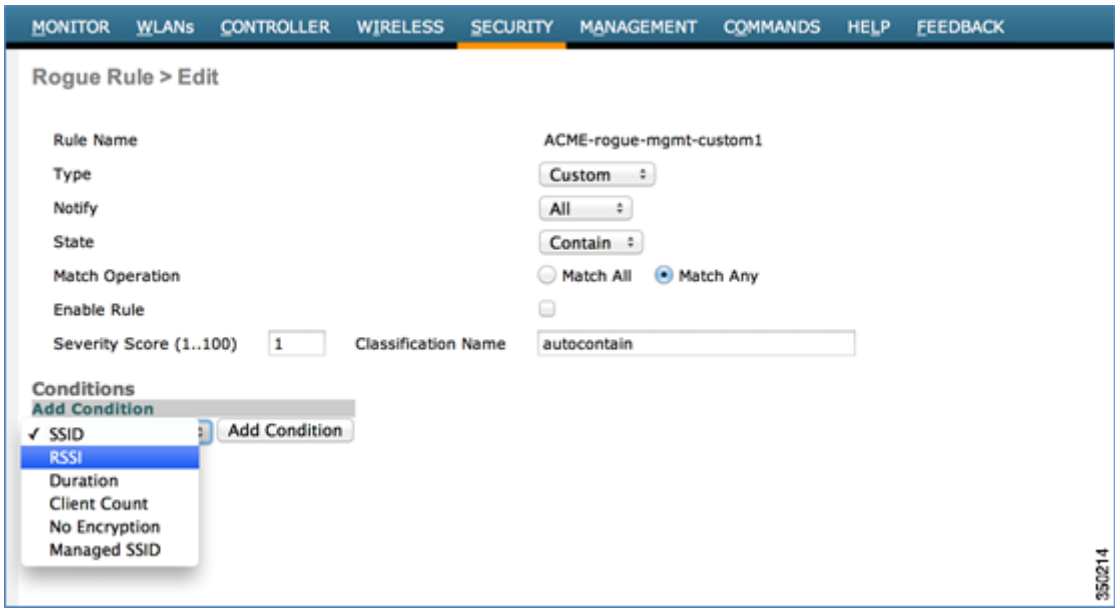
This Rogue Rule is also applied on Ad-hoc Rogue devices.

Malicious and Custom type Rogue classification can have containment option.

Rule Type	Notify/Action	Custom Severity
Friendly	• Alert • Internal • External	No
Malicious	• Alert • Contain	No
Custom	• Alert • Contain	Yes (Scale from 1 to 100)

Procedure to add custom rule with containment action:

Step 1 Create Rogue Rule with Containment Action.



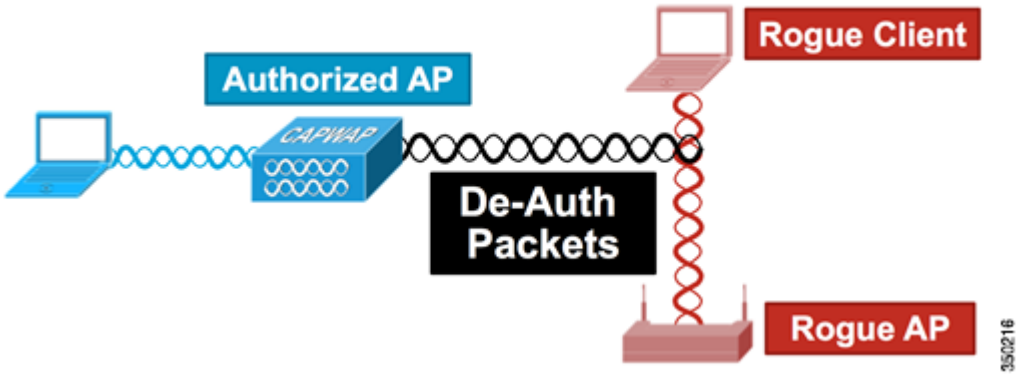
Step 2 Custom Rogue Filter Rule is created. If there is rogue device matched by this rogue rule, that rougue device will be auto-contained.

Read the document Rule Based Rogue Classification in Wireless LAN Controllers (WLC) and Wireless Control System (WCS) for more information on rogue rules in the WLCs.

Rogue Mitigation

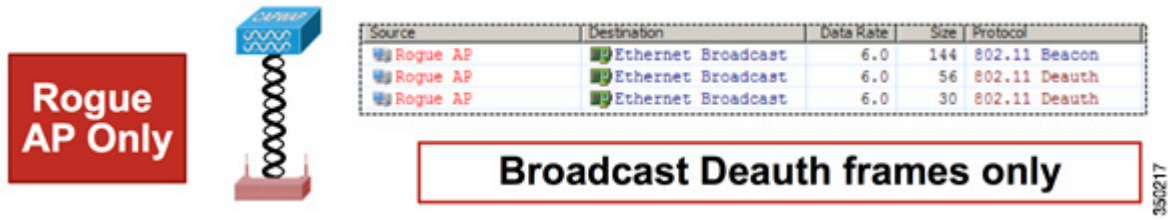
Rogue Containment

Containment is a method of using over-the-air packets to temporarily interrupt service on a rogue device until it can physically be removed. Containment works by spoofing de-authentication packets with the spoofed source address of the rogue AP so that any clients associated are kicked off.

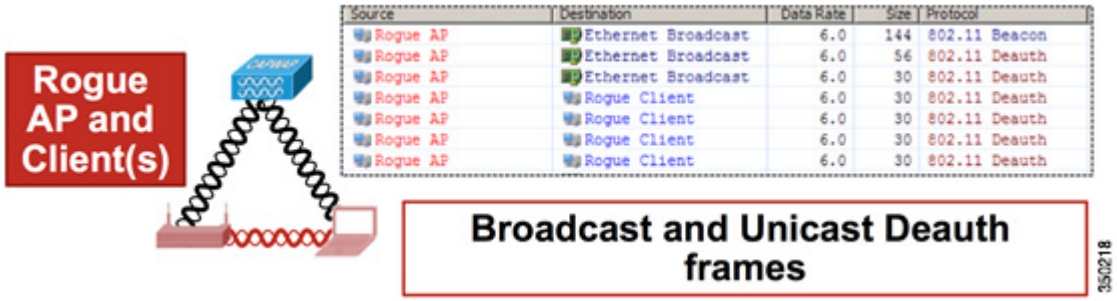


Rogue Containment Details

A containment initiated on a rogue AP with no clients will only use de-authentication frames sent to the broadcast address:

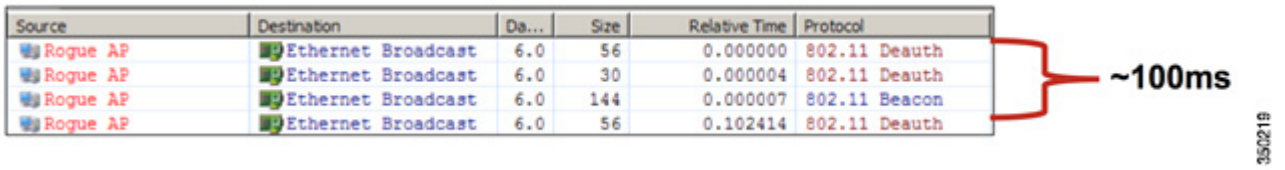


A containment initiated on a rogue AP with client(s) will use de-authentication frames sent to the broadcast address and to the client(s) address:



Containment packets are sent at the power level of the managed AP and at the lowest enabled data rate.

Containment sends a minimum of 2 packets every 100ms in Monitor mode AP:



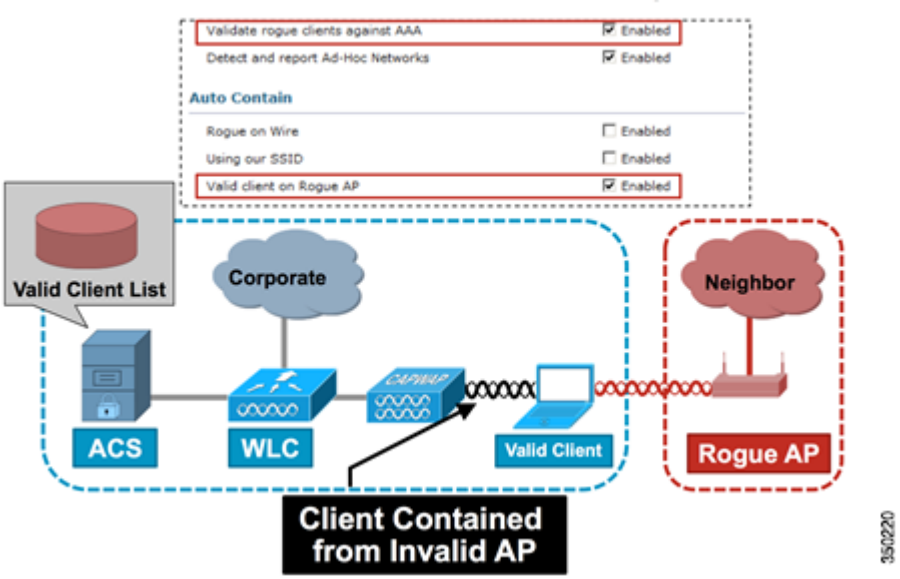
Note From 6.0 release, a containment performed by non-monitor mode APs is sent at an interval of 500ms instead of the 100ms interval used by monitor mode APs. Also, starting from 7.0.116, Monitor mode AP's containment traffic is only using unicast de-auth., and doesn't use broadcast de-auth. basis containment anymore. Local mode and ELM mode's APs are still using mixture of broadcast and unicast de-auth. packet.

- An individual rogue device can be contained by 1 to 4 managed APs which work in conjunction to mitigate the threat temporarily.
- Containment can be performed using local mode, ELM mode, monitor mode and FLEXCONNECT (Connected) mode APs. For local (and ELM) mode of FLEXCONNECT APs, a maximum of three rogue devices per radio can be contained. For monitor mode APs, a maximum of six rogue devices per radio can be contained.

Auto-Containment

In addition to manually initiating containment on a rogue device via PI or the WLC GUI, there is also the ability to automatically launch containment under certain scenarios. This configuration is found under General in the Rogue Policies section of the PI or controller interface. Each of these feature is disabled by default and should only be enabled to nullify the most damaging threats.

- Rogue on Wire – If a rogue device is identified to be attached to the wired network, then it is automatically placed under containment.
- Using our SSID – If a rogue device is using an SSID which is the same as that configured on the controller, it is automatically contained. This feature aims to address a honey-pot attack before it causes damage.
- Valid client on Rogue AP – If a client listed in AAA is found to be associated with a rogue device, containment is launched against that client only, preventing it from associating to any non-managed AP.



- AdHoc Rogue AP – If an ad-hoc network is discovered, it is automatically contained.

Rogue Containment Caveats

- Because containment uses a portion of the managed AP's radio time to send the de-authentication frames, the performance to both data and voice clients is negatively impacted by up to 20%. For data clients, the impact is reduced throughput. For voice clients, containment can cause interruptions in conversations and reduced voice quality. To avoid impact of data throughput and network service, administrator can limit Auto containment action only for Monitor mode APs.
- Containment can have legal implications when launched against neighboring networks. Ensure that the rogue device is within your network and poses a security risk before you launch the containment.

Switch Port Shutting

Once a switch port is traced using SPT, there is an option to disable that port in PI. Administrator has to do this exercise manually or automatically. An option is available to enable the switch port through PI if rogue is physically removed from the network.

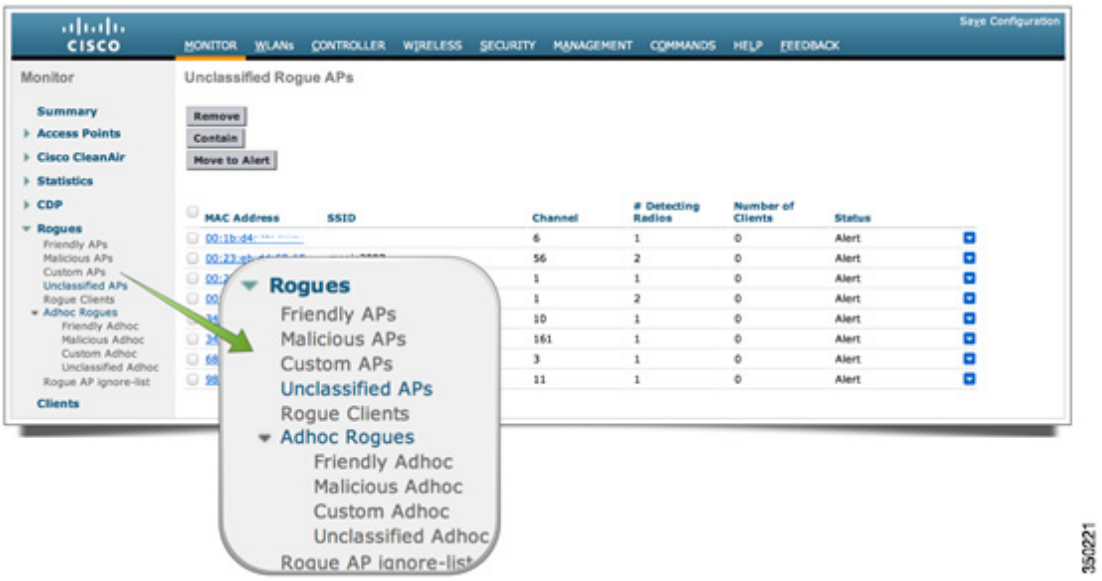
Configure Rogue Management

Configure Rogue Detection

Rogue detection is enabled in the controller by default and turn on/off per individual AP basis.

To find rogue details in a controller using the graphical interface:

Step 1 Go to **Monitor > Rogues**.



In this page, different classification for rogues are available:

- Friendly APs – APs which are marked as friendly by administrator. Friendly AP can be classified by manual entry input or by creating Rogue rule that automatically classify as Friendly APs.
- Malicious APs – APs which are identified as malicious using RLDP or Rogue detector AP or classified as Malicious AP Rogue rule.
- Custom APs – APs which are identified as custom using Custom Rogue Rule.
- Unclassified APs – By default rogue APs will be shown as unclassified list in controller.
- Rogue Clients – Clients connected to Rogue APs.
- Adhoc Rogues – Adhoc rogue clients. This Adhoc Rogue list also can be classified by Rogue Filter rule and categorized to Friendly, Malicious, Custom and Unclassified adhoc.
- Rogue AP ignore list – APs listed through PI.

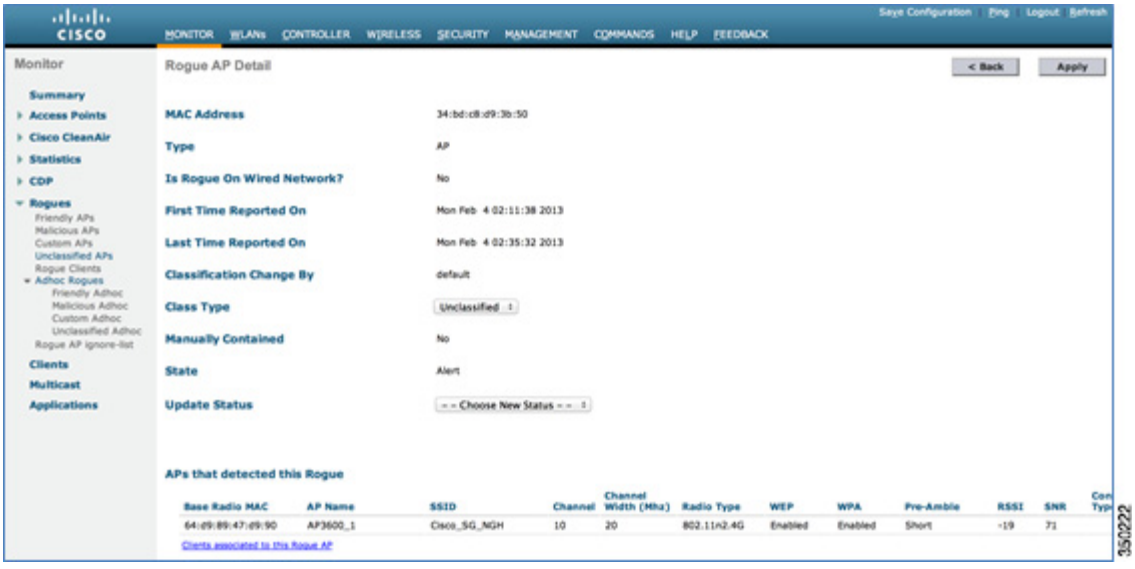
Note If WLC and autonomous AP is managed by the same PI, WLC will be automatically listing this autonomous AP in Rogue AP ignore list. There is no additional configuration required in WLC to enable this feature.

Step 2 From the CLI:

```
(Cisco Controller) >show rogue ap summary

Rogue on wire Auto-Contain....................... Disabled
Rogue using our SSID Auto-Contain................ Disabled
Valid client on rogue AP Auto-Contain............ Disabled
Rogue AP timeout................................. 1200
Rogue Detection Report Interval.................. 10
Rogue Detection Min Rssi......................... -128
Rogue Detection Transient Interval............... 0
Rogue Detection Client Num Threshold............. 0
Total Rogues(AP+Ad-hoc) supported................ 2000
Total Rogues classified.......................... 14
MAC Address        Classification     # APs # Clients Last Heard
-----------------  -----------------  ----- --------- -----------------------
00:01:36:42:46:57  Unclassified       1     0         Mon Feb  4 02:29:33 2013
00:1b:d4:2c:20:c0  Unclassified       1     0         Mon Feb  4 02:35:32 2013
00:23:eb:dd:68:10  Unclassified       2     0         Mon Feb  4 02:35:32 2013
00:23:eb:dd:68:11  Unclassified       1     0         Mon Feb  4 02:29:33 2013
00:23:eb:dd:68:12  Unclassified       1     0         Mon Feb  4 02:35:32 2013
00:23:eb:dd:68:1d  Unclassified       1     0         Mon Feb  4 02:30:43 2013
00:23:eb:dd:68:1e  Unclassified       1     1         Mon Feb  4 02:24:44 2013
00:23:eb:dd:68:1f  Unclassified       2     0         Mon Feb  4 02:33:42 2013
```

Step 3 Click a particular rogue entry in order to get the details of that rogue.



Step 4 From the CLI:

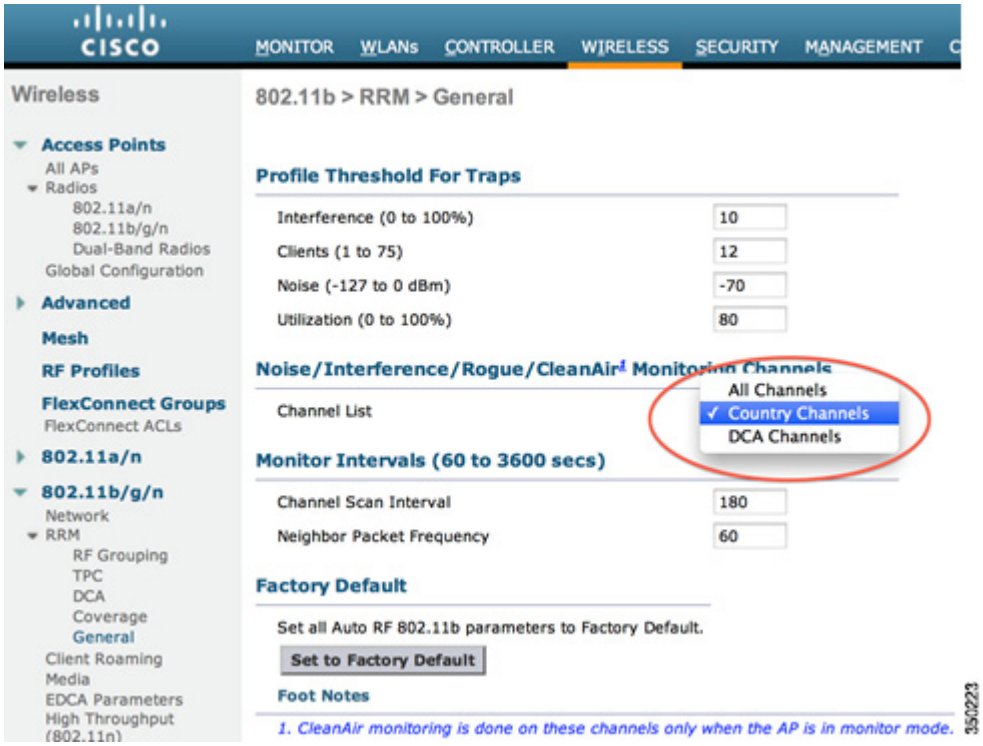
```
(Cisco Controller) >show rogue ap detailed 68:bc:0c:93:f4:70
Rogue BSSID..................................... 68:bc:0c:93:f4:70
Is Rogue on Wired Network....................... No
Classification.................................. Unclassified
Manual Contained................................ No
State........................................... Alert
First Time Rogue was Reported................... Mon Feb  4 02:24:44 2013
Last Time Rogue was Reported.................... Mon Feb  4 02:33:42 2013
Reported By
    AP 1
        MAC Address............................. 64:d9:89:47:d9:90
        Name.................................... AP3600_1
        Radio Type.............................. 802.11n5G
        SSID.................................... msnjs2012
        Channel................................. 165
        RSSI.................................... -41 dBm
        SNR..................................... 51 dB
        Encryption.............................. Enabled
        ShortPreamble........................... Not Supported
        WPA Support............................. Enabled
        Last reported by this AP................ Mon Feb  4 02:33:42 2013
```

Configure Channel Scanning for Rogue Detection

For a local/FlexConnect mode/Monitor mode AP there is an option under RRM configuration which allows the user to choose which channel is scanned for rogues. Depending on the config, the AP scans all channel/country channel/DCA channel for rogues.

To configure this from the GUI:

Step 1 Go to **Wireless > 802.11a/n or 802.11b/g/n > RRM > General**



Step 2 From the CLI:

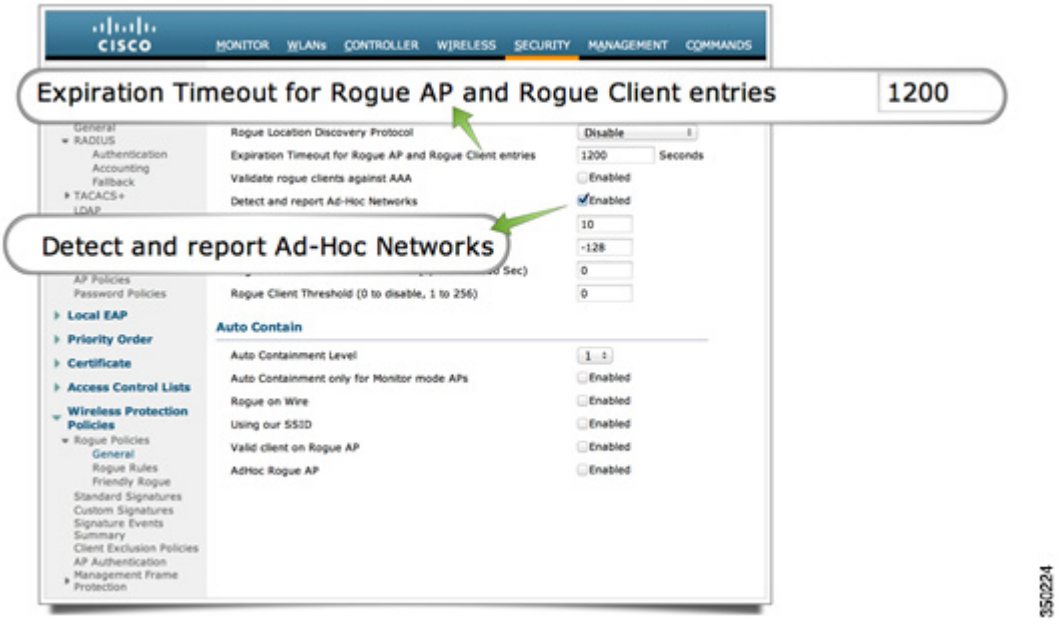
```
(Cisco Controller) >config  advanced 802.11a monitor channel-list ?

all             Monitor all channels
country         Monitor channels used in configured country code
dca             Monitor channels used by automatic channel assignment
```

a. To configure these options, go to **Security > Wireless Protection Policies > Rogue Policies > General**.

b. Change the timeout for rogue APs.

c. Enable the detection of ad-hoc rogue networks.



Step 3 From the CLI:

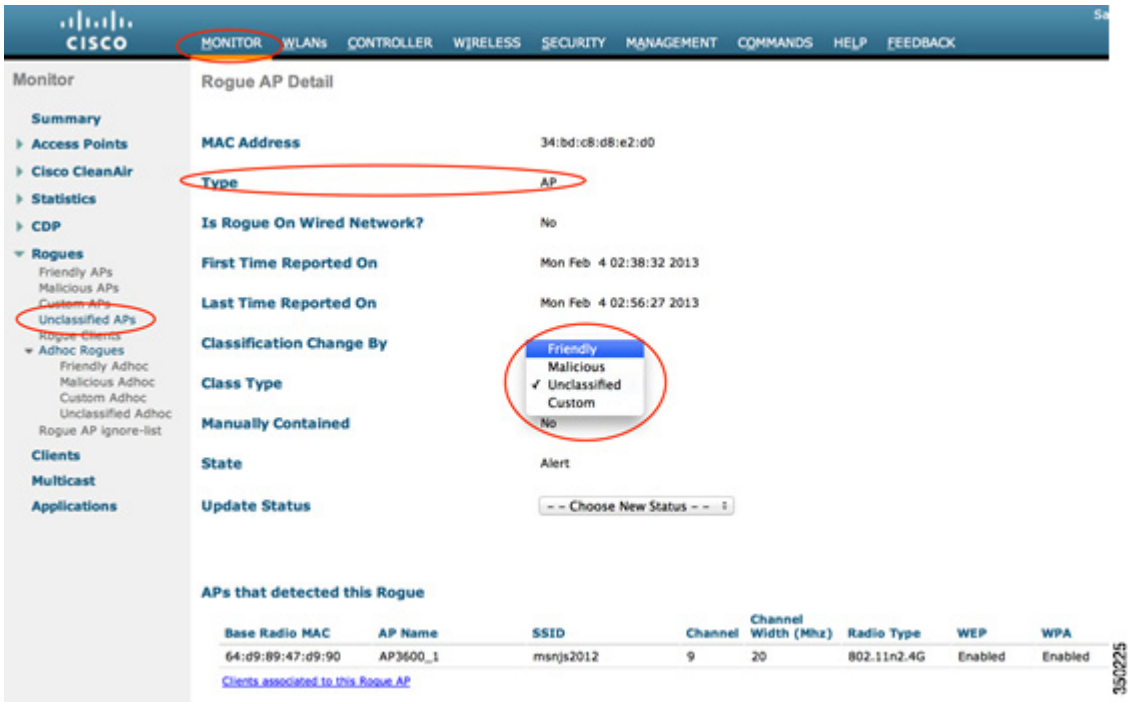
```
(Cisco Controller) >config rogue ap timeout ?
<seconds>      The number of seconds<240 - 3600> before rogue entries are flushed
(Cisco Controller) >config rogue adhoc enable/disable
```

Configure Rogue Classification

Manually Classify a Rogue AP

To classify a rogue AP as friendly, malicious, or unclassified:

Step 1 Go to **Monitor > Rogue > Unclassified APs**, and click the particular rogue AP name. Choose the option from the drop-down list.

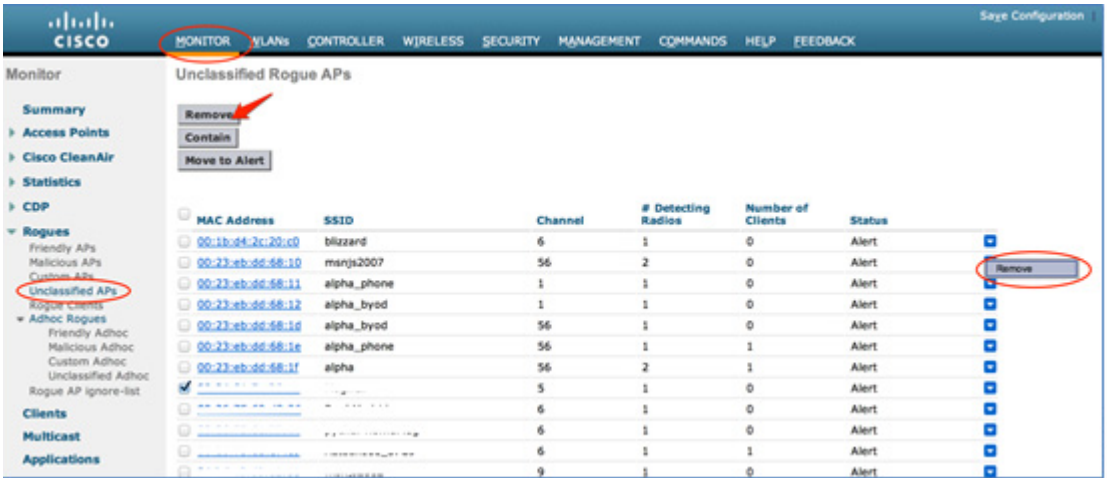


Step 2 From the CLI:

```
(Cisco Controller) >config rogue ap ?
classify        Configures rogue access points classification.
delete          Delete rogue ap
friendly        Configures friendly AP devices.
rldp            Configures Rogue Location Discovery Protocol.
ssid            Configures policy for rogue APs advertising our SSID.
timeout         Configures the expiration time for rogue entries, in seconds.
valid-client    Configures policy for valid clients using rogue APs.
```

To remove a rogue entry manually from the GUI:

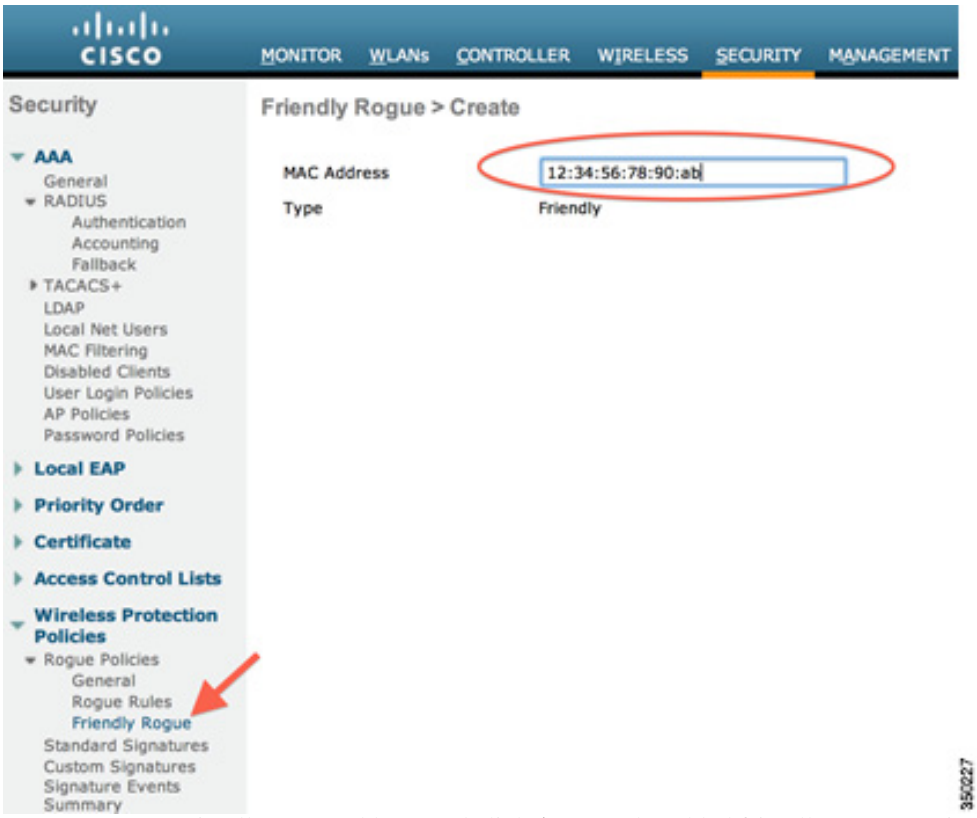
Step 1 Go to **Monitor > Rogue > Unclassified APs,** and click **Remove**.



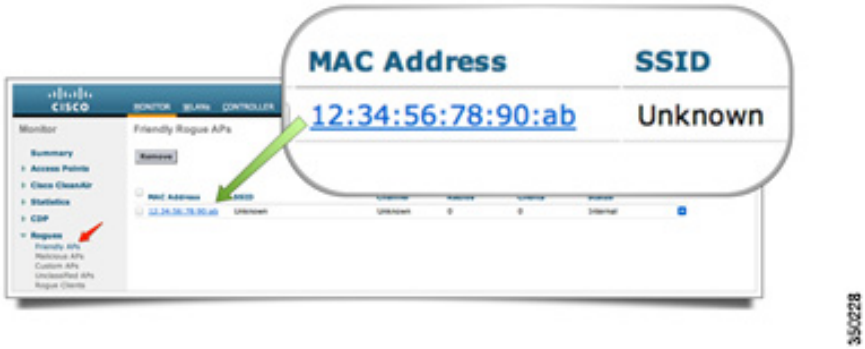
Note Another way to remove rogue AP from the list is using action button on top of the list. Network Administrator can select multiple rogues and execute **Remove** or **Contain** or **Move to Alert** action.

To configure a Rogue AP as a friendly AP:

Step 1 Go to **Security > Wireless Protection Policies > Rogue Policies > Friendly Rogues** and add the rogue MAC address.



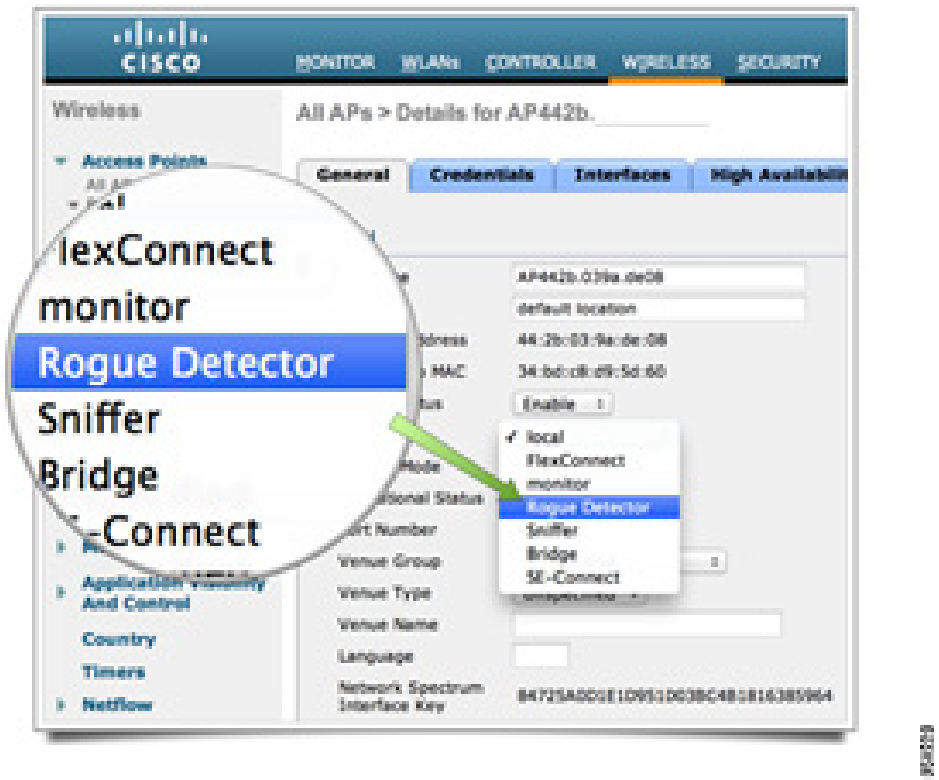
Step 2 Once you enter Friendly MAC address and click **Apply**. The added friendly rogue entries can be verified from **Monitor > Rogues > Friendly Rogue** page.



Configure a Rogue Detector AP

To configure the AP as a rogue detector using the GUI:

Step 1 Go to **Wireless > All APs**. Choose the AP name and change the AP mode.



Step 2 From the CLI:

```
(Cisco Controller) >config ap mode rogue AP_Managed

Changing the AP's mode will cause the AP to reboot.
Are you sure you want to continue? (y/n) y
```

Configure Switchport for a Rogue Detector AP

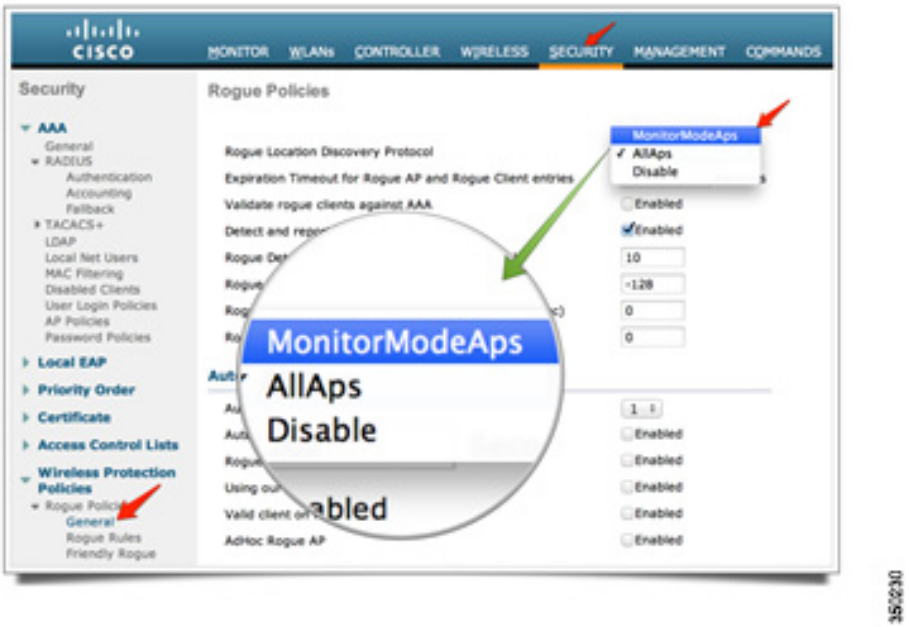
```
interface GigabitEthernet1/0/5
description Rogue Detector
switchport trunk encapsulation dot1q
switchport trunk native vlan 113
switchport mode trunk
spanning-tree portfast trunk
```

Note The native VLAN in this configuration is one that has IP connectivity to the WLC. Rogue AP can be on any (on or off of WLC's VLAN) wired VLAN on that switch, VLAN should be allowed on Trunk where Rogue detector is connected to that switch. Rogue Detector's AP port doesn't need any configuration to allow VLANs on AP itself.

Configure RLDP

To configure RLDP in the controller's GUI:

Step 1 Go to **Security > Wireless Protection Policies > Rogue Policies > General**.



- MonitorModeAps – Allows only APs in monitor mode to participate in RLDP.
- All APs – Local/FlexConnect/Monitor mode APs participate in the RLDP process.
- Disabled – RLDP is not triggered automatically. However, the user can trigger RLDP manually for a particular MAC address through the CLI.

Note Monitor mode AP will get preference over local/FlexConnect AP for performing RLDP if both of them are detecting a particular rogue above -85dbm RSSI.

Step 2 From the CLI:

```
(Cisco Controller) >config rogue ap rldp enable ?

alarm-only      Enables RLDP and alarm if rogue is detected
auto-contain    Enables RLDP, alarm and auto-contain if rogue is detected.

(Cisco Controller) >config rogue ap rldp enable alarm-only ?

monitor-ap-only Perform RLDP only on monitor AP
```

Note RLDP scheduling and triggering manually is configurable only through Command prompt.

To Initiate RLDP manually:

```
(Cisco Controller) >config rogue ap rldp initiate ?
<MAC addr>     Enter the MAC address of the rogue AP (e.g. 01:01:01:01:01:01).
For Scheduling RLDP
```

Note RLDP scheduling and option to configure RLDP retries are two options introduced in 7.0 through CLI.

Step 3 RLDP Scheduling :

```
(Cisco Controller) >config rogue ap rldp schedule ?

add            Enter the days when RLDP scheduling to be done.
delete         Enter the days when RLDP scheduling needs to be deleted.
enable         Configure to enable RLDP scheduling.
disable        Configure to disable RLDP scheduling.

(Cisco Controller) >config rogue ap rldp schedule add ?

mon            Configure Monday for RLDP scheduling.
tue            Configure Tuesday for RLDP scheduling.
wed            Configure Wednesday for RLDP scheduling.
thu            Configure Thursday for RLDP scheduling.
fri            Configure Friday for RLDP scheduling.
sat            Configure Saturday for RLDP scheduling.
sun            Configure Sunday for RLDP scheduling.
```

Step 4 RLDP retries can be configured using the command:

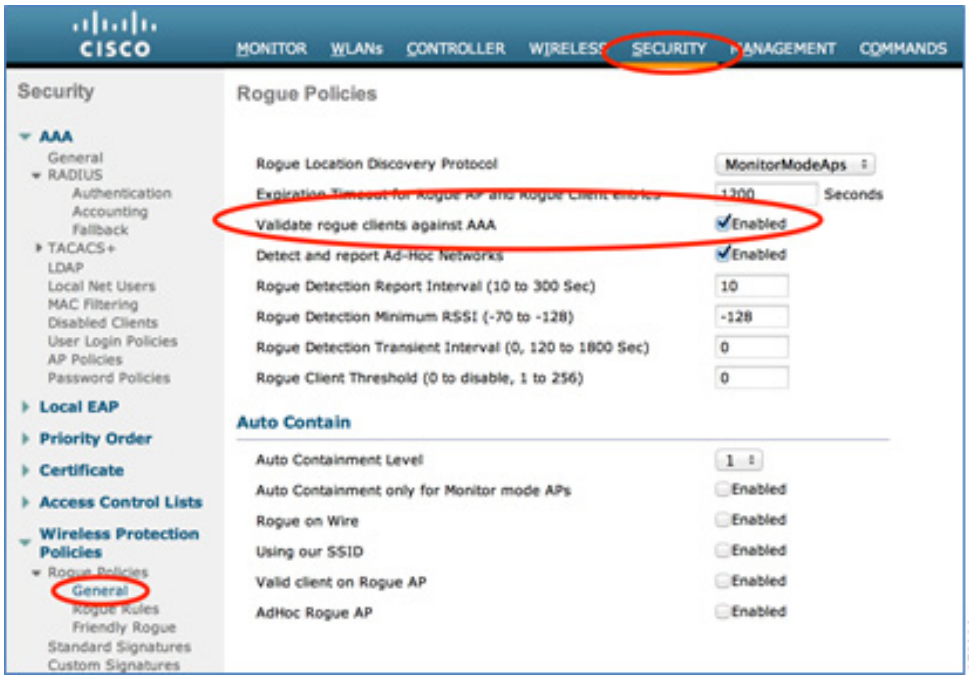
```
(Cisco Controller) >config rogue ap rldp retries ?

<count>        Enter the no.of times(1 - 5) RLDP to be tried per Rogue AP.
```

To configure AAA validation for rogue clients:

Step 1 Go to **Security > Wireless Protection Policies > Rogue Policies > General.**

Enabling this option makes sure the rogue client/AP address is verified with the AAA server before classifying it as malicious.

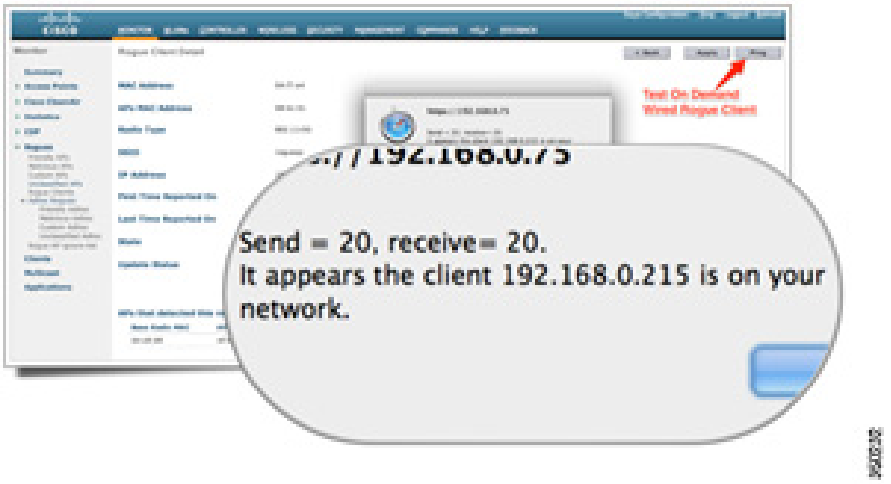


Step 2 From the CLI:

```
(Cisco Controller) >config rogue client aaa ?

disable         Disables use of AAA/local database to detect valid mac addresses.
enable          Enables use of AAA/local database to detect valid mac addresses.
```

Step 3 To validate if particular rogue client is a wired rogue, there is an option to check the reachability of that particular rogue from the controller (if the controller is able to detect the rogue client IP address). This option can be accessed in the rogue client's detail page and is available only through the graphical interface.



Note To configure switch port tracing, refer to the document Rogue Management White Paper (registered customers only) .

Configure Rogue Mitigation

Configure Manual Containment

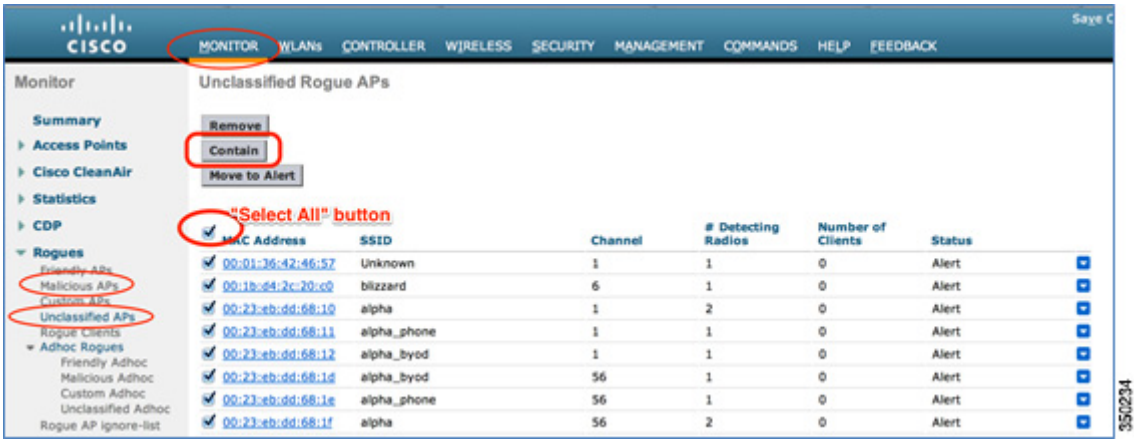
To contain a rogue device manually:

Step 1 Go to **Monitor > Rogues** and select Rogue device type. Malicious or Custom or Unclassified for Rogue AP or Rogue client and Adhoc rogue can be manually containable.

Step 2 When you select Contain Action from Update Status menu item, WLC will ask you to decide Maximum Number of AP that will participate containment action.

Multiple Rogue Containment

Using WLC GUI, Network Administration can launch Multiple Containment in a single click on Malicious APs and Unclassified APs.



This function allows containment and de-containment action in a single click, before 7.4, Administrator had to navigate through multiple screens and go through multiple steps of process to contain single Rogue Devices. Starting from 7.4, not only can Rogue device be automatically classified and containment by custom policy, but rougue devices can also be containment manually in a much enhanced way. Multiple rogue devices that breached wireless security policy can be classified first as Malicious rogue and later, contained manually in bulk.

From the CLI:

From the CLI, manual rogue containment is still be done in single rogue entry basis.

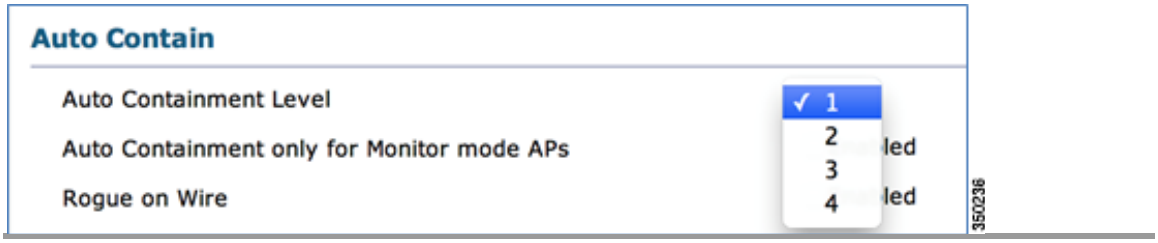
```
(Cisco Controller) >config rogue client ?

aaa             Configures to validate if a rogue client is a valid client using AAA/local
database.
alert            Configure the rogue client to the alarm state.
contain          Start containing a rogue client.
delete           Delete rogue Client

(Cisco Controller) >config rogue client contain 01:22:33:44:55:66 ?
<num of APs>   Enter the maximum number of Cisco APs to actively contain the rogue client
[1-4].
```

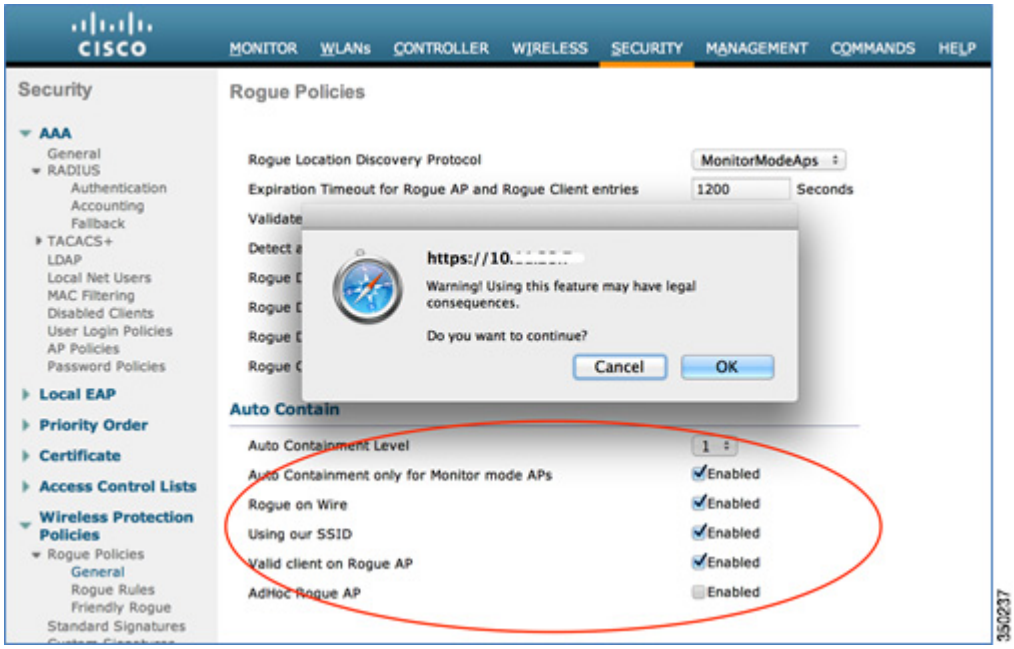
Note A particular rogue can be contained using 1-4 APs. By default, the controller uses one AP for containing a client. If two APs are able to detect a particular rogue, the AP with the highest RSSI contains the client regardless of the AP mode. Administrator can select number of AP that participate auto containment job.

```
(Cisco Controller) >config rogue auto-contain level ?
 <level>         Configures rogue auto-containment level <1 to 4>.
```



To configure auto containment:

Step 1 Go to **Security > Wireless Protection Policies > Rogue Policies > General**, and enable all applicable options for your network.



Step 2 From the CLI:

```
(Cisco Controller) >config rogue adhoc ?

alert          Stop Auto-Containment, generate a trap upon detection of the adhoc rogue.
auto-contain   Automatically containing adhoc rogue.
contain        Start containing adhoc rogue.
disable        Disable detection and reporting of Ad-Hoc rogues.
enable         Enable detection and reporting of Ad-Hoc rogues.
external       Acknowledge presence of a adhoc rogue.

(Cisco Controller) >config rogue adhoc auto-contain ?
(Cisco Controller) >config rogue adhoc auto-contain
 Warning! Using this feature may have legal consequences
         Do you want to continue(y/n) :y
```

Troubleshoot

If the rogue is not detected:

Verify that rogue detection is enabled on the AP using the following command. By default, rogue detection is enabled on the AP.

```
(Cisco Controller) >show ap config general Managed_AP

Cisco AP Identifier.............................. 0
```

```
Cisco AP Name..................................... Managed_AP
Country code...................................... Multiple Countries:SG,US
Regulatory Domain allowed by Country.............. 802.11bg:-AE    802.11a:-AS
AP Country code................................... SG  - Singapore
AP Regulatory Domain.............................. 802.11bg:-E    802.11a:-E
Switch Port Number ............................... 13
MAC Address....................................... 70:ca:9b:86:36:8b
IP Address Configuration.......................... Static IP assigned
IP Address........................................ 10.11.23.13
IP NetMask........................................ 255.255.255.0
Gateway IP Addr................................... 10.11.23.30
Fallback IP Address being used.................... 10.11.23.16
Domain.....................................
Name Server....................................
NAT External IP Address........................... None
CAPWAP Path MTU................................... 1485
Telnet State...................................... Disabled
Ssh State......................................... Disabled
Cisco AP Location................................. default location
Cisco AP Floor Label.............................. 0
Cisco AP Group Name............................... default-group
Primary Cisco Switch Name......................... MS2504_74
Primary Cisco Switch IP Address................... 10.11.23.7
Secondary Cisco Switch Name.....................
Secondary Cisco Switch IP Address................. Not Configured
Tertiary Cisco Switch Name.....................
Tertiary Cisco Switch IP Address.................. Not Configured
Administrative State ............................. ADMIN_ENABLED
Operation State .................................. REGISTERED
Mirroring Mode ................................... Disabled
AP Mode .......................................... Local
Public Safety .................................... Disabled
AP SubMode ....................................... Not Configured
Remote AP Debug .................................. Disabled
Logging trap severity level ...................... informational
Logging syslog facility .......................... kern
S/W  Version ..................................... 7.4.100.0
Boot  Version .................................... 12.4.23.0
Mini IOS Version ................................. 0.0.0.0
Stats Reporting Period ........................... 180
Stats Collection Mode ............................ normal
LED State......................................... Enabled
PoE Pre-Standard Switch........................... Disabled
PoE Power Injector MAC Addr....................... Disabled
Power Type/Mode................................... Power injector / Normal mode
Number Of Slots................................... 3
```

```
AP Model..................................... AIR-CAP3602I-S-K9
AP Image..................................... C3600-K9W8-M
IOS Version.................................. 15.2(20130107:162741)$
Reset Button................................. Enabled
AP Serial Number............................. FGL1552P0AY
AP Certificate Type.......................... Manufacture Installed
AP User Mode................................. AUTOMATIC
AP User Name................................. Not Configured
AP Dot1x User Mode........................... Not Configured
AP Dot1x User Name........................... Not Configured
Cisco AP system logging host................. 255.255.255.255
AP Up Time................................... 0 days, 03 h 39 m 44 s
AP LWAPP Up Time............................. 0 days, 01 h 33 m 22 s
Join Date and Time........................... Mon Feb  4 02:05:42 2013

Join Taken Time.............................. 0 days, 02 h 06 m 21 s
GPS Present.................................. NO
Ethernet Vlan Tag............................ Disabled
Ethernet Port Duplex......................... Auto
Ethernet Port Speed.......................... Auto
AP Link Latency.............................. Disabled
Rogue Detection.............................. Enabled
AP TCP MSS Adjust............................ Disabled
Hotspot Venue Group.......................... Residential
Hotspot Venue Type........................... Hotel or Motel
Venue Name in 'eng' language................. 'Hotel Lux'
      DNS server IP ......................... Not Available
```

Rogue detection can be enabled on an AP using the following command:

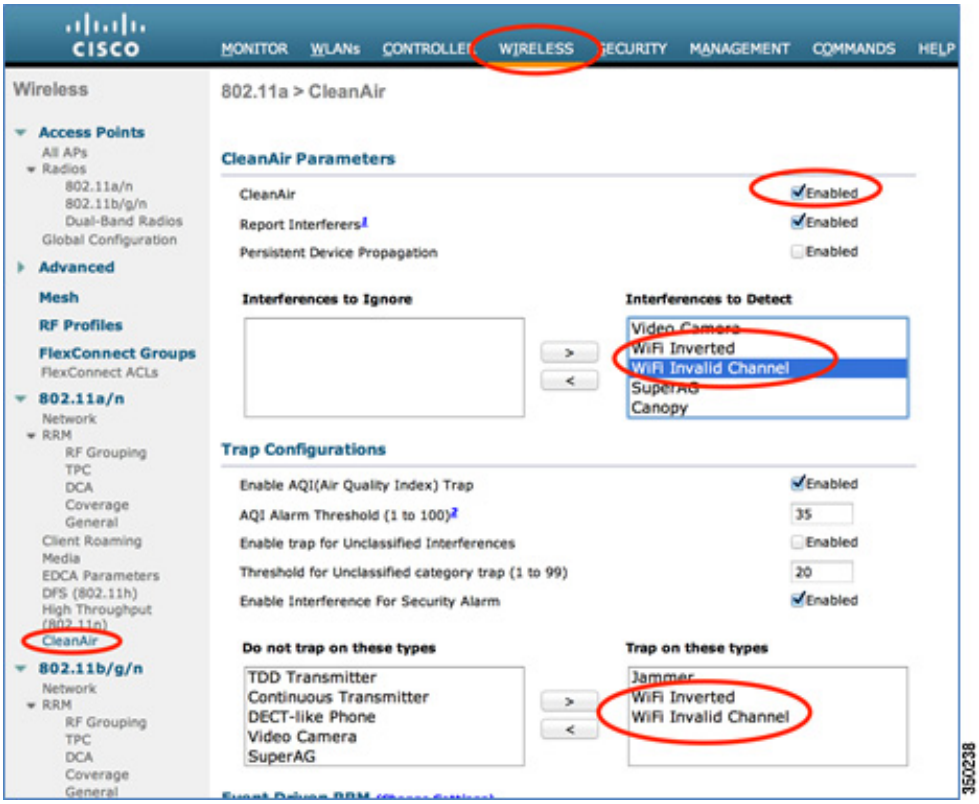
```
(Cisco Controller) >config rogue detection enable ?
all                    Applies the configuration to all connected APs.
<Cisco AP>     Enter the name of the Cisco AP.
```

- A local mode AP scans only country channels/DCA channels depending on the configuration. If the rogue is in any other channel, the controller will not be able to identify the rogue if you do not have monitor mode APs in the network. Issue this command in order to verify:

```
(Cisco Controller) >show advanced 802.11a monitor
Default 802.11a AP monitoring
  802.11a Monitor Mode......................... enable
  802.11a Monitor Mode for Mesh AP Backhaul..... disable
  802.11a Monitor Channels..................... Country channels
  802.11a RRM Neighbor Discover Type........... Transparent
  802.11a AP Coverage Interval................. 180 seconds
  802.11a AP Load Interval..................... 60 seconds
  802.11a AP Noise Interval.................... 180 seconds
  802.11a AP Signal Strength Interval.......... 60 seconds
  802.11a AP Neighbor Report Interval.......... 180 seconds
```

```
802.11a AP Interference Report Interval..... 120 seconds
```

- Rogue AP may not be broadcasting the SSID.
- Make sure the rogue AP's MAC address is not added in the friendly rogue list or white listed through PI.
- Beacons from the rogue AP may not be reachable to the AP detecting rogues. This can be verified by capturing the packet using a sniffer close to the AP-detecting rogue.
- A local mode AP may take up to 9 minutes to detect a rogue (3 cycles 180x3).
- Cisco APs are not able to detect rogues on frequencies like the public safety channel (4.9 Ghz).
- Cisco APs are not able to detect rogues working on FHSS (Frequency Hopping Spread Spectrum).
- In Cisco AP that support CleanAir (AP3600,3500,2600) can support detection of additional types of Rogue AP, such as WiFi Inverted and WiFi Invalid Channel.



- These two additional types of Rogue AP can be detected and alerted.

Useful debug commands from the WLC

```
debug client < mac> (If rogue mac is known)
debug dot11 rogue enable

(Cisco_Controller) >*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12
Looking for Rogue 00:27:0d:8d:14:12 in known AP table
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Rogue AP 00:27:0d:8d:14:12
is not found either in AP list or neighbor, known or Mobility group AP lists
```

```
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Change state from 0 to 1
for rogue AP 00:27:0d:8d:14:12
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 rg change state Rogue AP:
00:27:0d:8d:14:12
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 New RSSI report from AP
00:1b:0d:d4:54:20  rssi -74, snr -9 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg send new rssi -74
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Updated AP report
00:1b:0d:d4:54:20  rssi -74, snr -9
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Manual Contained Flag = 0
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg new Rogue AP:
00:27:0d:8d:14:12
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Found Rogue AP:
00:24:97:2d:bf:90 on slot 0
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Added Rogue AP:
00:24:97:2d:bf:90
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Looking for Rogue
00:24:97:2d:bf:90 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Rogue AP 00:24:97:2d:bf:90
is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Change state from 0 to 1
for rogue AP 00:24:97:2d:bf:90
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg change state Rogue AP:
00:24:97:2d:bf:90
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 New RSSI report from AP
00:1b:0d:d4:54:20  rssi -56, snr 34 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg send new rssi -56
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Updated AP report
00:1b:0d:d4:54:20  rssi -56, snr 34
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Manual Contained Flag = 0
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg new Rogue AP:
00:24:97:2d:bf:90
*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Found Rogue AP:
9c:af:ca:0f:bd:40 on slot 0
*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Added Rogue AP:
9c:af:ca:0f:bd:40
*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Looking for Rogue
9c:af:ca:0f:bd:40 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Rogue AP 9c:af:ca:0f:bd:40
is not found eithe*apfRogueTask: Jun 15 01:45:09.011: 00:25:45:a2:e1:62
Updated AP report 00:1b:0d:d4:54:20  rssi -73, snr 24
*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 Manual Contained Flag = 0
*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 rg new Rogue AP:
00:25:45:a2:e1:62
*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Found Rogue AP:
00:24:c4:ad:c0:40 on slot 0
```

```
*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Added Rogue AP:
00:24:c4:ad:c0:40
```

Expected Trap Logs

- Once a Rogue Is Detected

```
9Fri Jun 18 06:40:06 2010 Rogue AP : 00:1e:f7:74:f3:50 detected on Base Radio
MAC : 00:1d:71:22:f2:c0 Interface no:0(802.11b/g) with RSSI: -97 and SNR:
1 and Classification: unclassified

10Fri Jun 18 06:40:06 2010 Rogue AP : 00:22:0c:97:af:83 detected on Base Radio
MAC : 00:1d:71:22:f2:c0 Interface no:0(802.11b/g) with RSSI: -81 and SNR: 18
and Classification: unclassified

11Fri Jun 18 06:40:06 2010 Rogue AP : 00:26:cb:9f:8a:21 detected on Base Radio
MAC : 00:1d:71:22:f2:c0 Interface no:0(802.11b/g) with RSSI: -82 and SNR: 20
and Classification: unclassified

12Fri Jun 18 06:40:06 2010 Rogue AP : 00:26:cb:82:5d:c0 detected on Base Radio
MAC : 00:1d:71:22:f2:c0 Interface no:0(802.11b/g) with RSSI: -98 and SNR: -2
and Classification: unclassified
```

Once a Rogue Entry Is Removed from the Rogue List

```
50Fri Jun 18 06:36:06 2010 Rogue AP : 00:1c:57:42:53:40 removed from Base Radio
MAC : 00:1d:71:22:f2:c0 Interface no:0(802.11b/g)

51Fri Jun 18 06:36:06 2010 Rogue AP : 00:3a:98:5c:57:a0 removed from Base Radio
MAC : 00:1d:71:22:f2:c0 Interface no:0(802.11b/g)
```

Recommendations

- Configure the channel scanning to all channels if you suspect potential rogues in your network
- Depending on the layout of the wired network, the number and location of rogue detector APs can vary from one per floor to one per building. It is advisable to have at least one rogue detector AP in each floor of a building. Because a rogue detector AP requires a trunk to all layer 2 network broadcast domains that should be monitored, placement is dependent on the logical layout of the network.
- Wired MAC detection from Rogue Detector AP and Wireless MAC detection from other over the air scanning must be done in the same controller. If there are multiple controllers, mobility should be enabled between neighbor controllers to increase rogue on wire detection over multiple WLC.

If the Rogue Is Not Getting Classified

- Verify the rogue rules are configured properly.
- If the rogue is in the DFS channel, RLDP does not work.
- RLDP works only if the rogue's WLAN is open and DHCP is available.
- If the local mode AP is serving the client in the DFS channel, it will not participate in RLDP process.

Useful debugs

```
(Cisco Controller) > debug dot11 rogue rule enable
(Cisco Controller) > debug dot11 rldp enable

Received Request to detect rogue: 00:1A:1E:85:21:B0
00:1a:1e:85:21:b0 found closest monitor AP 00:17:df:a7:20:d0slot =1 channel = 44
Found RAD: 0x158f1ea0, slotId = 1
rldp started association, attempt 1
Successfully associated with rogue: 00:1A:1E:85:21:B0
```

!--- ASSOCIATING TO ROGUE AP

Starting dhcp

```
00:1a:1e:85:21:b0 RLDP DHCP SELECTING for rogue 00:1a:1e:85:21:b0
00:1a:1e:85:21:b0 Initializing RLDP DHCP for rogue 00:1a:1e:85:21:b0
.00:1a:1e:85:21:b0 RLDP DHCPSTATE_INIT for rogue 00:1a:1e:85:21:b0
00:1a:1e:85:21:b0 RLDP DHCPSTATE_REQUESTING sending for rogue 00:1a:1e:85:21:b0
00:1a:1e:85:21:b0 Sending DHCP packet through rogue AP 00:1a:1e:85:21:b0
00:1a:1e:85:21:b0 RLDP DHCP REQUEST RECV for rogue 00:1a:1e:85:21:b0
00:1a:1e:85:21:b0 RLDP DHCP REQUEST received for rogue 00:1a:1e:85:21:b0
00:1a:1e:85:21:b0 RLDP DHCP BOUND state for rogue 00:1a:1e:85:21:b0
Returning IP 172.20.226.246, netmask 255.255.255.192, gw 172.20.226.193
```

!--- GETTING IP FROM ROGUE

```
Found Gateway MacAddr: 00:1D:70:F0:D4:C1
Send ARLDP to 172.20.226.198 (00:1D:70:F0:D4:C1) (gateway)
Sending ARLDP packet to 00:1d:70:f0:d4:c1 from 00:17:df:a7:20:de
Send ARLDP to 172.20.226.197 (00:1F:9E:9B:29:80)
Sending ARLDP packet to 00:1f:9e:9b:29:80 from 00:17:df:a7:20:de
Send ARLDP to 0.0.0.0 (00:1D:70:F0:D4:C1) (gateway)
Sending ARLDP packet to 00:1d:70:f0:d4:c1 from 00:17:df:a7:20:de
```

!--- SENDING ARLDP PACKET

```
Received 32 byte ARLDP message from: 172.20.226.24642
Packet Dump:
sourceIp: 172.20.226.246
destIp: 172.20.226.197
Rogue Mac: 00:1A:1E:85:21:B0
```

!--- RECEIVING ARLDP PACKET

```
security: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Rogue Detection:

```
WLC>debug dot11 rogue enable
AP#show capwap ids rogue detection dot11Radio 0/d1
AP#show capwap rm rogue ap d0/d1
AP#debug capwap rm rogue detection address  <mac address of the rogue>
AP#debug capwap rm rogue detection all
```

Rogue Containment:

```
AP#show capwap ids rogue containment dot11Radio 0/1 chan
AP#debug capwap ids rogue containment address <mac add>
AP#debug capwap ids rogue containment
AP#show capwap ids rogue containment d0/d1 rad
```

Recommendations

- Initiate RLDP manually on suspicious rogue entries.
- Schedule RLDP periodically.
- If you have known rogue entries, add them in the friendly list or enable validation with AAA and make sure known client entries are there in the AAA database.
- RLDP can be deployed on local or monitor mode APs. For most scalable deployments, and to eliminate any impact on client service, RLDP should be deployed on monitor mode APs when possible. However, this recommendation requires that a monitor mode AP overlay be deployed with a typical ratio as 1 monitor mode AP for every 5 local mode APs. APs in Adaptive wIPS monitor mode can also be leveraged for this task.

Rogue Detector AP

- Rogue entry in a rogue detector can be seen using this command in the AP console. For wired rogues, the flag will be set.

```
Rogue_Detector_5500#show capwap rm rogue detector
CAPWAP Rogue Detector Mode
Current Rogue Table:
Rogue hindex = 0: MAC 0023.ebdc.1ac6, flag = 0, unusedCount = 1
Rogue hindex = 2: MAC 0023.04c9.72b9, flag = 1, unusedCount = 1
```

!--- once the flag is set, rogue is detected on wire

```
Rogue hindex = 2: MAC 0023.ebdc.1ac4, flag = 0, unusedCount = 1
Rogue hindex = 3: MAC 0026.cb4d.6e20, flag = 0, unusedCount = 1
Rogue hindex = 4: MAC 0026.cb9f.841f, flag = 0, unusedCount = 1
Rogue hindex = 4: MAC 0023.04c9.72bf, flag = 0, unusedCount = 1
Rogue hindex = 4: MAC 0023.ebdc.1ac2, flag = 0, unusedCount = 1
Rogue hindex = 4: MAC 001c.0f80.d450, flag = 0, unusedCount = 1
Rogue hindex = 6: MAC 0023.04c9.72bd, flag = 0, unusedCount = 1
```

Useful debug Commands in an AP Console

- Simulate Rogue Detector using below test command.
- Verify the existence of wireless Rogue MAC from Rogue Detector joined WLC - e804.620a.b66b Wired Rogue MAC address in test - e804.620a.b66c. Run the debug followed by the test command.

```
Rogue_Detector#debug capwap rm rogue detector


*Jun 18 08:37:59.747: ROGUE_DET: Received a rogue table update of length 170
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac4
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac5
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1aca
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acb
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acc
```

```
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acd
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acf
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0024.1431.e9ef
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0024.148a.ca2b
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2d
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2f
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3570
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3574
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357b
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357c
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357d
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357f
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3dcd
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff0
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff2
*Jun 18 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4aec
*Jun 18 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4b77
*Jun 18 08:37:59.774: ROGUE_DET: Flushing rogue entry 0040.96b9.4794
*Jun 18 08:37:59.774: ROGUE_DET: Flushing rogue entry 0022.0c97.af80
*Jun 18 08:37:59.775: ROGUE_DET: Flushing rogue entry 0024.9789.5710
*Jun 18 08:38:19.325: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 18 08:38:19.325: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
*Jun 18 08:39:19.323: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 18 08:39:19.324: ROGUE_DET: Got wired mac 001d.a1cc.0e9e

Rogue_Detector#test capwap ids rogue detection onwire e804.620a.b66c
capwap_rm_rogue_onwire_test MAC 0xE804620AB66C
AP1140_c47d.4f3b.2cfe# *Jun 18 08:38:11.709: ROGUE_DET: Got ARP src e804.620a.b66c
*Jun 18 08:38:11.709: ROGUE_DET: Got wired mac e804.620a.b66c
*Jun 18 08:38:11.709: ROGUE_DET: Found a match for rogue entry e804.620a.b66c
*Jun 18 08:38:11.709: ROGUE_DET: Sending notification to switch
*Jun 18 08:38:11.709: ROGUE_DET: Sent rogue e804.620a.b66c found on net msg
```

If Rogue Containment Does Not Occur:

The local/FlexConnect mode AP can contain 3 devices at a time per radio, and the monitor mode AP can contain 6 devices per radio. As a result, make sure the AP is already containing the maximum number of devices permitted. In this scenario, the client is in a containment pending state. Verify auto containment rules.

Expected Trap Logs:

```
Fri Jul 23 12:49:10 2010Rogue AP: Rogue with MAC Address: 00:17:0f:34:48:a1
has been contained manually by 2 APs 8
Fri Jul 23 12:49:10 2010 Rogue AP : 00:17:0f:34:48:a1 with Contained mode added
to the Classified AP List.
```

Conclusion

Rogue detection and containment within the Cisco Unified Wireless Solution is the most effective and least intrusive method in the industry. The flexibility provided to the Administrator allows for a more customized fit that can accommodate any network requirements.