# Wireless Network Management

## Contents

Overview ................................................. 13-3

Monitoring the Wireless Network ................. 13-4
  Wireless Stations .................................. 13-4
    Viewing Wireless Stations ...................... 13-4
    Disconnecting a Wireless Station ............. 13-7
    Viewing Details about a Wireless Station .... 13-8
  Viewing All Stations in a Layer 3 Mobility Domain .... 13-10

Wireless Statistics for Stations ................. 13-12
  Viewing a Graph of Wireless Station Statistics .... 13-14

Radio Statistics ................................. 13-18
  Viewing a Graph of Radio Statistics ........ 13-21

WLAN Statistics ................................. 13-26
  Viewing Traffic Statistics for the WLAN ...... 13-27
  Viewing Detailed WLAN Statistics ............ 13-28
  Viewing a Graph of WLAN Statistics .......... 13-30

Module Statistics ............................... 13-34

Radio Port Adoption Statistics .............. 13-36

AP Detection ........................................ 13-39
  Configuring AP Detection ..................... 13-40
  Creating Lists of Detected APs ............... 13-46
    Creating Rules That Define Allowed APs .... 13-47
Wireless Network Management

Contents

Monitoring Detected APs ........................................... 13-50
Managing the Unapproved APs List .............................. 13-50
Managing the Approved APs List ................................. 13-53
Configuring the Module to Report Unapproved APs ........ 13-54

Configuring Station Intrusion Detection ...................... 13-57
Configuring Thresholds for Station Intrusion Detection .... 13-58
Configuring the Module to Report Station Intrusion ......... 13-59
Viewing Blocked Stations ....................................... 13-61

Logging and Alarms .............................................. 13-62
Configuring Logging .............................................. 13-63
Enabling Logging .................................................. 13-63
Forwarding Logs to an External Server ....................... 13-64
Viewing Events in the Local Log File ......................... 13-65
Deleting and Transferring the Local Log File ............... 13-68
Managing the Alarm Log ......................................... 13-70
Details ............................................................. 13-72
Delete ............................................................. 13-72
Acknowledge ...................................................... 13-73
Export ............................................................. 13-73

MAC Filters (Local MAC Authentication) ..................... 13-74
Configuring MAC Standard ACLs (Filters) .................... 13-74
Configuring WLAN Memberships ............................... 13-77
Exporting and Importing MAC Standard ACLs (Filters) .... 13-81
Exporting MAC Standard ACLs ................................ 13-81
Importing MAC Standard ACLs ................................ 13-83

Network Self Healing ............................................. 13-88
Neighbor Recovery ............................................... 13-88
Enabling Neighbor Recovery .................................... 13-89
Specifying Neighbors Manually ................................ 13-91
Configuring Radios to Automatically Detect Neighbors .... 13-94
Selecting the Self-Healing Action .............................. 13-95
Configuring a Self Healing Offset ............................. 13-98

Interference Avoidance .......................................... 13-100
Overview

In this chapter you will learn how to monitor and manage your wireless network. You will learn about monitoring:

- wireless stations that are associated to a Wireless Edge Services xl Module's radio ports (RPs)
- access points (APs) detected by a module's RPs
- logged events
- alarm logs

When viewing such information in the Web browser interface, you can take several common actions, such as:

- clicking a Details button to view more in-depth information
- clicking an Export button to save the information to your workstation

You will also learn how to configure the Wireless Edge Services xl Module to collect information when necessary. For example, RPs do not automatically detect other APs. You must enable this feature and configure the module to manage the information that it receives.

Finally, you will learn how to implement self healing in your wireless network, which maximizes network performance by allowing RP radios to respond to changing conditions.
Monitoring the Wireless Network

This section explains how you can access information about wireless stations and wireless network activity. It then provides some tips for interpreting this information.

You can monitor:

■ wireless stations’ associations

■ wireless statistics:
  • individual statistics for traffic to and from each wireless station
  • average statistics for all traffic to and from an RP radio
  • average statistics for all traffic in a wireless LAN (WLAN)
  • average statistics for all traffic to and from all RPs adopted by a module

■ RPs

When troubleshooting, you can compare the various wireless statistics to determine, for example, whether congestion seems to be problem throughout a WLAN or is centered on a particular RP or group of RPs.

Wireless Stations

The Wireless Edge Services xl Module stores information about the associations that adopted RPs have established with wireless stations. You should view this information to monitor network activity and to detect intruders. You can also use this information to help a wireless user who is having difficulty with his or her connection.

Viewing Wireless Stations

To view the wireless stations, select Device Information > Wireless Stations, as shown in Figure 13-1.
Wireless Network Management
Monitoring the Wireless Network

The screen displays this information for each station associated with one of the WLANs on this module:

- **Station Index**—Stations are listed in the order in which they associated.
- **MAC Address**—Each station’s Media Access Control (MAC) address is listed.
- **IP Address**—A station must receive an IP address to receive complete network connectivity.
- **Ready**—A green check mark indicates that the station has completely authenticated and associated to a WLAN. A red X reveals that the station cannot yet send data, usually because it failed to authenticate.
- **Power Save**—A station that uses power save turns off the wireless connection except when actively sending or receiving data. The Wireless Edge Services x1 Module tracks these stations and ensures that packets are correctly buffered for them. A green checkmark indicates that the station is currently in power save mode.
Although power save extends a station’s battery life, it might result in jittery performance for real-time applications. If a user complains of low quality of service (QoS) and you see that the user’s station implements power save, you could suggest that the user disable this feature.

- **WLAN**—The index number of the WLAN to which the station has connected is listed. (This column does not show the service set identifier [SSID]). The WLAN defines the broadcast group for the station and determines settings such as encryption and QoS.

- **VLAN**—The virtual LAN (VLAN), or subnetwork, in which the module will forward traffic from this station is listed. This important setting determines the type of network access that the station receives. If the module implements user-based VLANs for a WLAN, you should verify that the station has received the correct VLAN assignment.

- **Tunnel**—If the station’s traffic is being forwarded through a Generic Routing Encapsulation (GRE) tunnel to another device on your network, the number of that tunnel is listed. (For information about configuring GRE tunnels on the Wireless Edge Services xl Module, see Chapter 12: Configuring Tunnels with Generic Routing Encapsulation.)

- **Radio Index**—The radio to which the station connects is listed. If you see an unauthorized station, this information will point you toward the intruder’s physical location.

- **Radio Type**—This setting indicates the 802.11 mode in which the station and the RP radio to which it connects operate.

You should be able to interpret the information on the Device Information > Wireless Stations screen to monitor and troubleshoot your wireless network.

For example, if the user of a wireless station listed in Figure 13-1 reports that he or she cannot connect to the network, the network administrator can quickly access the Network Setup > Wireless Stations screen while talking to the user. The administrator can immediately see that the user’s station is not ready to send and receive traffic and has not received an IP address. The administrator can then begin to troubleshoot the problem, working with the user to ensure that login credentials were entered correctly and that the station’s VLAN assignment is correct. The administrator can also troubleshoot the network’s Dynamic Host Configuration Protocol (DHCP) setup.

You can also save information about one or more wireless stations to a comma-separated file on your workstation. Select the stations, and then click the Export button. (Use the Ctrl or Shift keys to select more than one station.)
Disconnected a Wireless Station

If you access the **Device Information > Wireless Stations** screen and see a wireless station that should not connect to your network, you can immediately dissociate the station. Select the station and click the **Disconnect** button.

Because the station can immediately reassociate unless you take steps to prevent this, the prompt shown in Figure 13-2 is displayed.

![Figure 13-2. Preventing a Station from Reconnecting to the Wireless Network](image)

If you click the **Yes** button, the **Filter** dialog box is displayed. (See Figure 13-3.)

![Figure 13-3. Creating a Filter to Block an Unauthorized User's Access](image)

As the figure shows, the station’s MAC address is already listed in the **Starting MAC** and **Ending MAC** fields, allowing you to quickly create a MAC filter to prevent the station from reaccessing the wireless network.

You should also take steps to prevent the user from using another station (with a different MAC address) to access the wireless network. For example, you may need to change a preshared key that has been compromised or reset a user’s password.
Viewing Details about a Wireless Station

If you want to view more information about a particular station’s capabilities and connection, select that station on the Device Information > Wireless Stations screen, and then click the Details button. The Details screen is displayed. (See Figure 13-4.)

![Figure 13-4. Viewing Detailed Information about a Station](image)
In addition to the information that is listed on the **Device Information > Wireless Stations** screen (such as MAC address, IP address, Power Save, WLAN, and VLAN), you can view:

- **Authentication**—This field displays the authentication method used—802.1X Extensible Authentication Protocol (EAP), Web authentication (Web-Auth), MAC authentication, or none. None is displayed for Wi-Fi Protected Access (WPA)/WPA2-preshared keys (PSK) and Wired Equivalency Protocol (WEP).

- **Last Active**—You can view how many seconds it has been since the station last sent a frame. If the station is idle for longer than the WLAN’s inactivity timeout, the Wireless Edge Services xl Module will force the station to reassociate.

- **QoS Information**—Two fields are reported for QoS:
  - **UAPSD enabled for**—This field reports whether the Unscheduled Automatic Power Save Delivery (UAPSD) feature has been enabled. Designed for Voice over IP (VoIP) and Wi-Fi Multimedia (WMM), UAPSD preserves the mobile device’s battery life while allowing the device to control when it “sleeps” and “awakens.” At regular intervals (configured on and controlled by the mobile device), the mobile device queries the AP to determine whether the AP has any buffered frames. (With normal power save mode, the AP contacts the station—at intervals defined on and controlled by the AP—when the AP has buffered frames for the station.)
  - **Service Period**—When QoS is enabled for a WLAN, the AP grants a station a transmission opportunity, allowing the station to transmit a frame. If an AP grants a station two or more contiguous transmission opportunities, this is called the service period.

- **BSS Address**—This address is the basic SSID (BSSID) on the radio to which the station connects. Each RP radio has four BSSIDs, which carry traffic for different WLANs.

- **Voice**—This setting indicates whether this station sends voice frames. You can configure the Wireless Edge Services xl Module to grant higher QoS for voice traffic.

- **WMM**—This setting indicates whether the station supports Wi-Fi Multimedia (WMM). If it does, then the Web browser interface indicates the Access Category (AC) that the station is currently using to transmit traffic. The higher the AC, the better the QoS for the traffic. You can view the WMM settings associated with that AC on the station’s WLAN by selecting **Network Setup > WLAN Setup** and clicking the **WMM** tab.

- **Encryption**—This field displays the encryption method—WEP, WPA/WPA2 with Temporal Key Identity Protocol (TKIP), WPA2 with Advanced Encryption Standard (AES), or WPA/WPA2 with both TKIP and AES.
Wireless Network Management
Monitoring the Wireless Network

- **Roam Count (No de-authentication)**—The module tracks the number of times that the station has de-authenticated, which indicates the number of times that the station has roamed away from the module (not between RPs on the same module).

- **IDM Attributes**—If you are using ProCurve Identity Driven Manager (IDM), this section lists IDM settings received for the user accessing the network through this station. Possible settings include a dynamic VLAN (which is also called the user-based VLAN), access control lists (ACLs), priority (which is the 802.1p value assigned to the user’s traffic), and ingress bandwidth (which is displayed if rate limiting has been configured for the user).

Viewing All Stations in a Layer 3 Mobility Domain

When your Wireless Edge Services xl Module is in a Layer 3 mobility domain, it tracks all stations associated with any module in the domain. This information prepares the module for implementing Layer 3 roaming should one of these stations roam to it. In addition, the module must maintain information about stations that have roamed away from it, but for which it still acts as home module.

To view information about every station associated with any Wireless Edge Services xl Module in the Layer 3 mobility domain, follow these steps:

1. Select **Device Information > Wireless Stations**.
2. Click the **Layer 3 Mobility-Station Status** tab.
Figure 13-5. Device Information > Wireless Stations > Layer 3 Mobility-Station Status

The screen displays the following information for all Layer 3 mobility domain stations:

- **Station MAC**—station MAC address
- **Station IP**—station IP address
- **Home Module IP**—the IP address of the module responsible for forwarding the station’s traffic into the wired network
- **Home Module VLAN**—the static VLAN ID for the WLAN on the home module (HM)
- **Curr Module IP**—the IP address of the module to which the station is currently associated
- **Roam**—This column tracks Layer 3 roams. The station is considered to be in a roaming state (green check mark) if its current module (CM) differs from its HM.
Wireless Statistics for Stations

Like the Device Information > Wireless Stations screen, the Device Information > Wireless Statistics screen lists every station associated with RPs adopted by the Wireless Edge Services xl Module. However, this screen focuses on activity on the connection.

### Figure 13-6. Device Information > Wireless Statistics Screen

The first two columns, Radio Index and MAC Address, identify the station according to the RP radio to which the station connects and the station’s MAC address. The WLAN column indicates the station’s WLAN.

The next columns display traffic statistics for the connection:

- **Throughput Mbps**—the total throughput for data in Mbps
- **Bit Speed (Avg.) Mbps**—the average bit speed in Mbps when the station actually transmits or receives traffic
- **% Non Unicast**—the percentage of multicast and broadcast packets (as compared to total packets)
- **Retries**—the number of times that a station must retransmit a packet, whether due to a collision or another error

Select Last 30s or Last Hr to view the average statistics over either the last 30 seconds or the last hour.
Wireless Network Management
Monitoring the Wireless Network

A high number of retries can indicate interference or excessive congestion.

Wireless phones, which send traffic to a multicast address, may have a high percentage of nonunicast traffic. For traditional stations, a high percentage of nonunicast traffic can be normal for brief periods—for example, when the station first associates and requests a DHCP address. You may be able to decrease the number of frames that stations broadcast by enabling proxy ARP. (See Chapter 4: Wireless Local Area Networks (WLANs).)

Viewing Detailed Wireless Statistics

Viewing Detailed Wireless Statistics

For more detailed information about the connection to a particular station, select that station and click the Details button. The Details screen is displayed. (See Figure 13-7.)

![Figure 13-7. Viewing Detailed Statistics about a Wireless Station](image-url)
The **Station Properties** section displays the same information that is listed on the **Device Information > Wireless Stations** screen, including the station’s MAC and IP address. However, you can also see whether the station supports QoS capabilities such as Voice and WMM.

You can use the **Traffic** section to monitor the quality and performance of the connection. The Web browser interface reports speed in terms of packets per second, total throughput in Mbps, and average speed in Mbps. The Web browser interface further breaks down statistics into received and transmitted traffic.

Note that these statistics do not include retry overhead, which means that in a network with significant congestion or interference, a user might perceive the connection to be slower than these statistics would seem to indicate. The sections below can help you monitor that aspect of the wireless connection.

The **RF Status** section displays the status of the radio medium:
- **Avg Station Signal (dBm)**—average signal level detected for this station
- **Avg Station Noise (dBm)**—average background noise for this station
- **Avg Station SNR (dBm)**—average SNR for this station

In the **Errors** section, the Web browser interface reports the total number of error packets:
- **Avg Number of Retries**—average number of retries necessary to successfully transmit a packet to this station
  
  A high value (over 10 or 20 percent) may indicate excessive congestion or interference from another wireless device.
- **% Gave Up Pkts**—number of packets that the Wireless Edge Services xl Module never successfully transmitted to this station
- **% of Undecipherable Pkts**—percentage of packets received from this station that could not be deciphered
  
  A high percentage might indicate that someone is attempting to guess a static WEP key or WPA/WPA2 PSK.

The statistics in black apply to the last 30 seconds, giving you a snapshot of current performance. The statistics in blue show the station’s average performance over the last hour.

**Viewing a Graph of Wireless Station Statistics**

The Wireless Edge Services xl Module can create a graph of statistics for a wireless station, which displays how the statistics change over time.
To view this graph, follow these steps:

1. Select **Device Information > Wireless Statistics**.
2. Select the station (identified by MAC address) from the list.

### Figure 13-8. Graph Button in the Device Information > Wireless Statistics Screen

3. Click the **Graph** button.

The **Station Statistics** screen is displayed.
The **Station Statistics** screen displays the station’s MAC address and IP address in the upper right corner.

To generate a graph, you must select the statistic that you want to track. (Initially, the graph shows packets per sec.) You can choose any of the statistics displayed in the **Details** screen (refer to “Viewing Details about a Wireless Station” on page 13-8 for more information on a statistic):

- **Pkts per sec**—total packets transmitted and received by this station per second
  - **TX Pkts per sec**—packets transmitted by this station per second
  - **RX Pkts per sec**—packets received by this station per second
- **Throughput (Mbps)**—the actual throughput for data transmitted and received by this station
  - **TX Tput (Mbps)**—actual throughput for data transmitted by this station
  - **RX Tput (Mbps)**—actual throughput for data received by this station

---

![Station Statistics Graph](image-url)
■ **Avg Bits per sec**—average bit speed for all traffic sent and received by this station

■ **NUcast Pkts**—percentage of multicast and broadcast packets (as compared to total packets)

■ **Avg Retries**—average number of times the station must retransmit a packet, whether due to a collision or another error

■ **Avg Signal (dBm)**—average signal level detected from this station

■ **Avg Noise (dBm)**—average background noise in the wireless cell

■ **Avg SNR (dBm)**—average SNR for the connection to the station

■ **Dropped Pkts**—number of packets that the Wireless Edge Services xl Module never successfully transmitted to this station (also called gave up packets)

■ **Undecr Pkts**—number of packets from this station encrypted with the wrong key

Check the appropriate box for the statistic you want to view.

![Station Statistics](image)

**Figure 13-10. Comparing Station Statistics**
Wireless Network Management
Monitoring the Wireless Network

The x-axis of the graph displays the time—in Figure 13-10 the time is labelled in 10 second intervals. The y-axis adds a label that matches the box that you chose. It also displays the correct units for that type of statistic.

A line that is the same color as the y-axis label plots the statistic as it changes over time. For example, the graph in Figure 13-10 shows this station’s total throughput, which experienced a spike just before 15:00.

You can select more than one box and compare statistics against each other. For example, Figure 13-10 compares total throughput to the average bit speed. As you can see, the station’s bit speed averages about 50 Mbps—near the 54 Mbps theoretical data rate. However, the station’s throughput is actually much lower. The lines are distinguished by color, as indicated in the legend below the x-axis.

You can select a maximum of four boxes at once.

When you have finished viewing the graph, click the Close button.

Radio Statistics

The Wireless Edge Services xl Module stores information about the wireless network activity on each RP radio. To view these statistics, select Network Setup > Radio and click the Statistics tab.

**Table:**

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Type</th>
<th>Stations</th>
<th>Throughput</th>
<th>Average</th>
<th>RF Upl</th>
<th>% Non-Upl</th>
<th>% Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/RA001</td>
<td>802.11bg</td>
<td>20.02</td>
<td>30.81</td>
<td>0.02%</td>
<td>19.02</td>
<td>1342</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/RA002</td>
<td>802.11b</td>
<td>21.1</td>
<td>24.0</td>
<td>0.0%</td>
<td>100</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3/RA003</td>
<td>802.11bg</td>
<td>15.37</td>
<td>10.38</td>
<td>0.0%</td>
<td>89.65</td>
<td>0.0%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 13-11.** Network Setup > Radio > Statistics Screen
Every radio adopted by the module is listed, identified by:

- **Index**
- **Description**
- **Type** (802.11a or 802.11bg)

In addition to providing this information, the **Network Setup > Radio > Statistics** screens lists the number of stations that are connected to each RP. The following columns display average traffic statistics for connections to these stations, including:

- **Throughput Mbps**
- **Average Mbps**
- **RF Util**
- **% Non-UNI**
- **Retries**

These statistics are similar to those described for individual stations in “Wireless Statistics for Stations” on page 13-12. The **RF Util** percentage compares the radio’s actual utilization to its potential utilization by dividing the throughput by the average Mbps.

Again, you can select either **Last 30s** or **Last Hr** to view either the most current statistics or statistics over a more extended period.

**Viewing Detailed Radio Statistics**

To view more detailed statistics for a specific radio, select that radio and click the **Details** button. The **Details** screen is displayed. (See Figure 13-12.)
Wireless Network Management
Monitoring the Wireless Network

Figure 13-12. Radio Statistics Details

The Information section describes this radio and shows the number of stations currently associated to it. You should check the Current Channel listing; if the radio is configured with a manual channel but currently uses a different channel, the channel number is listed in red.

On the Details screen, statistics for wireless traffic are broken down into received and transmitted traffic.

You can view the average status of the wireless medium or all stations connected to this radio under RF Status:

- **Avg Station Signal (dBm)**—average signal level detected for all stations associated to the radio
- **Avg Station Noise (dBm)**—average background noise in the wireless cell
- **Avg Station SNR (dBm)**—average SNR for all stations associated to the radio
View the *Errors* section to monitor for congestion. Statistics include:

- **Avg Number of Retries**—average number of retries the radio must make to successfully transmit a packet
  
  A high value (over 10 or 20 percent) may indicate excessive congestion or interference from another wireless device.

- **% Gave Up Pkts**—number of packets that the Wireless Edge Services xl Module never successfully transmitted to a station associated to this radio

- **% of Undecipherable Pkts**—percentage of packets received by this radio that could not be deciphered
  
  A high percentage might indicate that someone is attempting to guess a static WEP key or WPA/WPA2 PSK.

The *Details* screen also allows you to simultaneously compare statistics for the last 30 seconds and the last hour.

### View a Graph of Radio Statistics

The Wireless Edge Services xl Module can create a graph of statistics for a radio, which displays how the statistics change over time.

To view this graph, follow these steps:

1. Select **Network Setup > Radio**.
2. Select the **Statistics** tab.
3. Select the radio.
4. Click the **Graph** button.

The **RP Statistics** screen is displayed.
The **RP Statistics** screen displays the radio’s name and MAC address in the upper right corner.

To generate a graph, you must select the statistic that you want to track. (Initially, the graph shows packets per second.) You can choose any of the statistics displayed in the **Details** screen for radio statistics. The statistics apply to all stations associated to the radio. Refer to “Viewing Detailed Radio Statistics” on page 13-19 for more information on a statistic.

You can choose:

- **Pkts per sec**—total packets transmitted and received by this radio per second
  - **TX Pkts per sec**—packets transmitted by this radio per second
  - **RX Pkts per sec**—packets received by this radio per second
Wireless Network Management
Monitoring the Wireless Network

- **Throughput (Mbps)**—total throughput for data transmitted and received by this radio
  - **TX Tput (Mbps)**—throughput for data transmitted by this radio
  - **RX Tput (Mbps)**—throughput for data received by this radio
- **Avg Bits per sec**—average bit speed for traffic when the radio actually transmits or receives it
- **NUcast Pkts**—percentage of multicast and broadcast packets sent and received by the radio (as compared to total packets)
- **Avg Retries**—average number of times that all stations must retransmit a packet, whether due to a collision or another error
- **Avg Signal (dBm)**—average signal level detected for all stations associated to the radio
- **Avg Noise (dBm)**—average background noise in the wireless cell
- **Avg SNR (dBm)**—average SNR for all stations associated to the radio
- **Dropped Pkts**—number of packets that the Wireless Edge Services xl Module never successfully transmitted to a station associated to this radio (also called gave up packets)
- **Undecr Pkts**—number of packets from this station encrypted with the wrong key
- **MUs associated**—number of stations associated to this radio

Check the appropriate box for the statistic you want to view.
Wireless Network Management
Monitoring the Wireless Network

Figure 13-15. Comparing RP Statistics

The x-axis of the graph displays the time—in Figure 13-15, marked at 5 second intervals. The y-axis adds a label that matches your choice. It also displays the correct units for that type of statistic.

A line that is the same color as the y-axis label plots the statistic as it changes over time. You can select more than one box and compare statistics against each other. For example, Figure 13-10 compares average retries and average SNR. The lines are distinguished by color, as indicated in the legend below the x-axis.

You can select a maximum of four boxes at once.

When you have finished viewing the graph, click the Close button.

---

13-25
WLAN Statistics

To monitor wireless activity on a WLAN-wide scale, select **Network Setup > WLAN Setup** and click the **Statistics** tab.

**Figure 13-16. Network Setup > WLAN Setup > Statistics Screen**

This screen lists every WLAN that is enabled on the module. WLANs are identified by:

- **Index** (the WLAN's number)
- **SSID**
- **Description**
- **VLAN**

The **Stations** column shows the number of stations currently connected to that WLAN.

The remaining columns display statistics similar to those described in “Wireless Statistics for Stations” on page 13-12; however, these statistics are averages for all stations in the WLAN:
Wireless Network Management
Monitoring the Wireless Network

- **Throughput Mbps**—the total throughput for all data transmitted in the WLAN in Mbps
- **Bit Speed (Avg.) Mbps**—the average bit speed for all data transmitted in the WLAN in Mbps
- **% Non Unicast**—the percentage of multicast and broadcast packets (as compared to total packets)
- **Retries**—the number of times that all stations in the WLAN must retransmit a packet, whether due to a collision or another error

Viewing Traffic Statistics for the WLAN

The **Network Setup > WLAN Setup > Statistics** screen includes a **Module Statistics** button.

![Module Statistics Button in the Network Setup > WLAN Setup > Statistics Screen](image)

<table>
<thead>
<tr>
<th>Index</th>
<th>SSID</th>
<th>Description</th>
<th>VLAN</th>
<th>Stations</th>
<th>Throughput Mbps</th>
<th>Avg Mbps</th>
<th>% Non-Uni</th>
<th>Retries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MAIN</td>
<td></td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>802.1X</td>
<td></td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Filtering is disabled
Select a WLAN and click this button to view:

- the percentage of packets in this WLAN transmitted at each data rate
- the percentage of packets in this WLAN that required a certain number of retries (for 0 to 15)

![Module Statistics Screen](image)

**Figure 13-18. Module Statistics Screen**

Click the **Refresh** button to update the statistics. When you have finished viewing the screen, click the **Close** button.

**Viewing Detailed WLAN Statistics**

To view more detailed statistics for a specific WLAN, select the WLAN and then click the **Details** button in the **Network Setup > WLAN Setup > Statistics** screen.
The **Information** section shows settings for this WLAN including:
- SSID
- VLAN
- security settings
  - authentication type
  - encryption type

The **Information** section also displays the number of stations associated to the WLAN and of radios mapped to the WLAN. (If the Wireless Edge Services x! Module is using normal mode configuration, all adopted radios are mapped to the WLAN.)

The **Traffic** section displays the same information that is listed on the **Network Setup > WLAN Setup > Statistics** screen. You can use the **Traffic** section to monitor the quality and performance of the WLAN. The Web browser interface reports speed in terms of packets per second, total throughput in Mbps, and average speed in Mbps. The Web browser interface further breaks down statistics into received and transmitted traffic.

**Figure 13-19. WLAN Statistics Details**

<table>
<thead>
<tr>
<th>SSID</th>
<th>MyWLAN</th>
<th>Authentication Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>1</td>
<td>Encryption Type</td>
<td>WPA2</td>
</tr>
<tr>
<td>Num Associated Stations</td>
<td>2</td>
<td>Mapped Radios</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic (does not include &quot;reply overhead&quot;)</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pkts per second</td>
<td>7,735</td>
<td>6,060</td>
<td>2,988</td>
</tr>
<tr>
<td>Throughput</td>
<td>0.04</td>
<td>0.00</td>
<td>0.01</td>
</tr>
<tr>
<td>Avg Bit Speed</td>
<td>54.06</td>
<td>54.06</td>
<td>54.06</td>
</tr>
<tr>
<td>Non-unicast Pkts</td>
<td>1.72</td>
<td>83.10%</td>
<td>1.72</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RF Status</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg Station Signal dBm</td>
<td>-82</td>
<td>-70</td>
<td>-82</td>
</tr>
<tr>
<td>Avg Station Noise dBm</td>
<td>-95</td>
<td>-89</td>
<td>-95</td>
</tr>
<tr>
<td>Avg Station SNR (dB)</td>
<td>33</td>
<td>26</td>
<td>33</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Errors</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg Num of retries</td>
<td>0.00</td>
<td>0.00</td>
<td></td>
</tr>
<tr>
<td>% Drop Up Pkts</td>
<td>0%</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>% of Under cry Pkts</td>
<td>0%</td>
<td>0%</td>
<td></td>
</tr>
</tbody>
</table>

Status:

- last 30 seconds
- last hour

13-29
The RF Status section displays statistics dealing with the status of the radio medium. The statistics apply to all radios mapped to the WLAN:

- **Avg Station Signal (dBm)**—average signal level detected for all stations associated to the WLAN
- **Avg Station Noise (dBm)**—average background noise for all stations associated to the WLAN
- **Avg Station SNR (dBm)**—average SNR for all stations associated to the WLAN

In the Errors section, the Web browser interface reports the total number of error packets in the entire WLAN:

- **Avg Number of Retries**—average number of attempts radios must make to successfully transmit a packet to stations in this WLAN
  
  A high value (over 10 or 20 percent) may indicate excessive congestion or interference from another wireless device.

- **% Gave Up Pkts**—number of packets that the Wireless Edge Services xl Module never successfully transmitted to a station associated to this WLAN

- **% of Undecipherable Pkts**—percentage of packets in this WLAN that could not be deciphered
  
  A high percentage might indicate that someone is attempting to guess a static WEP key or WPA/WPA2 PSK.

The statistics in black apply to the last 30 seconds, giving you a snapshot of current performance. The statistics in blue show activity in the WLAN over the last hour.

**Viewing a Graph of WLAN Statistics**

The Wireless Edge Services xl Module can create a graph of statistics for a WLAN, which displays how the statistics change over time.

To view this graph, follow these steps:

1. Select **Network Setup > WLAN**.
2. Select the **Statistics** tab.
3. Select the WLAN.
4. Click the Graph button.

The WLAN Statistics screen is displayed.
The **WLAN Statistics** screen displays the WLAN's SSID and static VLAN ID in the upper right corner.

To generate a graph, you must select the statistic that you want to track. (Initially, the graph shows packets per second.) You can choose any of the statistics displayed in the **Details** screen for WLAN statistics. (Refer to “Viewing Detailed WLAN Statistics” on page 13-28 for more information on a statistic.) The statistics apply to all radios and stations associated to the WLAN.

You can choose:

- **Pkts per sec**—total packets transmitted and received in this WLAN per second
  - **TX Pkts per sec**—packets transmitted in the WLAN per second
  - **RX Pkts per sec**—packets received in this WLAN per second
Wireless Network Management
Monitoring the Wireless Network

- **Throughput (Mbps)**—total throughput for data transmitted and received in this WLAN
  - **TX Tput (Mbps)**—throughput for data transmitted in this WLAN
  - **RX Tput (Mbps)**—throughput for data received in this WLAN
- **Avg Bits per sec**—average bit speed for all traffic transmitted and received in the WLAN
- **NUcast Pkts**—percentage of multicast and broadcast packets sent and received in the WLAN (as compared to total packets)
- **Avg Retries**—average number of times that all stations and radios in the WLAN must retransmit a packet, whether due to a collision or another error
- **Avg Signal (dBm)**—average signal level detected for all stations in the WLAN
- **Avg Noise (dBm)**—average background noise in all wireless cells in the WLAN
- **Avg SNR (dBm)**—average SNR for all stations in the WLAN
- **Dropped Pkts**—number of packets from this station dropped by the Wireless Edge Services x1 Module
- **Undecr Pkts**—number of packets from this station encrypted with the wrong key
- **# Radios**—number of radios mapped to this WLAN

Check the appropriate box for the statistic you want to view.
Wireless Network Management
Monitoring the Wireless Network

Figure 13-22. Comparing WLAN Statistics

The x-axis of the graph displays the time—in Figure 13-22, marked at 5 second intervals. The y-axis adds a label that matches your choice. It also displays the correct units for that type of statistic.

A line that is the same color as the y-axis label plots the statistic as it changes over time.

You can select up to four boxes at once and compare statistics against each other. When you have finished viewing the graph, click the Close button.

Module Statistics

You can also monitor all wireless traffic to and from stations associated with this Wireless Edge Services xl Module. Select Network Setup and click the Module Statistics tab.
Wireless Network Management
Monitoring the Wireless Network

Figure 13-23. Network Setup > Module Statistics Screen

The top of the screen displays:
- the number of stations currently associated with RPs on this module
- the number of RPs adopted by this module
- the number of RP radios adopted by this module

The Traffic section contains statistics similar to those discussed in “Wireless Statistics for Stations” on page 13-12:
- **Pkts per second**
- **Throughput** in Mbps
- **Avg. Bit Speed** in Mbps
- **% Non-unicast pkts**

These statistics apply to all wireless traffic associated with this module and are divided into statistics for the last 30 seconds (in black) and the last hour (in blue). The Traffic section also divides statistics into traffic received and traffic transmitted.
You can use the **RF Status** section to monitor the quality of radio media on a network-wide level, and you can use the **Errors** section to look for problems with congestion or interference. You can then examine these statistics for radios or for WLANs to pinpoint the source of a problem.

The **RF Status** includes these statistics:
- **Avg Station Signal (dBm)**—average signal level detected for all stations associated to the Wireless Edge Services xl Module
- **Avg Station Noise (dBm)**—average background noise for all stations associated to the module
- **Avg Station SNR (dBm)**—average SNR for all stations associated to the module

In the **Errors** section, the Web browser interface reports the total number of error packets for this Wireless Edge Services xl Module:
- **Avg Number of Retries**—average number of attempts to transmit a packet to a station
- **% Gave Up Pkts**—number of packets that the Wireless Edge Services xl Module never successfully transmitted to a station
- **% of Undecipherable Pkts**—percentage of packets received that could not be deciphered

A high percentage might indicate that someone is attempting to guess a static WEP key or WPA/WPA2 PSK.

**Radio Port Adoption Statistics**

To view information about all RPs detected by this Wireless Edge Services xl Module, select **Device Information > Radio Adoption Statistics**.
Select the **Adopted RP** tab to view the RPs that the module has actually adopted, and the **Unadopted RP** tab to view other detected RPs.

The number of RPs adopted by this module is listed at the bottom of the **Device Information > Radio Adoption Statistics > Adopted RP** screen.

For each adopted RP, the screen lists:

- **Base Radio MAC**—This is the MAC address on the RP's Ethernet interface.
- **Model**—The Wireless Edge Services XL Module adopts only ProCurve Radio Ports 210, 220, or 230.
- **Serial**—The serial number is unique to this device.
- **HW Version**—This column indicates the hardware used by the RP.
- **IP Address**—This column displays an IP address if you have configured Layer 3 adoption for RPs. For more information about Layer 3 adoption, see Chapter 2: Configuring the ProCurve Wireless Edge Services XL Module.
- **Bootloader**—This column indicates the software from which the RP boots. The RP requires version 2 bootloader code for Layer 3 adoption. The RP automatically downloads new bootloader code when it is adopted by a module running a more recent version of the software.
Wireless Network Management
Monitoring the Wireless Network

- **Protocol Version**—RPs and the Wireless Edge Services xl Module communicate with a particular protocol. If an RP experiences problems, you should verify that the two devices’ protocol versions match. Also check the hardware version and the bootloader version.

- **SW Version**—You should verify that the software version with which the RP loads is up-to-date.

- **Radio Indices**—The RP includes one or two radios. These radios are listed on the **Network Setup > Radio > Configuration** screen according to the indices displayed in this column. You can configure settings for these radios on that screen. (See *Chapter 3: Radio Port Configuration*.)

If you have configured manual radio adoption, the module may detect RPs that it is not authorized to adopt. These RPs are listed on the **Device Information > Radio Port Adoption Statistics > Unadopted RP** screen. (See Figure 13-25.)

<table>
<thead>
<tr>
<th>Unadopted RP</th>
<th>Index</th>
<th>MAC Address</th>
<th>Last Seen (In Seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3201c-24-6c-4e</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3201c-24-6c-40</td>
<td>131</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3201c-24-6c-42</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Number of unadopted RPs: 3

**Figure 13-25.Device Information > Radio Adoption Statistics > Unadopted RP Screen**

You should review this screen to determine whether you need to manually add an unadopted RP (see *Chapter 2: Configuring the ProCurve Wireless Edge Services xl Module*) or find and remove an unauthorized RP. The screen lists this information:

- **Index**—RPs are listed in the order in which they are detected.

- **MAC Address**—This is the MAC address on the RP’s Ethernet interface.

- **Last Seen (In Seconds)**—View this setting to determine how recent the information about this RP is.
AP Detection

People may introduce unauthorized APs into your network for several reasons.

Sometimes attackers set up rogue APs in your environment, hoping to lure wireless users to authenticate to them instead of to your network’s RPs. In this way, attackers can collect sensitive information, including passwords with which they can then access your private network and view, steal, or damage data.

More commonly, users introduce APs for their own convenience, not meaning any particular harm. However, because users often take inadequate measures to secure these APs, the unauthorized APs open vulnerabilities for hackers to exploit.

The ProCurve RPs 210, 220, and 230 can listen for such unauthorized APs, collecting information about them to be sent to the Wireless Edge Services xl Module.

The module helps you to manage this information. You can even configure the module to automatically send an alarm when an unauthorized AP is detected.

**Note**

AP detection tracks devices that are *not* connected, either directly or indirectly, to the Wireless Edge Services xl Module. It does not prevent unauthorized RPs from being adopted. To control RPs that connect to your network, you must configure the module’s adoption settings as described in *Chapter 2: Configuring the ProCurve Wireless Edge Services xl Module*.

You can enable and manage AP detection from the **Special Features > Access Point Detection** screen, which is shown in Figure 13-26.
AP Detection

By default, AP detection is disabled. To configure AP detection, you must complete two main steps: you must enable AP detection, and you must configure at least one radio to scan for APs.

When you configure a radio to scan for APs, you can select one of these options:

- **Single-channel scan for Unapproved APs**—If you select this option, the radio listens for beacons from other APs operating on its own channel. When a radio hears such a beacon, it forwards information in the beacon to the Wireless Edge Services x1 Module. The radio can send and receive traffic from associated wireless stations at the same time it listens for beacons from APs.

- **Dedicate this Radio as a Detector**—If you select this option, the radio constantly scans for neighboring APs. Such a radio is called a detector, and it cannot connect to wireless stations. A detector uses auto channel select (ACS) to change to and scan all channels that are:
  - in its frequency (either 802.11a’s 5 GHz or 802.11bg’s 2.4 GHz)
  - allowed by its country’s regulations

Table 13-1 and Figure 13-27 compare single-channel detectors and dedicated detectors.
### Table 13-1. Comparing Single-Channel Detectors and Dedicated Detectors

<table>
<thead>
<tr>
<th>Single-Channel Detector</th>
<th>Dedicated Detector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio passively listens for beacons</td>
<td>Radio actively sends probe requests</td>
</tr>
<tr>
<td>Radio listens on its own channel only</td>
<td>Radio sends probes on all channels in its frequency that are allowed by its country’s regulations</td>
</tr>
<tr>
<td>Radio supports wireless stations</td>
<td>Radio does not support wireless stations</td>
</tr>
</tbody>
</table>

![Diagram of AP Detection](image)

**Figure 13-27.** AP Detection on Single-Channel Detectors and Dedicated Detectors
You can configure a radio as a single-channel detector or a dedicated detector in one of two ways:

- as part of an override configuration for a particular radio
  
  For example, your organization might install an RP that is entirely dedicated to searching out rogue APs.
  
  Another reason to dedicate a radio as a detector is so it can monitor all nearby RPs in your wireless network and take action if an RP experiences problems. See “Network Self Healing” on page 13-88 for more information on how detectors participate in neighbor recovery.

- as part of the radio adoption default configuration for all radios of a certain type
  
  If your network does not include any stations that use, for example, 802.11a mode, then you could dedicate all 802.11a radios to scanning for rogue APs. (Note, however, that these radios will only detect APs operating on an 802.11a channel.)

---

**Note**

You can enable the detector option in both radio adoption default configurations as a security measure. In this case, all RP radios are adopted as detectors. Thus, a radio cannot forward wireless traffic into your network until you determine that it is authorized to do so and explicitly disable the detector option on it.

---

To configure AP detection, complete the following steps:

1. Enable AP detection.
   
   a. Select **Special Features > Access Point Detection > Configuration.**
b. Check the **Enable** box.

c. Customize the timeout setting for approved and unapproved APs. (For more information about approved and unapproved APs, see “Creating Lists of Detected APs” on page 13-46.)
   - **Approved AP timeout**—specifies how long the module retains information about APs that you have defined as allowed.
   - **Unapproved AP timeout**—specifies how long the module retains information about APs that are not allowed.

   Enter a time from 1 through 65,535 seconds (approximately 18 hours), or accept the default setting of 300 seconds (five minutes).

d. Click the **Apply** button.

2. Configure a particular radio or radios to scan for APs.

   a. Select **Network Setup > Radio > Configuration**.

   b. Select the radio or radios.

   c. Click the **Edit** button. The **Configuration** screen for the radio is displayed. (See Figure 13-29.)
d. On the radio's **Configuration** screen, check the option that you want for AP detection:
   - **Dedicate this Radio as a Detector**
   - **Single-channel scan for Unapproved APs**

e. Click the **OK** button.
The radio state should now be listed as Detector on the Network Setup > Radio > Configuration screen, as shown in Figure 13-30.

**Note**

The Wireless Edge Services xl Module stores the configuration for a particular radio with its MAC address so that this configuration persists even if the radio powers down.

For more information on radio configurations, see Chapter 3: Radio Port Configuration.

3. Configure all radios of a particular type to scan for APs.
   a. Select Network Setup > Radio Adoption Defaults > Configuration.
Wireless Network Management
AP Detection

Figure 13-31. Network Setup > Radio Adoption Default > Configuration Screen

b. Select the radio type (802.11a, 802.11b, or 802.11bg).

c. Click the Edit button.

d. On the radio type’s Configuration screen, check the option that you want for AP detection:
   – Dedicate this Radio as a Detector
   – Single-channel scan for Unapproved APs

e. Click the OK button.

4. Click the Save link at the top of the screen to save your changes to the startup-config.

Creating Lists of Detected APs

AP detection simply enables RPs to report the APs that they detect. The Wireless Edge Services xl Module then sorts the detected APs into approved and unapproved lists.

By default, the module considers all APs to be unallowed, which means that they are displayed on the unapproved list.
You should configure the module to allow APs that meet certain criteria—for example, that are part of your wireless network. The module then moves these APs to an approved APs list so that they do not clutter the unapproved list and make it difficult for you to identify actual threats to network security.

You can use two criteria to define allowed APs:

- MAC address
- SSID

For example, you can list the MAC address of every AP and RP in your network (not connected to this module) and allow those addresses. Or, you can simply allow all APs and RPs that are members of one of your network's WLANs (as defined by the SSID). These solutions are appropriate only in a relatively secure environment.

For tighter security, you can force the module to match APs to both a MAC address and an SSID. For example, a rogue AP might mimic your network's SSID; if you allow all APs using that SSID, then you will overlook this security hazard.

You specify these criteria in a series of up to 200 rules, each identified by an index number. Each rule can specify one of the following:

- one MAC address
- one SSID
- one MAC address and one SSID

For example, if you want to use hardware-based rules to allow APs and your network includes 14 RPs adopted by a different module and two APs, then you must create 16 rules.

Creating Rules That Define Allowed APs

To create a rule, complete these steps:

1. Select **Special Features > Access Point Detection > Configuration**. The screen displays, in the **Allowed APs** section, the APs that are currently allowed, listed in order of index number.

   This section shows the **rules** for allowed APs. Your RPs may or may not detect the APs in question at the moment.
Wireless Network Management
AP Detection

Figure 13-32. Viewing Allowed APs

2. Click the **Add** button.

3. In the **Index** field, enter a value from 1 through 200. Each rule must have a unique index.

   By default, the field displays the next available index number.

4. Create one of the three types of rules:
   a. Allow an AP with a particular MAC address no matter what WLAN it supports, as shown in Figure 13-33:
      i. Select the second field under **Radio MAC Address** and then enter the address.
      ii. Under **SSID**, keep the selection at **Any SSID**.

<table>
<thead>
<tr>
<th>Index</th>
<th>BSS MAC Address</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00:14:22:40:08:14</td>
<td>Any SSID</td>
</tr>
</tbody>
</table>
b. Allow any AP that is a member of a particular WLAN, as shown in Figure 13-34:
   i. Select the second field under SSID and then enter the WLAN’s SSID.
   ii. Leave the Radio MAC Address selection at Any MAC Address.
Wireless Network Management
AP Detection

c. Allow a particular AP only if it is a member of the correct WLAN, as shown in Figure 13-35:
   i. Select the **Radio MAC Address** field and then enter the address.
   ii. Select the **SSID** field and then enter the WLAN’s SSID.

![Figure 13-35. Allowing a Particular AP in a Particular WLAN](image)

5. Click the **OK** button.

The AP is now listed in the **Allowed APs** section of the **Special Features > Access Point Detection > Configuration** screen.

**Monitoring Detected APs**

You should periodically check the unapproved APs list for rogue APs. You may also want to configure the Wireless Edge Services xl Module to automatically generate and send an alarm whenever a radio detects an unapproved AP.

**Managing the Unapproved APs List**

Select **Special Features > Access Point Detection** and click the **Unapproved APs** tab to view a list of detected APs not expected in your environment. (In other words, this list displays any APs that the rules do not allow.)
As shown in Figure 13-36, the list includes the following information for each AP:

- **BSS MAC Address**—This address is the AP’s BSSID. RPs report each BSSID that is a source of a beacon as a detected AP. Because an AP might send beacons using several different BSSIDs, RPs might report the same physical AP several times.

- **Reporting Radio**—This is the index for the adopted radio that detected this AP. This information can help you pinpoint a rogue AP's location.

- **Channel**—This is the channel on which the detected AP operates.

- **Signal Strength (In dBm)**—This field lists the detected AP’s signal strength, expressed in dBm. This information can help you determine how close the AP is to the reporting radio.

---

Figure 13-36.Viewing the Unapproved APs List

**Note**

You can also view this list by selecting Device Information > Access Point Detection and clicking the Unapproved APs tab. However, you can only view information about APs on the other screen; you cannot allow the APs as described below.
Wireless Network Management
AP Detection

- **Last Seen (In Seconds)**—This column indicates how recent the information is.
- **SSID**—If a radio has an unapproved MAC address but one of your WLAN’s SSIDs, this may signal a hacker phishing for passwords and other sensitive data.

If this list becomes too long and unmanageable, you should take one or more of these steps:
- Lower the timeout value for unapproved APs. (See “Configuring AP Detection” on page 13-40.)
- Move legitimate APs to the approved APs list.

**Allowing an Unapproved AP.** Not all APs in the unapproved list are necessarily rogue APs. Some may be APs adopted by another module or APs that belong to your organization; others may belong to legitimate neighboring organizations.

To move an AP to the approved list, complete these steps:

1. Select the AP and click the **Allow** button. The **Add Allowed AP** screen is displayed.

   As shown in Figure 13-37, the Web browser interface automatically fills in the AP’s MAC address and SSID. It also fills in the next available index number.

![Figure 13-37. Add Allowed AP Screen](image)
2. If you so desire, you can change these settings. (For example, you could allow the MAC address, but any SSID.)

3. Click the **OK** button.

In a way, allowing an AP is like acknowledging an alarm. You are letting other administrators know that you have checked the potential threat. This feature is particularly useful for allowing APs that do not belong to your network—so you cannot create a rule to allow them in advance—but that you have verified as legitimate APs in a nearby organization.

**Managing the Approved APs List**

You should also periodically check the approved APs list to make sure that no rogue APs have been added.

You can view this list in two ways:

- Select **Special Features > Access Point Detection** and click the **Approved APs** tab.
- Select **Device Information > Access Point Detection > Approved APs**.

The approved APs list includes all detected APs that match the criteria for one of the rules on the **Allowed APs** screen. For each AP, the list displays information similar to that in the unapproved list, as shown in Figure 13-38.

<table>
<thead>
<tr>
<th>Special Features &gt; Access Point Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>BSSID/MAC Address</td>
</tr>
<tr>
<td>10:10:00:AF:BC:60</td>
</tr>
<tr>
<td>10:10:00:AF:BC:61</td>
</tr>
</tbody>
</table>

![Figure 13-38.Managing the Approved APs List](image)
Wireless Network Management
AP Detection

If a rogue AP is on this list, you should reconfigure the rule that allowed it. For example, to screen APs you may need to use MAC addresses instead of, or in addition to, SSIDs.

Configuring the Module to Report Unapproved APs

You can configure the Wireless Edge Services xl Module to trigger a Simple Network Management Protocol (SNMP) trap whenever a radio detects an unapproved AP.

Complete these steps:
1. Select **Management > SNMP Trap Configuration > Configuration**.

![Figure 13-39. Management > SNMP Trap Configuration > Configuration Screen](image)

2. Expand the **Wireless** heading and then the **RP Detection** heading.
3. Click the **Enable all sub-items** button.
4. Make sure that the **Allow Traps to be generated** box is checked.
Figure 13-40. Enabling an SNMP Trap for AP Detection

5. Click the **Apply** button.

If an RP detects an external AP, a log is displayed on the **Device Information > Alarm Log** screen, as shown in Figure 13-41.
Wireless Network Management

AP Detection

Figure 13-41. Receiving an Alarm about an External AP

The module will log the alarm, as well as forward it to a trap receiver (if one has been specified). (For instructions on configuring the trap receiver, see Chapter 2: Configuring the ProCurve Wireless Edge Services xl Module.)
Configuring Station Intrusion Detection

AP detection protects your network against unauthorized APs. The Wireless Edge Services xl Module can also guard against hackers who use stations to launch attacks. Using station intrusion detection, the module monitors stations for suspicious behavior that might indicate an attack such as the following:

- **Reconnaissance attack**—An attacker sends probes to discover APs and the stations that are associating with those APs. Using the information discovered, the attacker can launch additional attacks.

- **Association flood attack**—An attacker spoofs multiple clients, sending so many association requests that the AP cannot handle them all. The AP begins to deny additional associations.

- **Disassociation flood attack**—After launching a reconnaissance attack, the attacker identifies the stations attached to a particular AP. The attacker then masquerades as the AP and sends disassociation frames to the stations. Although the stations quickly re-associate with the AP, the attacker continues to send disassociation frames to end the stations’ sessions.

- **Authentication failure attack**—The attacker uses a tool to masquerade as an AP. When a station submits its login credentials, the attacker sends an authentication failed message to the station. The station then removes itself from the WLAN. An attacker may also launch this attack by spoofing a station, sending invalid login credentials. The AP then denies the station access to the WLAN.

- **802.11 replay attack**—The attacker captures and resends legitimate frames. This attack can be used to overwhelm the network, spoof a legitimate user, or learn additional information about the network.

- **Decryption attack**—If an attacker is trying to crack the encryption used on your WLAN, your AP will receive a high number of encryption failures.

- **EAP start frame attack**—An attacker floods the AP with EAP start frames, causing the AP to allocate resources for each session. Eventually, the attack consumes all of the AP’s resources, creating a DoS.

- **TKIP attack**—An attacker tries to alter a frame and bypass the Michael integrity check. TKIP is designed to take countermeasures against such attacks, such as closing the session or refreshing the master key.

When a station exhibits a potentially harmful behavior, the Wireless Edge Services xl Module filters all traffic from the station for a certain period.
Configuring Station Intrusion Detection

To configure station intrusion detection, complete these steps:

1. Select **Special Features > Station Intrusion Detection > Configuration**.

2. In the **Detection Window** field, enter a value from 5 through 300 seconds. This setting determines the length of time to which each threshold applies. For example, if the threshold for **Excessive Probes** is 60 and the **Detection Window** is 10 seconds, the Wireless Module will count how many probes it detects in each 10-second time period.

3. Set the **Station** threshold for each field. Enter a number from 0 through 65,535. The Wireless Edge Services xl Module will apply this threshold to each station.

4. Set a **Radio** threshold and a **Wireless Module** threshold for:
   - **Excessive Probes**
   - **Excessive Association**
Wireless Network Management
Configuring Station Intrusion Detection

- Excessive Disassociation
- Excessive Authentication failure
- Excessive Crypto replays
- Excessive 802.11 replays
- Excessive Decryption failures
- Excessive Unassociated Frames
- Excessive EAP Start Frames

Again, enter a number from 0 through 65,535.

5. In the **Time to Filter** field, enter a time from 0 through 86,400 seconds to control how long the module will filter, or block, traffic from a station that exceeds a threshold. The default time is 60 seconds.

6. Click the **Apply** button.

Configuring the Module to Report Station Intrusion

You can also configure the module to send an alarm when it detects station intrusion. To configure this SNMP trap, complete these steps:

1. Select **Management** > **SNMP Trap Configuration** > **Configuration**.
2. Expand the **Wireless** heading and then the **Intrusion Detection** heading.
3. Select **Intrusion Detection** and click the **Enable all sub-items** button. (Alternatively, select one of the sub-items and click the **Enable** button.)

4. Make sure that the **Allow Traps to be generated** box is checked.

5. Click the **Apply** button.

The module will log the alarm, as well as forward it to a trap receiver (if one has been specified). (For instructions on configuring the trap receiver, see *Chapter 2: Configuring the ProCurve Wireless Edge Services xl Module*.)
Viewing Blocked Stations

If a station exceeds the thresholds that you set, the Wireless Edge Services xl Module blocks the station. You can view any stations that have been blocked by selecting Special Features > Station Intrusion Detection and clicking the Filtered Stations tab.

![Figure 13-44.Special Features > Station Intrusion Detection > Filtered Stations Screen](image)
Logging and Alarms

The Wireless Edge Services xl Module generates logs for various events that occur on a system; these logs report on messages that the module receives and actions that the module takes. The module can log events to:

- its buffer
- the console
- an external server

Events are ranked according to severity, as shown in Table 13-2. The lower the number, the greater the risk to network functionality.

**Table 13-2. Event Severity**

<table>
<thead>
<tr>
<th>Level</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergency</td>
</tr>
<tr>
<td>1</td>
<td>Alert</td>
</tr>
<tr>
<td>2</td>
<td>Critical</td>
</tr>
<tr>
<td>3</td>
<td>Error</td>
</tr>
<tr>
<td>4</td>
<td>Warning</td>
</tr>
<tr>
<td>5</td>
<td>Notice</td>
</tr>
<tr>
<td>6</td>
<td>Info</td>
</tr>
<tr>
<td>7</td>
<td>Debugs</td>
</tr>
</tbody>
</table>

The Wireless Edge Services xl Module can also log alarms, which it receives when an SNMP trap is triggered. These alarms are stored in the module's local alarm log; the module can also forward alarms to an external server.
Table 13-3. Logged Events and Alarms

<table>
<thead>
<tr>
<th>Logged Events</th>
<th>Alarms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triggered when an event occurs on the module:</td>
<td>Triggered when an SNMP trap is generated</td>
</tr>
<tr>
<td>- the module receives a message</td>
<td></td>
</tr>
<tr>
<td>- the module takes an action</td>
<td></td>
</tr>
<tr>
<td>Can be sent to:</td>
<td>Can be sent to:</td>
</tr>
<tr>
<td>- the module’s local buffer (log file)</td>
<td>- the module’s local alarm log</td>
</tr>
<tr>
<td>- the CLI console</td>
<td>- an external SNMP server</td>
</tr>
<tr>
<td>- an external syslog server</td>
<td>Events are logged or not depending upon severity</td>
</tr>
<tr>
<td>Alarms are generated or not depending upon whether the corresponding trap type is enabled</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Logging

To configure logging, select Management > System Logging > Log Options.

Enabling Logging

As shown in Figure 13-45, logging is enabled by default, and the Wireless Edge Services xl Module logs events to:

- **Its buffer**—The module saves events that have collected in the buffer to its local log as they occur. Viewing this log is described in “Viewing Events in the Local Log File” on page 13-65. You can disable this feature by unchecking the Enable logging to Buffer box.

  By default, the module logs all events of severity level 3 or lower (more severe)—that is, all events from severity level 0 through level 3. You can raise or lower this level according to the needs of your network by selecting a level in the Enable logging to Buffer drop-down menu. Keep in mind that the higher the level, the more events through which you will have to search.

- **The console**—If you are managing your module through the console port, events will appear on the command line as they occur. You can disable this feature by unchecking the Enable logging to Console box. By default, events of severity level 3 or lower (more severe) are listed; you can raise or lower this setting.
Wireless Network Management
Logging and Alarms

**Figure 13-45.Configuring Logging**

You can configure the module to store events for up to 60 seconds before logging them, by entering a value in the *Logging aggregation time* field. (If the value is 0, then events are logged immediately.)

**Forwarding Logs to an External Server**

You can also configure the Wireless Edge Services xl Module to forward logs to up to three external syslog servers. Complete these steps:

1. Select *Management > System Logging > Log Options.*
2. Check the Enable logging to Syslog Server box.

3. From the corresponding drop-down menu, select the lowest severity for logs that the module will forward. The default level is level 6, Info.

4. In the Server Facility field, use the drop-down menu to select the facility that your syslog server uses to receive such logs. Local7 is typically reserved for network devices.

5. In one of the Server fields, enter the server's IP address. You can specify up to three syslog servers.

6. Click the Apply button.

Viewing Events in the Local Log File

To view the events that the Wireless Edge Services xl Module has stored in its own log file, select Management > System Logging and click the File Mgmt tab.
The top section of the screen displays files of logs that the module has stored. Each file is identified by its name, its size in bytes, the time at which it was created, and the time at which it was last modified (that is, when a new event was added to it).

The local log file stores the events that the Wireless Edge Services xl Module logs to its buffer.

You can view the types of events in a file by selecting the file. The preview id displayed in the bottom section of the screen, as illustrated in Figure 13-47.

Figure 13-47.Management > System Logging > File Mgmt Screen

To view the actual log file with all saved events, select the file and click the View button. A screen similar to the one shown in Figure 13-48 is displayed.
The most recent events are listed at the top of the screen. The color code helps you to quickly identify the most important events (that is, those with the lowest level, or greatest severity).

For each event, the log reports:

- **Time stamp**—Remember to look at the time stamp to make sure that you are not examining obsolete logs. (Quickly checking the time stamp when you preview the log file can also save you time.)

- **Module**—The module indicates which part of the system has reported this event. (Different modules report different types of activity.)

- **Severity**—It is often important to focus quickly on the most severe events, which, as mentioned above, the color code helps you to do.
Wireless Network Management
Logging and Alarms

- **Mnemonic**—This field includes an abbreviated identification of the type of event.
- **Description**—The description gives you the most information about the event.

You can click on any column heading to organize events according to the information in that column. The bottom of the screen shows you which line in the log file that you are currently examining.

You can also enter a value in the field at the bottom of the screen to quickly move to another page in the log.

Note that the Wireless Edge Services XL Module will continue to save events to this log. You can view newly saved events without leaving this screen by clicking the **Refresh** button.

Click the Close button to close the log and return to the Management > System Logging > File Mgmt screen.

Deleting and Transferring the Local Log File

If you are certain that neither you nor other administrators need to review the events in the log, you can select the log file on the Management > System Logging > File Mgmt screen and click the **Clear Buffer** button. The module erases the contents of the file, allowing you to focus on the most important events.

If the buffer should become full, the next event will overwrite the oldest (least recent) event.

It is often a good idea to store a copy of the log remotely before you clear it. Your organization might also have a policy of periodically collecting device information and storing it on a central server.
To transfer the local log file, complete these steps:

1. Click the **Transfer Files** button. The **Transfer** screen is displayed.

![Figure 13-49. Transferring Log Files to a Server or Workstation](image)

2. In the **From** field in the **Source** section, use the drop-down menu to select **Wireless Services Module**. In the **File** field, use the drop-down menu to select the log file that you want to transfer.

3. Select the destination for the file. You can save the log to your workstation or to a remote server:
   
a. To save the log to your workstation, in the **To** field, use the drop-down menu to select **Local Disk**.
      
      You can then enter the filename in the **File** field and click the **Browse** button to select the destination for the file.

   b. To save the log to a remote server, in the **To** field, use the drop-down menu to select **Server**. Then enter this information in the fields below:
      
      - **File**—Name the file on the remote server. (This name can be different from that of the source file.)
      - **Using**—Use the drop-down menu to select the type of server. You can use a TFTP or an FTP server.
      - **IP Address**—Specify the server’s IP address.
      - **User ID** and **Password**—FTP servers may require you to enter the correct username and password.
Path—Enter the path for the directory in which the destination file should be saved. Depending on your server, you may or may not need to enter / before the directory name. Leave this field empty (or simply enter /) to save the file to the server’s default directory.

4. Click the Transfer button.

Managing the Alarm Log

In order for the Wireless Edge Services xl Module to log an alarm, you must activate the corresponding trap. See “SNMP Traps” on page 2-112 of Chapter 2: Configuring the ProCurve Wireless Edge Services xl Module for information on setting these traps. When an enabled trap is triggered, the module generates an entry in its alarm log. If you have configured an SNMP server, the module will also send the alarm to it.

View the alarm log by selecting Device Information > Alarm Log.

A list of alarms that the module has logged is displayed, as shown in Figure 13-50.

For each alarm, the screen displays this information:

- **Index**—Alarms are numbered in the order in which they were received.

![Figure 13-50.Viewing the Alarm Log](image-url)
Wireless Network Management
 Logging and Alarms

- **Status**—If the alarm has been acknowledged, then an administrator has seen it and presumably dealt with it.

- **Time Stamp**—Among other purposes, you can view the time stamp to:
  - check whether a problem is ongoing
  - look for the cause of a behavior that you know occurred at a particular time
  - track patterns of activity
  - determine the duration of a problem

- **Severity**—Severity signals the relative threat to network functions and security.

- **Module Name**—You can use the name of the module that reported the alarm to point you toward the cause.

- **Type**—You should quickly focus on this information, as it is, in many ways, the alarm. It indicates the type of problem or behavior.

- **Message**—The message, which varies according to the alarm’s type, includes specific information about the particular event. For example, the message for the “radiusAuthFailed” alarm is the MAC address of the station that failed to authenticate and the radio to which the station attempted to connect. You could use this information to track down the station.

By default, the alarm log lists alarms according to index number. However, you can sort the alarms according to any of the information described above, by simply clicking on the heading for the column.

For example, you might want to focus on only the most serious events. Click Severity and scroll to the top of the list to view the most crucial alarms.

Or, if you are troubleshooting a particular problem, you might want to group alarms by Module Name—to see, for example, all the logs associated with wireless stations when you are troubleshooting a station having difficulty with its connection.

You can take action on alarms using the four buttons at the bottom of the screen:

- Details
- Delete
- Acknowledge
- Export
Details

When you do not know what an alarm means, or when you need direction in solving the problem indicated, you should view alarm details.

Select the alarm from the list, and then click the Details button. The screen that is displayed points you toward the cause of the alarm and possible solutions for an associated problem. (See Figure 13-51.)

![Figure 13-51.Viewing Alarm Details](image)

General information that applies to all alarms of this type is listed in the Alarm Details section. The interface explains what the alarm means and suggests possible solutions or causes. For example, details for a “radiusAuthFailed” alarm suggest that you verify that your Wireless Edge Services xl Module can connect to its RADIUS server.

The Alarm Message shows information specific to this alarm—in Figure 13-51, identifying the station that failed to authenticate. Other information specific to the log is listed throughout the screen, with the time stamp at the top and the status at the bottom.

Delete

You should periodically delete from the log alarms that are unimportant or no longer relevant, so that you can easily focus on the most current alarms. For example, you could group alarms by time stamp, use the Shift key to select all events before a particular date, and then click the Delete button.
Sometimes you will want to store an alarm in the log even after you have viewed it, either because you want another administrator to see it or because you want to track a particular pattern of activity. In this case, instead of deleting the alarm, you should click the **Acknowledge** button to change its status.

You should only acknowledge an alarm, of course, if you have addressed any associated problems; otherwise, other administrators may also neglect to do so.

**Export**

The Wireless Edge Services xl Module allows you to save logged information to your workstation. This useful feature lets you:

- save information that might be important later, while keeping the log clear for future events
- send a file of alarms to support staff for troubleshooting help
pool information from multiple devices in a central location
- track patterns of network activity

To export the information in one or more alarms, select those alarms and click the Export button. On the screen that is displayed, select a filename and a location for the logs, which are saved as a comma-separated file.

---

**MAC Filters (Local MAC Authentication)**

The Wireless Edge Services xl Module can control which wireless stations connect to a WLAN according to their MAC, or hardware-based, addresses. You configure standard MAC ACLs, or filters, and the module blocks stations denied by those ACLs before they can authenticate and associate with the WLAN.

MAC authentication can act by itself or in conjunction with another form of authentication. For example, you could configure ACLs for MAC authentication and apply them to a WLAN; you could also enable Web authentication on that WLAN. When a station attempts to connect to the WLAN, the module first checks the station’s MAC address. If the ACLs allow the station, the module lets the station proceed to associate to the WLAN and complete the Web authentication.

MAC authentication is particularly important with Web authentication because without it, stations can actually connect to the WLAN before they authenticate.

The module supports up to 1,000 ACLs, each of which can specify a range of MAC addresses.

To configure MAC authentication, complete these steps:

1. Configure one or more filters, or ACLs.
2. Configure WLAN memberships for each ACL.

**Configuring MAC Standard ACLs (Filters)**

When configuring ACLs on the module, keep these rules in mind:

- ACLs are ordered by index number.
The module processes ACLs that are applied to a WLAN starting with the ACL that has the lowest index number. The module stops processing the ACLs as soon as it finds a match for the station’s MAC address.

The module supports two types of ACLs:

- **Allow ACLs**—If the module matches a station to this ACL, it permits traffic from the station.
- **Deny ACLs**—If the module matches a station to this ACL, it blocks all traffic from the station, and the station cannot associate to the WLAN.

By default, the module allows all stations. Unless you explicitly deny a station in an ACL, it can connect.

You will generally follow one of two strategies for MAC authentication:

- Deny all stations except a select group of authorized stations.
  
  In this case, you should create one or more allow ACLs that specify the group of authorized stations. Then you should create a deny ACL that specifies all stations (00-00-00-00-00-01 through FF-FF-FF-FF-FF-FE). The index numbers for the allow ACLs must be lower than that for the deny ACL.

- Allow all stations except a select group of unauthorized stations.
  
  In this case, you should create one or more deny ACLs that specify the MAC addresses of unauthorized stations. You do not need to create an allow ACL, because allowing all stations is the module’s default behavior.

You can, of course, also combine the strategies—for example, deny a station with a range of allowed stations.

To configure an ACL, complete these steps:

1. Select **Security > MAC Filters**.
MAC Filters (Local MAC Authentication)

2. Click the **Add** button. The **Add ACL** screen is displayed.

![Add ACL Screen](image-url)
Wireless Network Management
MAC Filters (Local MAC Authentication)

3. Enter a value from 1 through 1,000 in the **Station-ACL Index** field. Each ACL must have a unique index number. Pay close attention to this number because, when a station matches more than one entry, only the entry with the lowest number affects the station.

4. Enter a range of MAC addresses, placing the first address in the **Starting MAC** field and the last address in the **Ending MAC** field. Every MAC address between the two is included in the list. You cannot add noncontiguous MAC addresses to the ACL; instead, you must create a new ACL.

5. Using the **Allow/Deny** drop-down menu, select whether the module will permit traffic from these stations (**Allow**) or block it (**Deny**).

6. Click the **OK** button.

The ACL is listed on the **Security > MAC Filters** screen.

**Configuring WLAN Memberships**

The ACL will not affect traffic until you associate the ACL with one or more WLANs. To do so, you make the ACL a member of those WLANs.

Complete these steps:

1. On the **Security > MAC Filters** screen, select the ACL.

   You can select multiple ACLs by holding down **Ctrl** as you select them.

2. Click the **Memberships** button. The **Edit Memberships** screen is displayed. (See Figure 13-55.)
3. Check the boxes for the WLANs to which you want to apply the ACL.

WLANs are displayed by index (not SSID). The module will use the ACL to filter traffic on the selected WLANs.

If you have selected multiple ACLs, they are listed in separate columns by index number. (See Figure 13-56.)
4. Click the OK button.

When you select this ACL on the Security > Wireless Filters screen, the selected WLANs appear in the Associated WLANs section. (See Figure 13-57.) In this screen, you can view the WLAN's SSID, as well as other security options for that WLAN.
Wireless Network Management
MAC Filters (Local MAC Authentication)

Security > MAC Filters

<table>
<thead>
<tr>
<th>Station ACL Index</th>
<th>Starting MAC</th>
<th>Ending MAC</th>
<th>Allow/Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00-0E-35-34-12-B3</td>
<td>00-0E-35-34-12-B3</td>
<td>Deny</td>
</tr>
<tr>
<td>2</td>
<td>00-00-00-00-00-27</td>
<td>00-00-00-00-00-27</td>
<td>Allow</td>
</tr>
<tr>
<td>3</td>
<td>00-0E-35-48-12-B1</td>
<td>00-0E-35-48-12-B1</td>
<td>Allow</td>
</tr>
<tr>
<td>100</td>
<td>FF-FF-FF-FF-FF-FF</td>
<td>FF-FF-FF-FF-FF-FF</td>
<td>Deny</td>
</tr>
</tbody>
</table>

Associated WLANs

<table>
<thead>
<tr>
<th>WLAN Index</th>
<th>SSID</th>
<th>Authentication</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MyWLAN</td>
<td>Web-Auth</td>
<td>None</td>
</tr>
</tbody>
</table>

Figure 13-57. Associating ACLs with WLANs

Note that it is possible to prevent a station from associating to one WLAN but to allow the station to associate to another.

Just as you can make an ACL a member of more than one WLAN, you can associate more than one ACL to a WLAN. The module filters traffic first against the ACL with the lowest index number, then against the ACL with the next lowest number, and so on. Parsing stops with the first successful match to an ACL.

In Figure 13-57, network administrators have created four ACLs. The first ACL denies a single station, the second and third ACLs allow stations, and the fourth ACL denies all stations. The network administrators made all these ACLs members of the WLAN called MyWLAN.

With this configuration, only the stations allowed by ACLs 2 and 3 can connect to MyWLAN. Notice that the network administrators have numbered the ACL that denies all stations as 100. They can add ACLs to allow other stations,
and as long as these ACLs have an index number lower than 100, the Wireless Edge Services xl Module will process them before it processes the ACL that denies all stations.

Exporting and Importing MAC Standard ACLs (Filters)

You can export the MAC standard ACLs (filters) configured on the Wireless Edge Services xl Module to the local disk of the management station. Exporting the ACLs enables you to archive them and also to upload them to another device that needs to enforce the same policies.

The filters save as a .cvs file, which you can open with a spreadsheet application. This file includes four columns for information in the ACL:

- Station ACL Index
- Starting MAC
- Ending MAC
- Allow/Deny

The first line in the file lists these four names. Each subsequent line specifies the values associated with one of the exported ACLs.

You can also import a .cvs file to the Wireless Edge Services xl Module. In this way, you can quickly configure all of your modules with the same MAC standard ACLs. See “Importing MAC Standard ACLs” on page 13-83 for information on information that the .cvs file must include.

Exporting MAC Standard ACLs

To export the MAC standard ACLs configured on your module, follow these steps:

1. Select **Security > MAC Filters**.
2. Select the ACL that you want to export.

   If you want to export all of the ACLs in the same file, select an ACL and then press **Ctrl+A**.
Wireless Network Management
MAC Filters (Local MAC Authentication)

### Figure 13-58. Exporting ACLs

3. Click the **Export** button.

4. A dialog screen is displayed for saving the file to the local disk of your management station. Name the file and choose the directory in which to save it. Then confirm the save.

5. A screen reports that the export was successful. Click the **OK** button.

### Figure 13-59. Export Success Message
Importing MAC Standard ACLs

Instead of (or in addition to) manually configuring MAC standard ACLs (filters) on your Wireless Edge Services xl Module, you can import a .cvs file that includes these ACLs to your module. The file should be saved on the local disk of your management station.

You can create the ACLs file using a spreadsheet application. Include four columns for each ACL. Table 13-4 displays the information specified in that column and valid values for that column. The column number matters; in other words, the first column for each row must include a number from 1 to 1000, and this number specifies the ACLs index number.

Table 13-4. Required Information in a File To Be Imported to the Wireless Edge Services xl Module’s List of MAC Filters

<table>
<thead>
<tr>
<th>Column Number</th>
<th>Specifies</th>
<th>Valid Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Station-ACL Index—the order in which the module processes this ACL (as compared to other MAC standard ACLs)</td>
<td>1 to 1000</td>
</tr>
<tr>
<td>2</td>
<td>Starting MAC—first MAC address in the range of addresses selected by this ACL</td>
<td>any MAC address in AA-BB-CC-DD-EE-FF format</td>
</tr>
<tr>
<td>3</td>
<td>Ending MAC—final MAC address in the range of addresses selected by this ACL (often the same as the starting address)</td>
<td>any MAC address in AA-BB-CC-DD-EE-FF format</td>
</tr>
<tr>
<td>4</td>
<td>Allow/Deny—the action the module performs on selected stations (does or does not allow them to connect to the WLAN)</td>
<td>• Allow • Deny</td>
</tr>
</tbody>
</table>

Alternatively, you can configure ACLs on another module, export the ACLs to a .cvs file, and then import that file to your module.

When you import the file, the Wireless Edge Services xl Module saves each row in the imported file as an ACL in its list of MAC standard ACLs (filters). Your module can already have filters configured on it; the ACLs in the imported file are simply added to the list.

The new ACLs should have different index numbers than the current ACLs. If you want the imported ACLs to override the currently configured ACLs, you should delete those ACLs first.
To import MAC standard ACLs to your Wireless Edge Services xl Module, follow these steps:

1. Select Security > MAC Filters.
2. Click the Import button.

3. A dialog screen is displayed for choosing the file from the local disk of your management station. Find your file and confirm the import.

4. A screen reports the results of the import. If the import is completely successful, the message shown in Figure 13-61 is displayed.

If you see any errors, refer to “Resolving Import Errors” on page 13-85.
5. Click the **OK** button.

6. For the imported ACLs to take effect, you must assign them WLAN memberships:
   a. Select the new ACLs. You can select multiple ACLs by holding down **Ctrl** as you select them.
   b. Click the **Memberships** button.
   c. Check boxes to assign the ACLs to WLANs.
   d. Click the **OK** button.

   See “Configuring WLAN Memberships” on page 13-77 for more information.

**Resolving Import Errors.** When you attempt to import ACLs, the **ACL Import Result** screen may display one or more errors.

The errors are listed by the line in the .cvs file at which the error occurs.
Wireless Network Management
MAC Filters (Local MAC Authentication)

Figure 13-62.ACL Import Result Screen Error Messages

Errors include:

- messages informing you that a field contains an invalid value:
  
  - “ACL index must be an integer”
  - “Invalid starting MAC.”
  - “Invalid ending MAC.”
  - “ACL mode must be either Allow or Deny”

As explained earlier, each line in the file must include four fields with valid values for index number, MAC addresses, and ACL mode (allow or deny).

The screen in Figure 13-62 displays four such errors—all in line 1. In this case, the imported file is a file exported from another module. Exported files use the first line to list the names of columns rather than to specify an ACL. You can ignore the errors. Click OK, and the ACLs are imported to the module.

If the line indicated should specify an actual ACL, click the Cancel button. Open the file, find the line with the error, and make the correction. See Table 13-4 on page 13-83 for help in specifying correct values.

Then re-import the file, as described in “Importing MAC Standard ACLs” on page 13-83.

- “ACL index already exists - please choose another”
The ACL in the line indicated conflicts with an ACL already configured on the Wireless Edge Services xl Module. That is, they have the same index number.

Make one of two choices:

- Click the **OK** button, and import the file despite the conflict. The module retains all of its already-configured ACLs. However, any non-conflicting ACLs are imported normally.

- Click the **Cancel** button, and cancel the import. The module retains all of its already-configured ACLs, and no new ACLs are saved to the module. You can fix the problem in one of two ways:
  - If you want your Wireless Edge Services xl Module to keep its current ACLs, but also to receive all of the imported ACLs, edit the .cvs file. Change the index numbers so that they no longer conflict with those on the module.
    
    Then re-import the file, as described in “Importing MAC Standard ACLs” on page 13-83.
  
  - If you want the ACLs in the imported file to override already-configured ACLs, you must delete these ACLs from your Wireless Edge Services xl Module.
    
    In **Security > MAC Filters** screen, select the ACLs that conflict with imported ACLs. Click the **Delete** button.
    
    Then re-import the file, as described in “Importing MAC Standard ACLs” on page 13-83.
Network Self Healing

Self healing keeps your wireless network functioning optimally in response to changing conditions. A radio in a self-healing network can automatically change the properties of its RF network, which include:

- channel
- transmit power
- supported rates

By managing this ability, the Wireless Edge Services xl Module provides two basic services:

- **Neighbor recovery**—When radios detect that a neighbor has failed, they automatically adjust settings so that they can support as many of the stations associated with the failed radio as possible.
- **Interference avoidance**—Radios adjust their channel setting to avoid interfering with neighboring radios.

Neighbor Recovery

When enabled on the Wireless Edge Services xl Module, neighbor recovery can automatically configure radios to change their settings to compensate for another radio’s failure.

Both the Wireless Edge Services xl Module and RP radios monitor for failed radios. The RPs monitor neighbors by listening for beacons from RPs that they have learned that they can hear on their channel.

**Note**

Both single-channel detectors and dedicated detectors can monitor neighbors. However, dedicated detectors monitor all channels instead of just one. For this reason, it can be a good idea to configure one RP in a self-healing network as a dedicated detector (depending, of course, on the total number of RPs).

A radio “fails” in any of these circumstances:

- The module no longer recognizes the RP as adopted.

  In other words, the module and the RP cannot communicate, whether due to a physical or a logical problem.
Neighbors no longer receive beacons from the radio. An RP checks the beacons that it has received every 30 seconds. If the RP has not received beacons from a neighbor in the last two seconds, it reports that neighbor as down. In other words, an RP considers a neighbor failed when it loses contact with that neighbor for more than two seconds; however, the RP only checks whether it has lost contact with a neighbor every 30 seconds.

- Neighbors fail to detect Wireless Internet Service Provider (WISP) heartbeats from the radio.

## Enabling Neighbor Recovery

To enable neighbor recovery, complete these steps:

1. Select **Special Features > Self Healing > Configuration**.

   ![Special Features > Self Healing](image)

   **Figure 13-63. Enabling Neighbor Recovery**

   2. Check the **Enable Neighbor Recovery** box.

   3. Click the **Apply** button.
An RP radio only responds to the loss of a radio if that radio is defined as one of its neighbors. To further configure neighbor recovery, you must:

- specify neighbors
- specify the action that a radio takes if one of its neighbors fails

Select **Special Features > Self Healing** and click the **Neighbor Details** tab.

---

**Figure 13-64: Neighbor Relationships**

The screen lists all RP radios adopted by this module, displaying this information for each:

- **Radio Index**—index number
- **Description**—name
- **Type**—802.11bg or 802.11a
- **RP Ethernet MAC**—Ethernet MAC address for the RP that includes this radio
- **Action**—self-healing action when a neighbor fails
- **Neighbor Radio Indices**—neighbors' index numbers

When you first enable the self-healing feature, all radios display **None** in the **Neighbor Radio Indices** column.
You can configure the neighbors in one of two ways: manually or with automatic neighbor detection.

Specifying Neighbors Manually

Keep these concepts in mind as you configure neighbors:

- The neighbor relationship is reciprocal: if you configure a neighbor list on radio 1 that includes radio 3, radio 3’s neighbor list automatically adds radio 1. (See Figure 13-64.)

- However, the relationship is not communicative: if radio 1’s neighbor list includes both radio 3 and radio 4, radio 3’s list will include radio 1, but radio 3’s list will not include radio 4 unless you explicitly configure radio 4 and radio 1 as neighbors.

- You configure neighbors on a per-radio basis. That is, instead of configuring a group of neighbors with certain members, you assign each radio a list of neighbors.

To assign neighbors to a radio, complete these steps:

1. Select **Special Features > Self Healing** and click the **Neighbor Details** tab. In the upper-right corner of the screen, verify that neighbor recovery is enabled.

![Figure 13-65. Configuring Neighbors](image-url)
All RP radios adopted by this module are listed.

The screen lists all RP radios adopted by this module, displaying this information for each:

- **Radio Index**—index number
- **Description**—name
- **Type**—802.11bg or 802.11a
- **RP Ethernet MAC**—Ethernet MAC address for the RP that includes this radio
- **Action**—self-healing action when a neighbor fails
- **Neighbor Radio Indices**—neighbors’ index numbers

2. Select a radio and click the **Edit** button. The **Edit Neighbor** screen is displayed. (See Figure 13-66.)

![Figure 13-66: Specifying Neighbors](image)

The available RP radios—those adopted by this module—are listed on the left under **Available Radios**: these are potential neighbors.
3. To add a neighbor, select a radio from the field on the left and then click the **Add** button. The radio moves to the right; it is now the neighbor of the radio that you are editing.

   You can add up to 16 neighbors, including radios that use a different 802.11 mode than the radio for which you are selecting neighbors. Keep in mind, however, that if the second radio’s wireless stations do not support the other mode, then this radio cannot help them.

4. To remove a radio from the neighbor list, select that radio from the list on the right and click the **Remove** button.

5. In the **Self Healing Action** field, use the drop-down menu to select the action that this radio takes when a neighbor fails. Because you must also complete this step when you use automatic neighbor detection, configuring this setting is described in “Selecting the Self-Healing Action” on page 13-95.

6. Click the **OK** button.

You return to the Special Features > Self Healing > Neighbor Details screen, on which you can confirm the neighbors in the Neighbor Radio Indices column for the radio that you were editing. Note that the neighbors also display the edited radio in their Neighbor Radio Indices column.
Configuring Radios to Automatically Detect Neighbors

Instead of manually configuring neighbors, you can have RP radios detect each other and choose their own neighbors. In this case, each radio will select the three other radios from which it receives the strongest signal.

To use this option, complete these steps:

1. Select **Special Features > Self Healing** and click the **Neighbor Details** tab.

2. Click the **Detect Neighbors** button. The **Automatic Neighbor Detection** screen is displayed. (See Figure 13-68.)

![Figure 13-67.Configuring Neighbors](image)

![Figure 13-68.Automatic Neighbor Detection Screen](image)
Note

As soon as you enable this feature, every RP disassociates its wireless stations and begins scanning for neighboring RPs. For this reason, it is particularly important that you configure self healing when the wireless network is inactive.

Remember also that any manually defined neighbors for radios are erased when you click the Detect Neighbors button.

3. To confirm that you want RPs to begin detecting neighbors, click the Yes button.

After RPs have selected their neighbors, you must define the action that they will take when a neighbor fails, as described in the next section.

Selecting the Self-Healing Action

The Wireless Edge Services xl Module can configure RPs to take one of several actions in response to a failed neighbor. A radio can:

- open its data rates so that it supports both 802.11g and 802.11b stations
  
  For example, one radio in your network might operate in G-only mode (that is, it supports higher data rates only) while a nearby radio also supports the lower data rates of 802.11b. You might configure the first radio to add the lower data rates so that it can support both types of stations if the second fails.

- raise its transmit power to the maximum allowable power in your regulatory domain
  
  You might have lowered the transmit power because you have placed RPs close together for denser coverage. Raising the transmit power when one RP fails increases the chance that stations can receive a good signal from remaining radios.

  In some cases, you may need to configure a self healing offset to prevent the RP radio from raising its power too high. See “Configuring a Self Healing Offset” on page 13-98.
Wireless Network Management  
Network Self Healing

Figure 13-69. Self Healing Action for Neighbor Recovery

- both raise its transmit power and open its data rates (see Figure 13-69)

Sometimes you lower radios' transmit power so that closely grouped RPs can support higher data rates within their relatively small coverage areas. When an RP radio raises its transmit power to take over a failed neighbor's coverage area, it can no longer support high data rates for all stations (some are too far away). In this case, you should remember to configure the radio to open its data rates as well as raise its power. (This is the default action.)
Wireless Network Management
Network Self Healing

- take no action

Remember that radios are always neighbors to each other. However, you might want one radio to respond to the failure of a second radio, but you might not want the second radio to respond to the failure of the first radio. For example, the second radio might be in a more important location. When editing the second radio, configure it to take no action.

**Note**
If you configure a dedicated detector to take action when a neighbor fails, that radio automatically changes to single-channel detector mode when it takes the action so that it can support wireless stations.

Keep these considerations in mind as you configure the action:
- You configure an action for a radio, not for a neighbor. The radio must take the same action no matter which of its neighbors fails.
- You can configure one action for one radio and another for one of its neighbors. For example, you might configure one radio to open its data rates, but you might configure the neighbor to take no action.

To configure the self-healing action, complete these steps:

1. Select **Special Features > Self Healing** and click the **Neighbor Details** tab. In the upper-right corner of the screen, verify that neighbor recovery is enabled.

2. Select the radio for which you want to define the action, and then click the **Edit** button. The **Edit Neighbors** screen is displayed. (See Figure 13-70.)
3. In the **Self Healing Action** field, use the drop-down menu to select the action:
   - **Open Rates**—to configure the radio to support all data rates
   - **Raise Power**—to configure the radio to raise its power to the legal maximum. See “Configuring a Self Healing Offset” on page 13-98 to determine whether you will need to configure a self healing offset.
   - **Both**—to configure the radio to take both of these actions. This is the default setting.
   - **None**—to configure the radio to take neither of these actions.

4. Click the **OK** button.

**Configuring a Self Healing Offset**

When you configure a radio to raise its transmit power as part of neighbor recovery, you must configure a self healing offset for that radio if it meets either of these criteria:
- It uses an external antenna.
- It is located close to another RP radio.
The Wireless Edge Services xl Module subtracts the offset from the maximum power allowed in your regulatory domain to define the maximum power for that radio. To configure this parameter, complete these steps:

1. Select **Network Setup > Radio > Configuration**.

2. Select the radio and click the **Edit** button. The **Configuration** screen for the selected radio is displayed. (See Figure 13-71.)

3. In the **Advanced Properties** section, enter a value in the **Self Healing Offset** field.

   Base the offset on the radio’s antenna gain and the rules of your regulatory domain as explained in [http://www.hp.com/rnd/support/manuals/rports.htm](http://www.hp.com/rnd/support/manuals/rports.htm).

4. Click the **OK** button.
Interference Avoidance

Also called dynamic channel selection, interference avoidance helps your RP radios choose the best channel in your environment at the moment. If the Wireless Edge Services xl Module detects interference on a radio’s current channel, it has the radio use Auto-Channel Selection (ACS) to choose a new channel.

The module implements this procedure for interference avoidance:

1. Every time a wireless station’s packet fails to reach its destination, presumably because of a collision, the station resends the packet. For each RP radio, the module tracks the average number of times in the last 30 seconds that stations reattempted to send a packet.

2. If a radio’s average retries exceed a specified threshold, the module assumes that the excessive collisions are caused by another device operating on the same channel. (This could be an RP in another WLAN, a rogue RP, or even wireless headsets.)

3. The module has the RP radio use ACS to select a new channel based on the best SNR.

To enable interference avoidance, complete these steps:

1. Select Special Features > Self Healing > Configuration.
2. Select the **Enable Interference Avoidance** box.

3. Typically, you should leave the settings for this feature at their defaults. However, you can customize them:
   
a. In the **Average Retries** field, enter a value from 1 through 15 to set the threshold for the number of times stations must resend frames during a 30-second interval. The default value is 14, which means that, if in a 30-second interval the average station must resend a packet 15 times, the radio will select a new channel.

   Resending packets 14 times implies a relatively high latency, and you can lower the threshold. Be aware, however, that changing channels is a relatively drastic action that radios should not take too often.
b. In the Hold Time field, enter a time from 0 through 65,535 seconds. This setting determines how long a radio must wait in between selecting a new channel and again running ACS. If you set this value too low, then radios might begin to run ACS continuously, preventing stations from associating to them.

By default, the Hold Time is set at 3,600 seconds (one hour).

4. Click the Apply button.