Managing Rogue Devices

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Rogue Devices

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of Clear to Send (CTS) frames. This action mimics an access point, informing a particular client to transmit, and instructing all the other clients to wait, which results in legitimate clients being unable to access network resources. Wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Because rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad hoc wireless networks without their IT department's knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to

intercept network traffic and hijack client sessions. Even more alarming, wireless users frequently publish unsecured access point locations, increasing the odds of having enterprise security breached.

The following are some guidelines to manage rogue devices:

- The containment frames are sent immediately after the authorization and associations are detected. The enhanced containment algorithm provides more effective containment of ad hoc clients.

- The local mode access points are designed to serve associated clients. These access points spend relatively less time performing off-channel scanning: about 50 milliseconds on each channel. If you want to perform high rogue detection, a monitor mode access point must be used. Alternatively, you can reduce the scan intervals from 180 seconds to a lesser value, for example, 120 or 60 seconds, ensuring that the radio goes off-channel more frequently, which improves the chances of rogue detection. However, the access point will still spend about 50 milliseconds on each channel.

- Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

- Client card implementations might mitigate the effectiveness of ad hoc containment.

- It is possible to classify and report rogue access points through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states.

- Each controller limits the number of rogue containment to three per radio (or six per radio for access points in the monitor mode).

- Rogue Location Discovery Protocol (RLDP) detects rogue access points that are configured for open authentication.

- RLDP detects rogue access points that use a broadcast Basic Service Set Identifier (BSSID), that is, the access point broadcasts its Service Set Identifier in beacons.

- RLDP detects only those rogue access points that are on the same network. If an access list in the network prevents the sending of RLDP traffic from the rogue access point to the controller, RLDP does not work.

- RLDP does not work on 5-GHz dynamic frequency selection (DFS) channels. However, RLDP works when the managed access point is in the monitor mode on a DFS channel.

- If RLDP is enabled on mesh APs, and the APs perform RLDP tasks, the mesh APs are dissociated from the controller. The workaround is to disable RLDP on mesh APs.

- If RLDP is enabled on nonmonitor APs, client connectivity outages occur when RLDP is in process.

- If the rogue is manually contained, the rogue entry is retained even after the rogue expires.

- If the rogue is contained by any other means, such as auto, rule, and AwIPS preventions, the rogue entry is deleted when it expires.

- The controller will request to AAA server for rogue client validation only once. As a result, if rogue client validation fails on the first attempt then the rogue client will not be detected as a threat any more. To avoid this, add the valid client entries in the authentication server before enabling **Validate Rogue Clients Against AAA**.

- In the 7.4 and earlier releases, if a rogue that was already classified by a rule was not reclassified. In the 7.5 release, this behavior is enhanced to allow reclassification of rogues based on the priority of the rogue rule. The priority is determined by using the rogue report that is received by the controller.

- The rogue detector AP fails to co-relate and contain the wired rogue AP on a 5Mhz channel because the MAC address of the rogue AP for WLAN, LAN, 11a radio and 11bg radio are configured with a difference of +/-1 of the rogue BSSID. In the 8.0 release, this behavior is enhanced by increasing the range of MAC address, that the rogue detector AP co-relates the wired ARP MAC and rogue BSSID, by +/-3.
- The rogue access points with open authentication can be detected on wire. The NAT wired or rogue wired detection is not supported in by WLC (both RLDP and rogue detector AP). The non-adjacent MAC address is supported by rogue detector mode of AP and not by RLDP.

Note A rogue AP or client or adhoc containment configuration is not saved after the reload. You have to configure all the rogues again after the reload.

Note No separate command exists for controlling rogue client traps. However, you can enable or disable rogue client traps using the **config trapflags rogueap {enable | disable}** command, which is also used for rouge APs. In GUI configuration also, you should use the rogue AP flag under **Management->SNMP->TrapControl->Security->Rogue AP** to control rogue clients.

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol (RLDP) is an active approach, which is used when rogue AP has no authentication (Open Authentication) configured. This mode, which is disabled by default, instructs an active AP to move to the rogue channel and connect to the rogue as a client. During this time, the active AP sends de-authentication messages to all connected clients and then shuts down the radio interface. Then, it associates to the rogue AP as a client. The AP then tries to obtain an IP address from the rogue AP and forwards a User Datagram Protocol (UDP) packet (port 6352) that contains the local AP and rogue connection information to the controller through the rogue AP. If the controller receives this packet, the alarm is set to notify the network administrator that a rogue AP was discovered on the wired network with the RLDP feature.

RLDP has 100 % accuracy in rouge AP detection. It detects Open APs and NAT APs.

Note Use the **debug dot11 rldp enable** command in order to check if the Lightweight AP associates and receives a DHCP address from the rogue AP. This command also displays the UDP packet sent by the Lightweight AP to the controller.

A sample of a UDP (destination port 6352) packet sent by the Lightweight AP is shown here: 0020 0a 01 01 0d 0a 01 ....(.*...... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00 ......x......... 0040 00 00 00 00 00 00 00 00 00 00 00

The first 5 bytes of the data contain the DHCP address given to the local mode AP by the rogue AP. The next 5 bytes are the IP address of the controller, followed by 6 bytes that represent the rogue AP MAC address. Then, there are 18 bytes of zeroes.

Steps of how RLDP works are 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 are 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 negatively impacts 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.

Note RLDP is not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS). If the automatic RLDP attempt does not detect the rogue (due to a noisy RF environment, for example), the controller does not retry. However, you can initiate RLDP manually on a rogue device.

Detecting Rogue Devices

The controller continuously monitors all the nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) and the rogue detector mode access point is connected to determine if the rogue is attached to your network.

Controller initiates RLDP on rogue devices that have open authenticated and configured. If RLDP uses Flexconnect or local mode access points, then clients are disconnected for that moment. After the RLDP cycle, the clients are reconnected to the access points. As and when rogue access points are seen (auto-configuration), the RLDP process is initiated.

You can configure the controller to use RLDP on all the access points or only on the access points configured for the monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded radio frequency (RF) space, allowing monitoring without creating unnecessary interference and without affecting the regular data access point functionality. If you configure the controller to use RLDP on all the access points, the controller always chooses the monitor access point for RLDP operation if a monitor

access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to contain the detected rogue either manually or automatically.

RLDP detects on wire presence of the rogue access points that are configured with open authentication only once, which is the default retry configuration. Retries can be configured using the **config rogue ap rldp retries** command.

You can initiate or trigger RLDP from controller in three ways:

1. Enter the RLDP initiation command manually from the controller CLI. The equivalent GUI option for initiating RLDP is not supported.

    config rogue ap rldp initiate *mac-address*

2. Schedule RLDP from the controller CLI. The equivalent GUI option for scheduling RLDP is not supported.

    config rogue ap rldp schedule

3. Auto RLDP. You can configure auto RLDP on controller either from controller CLI or GUI but keep in mind the following guidelines:

    - The auto RLDP option can be configured only when the rogue detection security level is set to custom.
    - Either auto RLDP or schedule of RLDP can be enabled at a time.

A rogue access point is moved to a contained state either automatically or manually. The controller selects the best available access point for containment and pushes the information to the access point. The access point stores the list of containments per radio. For auto containment, you can configure the controller to use only the monitor mode access point. The containment operation occurs in the following two ways:

- The container access point goes through the list of containments periodically and sends unicast containment frames. For rogue access point containment, the frames are sent only if a rogue client is associated.

- Whenever a contained rogue activity is detected, containment frames are transmitted.

Individual rogue containment involves sending a sequence of unicast disassociation and deauthentication frames.

Cisco Prime Infrastructure Interaction and Rogue Detection

Cisco Prime Infrastructure supports rule-based classification and uses the classification rules configured on the controller. The controller sends traps to Cisco Prime Infrastructure after the following events:

- If an unknown access point moves to the Friendly state for the first time, the controller sends a trap to Cisco Prime Infrastructure only if the rogue state is Alert. It does not send a trap if the rogue state is Internal or External.

- If a rogue entry is removed after the timeout expires, the controller sends a trap to Cisco Prime Infrastructure for rogue access points categorized as Malicious (Alert, Threat) or Unclassified (Alert). The controller does not remove rogue entries with the following rogue states: Contained, Contained Pending, Internal, and External.

How to Configure Rogue Detection

Configuring Rogue Detection (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wireless wps rogue detection min-rssi** *rssi in dBm*
3. **wireless wps rogue detection min-transient-time** *time in seconds*
4. **wireless wps rogue client** {**aaa** | **mse**}
5. **wireless wps rogue ap valid-client auto-contain**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** Device# **configure terminal**	Enters global configuration mode.
Step 2	**wireless wps rogue detection min-rssi** *rssi in dBm* **Example:** Device(config)# **wireless wps rogue detection min-rssi 100**	Specify the minimum RSSI value that rogues should have for APs to detect and for rogue entry to be created in the device. Valid range for the rssi in dBm parameter is –128 dBm to -70 dBm, and the default value is -128 dBm. **Note** This feature is applicable to all the AP modes. There can be many rogues with very weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs should detect rogues.
Step 3	**wireless wps rogue detection min-transient-time** *time in seconds* **Example:** Device(config)# **wireless wps rogue detection min-transient-time**	Specify the time interval at which rogues have to be consistently scanned for by APs after the first time the rogues are scanned. Valid range for the time in sec parameter is 120 seconds to 1800 seconds, and the default value is 0.

	Command or Action	Purpose
		Note This feature is applicable to APs that are in monitor mode only.
		Using the transient interval values, you can control the time interval at which APs should scan for rogues. APs can also filter the rogues based on their transient interval values.
		This feature has the following advantages:
		• Rogue reports from APs to the controller are shorter
		• Transient rogue entries are avoided in the controller
		• Unnecessary memory allocation for transient rogues are avoided
Step 4	**wireless wps rogue client** {**aaa** | **mse**} **Example:** `Device(config)# wireless wps rogue client aaa` `Device(config)# wireless wps rogue client mse`	Set the AAA server or local database, or the MSE to validate if rogue clients are valid clients.
Step 5	**wireless wps rogue ap valid-client auto-contain** **Example:** `Device(config)# wireless wps rogue ap valid-client` `auto-contain`	Specify to automatically contain a rogue access point to which trusted clients are associated.
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Rogue Detection

This section describes the new command for rogue detection.

The following command can be used to monitor rogue detection on the .

Table 1: Monitoring Rogue Detection Command

Command	Purpose
show wireless wps rogue ap summary	Displays a list of all rogue access points detected by the .
show wireless wps rogue client detailed *client-mac*	Displays detailed information for a specific rogue client.

show wireless wps rogue client summary	Displays a list of all rogue clients detected by the .
show nmsp capability	Displays the NMSP capabilities.

Examples: Rogue Detection Configuration

This example shows how to configure the minimum RSSI that a detected rogue AP needs to be at, to have an entry created at the :

```
Device# configure terminal
Device(config)# wireless wps rogue detection min-rssi -100
Device(config)# end
Device# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

This example shows how to configure the classification interval:

```
Device# configure terminal
Device(config)# wireless wps rogue detection min-transient-time 500
Device(config)# end
Device# show wireless wps rogue client detailed/show wireless wps rogue ap summary
```

This example shows how to configure the MSE to validate if rogue clients are valid clients:

```
Device# configure terminal
Device(config)# wireless wps rogue client mse
Device(config)# end
Device# show wireless wps rogue client summary
```

This example shows how to automatically contain a rogue access point to which trusted clients are associated:

```
Device# configure terminal
Device(config)# wireless wps rogue ap valid-client auto-contain
Device(config)# end
Device# show wireless wps rogue ap summary
Device# show nmsp capability
```

Additional References for Rogue Detection

Related Documents

Related Topic	Document Title
Security commands	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History and Information For Performing Rogue Detection Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.
Cisco IOS XE 3E	Rogue validation against MSE.