Rogue AP Detection under Unified Wireless Networks

Document ID: 70987

Contents

Introduction
Feature Overview
Infrastructure Rogue Discovery
Rogue Details
Determine Active Rogues
Active Rogue Containment
Rogue Detection Configuration Steps
Troubleshooting Commands
Conclusion
Related Information

Introduction

Wireless networks extend wired networks and increase worker productivity and access to information. However, an unauthorized wireless network presents an additional layer of security concerns. Less thought is put into port security on wired networks, and wireless networks are an easy extension to wired networks. Therefore, an employee who brings his or her own Cisco Access Point (AP) into a well−secured wireless or wired infrastructure and allows unauthorized users access to this otherwise secured network can easily compromise a secure network.

Rogue detection allows the network administrator to monitor and eliminate this security concern. Cisco Unified Network Architecture provides two methods of rogue detection that enable a complete rogue identification and containment solution without the need for expensive and hard−to−justify overlay networks and tools.

Feature Overview

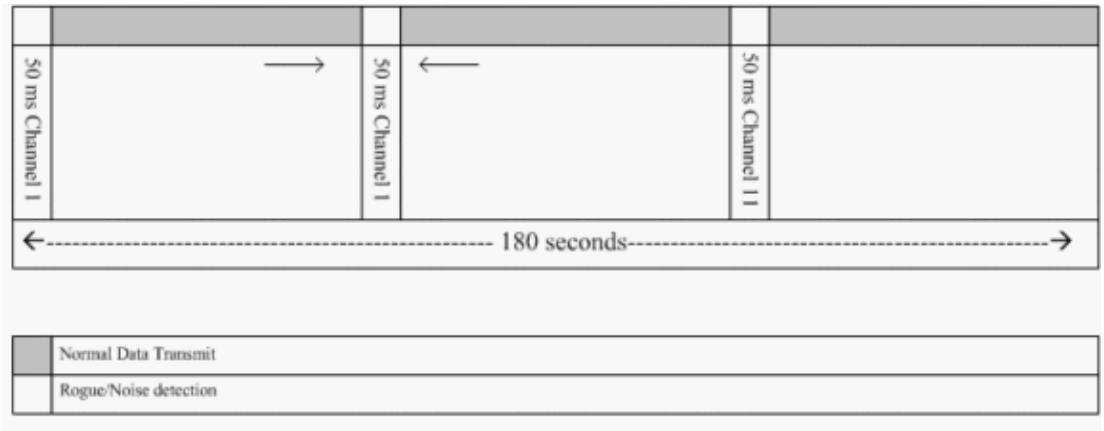
Rogue detection is not bound by any regulations and no legal adherence is required for its operation. However, rogue containment usually introduces legal issues that can put the infrastructure provider in an uncomfortable position if left to operate automatically. Cisco is extremely sensitive to such issues and provides these solutions. Each controller is configured with a RF Group name.Once a Lightweight AP registers with a controller, it embeds an **authentication Information Element (IE)** that is specific to the RF Group configured on the controller in all its beacons/probe response frames. When the Lightweight AP hears beacons/ probe response frames from an AP either without this **IE** or with **wrong IE**, then the Lightweight AP reports that AP as a rogue, records its BSSID in a rogue table, and sends the table to the controller. There are two methods, namely Rogue Location Discovery Protocol (RLDP) and passive operation, which are explained in detail; see the Determine Active Rogues section.

Infrastructure Rogue Discovery

Rogue discovery in an active wireless environment can be costly. This process asks the AP in service (or local mode) to cease service, listen for noise, and perform rogue detection. The network administrator configures the channels to scan, and configures the time period in which all stations are scanned. The AP listens for 50 ms for rogue client beacons, then returns to the configured channel in order to service clients again. This

active scanning, combined with neighbor messages, identifies which APs are rogues and which APs are valid and part of the network. In order to configure the scanned channels and the scanning time period, browse to **Wireless > 802.11b/g Network** (either **b/g** or **a** depending on the network requirement) and select the **Auto RF** button in the top right−hand corner of the browser window.

You can scroll down to **Noise/Interference/Rogue Monitoring Channels** in order to configure the channels to be scanned for rogues and noise. The available choices are: All Channels (1 through 14), Country Channels (1 through 11) or Dynamic Channel Association (DCA) Channels (by default 1, 6 and 11). The scanning time period through these channels can be configured in the same window, under **Monitor Intervals (60 to 3600 secs)** along with the noise measurement interval. By default, the listening interval for off−channel noise and rogues is 180 seconds. This means that each channel is scanned every 180 seconds. This is an example of the DCA channels that are scanned every 180 seconds:



As illustrated, a high number of channels configured to be scanned combined with the short scanning intervals, leaves less time for the AP to actually service data clients.

The Lightweight AP waits in order to label clients and APs as rogues because these rogues are possibly not reported by another AP until another cycle is completed. The same AP moves to the same channel again in order to monitor for rogue APs and clients, as well as noise and interference. If the same clients and/or APs are detected, they are listed as rogues on the controller again. The controller now begins to determine if these rogues are attached to the local network or simply to a neighboring AP. In either case, an AP that is not part of the managed local wireless network is considered a rogue.

Rogue Details

A Lightweight AP goes off−channel for 50 ms 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 this information:

- The rogue AP MAC address
- The rogue AP name
- 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)

Rogue Detector Access Point

You can make an AP operate as a rogue detector, which allows it to be placed on a trunk port so that it can hear all wired−side connected VLANs. It proceeds to find the client on the wired subnet on all the VLANs.

The rogue detector AP listens for Address Resolution Protocol (ARP) packets in order to determine the Layer 2 addresses of identified rogue clients or rogue APs sent by the controller. If a Layer 2 address that matches is found, the controller generates an alarm that identifies the rogue AP or client as a threat. This alarm indicates that the rogue was seen on the wired network.

Determine Active Rogues

Rogue APs must be seen twice before they are added as a rogue by the controller. Rogue APs are not considered to be a threat if they are not connected to the wired segment of the corporate network. In order to determine if the rogue is active, various approaches are used. Those approaches include RLDP.

Rogue Location Discovery Protocol (RLDP)

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 deauthentication messages to all connected clients and then shuts down the radio interface. Then, it will associate 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.

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
```

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 zeros.

Passive Operation:

This approach is used when rogue AP has some form of authentication, either WEP or WPA. When a form of authentication is configured on rogue AP, the Lightweight AP cannot associate because it does not know the key configured on the rogue AP. The process begins with the controller when it passes on the list of rogue client MAC addresses to an AP that is configured as a rogue detector. The rogue detector scans all connected and configured subnets for ARP requests, and ARP searches for a matching Layer 2 address. If a match is discovered, the controller notifies the network administrator that a rogue is detected on the wired subnet.

Active Rogue Containment

Once a rogue client is detected on the wired network, the network administrator is able to contain both the rogue AP and the rogue clients. This can be achieved because 802.11 de−authentication packets are sent to clients that are associated to rogue APs so that the threat that such a hole creates is mitigated. Each time there is an attempt to contain the rogue AP, nearly 15% of the Lightweight AP's resource is used. Therefore, it is suggested to physically locate and remove the rogue AP once it is contained.

Note: From the WLC release 5.2.157.0, once the rouge is detected you can now choose to either manually or automatically contain the detected rogue. In controller software releases prior to 5.2.157.0, manual containment is the only option.

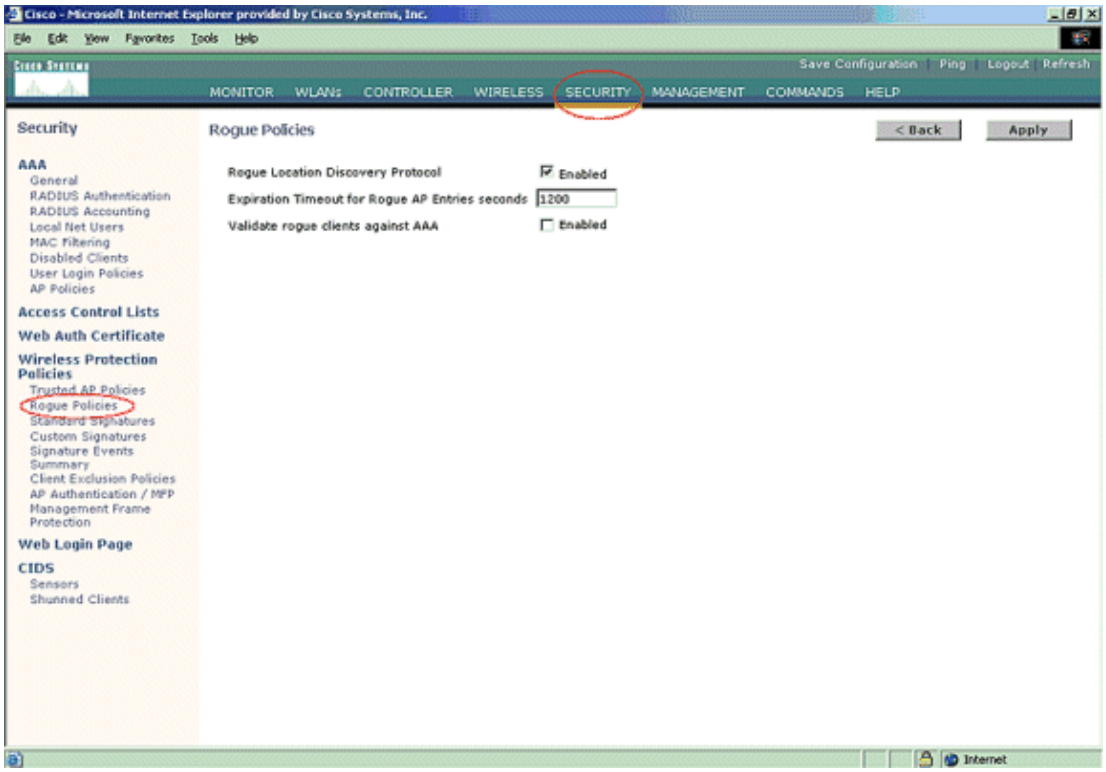
Rogue Detection Configuration Steps

Almost the entire rogue detection configuration is enabled by default to allow for maximized, out−of−the−box network security. These configuration steps assume that no rogue detection is set up on the controller in order to clarify important rogue detection information.

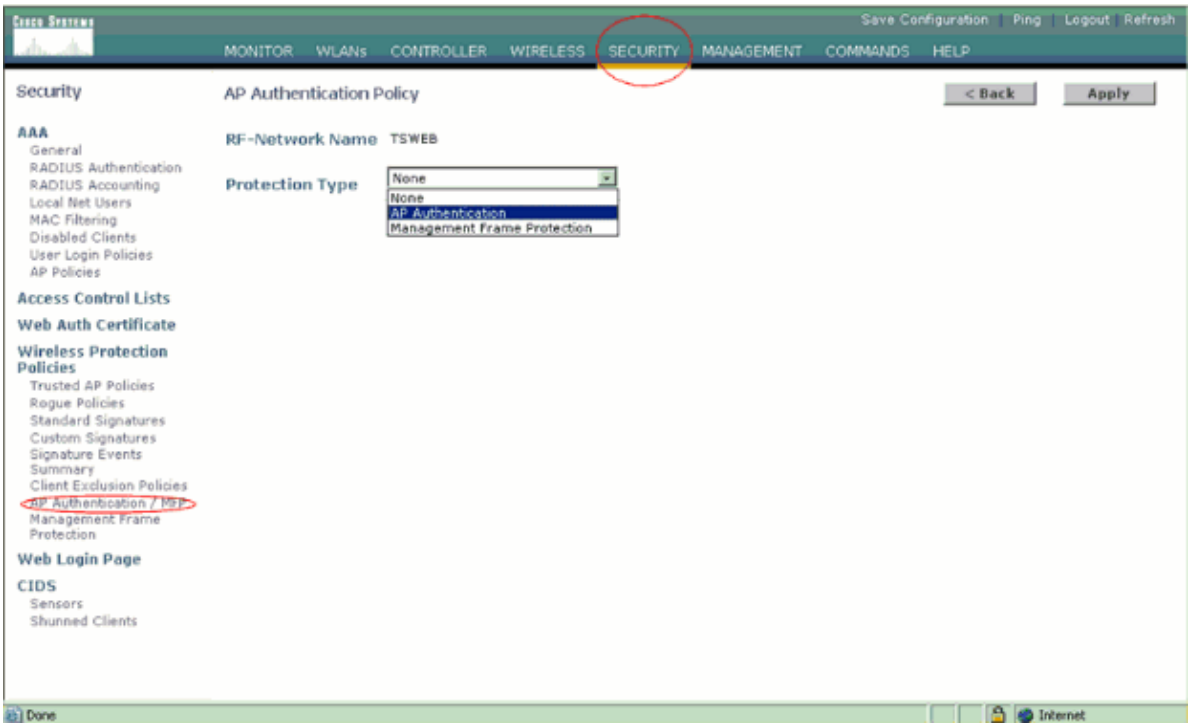
In order to set up rogue detection, complete these steps:

1. Ensure that Rogue Location Discovery protocol is turned on. In order to turn it on, choose **Security > Rogue Policies** and click **Enabled** on the **Rogue Location Discovery Protocol** as shown in the figure.

   Note: If a rogue AP is not heard for a certain amount of time, it is removed form the controller. This is the **Expiration Timeout** for a rogue AP, which is configured below the RLDP option.

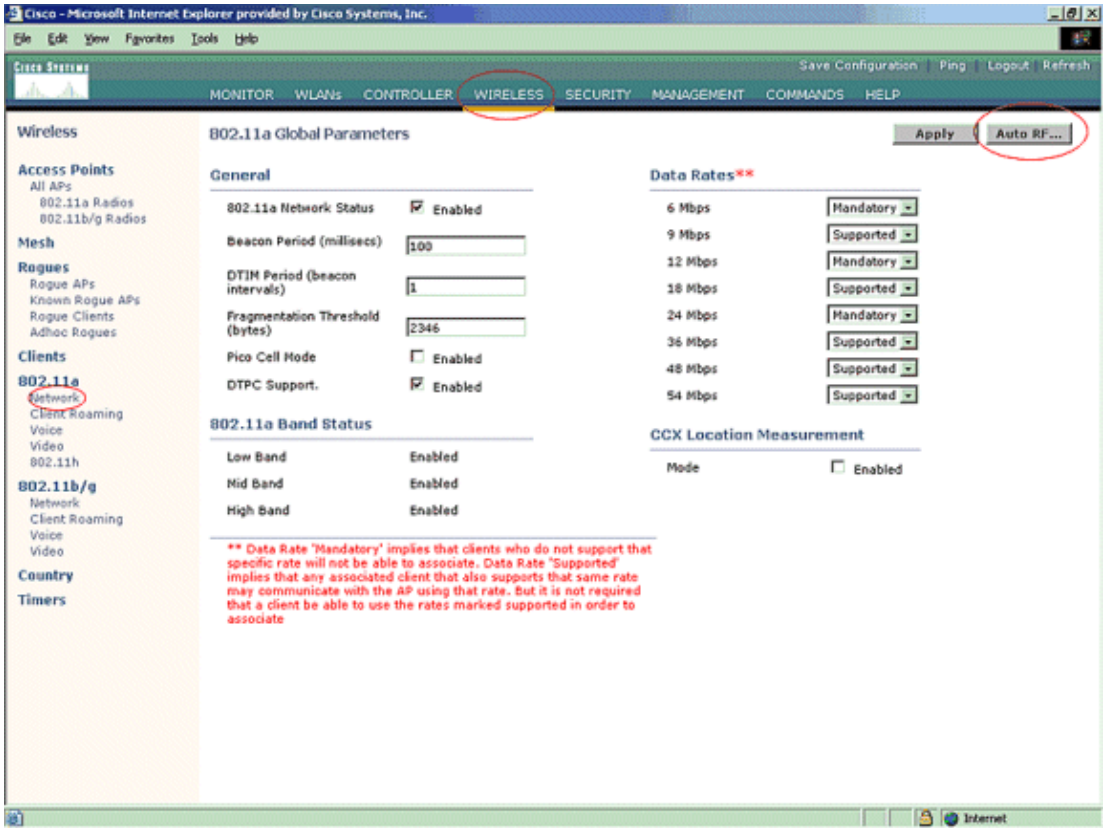


2. This is an optional step. When this feature is enabled, the APs sending RRM neighbor packets with different **RF Group** names are reported as rogues. This will be helpful in studying your RF environment. In order to enable it, choose **Security−> AP Authentication**. Then, choose **AP Authentication** as the Protection Type as shown in the figure.

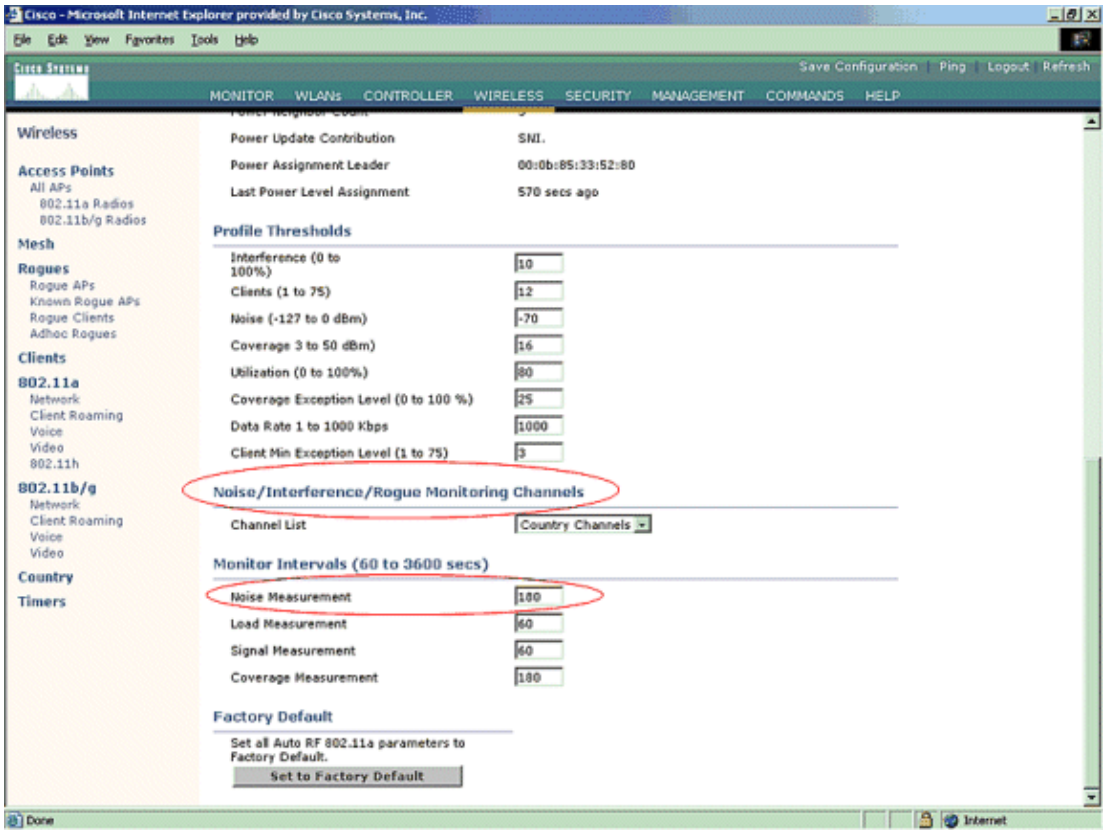


3. Verify the channels to be scanned in these steps:

   a. Select **Wireless > 802.11a Network**, then **Auto RF** in the right hand side as shown in the figure.



   b. On the **Auto RF** page, scroll down and choose **Noise/Interference/Rogue Monitoring Channels**.



c. The Channel List details the channels to be scanned for rogue monitoring, in addition to other controller and AP functions. Refer to Lightweight Access Point FAQ for more information on Lightweight APs, and Wireless LAN Controller (WLC) Troubleshoot FAQ for more information on wireless controllers.



Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

4. Set the Time Period for scanning selected channels:

The scanning duration of the defined group of channels is configured under **Monitor Intervals > Noise Measurement**, and the allowable range is from 60 to 3600 seconds. If left at the default of 180 seconds, the APs scan each channel in the channel group once, for 50 ms, every 180 seconds. During this period, the AP radio changes from its service channel to the specified channel, listens and records values for a period of 50 ms, and then returns to the original channel. The hop time plus the dwell time of 50 ms takes the AP off−channel for approximately 60 ms each time. This means that each AP spends approximately 840 ms out of the total 180 seconds listening for rogues.

The listen or dwell time cannot be modified and is not changed with an adjustment of the Noise Measurement value. If the Noise Measurement timer is lowered, the rogue discovery process is likely to find more rogues and to find them more quickly. However, this improvement comes at the expense of data integrity and client service. A higher value, on the other hand, allows for better data integrity but lowers the ability to find rogues quickly.

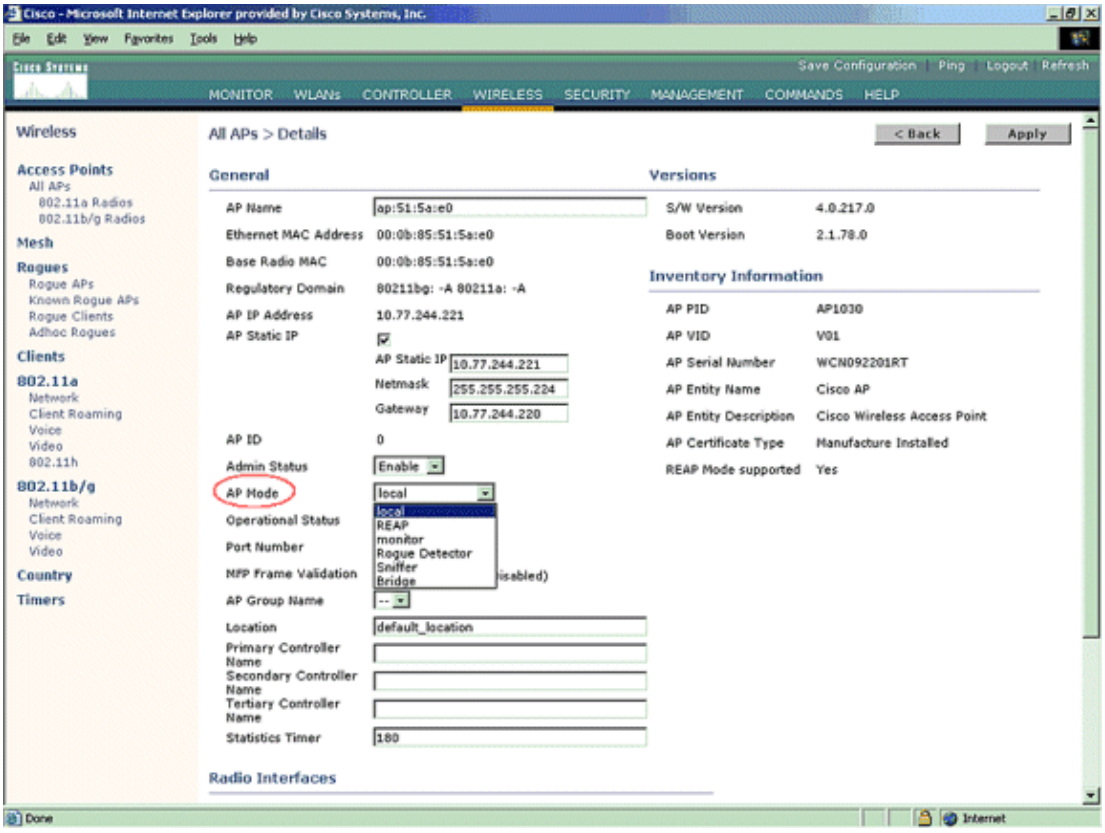
5. Configure the AP mode of operation:

A Lightweight AP mode of operation defines the role of the AP. The modes related to the information presented in this document are:

- **Local** This is the normal operation of an AP. This mode allows data clients to be serviced while configured channels are scanned for noise and rogues. In this mode of operation, the AP goes off−channel for 50 ms and listens for rogues. It cycles through each channel, one at a time, for the period specified under the Auto RF configuration.
- **Monitor** This is radio receive only mode, and allows the AP to scan all configured channels every 12 seconds. Only de−authentication packets are sent in the air with an AP configured this way. A monitor mode AP can detect rogues, but it cannot connect to a suspicious rogue as a client in order to send the RLDP packets.

  Note: DCA refers to non−overlapping channels that are configurable with the default modes.
- **Rogue Detector** In this mode, the AP radio is turned off, and the AP listens to wired traffic only. The controller passes the APs configured as rogue detectors as well as lists of suspected rogue clients and AP MAC addresses. The rogue detector listens for ARP packets only, and can be connected to all broadcast domains through a trunk link if desired.

You can configure an individual AP mode simply, once the Lightweight AP is connected to the controller. In order to change the AP mode, connect to the controller web−interface and navigate to **Wireless**. Click on **Details** next to the desired AP to in order to display a screen similar to this one:



Use the AP Mode drop−down menu in order to select the desired AP mode of operation.

Troubleshooting Commands

You can also use these commands in order to troubleshoot your configuration on the AP:

- **show rogue ap summary** This command displays the list of rogue APs detected by the Lightweight APs.
- **show rogue ap detailed** *<MAC address of the rogue ap>* Use this command in order to view details about an individual rogue AP. This is the command that helps to determine if the rogue AP is plugged onto the wired network.

Conclusion

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

Related Information

- **Overview of RF Groups**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2014 − 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Sep 25, 2007 Document ID: 70987