



CHAPTER 14

Using the Intrusion Detection System

Use the WLSE Intrusion Detection System (IDS) tab to display intrusion detection information for devices in your network, manage IDS settings, and set up IDS notifications. Using the WLSE Intrusion Detection System features, you can:

- Detect unknown access points. See [Detecting Rogue APs, page 14-12](#).
- Detect and suppress the switch ports of rogue APs. See [Detecting Switch Port Locations and Suppressing Ports, page 14-30](#).
- Detect ad-hoc networks. See [Detecting Ad-Hoc Networks, page 14-37](#).
- Detect non-802.11 interference. See [Detecting Interference, page 14-43](#).
- Detect excessive management frame transmissions. See [Detecting Excessive Management Frame Transmissions, page 14-47](#).
- Implement management frame protection. See [Detecting Management Frame Protection Faults, page 14-52](#).
- Detecting unregistered clients. See [Detecting Unregistered Clients, page 14-60](#).
- Detect authentication and protection attacks. See [Detecting Authentication and Protection Attacks, page 14-65](#).

Getting Started with IDS

Before you can use the features provided by the Intrusion Detection System, you should configure your network to manage your radio environment.



Note

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

Related Topics

- [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)
- [Configuring Your WLAN Radio Environment, page 11-1](#)
- [Enabling and Disabling Radio Management Features, page 11-4](#)

- [Understanding the IDS Subtabs, page 14-2](#)

Understanding the IDS Subtabs

The following sections describe the IDS subtabs:

- [Using the Summary Subtab, page 14-2](#)
- [Using the Faults Subtab, page 14-4](#)
- [Using the IDS Reports Subtab, page 14-5](#)
- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Using the Manage Rogues Subtab, page 14-11](#)
- [Using the Manage Network-Wide IDS Settings Subtab, page 14-11](#)
- [Using the Notification Settings Subtab, page 14-12](#)

Using the Summary Subtab

The Intrusion Detection System Summary allows you to view a summary of all intrusions that have been detected.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **IDS > Summary**. The Intrusion Detection Summary window appears.

Figure 14-1 Sample IDS Summary Screen

The screenshot shows the 'Wireless LAN Solution Engine' interface in a Microsoft Internet Explorer browser. The page title is 'Wireless LAN Solution Engine' and the current subtab is 'IDS'. The main content area displays the 'Intrusion Detection Summary' section. At the top of this section is a 'Refresh(Sec)' input field set to 300 and an 'Apply' button. Below this is a table with two columns: 'Intrusion Fault Type' and 'Number Detected'. The data rows are: Rogue APs Detected (1020), Ad-Hoc Networks Detected (2), Interference Detected (0), Unregistered Clients Detected (0), Association Error Rate (0), Authentication Failures (0), Wireless Client MAC Spoofing (0), EAPOL Flood Detection (0), Excessive Management Frames (0), and MFP Errors (4). Below the first table is a 'Management Frame Protection Anomaly' table with three columns: 'Category', 'Number of Reports', and 'Most Recent Report'. The data row shows 'no MFP anomalies reported', '0', and 'N/A'.

Intrusion Fault Type	Number Detected
Rogue APs Detected	1020
Ad-Hoc Networks Detected	2
Interference Detected	0
Unregistered Clients Detected	0
Association Error Rate	0
Authentication Failures	0
Wireless Client MAC Spoofing	0
EAPOL Flood Detection	0
Excessive Management Frames	0
MFP Errors	4

Management Frame Protection Anomaly Category	Number of Reports	Most Recent Report
no MFP anomalies reported	0	N/A

Step 2 The Intrusion Fault Type table summarizes the number of occurrences of each of the IDS fault types. You can use this table to acknowledge, unacknowledge, or clear selected faults or to view the details of a selected fault.

To display the faults of a particular type, select one of the following fault types from the Intrusion Fault Type table:

- Rogue APs Detected
- Ad-Hoc Networks Detected
- Interference Detected
- Unregistered Clients Detected
- Association Error Rate
- Authentication Failures
- Wireless Client MAC Spoofing
- EAPOL Flood Detection
- Excessive Management Frames
- MFP Errors

The Faults Summary table appears, displaying only the data for that type of fault. For information about the contents of this table, see [Display Faults Table, Table 3-2 on page 3-5](#).



Note For an explanation of the faults, in the online help click **Troubleshooting**, or on Cisco.com see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.15*.

Step 3 The Management Frame Protection Anomaly Category panel summarizes the number of MFP reports that are reporting different MFP errors.

Related Topics

- [Clearing Summary Table Faults, page 3-6](#)
- [Displaying Rogue AP Faults, page 14-19](#)
- [Displaying Ad-Hoc Network Faults, page 14-39](#)
- [Displaying Interference Faults, page 14-46](#)
- [Displaying EMF Detection Faults, page 14-50](#)
- [Displaying Management Frame Protection Faults, page 14-55](#)
- [Displaying Unregistered Client Faults, page 14-62](#)
- [Displaying Authentication and Protection Attack Faults, page 14-81](#)

Using the Faults Subtab

The **IDS > Faults** option displays only the IDS (Intrusion Detection System) faults. To display all fault information, select **Faults > Display Faults**.



Note For an explanation of the faults, in the online help click **Troubleshooting**, or on Cisco.com see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.15*.



Note Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Faults**. The Fault Summary table appears. This table displays device fault information for all intrusion detection faults.

You can use this table to acknowledge, unacknowledge, clear selected faults, or view fault details (see [Displaying Faults, page 3-4](#)).

Step 2 Use the Filter Faults bar to display the faults you want to view (see [Displaying Faults, page 3-4](#)).



Note If no data is displayed in the table, there are no faults for your filtering selection to report.

Step 3 Click the Description or Timestamp fields for a fault. A new window containing the details for that fault appears. The contents of the window depends on the fault type.

Step 4 To clear a fault, see [Clearing Summary Table Faults, page 3-6](#).

Related Topics

[Clearing Summary Table Faults, page 3-6](#)

Using the IDS Reports Subtab

The Intrusion Detection Reports subtab displays Intrusion Detection information about the devices in your network.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Reports**. The Rogue AP report is displayed.

Step 2 To view other IDS reports, select the report type from the **Report Name** dropdown list.

The following IDS reports are available:

- Rogue AP Report—see [Viewing Rogue AP Reports, page 14-26](#)
 - Friendly AP Report—see [Viewing Friendly AP Reports, page 14-28](#)
 - EMF Detection Report—see [Viewing EMF Detection Reports, page 14-50](#)
 - Unregistered Client Report—see [Viewing Unregistered Client Reports, page 14-63](#)
 - Ad-Hoc Network Report—see [Viewing Ad-Hoc Network Reports, page 14-41](#)
 - MFP Capabilities Report—see [Viewing MFP Capabilities Reports, page 14-56](#)
 - MFP Events Report—see [Viewing MFP Events Reports, page 14-57](#)
 - MFP-Client Events Report—see [Viewing MFP-Client Events Reports, page 14-58](#)
-

Related Topics

- [Using the Basic Report Features, page 10-1](#)
- [Detecting Rogue APs, page 14-12](#)
- [Detecting Ad-Hoc Networks, page 14-37](#)
- [Detecting Excessive Management Frame Transmissions, page 14-47](#)
- [Detecting Management Frame Protection Faults, page 14-52](#)
- [Detecting Unregistered Clients, page 14-60](#)

Using the Manage IDS Settings Subtab

Every device managed by the WLSE has an IDS fault profile (also called a fault setting) assigned to it. IDS fault profiles include threshold values and security policies. You can create an IDS fault profile, customize it, and then assign it to a single device or a group of devices.



Note If you have not assigned a specific profile to a device, it uses the system IDS Default profile. The IDS Default profile can be edited, but cannot be deleted and you cannot change its name.

The **IDS > Manage IDS Settings** tab allows you to:

Task	For More Information, See:
Create a new IDS profile	Creating IDS Fault Profiles, page 14-6
Copy an existing profile to create a new profile	Copying an IDS Fault Profile, page 14-7
Rename an existing profile	Renaming an IDS Fault Profile, page 14-7
Edit an existing profile	Editing an IDS Fault Profile, page 14-8
Delete a profile	Deleting an IDS Fault Profile, page 14-8
View the IDS fault profile summary	Viewing the IDS Fault Profile Summary, page 14-9
Assign an IDS fault profile to one or more devices	Assigning Devices to an IDS Fault Profile, page 14-9

Related Topics

- [Managing Fault Settings, page 3-10](#)
- [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)

Creating IDS Fault Profiles

Use this option to create an IDS fault profile. After you create a new IDS fault profile, you can customize it and then assign it to one or more devices.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings dialog box appears.
- Step 2** Enter a unique name in the **Name** text box (see [Naming Guidelines, page B-1](#)).
- Step 3** Click **Create New**. The new name appears in the Existing IDS Fault Profiles list.



Note All the settings in the new profile are assigned default values.

- Step 4** Select the name, then click **Edit**. The Editing Profile window appears (see [Editing an IDS Fault Profile, page 14-8](#)).
-

Related Topics

- [Editing an IDS Fault Profile, page 14-8](#)
- [Assigning Devices to an IDS Fault Profile, page 14-9](#)
- [Using the Manage IDS Settings Subtab, page 14-6](#)

Copying an IDS Fault Profile

Use this option to copy an existing IDS fault profile to use as a base for a new profile.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings dialog box appears.
- Step 2** Select the profile you want to copy from the Existing IDS Fault Profiles box.
- Step 3** Click **Create Copy**. A dialog box appears asking you to enter a name for the copy.
- Step 4** Enter a unique name (see [Naming Guidelines, page B-1](#)).
- Step 5** Click **OK**. The new name appears in the Existing IDS Fault Profiles list.
- Step 6** Select the name, then click **Edit**. The Editing Profile window appears (see [Editing an IDS Fault Profile, page 14-8](#)).
-

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Renaming an IDS Fault Profile

Use this option to rename an IDS fault profile.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings dialog box appears.
- Step 2** Select the profile you want to rename from the Existing IDS Fault Profiles box.



Note You can edit the IDS Default profile, but you cannot delete it or change its name.

- Step 3** Click **Rename**. A dialog box appears asking you to enter a new name.
- Step 4** Enter a unique name (see [Naming Guidelines, page B-1](#)).
- Step 5** Click **OK**. The new name appears in the Existing IDS Fault Profiles list.

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Editing an IDS Fault Profile

Use this option to edit an IDS fault profile (including the IDS Default profile).



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings dialog box appears.
- Step 2** Select the profile you want to edit from the Existing IDS Fault Profiles box.
- Step 3** Click **Edit**. The Editing Setting window appears.
- Step 4** Select the policies and thresholds in the left pane that you want to assign to the profile (see [Setting Policies and Thresholds, page 3-14](#)).

Related Topics

- [Renaming an IDS Fault Profile, page 14-7](#)
- [Creating IDS Fault Profiles, page 14-6](#)
- [Using the Manage IDS Settings Subtab, page 14-6](#)

Deleting an IDS Fault Profile

Use this option to delete an IDS fault profile.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings dialog box appears.
- Step 2** Select the profile you want to delete from the Existing IDS Fault Profiles box.



Note You can edit the IDS Default profile, but you cannot delete it or change its name.

- Step 3** Click **Delete**. A window appears asking if you want to delete the profile.



Note Any devices that were assigned the deleted profile will be automatically assigned the IDS Default profile.

Step 4 Click **OK** to delete the profile.

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Viewing the IDS Fault Profile Summary

Use this option to view a summary of the current settings for a particular IDS fault profile.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings dialog box appears.
- Step 2** Select the profile you want to view from the Existing IDS Fault Profiles box.
- Step 3** Click **View Summary**. A window displays the current fault settings and the devices to which this IDS fault profile is assigned.
- Step 4** Click **OK** to close the window.
-

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Assigning Devices to an IDS Fault Profile

Use this option to assign a single device or a group of devices to a fault profile. Devices can be assigned to only one profile at a time.

If you have not assigned a device to a specific profile, it uses the IDS Default profile.



Note Your login determines whether you can use this option.

Procedure

- Step 1** To access the windows that allow you to assign devices to a profile:
- From the IDS Fault Settings window, select **IDS > Manage IDS Settings**, select an existing IDS fault profile, then select:
 - **Assign Devices** (located in the top right of the screen under the subtabs).
 - **Assign Devices to <profilename>** (located to the left of the Reset button).

- From any IDS Editing Setting window, select the **Assign Devices** link located at the top right of the window.

The window refreshes with a device selector in the left pane.

- Step 2** To search for devices, use the dialog box in the left pane above the device selector. For information on how to search or use the device selector, see [Using the Device Selector, page 1-12](#).
- Step 3** If you know which device or device group you want, use the device selector to select the devices. They are added to the list of Available Devices.
- Step 4** From the list of Available Devices, select the device you want to assign to the profile and click >>. The devices are moved to the Selected Devices list.
- Step 5** Click **Continue**. A confirmation dialog box appears for the device assignment.
- Step 6** Click **OK** to accept the device assignment or **Cancel** to cancel the device assignment.
-

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting IDS Policies and Thresholds

Use the IDS settings to activate or deactivate a set of predefined policies for access points and radio interfaces and to set polling and **exception** threshold values collected from the devices you are monitoring. The policies and threshold values you set in this window will determine how the faults are displayed in the **IDS > Faults** subtab.

You can set pre-defined policies for general and radio interface-specific settings:

- General IDS settings are applicable to the access point or bridge. They are set on the access point or bridge and are reported on the faults page. For each profile, you can set the following general IDS settings:
 - Unregistered Client—See [Enabling Unregistered Client Detection, page 14-61](#)
 - Excessive Management Frame Detection—See [Setting the Excessive Management Frame Detection Policy, page 14-49](#)
 - Authentication and Protection Attack Detection—See [Enabling Authentication and Protection Attack Detection, page 14-67](#)
- Radio interface-specific settings (see [Setting the Association Error Rate Policy, page 14-75](#)) are applicable only to the radio interface type (11a, 11b, or 11g) on which they are set. They are set on the radio interface and are reported by interface type on the faults page.



Note

Policies (settings) are disabled by default unless otherwise noted.

Using the Manage Remaining IDS Settings Subtab

When Radio Management is disabled, the **IDS > Manage IDS Settings** subtab is replaced with the subtab **Manage Remaining IDS Settings**. This subtab allows you to create policies and thresholds for the IDS monitoring features that can still be used when Radio Management is disabled.

Although they still appear, the following general IDS fault settings are *not* active when Radio Management is disabled:

- Unregistered Client
- Excessive Frame Management
- EAPOL Settings

Other Radio Management related faults (including rogue detection, ad-hoc detection, interference, self healing, and other non-IDS faults) are also either inactive or not displayed when Radio Management is disabled. For more information, see [Enabling and Disabling Radio Management Features, page 11-4](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Using the Manage Rogues Subtab

See [Managing Rogue APs, page 14-24](#).

Using the Manage Network-Wide IDS Settings Subtab



Note

The Rogue, Ad-Hoc, and Interference network-wide settings were moved here from Faults > Manage Network-Wide Settings in the previous release.

You can use the **IDS > Manage Network-Wide IDS Settings** option to set the following network-wide IDS policies:

- Rogue AP Detection—See [Setting the Rogue AP Detection Policy, page 14-16](#)
- Automatic Rogue AP Detection and Suppression—See [Setting the Automatic Rogue AP Suppression Policy, page 14-32](#)
- Automatic Friendly AP to Rogue AP Reclassification—See [Setting the Friendly AP to Rogue AP Reclassification Policy, page 14-18](#)
- Ad-Hoc Network Detection—See [Setting the Ad-Hoc Network Detection Policy, page 14-38](#)
- Interference Detection—See [Setting the Interference Detection Policy, page 14-45](#)
- Management Frame Protection—See [Setting the Management Frame Protection Policy, page 14-54](#)

Using the Notification Settings Subtab

When a fault is detected, the WLSE can send automated notifications in the form of SNMP traps, syslog messages, and email alerts. You can specify multiple recipients for each notification type, and choose to deliver the message using either a plain text or XML format.

To create fault notification targets for IDS traps, syslog messages, and emails, select either of these options:

- **IDS > Notification Settings**
- **Faults > Notification Settings**

For more information about this dialog, see [Notification Settings, page 3-56](#).

Detecting Rogue APs

The following sections will help you understand how and where to use the rogue AP detection feature:

- [Understanding Rogue AP Detection, page 14-12](#)
- [Guidelines for Detecting Rogue APs, page 14-14](#)
- [Setting the Rogue AP Detection Policy, page 14-16](#)
- [Displaying Rogue AP Faults, page 14-19](#)
- [Managing Rogue APs, page 14-24](#)
- [Viewing Rogue AP Reports, page 14-26](#)
- [Viewing Friendly AP Reports, page 14-28](#)

Understanding Rogue AP Detection

Radio Monitoring continuously monitors your WLAN radio environment to discover the presence of any new APs that are transmitting beacons. Any newly discovered AP that is not currently managed by WLSE generates a new rogue AP fault. You can view rogue AP faults using any of these options: **IDS > Summary > Rogue APs Detected**, **IDS > Faults**, **IDS > Reports**, or **IDS > Manage Rogues**.

The Radio Monitoring feature uses the radio measurement capabilities on Cisco IOS APs and Cisco client adaptors and CCX V2 clients to discover any new 802.11 access points that are transmitting beacons. Both clients and APs periodically scan for other 802.11 beacon frames on all channels. Reports of detected beacons are returned to the Radio Manager, which validates these beacons against a list of APs known to be authorized to provide wireless access.

**Note**

For the access points that support this feature, see the *Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine, 2.15*, on Cisco.com.

A newly discovered AP that cannot be identified as a known authorized AP generates an administrator alert. You can categorize this new AP as one of the following AP types:

Type	Description
Managed AP	<p>An AP that is authorized to provide wireless access to the LAN and requires management services provided by the WLSE.</p> <p>Note Only managed APs can participate in Radio Manager operations (see Configuring Your Network for Radio Management, page 11-5).</p>
Unmanaged AP	<p>An AP that is authorized to provide wireless access to the LAN but does <i>not</i> require any management services from the WLSE.</p> <p>The WLSE categorizes unmanaged devices into two groups:</p> <ul style="list-style-type: none"> • Rogue—An AP that may or may not be connected to the LAN, is detected by client's or AP's 802.11 radios within the managed WLAN, and has not been identified as Friendly. By default, all unmanaged radios are classified as Rogue until you change them to Friendly. <p>When WLSE detects a rogue device, it sends alerts to the administrators and starts extra processing (such as switch port tracking).</p> <ul style="list-style-type: none"> • Friendly—An AP that is not connected to the LAN, but is known to be detectable by client's or AP's 802.11 radios within the managed WLAN. A Friendly AP is an AP that you know exists, for example, a neighboring network's AP or a neighboring company's AP. <p>All friendly devices begin on the WLSE as rogue devices and are explicitly categorized as friendly by the WLSE administrator.</p>

How Rogue AP Detection Works

Rogue AP detection is based on the detection of an unknown radio broadcasting over the air. When Radio Monitoring detects a rogue AP, a new rogue AP fault is generated. When you select the link in the Description or Timestamp fields in the Fault Summary Table for an unknown access point, the Rogue Access Point Details window displays information about the rogue AP (see [Managing Rogue APs, page 14-24](#)).

Some networks might experience large numbers of rogues due to the nature of their neighboring networks or a one-time storm. When the number of unknown (rogue infra-structure or ad-hoc) radios is high (greater than 5000), your network might experience performance degradation. This can occur when your network is in a crowded airspace, you have products such as printers that have wireless functions that create and/or rotate ad-hoc network IDs, that are attacked by the FakeAP program, or that have APs sending corrupt beacon reports.



Note For an explanation of the fault that is generated when this occurs, in the online help click **Troubleshooting**, or on Cisco.com see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.15*.

How Friendly AP to Rogue AP Reclassification Works

For each unmanaged AP that has been classified as friendly, the WLSE periodically compares the present set of observers of that AP to its previous set of observers. If the relative power levels received by the observers changes, or the ratio of power levels between observers substantially changes, the friendly AP will be considered to have been relocated and will be reclassified as a rogue.

**Note**

To be less sensitive to changes in friendly AP power levels, only those observer APs in common between the two sets are considered in this comparison. If only one (or zero) APs remain in common between the two observer sets, the AP is reclassified as rogue unless the reason for this change is that one or more observers have been removed from the network or the observer AP in question has been moved to a new location.

When the Friendly-to-Rogue policy evaluates a site, any device that has not been seen in “too long a time” is reclassified as rogue. This time period starts when WLSE *last observed* the device, not after the administrator has set it to Friendly. To keep an unmanaged device as Friendly, set the maximum unobserved time to a value larger than the amount of time the device is *expected* to not be observed (see [Setting the Friendly AP to Rogue AP Reclassification Policy, page 14-18](#)). For example, if a friendly AP is turned off after business hours, the maximum unobserved time should be at least 14 hours (or more for weekends) or the WLSE will reclassify it as rogue.

Upon reclassification, the WLSE default actions for a newly-discovered rogue AP are performed, including (but not limited to) switchport-tracing within the managed network to ensure that the AP is not connected to that network.

Related Topics

- [Guidelines for Detecting Rogue APs, page 14-14](#)
- [Setting the Rogue AP Detection Policy, page 14-16](#)
- [Setting the Friendly AP to Rogue AP Reclassification Policy, page 14-18](#)
- [Displaying Information About Rogue Access Points, page 13-22](#)

Guidelines for Detecting Rogue APs

Prerequisites

Before you can detect rogue APs, you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management, page 11-5](#)).

**Note**

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

**Note**

During initial network deployment, rogue detection must be turned off. Otherwise, between the time an AP is deployed and it is put into the managed state in WLSE, WLSE will attempt to locate the switch port of the newly deployed AP. This can generate many unnecessary faults.

2. Define the location elements (buildings and floors) and place the APs on the floor images. This step is optional, but will help you get the best results from the Location Manager displays. For more information, see:
 - [Entering Building Information, page 13-4](#)
 - [Adding Floors to Location Manager, page 13-9](#)
 - [Adding Devices to Floors, page 13-14](#)
3. Optional (but necessary to accurately locate rogue APs): Perform an AP Radio Scan on all APs on the specified floor (see [Using AP Radio Scans to Collect RM Data, page 13-43](#)).
4. Be sure Radio Monitoring is enabled on all APs (for both serving and non-serving channels) on the specified floor (see [Starting Radio Monitoring, page 12-4](#)).



Note Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it.



Note If only serving channel scanning is enabled, then only the APs configured on the same channel as the rogue will actually report the rogue.

5. Set policies to enable rogue AP detection and assign a severity level to the fault that is generated when a rogue AP is detected (see [Setting the Rogue AP Detection Policy, page 14-16](#)).

Tips

- To detect rogue APs, Radio Monitoring *must* be running.
- Although you might be tempted to disable Radio Monitoring and detect rogue APs only during AP Radio Scans, *this approach is not recommended*. AP Radio Scan jobs can detect rogues, but only during the scan (approximately 3 to 4 minutes); any rogues that show up after the scan are not detected. In addition, because the scan is so short, it is possible that some rogues will not be detected because they do not respond with a Probe Request during the active scan. When Radio Monitoring is enabled, the rogue will eventually be detected by the beacon frame; it is statistically possible that a beacon will not be seen during an AP scan.



Note If you disable Radio Monitoring and do not run AP Radio Scan, no unknown radios (rogue or friendly) will be detected. If you run AP Radio Scan but disable Radio Monitoring, some unknown radios will be detected, but not as many as would be detected if Radio Monitoring was running.

- An 11a-capable client that is associated with an 11g network *cannot* detect 11a rogues. No matter what the client is capable of supporting, it only searches for rogues that match the band of the AP. Therefore, when a client is associated to a 2.4Ghz AP (b or g), it only detects 2.4Ghz rogues (b or g). When it is associated to a 5Ghz (11a) AP, it only detects 5Ghz (11a) rogues.
- To detect all rogue APs in a network in which several hundred 11g APs have been deployed, you must also deploy 11a APs. Depending on the deployment, however, you might not have to deploy one 11a for each 11g radio. Using scanning-only APs, it is possible to completely cover the area for 11a rogue AP detection using fewer APs.
- A scanning-only AP that has a dual radio (both a and g) can detect all types of rogues (a, b, and g).
- If several rogue APs with similar MAC addresses appear in exactly the same location, there might be only one physical AP.

- If you disable the rogue AP fault detection, only the notification is removed; the rogue AP detection still occurs. The Location Manager still displays all the rogues in the system regardless of the fault detection setting.
- If you delete a rogue and the rogue still exists in the network, WLSE will detect it the next time AP Radio Scan or Radio Monitoring runs. Deleting the rogue will not mark it to be ignored; it is removed from the system as if it never occurred.



Note If the rogue is persistent in the network and not a problem, change the access point category type to Friendly. Then it will appear in the Friendly AP report and the Friendly list in Location Manager.

To handle large numbers of rogues:

- Use **IDS > Manage Network Wide Settings** to disable all rogue detection and processing from either infrastructure or ad-hoc rogues (or both).
- If your network is in a crowded airspace, examine the report **IDS > Manage Rogues**. This report shows you the RSSI value for the detected rogues. Sorting by RSSI might give you a limit of RSSI values that you could use in **IDS > Manage Network Wide Settings** as a threshold.
- Use **IDS > Manage Rogues** to delete the rogues that are no longer an issue (for example, from a temporary storm or isolated occurrence) to free up space in the WLSE.
- For an explanation of the fault, in the online help click **Troubleshooting**, or on Cisco.com see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.15*.

Related Topics

- [Understanding Rogue AP Detection, page 14-12](#)
- [Displaying Information About Rogue Access Points, page 13-22](#)
- [Viewing Rogue AP Reports, page 14-26](#)
- [Viewing Friendly AP Reports, page 14-28](#)

Setting the Rogue AP Detection Policy

Use **IDS > Manage Network-Wide IDS Settings** to enable rogue AP detection and to assign a severity level to the fault that is generated when a rogue AP is detected.

When a rogue AP is detected, a fault is generated and can be viewed under **IDS > Summary**, **IDS > Faults**, **IDS > Manage Rogues**, or **IDS > Reports**.



Note For information about setting the friendly AP to rogue AP reclassification policy, see [Setting the Friendly AP to Rogue AP Reclassification Policy, page 14-18](#).

Typical Scenarios and FAQs

- I want (or no longer want) to be notified when a rogue AP is detected.
- I want to specify the severity of rogue AP detection notifications.
- I want to view the current rogue AP detection faults associated with the current [P1...P5] setting.



Note Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage Network-Wide IDS Settings**.

Step 2 Select **Rogue AP Detection**.

Step 3 Complete the following:

Field	Description
Enable	Click Enable to start rogue AP fault detection. This policy is enabled by default. Note If you disable rogue AP fault detection, only the fault notification is removed; the rogue AP detection still occurs. The Location Manager displays all the rogues in the system regardless of the fault detection setting.
Priority	From the dropdown list, select the severity level to assign the fault when a rogue access point is detected.
RSSI	Enter the minimum RSSI value. This is the received signal strength indicator of the reporting AP, and is used to estimate the location of the rogue AP relative to the reporting AP. Note This threshold is applied only when the rogue AP is <i>first detected</i> . Over time, this value may fall below the minimum value.
Enable Switch Port Tracing for Rogue	Click Enable to start rogue AP switch port tracing. This policy is enabled by default. Note For information about rogue AP switch port suppression, see Detecting Switch Port Locations and Suppressing Ports, page 14-30 .

Step 4 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 5 To see the faults associated with this setting, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary > Rogue APs Detected**.

Related Topics

- [Detecting Rogue APs, page 14-12](#)
- [Setting the Automatic Rogue AP Suppression Policy, page 14-32](#)
- [Managing Rogue APs, page 14-24](#)
- [Viewing Rogue AP Reports, page 14-26](#)
- [Guidelines for Detecting Rogue APs, page 14-14](#)

- [Understanding Rogue AP Detection, page 14-12](#)

Setting the Friendly AP to Rogue AP Reclassification Policy

Use **IDS > Manage Network-Wide IDS Settings** to enable friendly AP to rogue AP reclassification and to assign threshold levels to determine when a friendly AP should be reclassified.

Typical Scenarios and FAQs

- I want (or no longer want) to enable automatic friendly AP to rogue AP reclassification.
- I want to specify how long a friendly AP may be undetected before it is reclassified as a rogue.
- I want to specify the maximum difference in RSSI values that will be allowed before a friendly AP is reclassified.



Note Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage Network-Wide IDS Settings**.

Step 2 Select **Rogue AP Detection**.

The friendly AP to rogue AP reclassification settings appear *below* the rogue AP settings and the switch port suppression settings.

Step 3 Complete the following:

Field	Description
Enable	Click Enable to start automatic friendly AP to rogue AP reclassification. This policy is <i>not</i> enabled by default.
Unobserved time	The time a friendly AP can be unobserved before it is reclassified as a rogue, specified using days, hours, and minutes dropdown lists. Increments of 5 minutes can be specified. To keep an unmanaged device as Friendly, set the maximum unobserved time to a value larger than the amount of time the device is <i>expected</i> to not be observed (see How Friendly AP to Rogue AP Reclassification Works, page 14-13).
RSSI difference	Enter the maximum difference between the original and currently-observed RSSI (received signal strength indicator) values from one observer to the next that is allowed before the friendly AP is reclassified as a rogue.

Step 4 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Related Topics

- [Detecting Rogue APs, page 14-12](#)

- [Understanding Rogue AP Detection, page 14-12](#)

Displaying Rogue AP Faults

You can view rogue AP faults using options under **IDS > Summary**, **IDS > Faults**, **IDS > Reports**, or **IDS > Manage Rogues**.



Note You can also display a graphical view of the estimated location of rogue radios using the Location Manager (see [Displaying Information About Rogue Access Points, page 13-22](#)).

Typical Scenarios and FAQs

- How do I view a list of APs that have reported the rogue AP and the location of the AP?
- How do I find the switch port to which the rogue AP is connected?
- I have just been notified of a rogue AP and I have determined it is a friendly AP. How do I delete the AP and clear the fault?
- I have just been notified of a rogue AP. Which APs are reporting the rogue AP?
- I have just been notified of a rogue AP. Where is its physical location in my network?
- How do I change the category type of a rogue AP to friendly?
- How do I delete a rogue AP from the database?



Note Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting rogue APs (see [Guidelines for Detecting Rogue APs, page 14-14](#)).

Procedure

- Step 1** Select **IDS > Summary**. The Intrusion Detection Summary window appears.
- Step 2** Select **Rogue APs Detected**. The Faults for Rogue APs Detected window appears.
- Step 3** Select the Description or Timestamp fields for the fault. The Unknown AP Details window displays information about the selected fault.

Figure 14-2 Sample Unknown AP Detail Window

The screenshot shows the 'WLSE Unknown AP Detail' window. It contains several sections:

- Rogue Access Point Details:** A table with columns BSSID, State, Vendor, and buttons for 'Change to Friendly' and 'Delete'. The BSSID is 0012d9c8c103, State is Rogue Access Point, and Vendor is unknown.
- Beacon Information:** A table with columns SSID, Beacon Interval, Channel, PHY, and Data Rates. The SSID is '[7] "leapmhc"', Beacon Interval is 100, Channel is 36, PHY is 802.11a, and Data Rates are Basic: 6.0Mbps, 9.0Mbps, Basic: 12.0Mbps, 18.0Mbps, Basic: 24.0Mbps, 36.0Mbps, 48.0Mbps, 54.0Mbps.
- Location Estimation:** A table with columns Location and Timestamp. The Location is 'Estimated location SJC/Second' and the Timestamp is 'Wed Jan 12 23:23:11 GMT+00:00 2005'. There is a 'View in Location Manager' button.
- Switch Port Tracing:** A table with columns Switch IP, Switch Port, Traced MAC Address, and Timestamp. The Switch IP is 'unknown' and there is a 'Re-Trace' button.
- Reporting APs:** A table with columns Reporting AP IP Address, Reporting AP BSSID, RSSI, and Reporting AP Location. The Reporting AP IP Address is 12.10.80.21, Reporting AP BSSID is 000dbc9332b3, RSSI is -91, and Reporting AP Location is SJC/Second.
- Associated Clients:** A section for Client MAC Address, currently empty.
- Fault History:** A table with columns State, Severity, Description, Change, Timestamp, and By. The State is Active, Severity is P1, Description is 'Device state is rogue access point', Change is 'Device state is rogue access point', and Timestamp is 16:45:06 01/11/2005.



Note For rogue AP faults, the Unknown AP Details window contains this information:

Rogue Access Point Details

This table contains information about the rogue AP. It also allow you to:

- Change the classification of an access point from Rogue to Friendly.
- Delete the rogue AP from the database.

Table 14-1 Rogue Access Point Details Table

Column	Description
BSSID	Basic Service Set (BSS) identifier.
State	The state of the device.
Vendor	The name of the vendor that manufactured this AP.

Table 14-1 *Rogue Access Point Details Table (continued)*

Column	Description
Change To Friendly AP	To add this AP to the list of recognized APs, click Change To Friendly AP . Then refresh your browser window to view the updated fault display. Note It may be a few seconds before the classification is changed. Note When a rogue AP is changed to Friendly, the fault will be cleared and will subsequently be displayed as a Friendly AP.
Delete	To delete this unknown AP, click Delete . Then refresh your browser window to view the updated fault display. Note It may be a few seconds before the rogue AP is deleted.

Beacon Information

This table contains information about the beacon on which the rogue AP is transmitting.

Table 14-2 *Beacon Information Table*

Column	Description
SSID	Service set identifier used by client devices to associate with an access point. Note When an AP is configured to not broadcast its SSID, this field will either be blank or contain hex zeros. (When a Cisco AP is configured to not broadcast its SSID, that AP sends null characters (hex zeros) in place of the SSID in the beacon.)
Beacon Interval	The amount of time between beacons in kilo microseconds (one kilo microsecond equals 1,024 microseconds).
Channel	The channel on which the rogue AP is transmitting.
PHY	The physical interface type (11a, 11b, or 11g) of the radio interface.
Data Rates	The data rates supported by this interface (in Mbps).

Location Estimation**Table 14-3** Location Estimation Table

Column	Description
Location	<p>The estimated location (building and floor) of the rogue AP.</p> <p>The following messages indicate that a problem occurred when trying to identify the location:</p> <ul style="list-style-type: none"> Estimated location could not be determined. Reporting AP location was not specified. <p>When the APs are not placed using the Location Manager, WLSE cannot determine the location of the rogue because it does not know the location of the reporting AP. Use the Location Manager to define the location elements (buildings and floors) and place the APs in the floors.</p> <ul style="list-style-type: none"> Location could not be determined. Device was reported by clients only. <p>When a rogue access point is detected only by clients, the Location Manager cannot determine the location of the rogue because the client's own location can change rapidly.</p>
Timestamp	The time, based on the client browser, the rogue was detected (see Understanding WLSE Time Displays, page 1-10).
View in Location Manager	<p>Click View in Location Manager to display a graphical view of the approximate location of the rogue AP.</p> <p>For more information about how the Location Manager locates an unknown radio, see Displaying Information About Rogue Access Points, page 13-22.</p>

Switch Port Tracing

See [Tracing Switch Ports and Monitoring Automatic Rogue AP Suppression, page 14-34](#).

Reporting APs

This table contains information about the APs that have detected the rogue AP.

Table 14-4 Reporting APs Table

Column	Description
Reporting AP IP Address	The IP address of the AP that has located the rogue AP.
Reporting AP BSSID	The basic service set (BSS) identifier that contains the AP that has located the rogue AP.
Current RSSI	Received signal strength indicator of the reporting AP. This value is used to estimate the location of the rogue AP relative to the reporting AP.
Reporting AP Location	The physical location of the AP that has located the rogue AP.

Associated Clients

This table contains information about the clients associated with the rogue AP.

Table 14-5 Associated Clients Table

Column	Description
Client MAC Address	The MAC address of each client radio (that WLSE knows of) that is associated with the rogue AP.

Fault History

This table contains a history of the faults raised against this rogue AP.

Table 14-6 Fault History Table

Column	Description
State	The state of the device. For a description of the states, see Understanding Fault States, page 3-2 .
Severity	The severity level to be assigned to the fault.
Description	A description of the fault. Note For an explanation of the faults, in the online help click Troubleshooting , or on Cisco.com see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.15</i> .
Change	A description of the state change.
Timestamp	The time, based on the client browser, that the state of the device last changed (see Understanding WLSE Time Displays, page 1-10).
By	Displays the username of the person who changed the fault state. Note If the fault state has not been cleared or acknowledged, nothing is displayed in this column.

Related Topics

- [Managing Rogue APs, page 14-24](#)
- [Viewing Rogue AP Reports, page 14-26](#)
- [Viewing Friendly AP Reports, page 14-28](#)
- [Detecting Switch Port Locations and Suppressing Ports, page 14-30](#)
- [Guidelines for Detecting Rogue APs, page 14-14](#)

Managing Rogue APs

You can use the **IDS > Manage Rogue** option to manage rogue and friendly AP faults.



Note Similar functionality is also available from the **IDS > Faults** and **Faults > Display Faults** subtabs.

Typical Scenarios and FAQs

- How do I change the category type of a rogue AP to friendly?
- How do I delete a rogue AP from the database?



Note Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting rogue APs (see [Guidelines for Detecting Rogue APs, page 14-14](#)).

Procedure

- Step 1** Select **IDS > Manage Rogue**. The Rogue AP List appears.
- Step 2** From the **Select Unknown Station Type**, select the type of unknown stations you want to display (Infrastructure or Adhoc).
- Step 3** To display the rogue AP list, select **Rogue** from the **Select Status** bar (this is the default).
This table contains the following information:

Table 14-7 Rogue AP List

Column	Description
BSSID	Basic Service Set (BSS) identifier.
SSID	The Service Set ID broadcast by the rogue access point. Note When an AP is configured to not broadcast its SSID, this field will either be blank or contain hex zeros. (When a Cisco AP is configured to not broadcast its SSID, that AP sends null characters (hex zeros) in place of the SSID in the beacon.) Note This column displays non-printable characters as \xNN, where NN is the hex value of each character, followed by the length of the SSID in bytes. For example, "\x00" [1] means that the SSID contains the hex value \x00 and is 1 byte long. In addition, any double quote marks or backslashes that are part of the SSID octets are displayed using a preceding backslash (for example, \" or \\).
Vendor Name	The name of the vendor that manufactured this AP.
Reported By	The AP that is reporting the rogue AP.
RSSI	Received signal strength indicator of the reporting AP. This value is used to estimate the location of the rogue AP relative to the reporting AP.
Channel	The channel on which the rogue AP is transmitting.

Table 14-7 *Rogue AP List*

Column	Description
PHY	The physical interface type (11a, 11b, or 11g) of the radio interface.
Building	The estimated location (building) of the rogue AP.
Floor	The estimated location (floor) of the rogue AP.
Reporting Time	The time, based on the client browser, the rogue AP was reported by the AP (see Understanding WLSE Time Displays, page 1-10).

- Step 4** To add one or more rogue APs to the list of recognized (friendly) APs, select the corresponding check boxes and click **Change to Friendly** from the Select AP Type bar.



Note It may be a few seconds before the classification is changed.



Note When the rogue AP is marked as friendly, the fault will be cleared and will subsequently be displayed as a Friendly AP.

- Step 5** To view the list of recognized APs, select **Friendly** from the **Select Status** bar. The Friendly AP List appears. This table contains one additional field:

Table 14-8 *Friendly AP List*

Column	Description
AP Name	A text entry box that contains the user-defined name for this AP. To create a new name for this friendly AP or change the existing name, enter the name in the text entry box and click Save Name(s) .

- Step 6** To change the AP type for one or more friendly APs to Rogue, select the corresponding checkboxes and click **Change to Rogue** from the Select AP Type bar.



Note It may be a few seconds before the classification is changed.

- Step 7** To delete one or more rogue or friendly APs, select the corresponding checkboxes and click **Delete**.



Note It may be a few seconds before the APs are deleted.

Related Topics

- [Viewing Rogue AP Reports, page 14-26](#)
- [Viewing Friendly AP Reports, page 14-28](#)
- [Guidelines for Detecting Rogue APs, page 14-14](#)

Viewing Rogue AP Reports

The **IDS > Reports > Rogue AP Report** option displays any rogue access points that are present in the wireless network. A rogue AP is an AP that may or may not be connected to the LAN, is detected by client's or AP's 802.11 radios within the managed WLAN, and has not been identified as Friendly. By default, all unmanaged radios are classified as Rogue until you change them to Friendly.

Typical Scenarios and FAQs

- I want to view the rogue APs that are present in my network.



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting rogue APs (see [Guidelines for Detecting Rogue APs, page 14-14](#)).

Procedure

Step 1 Select **IDS > Reports**.

Step 2 Select **Rogue AP Report** from the Report Name list.

Step 3 To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).



Note

To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.

Step 4 To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.

Step 5 To narrow the search criteria:

- Select **Building Name** or **Floor Name** from the dropdown list.
- Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
- Click **Search**.

The building or floor names are displayed below the Search field. The Rogue AP report, which appears to the right of this list, displays the information for the first entry in the list.

- Click any other entry in the list to display its corresponding report.

The Rogue AP report contains the following information:

Table 14-9 *Rogue AP Report*

Column	Description
BSSID	Basic Service Set (BSS) identifier of the rogue AP.
SSID	<p>The Service Set ID broadcast by the rogue access point.</p> <p>Note When an AP is configured to not broadcast its SSID, this field will either be blank or contain hex zeros. (When a Cisco AP is configured to not broadcast its SSID, that AP sends null characters (hex zeros) in place of the SSID in the beacon.)</p> <p>Note This column displays non-printable characters as \xNN, where NN is the hex value of each character, followed by the length of the SSID in bytes. For example, "\x00" [1] means that the SSID contains the hex value \x00 and is 1 byte long. In addition, any double quote marks or backslashes that are part of the SSID octets are displayed using a preceding backslash (for example, \" or \\).</p>
Vendor Name	The name of the vendor that manufactured this AP.
Reported By	The name of the AP that located the rogue AP.
RSSI	Received signal strength indicator of the reporting AP. This value is used to estimate the location of the rogue AP relative to the reporting AP.
Channel	The channel on which the rogue AP is transmitting
PHY	The physical interface type (11a, 11b, or 11g) of the radio interface.
Building	The estimated location (building) of the rogue AP.
Floor	The estimated location (floor) of the rogue AP.
Switch IP	The IP address of the switch to which the rogue access point is connected.
Switch Port	The port of the switch to which the rogue access point is connected.
Reporting Time	The time the rogue was reported by the AP (based on the client browser—see Understanding WLSE Time Displays, page 1-10).

- Step 6** To view the fault details for a selected AP, click the value in the BSSID column. The Rogue Access Point Details window displays this information (see [Table 14-1Rogue Access Point Details Table, page 14-20](#)).
- Step 7** Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Managing Rogue APs, page 14-24](#)
- [Using the IDS Reports Subtab, page 14-5](#)
- [Viewing Friendly AP Reports, page 14-28](#)

Viewing Friendly AP Reports

The Friendly AP Report displays any friendly access points that are present in the wireless network. A Friendly AP is an AP that is not connected to the LAN, but is known to be detectable by client's or AP's 802.11 radios within the managed WLAN. A Friendly AP is an AP that you know exists, such as a neighboring network's AP or a neighboring company's AP.

Typical Scenarios and FAQs

- I want to view the APs that have been identified as friendly in my network.



Note

Your login determines whether you can use this option.

Before You Begin

- Satisfy the prerequisites for detecting rogue APs (see [Guidelines for Detecting Rogue APs, page 14-14](#)).
- Designate one or more unknown APs as Friendly (see [Managing Rogue APs, page 14-24](#)).

Procedure

Step 1 Select **IDS > Reports**.

Step 2 From the Report Name list, select **Friendly AP Report**.

Step 3 To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).



Note

To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.

Step 4 To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.

Step 5 To narrow the search criteria:

- Select **Building Name** or **Floor Name** from the dropdown list.
- Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
- Click **Search**.

The building or floor names are displayed below the Search field. The Friendly AP report, which appears to the right of this list, displays the information for the first entry in the list.

- Click any other entry in the list to display its corresponding report.

The Friendly AP report displays the following information:

Table 14-10 Friendly AP Report

Column	Description
AP Name	The user-defined name of the friendly AP.
BSSID	Basic Service Set (BSS) identifier of the friendly AP.

Table 14-10 Friendly AP Report (continued)

Column	Description
SSID	<p>The Service Set ID broadcast by the friendly access point.</p> <p>Note When an AP is configured to not broadcast its SSID, this field will either be blank or contain hex zeros. (When a Cisco AP is configured to not broadcast its SSID, that AP sends null characters (hex zeros) in place of the SSID in the beacon.)</p> <p>Note This column displays non-printable characters as \xNN, where NN is the hex value of each character, followed by the length of the SSID in bytes. For example, "\x00" [1] means that the SSID contains the hex value \x00 and is 1 byte long. In addition, any double quote marks or backslashes that are part of the SSID octets are displayed using a preceding backslash (for example, \' or \).</p>
Vendor Name	The name of the vendor that manufactured this AP.
Reported By	The name of the AP that located the friendly AP.
RSSI	Received signal strength indicator of the reporting AP. This value is used to estimate the location of the friendly AP relative to the reporting AP.
Channel	The channel on which the friendly AP is transmitting
PHY	The physical interface type (11a, 11b, or 11g) of the radio interface.
Building	The estimated location (building) of the friendly AP.
Floor	The estimated location (floor) of the friendly AP.
Switch IP	The IP address of the switch to which the access point is connected.
Switch Port	The port of the switch to which the access point is connected.
Reporting Time	The time the friendly AP was reported (based on the client browser—see Understanding WLSE Time Displays, page 1-10).

- Step 6** To view the fault details for a selected AP, click the value in the BSSID column. The Friendly Access Point Details window displays this information (see [Table 14-1 Rogue Access Point Details Table, page 14-20](#)).
- Step 7** Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Using the IDS Reports Subtab, page 14-5](#)
- [Viewing Rogue AP Reports, page 14-26](#)
- [Guidelines for Detecting Rogue APs, page 14-14](#)
- [Understanding Rogue AP Detection, page 14-12](#)

Detecting Switch Port Locations and Suppressing Ports

When a rogue AP fault is generated, the Rogue Access Point Details window displays information about the switch port to which the rogue AP is connected. The following sections describe how and where to use the switch port location and suppression feature:

- [Understanding Switch Port Tracing and Suppression, page 14-30](#)
- [Guidelines for Detecting and Suppressing Switch Ports, page 14-31](#)
- [Setting the Automatic Rogue AP Suppression Policy, page 14-32](#)
- [Tracing Switch Ports and Monitoring Automatic Rogue AP Suppression, page 14-34](#)

Understanding Switch Port Tracing and Suppression

To find the switch port to which the rogue AP is connected (if it is connected), the Switch Port Location feature uses BSSIDs of the rogue APs that it hears over the air to make a heuristic guess of the rogue's Ethernet MAC address.


Note

Switch port tracing and suppression is a best-effort approach and is not 100% guaranteed to yield accurate results.


Note

When an IP address is added to the Excluded list (Devices > Discover > Discover > IP Filter Rules), Switch port tracing will not be done for that device.


Note

Catalyst Operating System (CatOS) software is not supported for switch port tracing.

How It Works

The WLSE determines whether an AP is a rogue:

1. While Radio Monitoring is enabled, the APs report the BSSIDs of their neighboring APs.
2. WLSE compares the BSSIDs of the APs with those in the managed list. Any AP not in the managed list is considered to be rogue and a fault is reported.

After a rogue AP has been detected by WLSE:

1. The WLSE receives frame reports from the reporting and scanning APs. These reports contain the MAC addresses of any clients associated with the rogue AP.
2. WLSE tries to locate the MAC addresses of both the client and the rogue in the switches via a CAM table search (using the approach described in the following note) to determine which port is forwarding packets to the client via the rogue.


Note

While searching the CAM table, WLSE tries to locate the client MAC address, the radio MAC of the rogue, the (radio MAC + 1) of the rogue, and the (radio MAC - 1) of the rogue.

To start the CDP neighbor search, the “Seed IP Addresses” list is pre-populated with one of the following:

- The IP address of the directly connected switch (if available) of the reporting APs.
 - The IP address of the reporting AP.
3. Switch port tracing starts with the rogue MAC address and resumes tracing when it receives a client MAC address. To search for the associated client’s MAC address, WLSE includes managed switches in the same subnet as the switch that is directly connected with the reporting AP.

You can manually add and delete devices to this list. CDP traversal will use these devices as seed devices. This list of devices, called the “Suspected Device List”, will change as the client addresses are reported by the reporting APs.



Note Restarting the Scan & Trace will start the algorithm from the beginning, including the CAM table search.

4. After a CAM search yields a port, an elimination algorithm is run to reduce false positives:
- If a port is a Gig port, skip.
 - If a port is part of channeling ports, skip.
 - If a port is part of port grouping, skip.
 - If CDP neighbor of a port is a managed AP, skip.
 - If CDP neighbor of a port is a non-AP Cisco device, skip.



Note If a hub is connected to a switch port and the hub connects a managed AP and a rogue AP on its downlink, the port will not be suppressed.

5. If the switch port location is found and the switch port suppression feature has been enabled, the WLSE will attempt to shut down the switch port using SNMP.



Note A switch port is suppressed only if a single switch port is traced. When multiple STA addresses are reported and more than one switch port is traced, all switch ports are reported and switch port suppression is skipped. In rare cases, multiple switch ports might appear in the report, for example, when a client is moved in the time between a radio scan and a CAM search.

6. When the switch port location fault is cleared, the WLSE will send a notification to the reporting APs.

Data Produced

When a rogue AP fault is generated and if the rogue AP can be traced, the Rogue Access Point Details window displays information about the switch port to which the rogue AP is connected (see [Tracing Switch Ports and Monitoring Automatic Rogue AP Suppression](#), page 14-34).

Guidelines for Detecting and Suppressing Switch Ports

Prerequisites

Before you can suppress the switch ports of rogue APs, you must:

1. Satisfy the rogue AP detection prerequisites (see [Guidelines for Detecting Rogue APs](#), page 14-14).

**Note**

During initial network deployment, rogue detection must be turned off. Otherwise, between the time an AP is deployed and it is put into the managed state in WLSE, WLSE will attempt to locate the switch port of the newly deployed AP. This will generate many unnecessary faults.

2. Enable rogue AP switch port tracing (see [Setting the Rogue AP Detection Policy, page 14-16](#)).
3. Assign the network-wide settings for enabling automatic rogue access point suppression (see [Setting the Automatic Rogue AP Suppression Policy, page 14-32](#)).

Tips

- To find the switch port to which the rogue AP is connected, check the Switch Port Location information displayed in the Unknown AP Detail window (see [Table 14-11 on page 14-35](#)). If the rogue AP can be traced, this window displays information about the switch port to which the rogue AP is connected.
- If you suspect that a rogue AP was moved and connected to a different port (and automatic suppression has not been enabled), you can click **Re-Trace** on the Rogue Access Point Details window to locate the switch port again (see [Tracing Switch Ports and Monitoring Automatic Rogue AP Suppression, page 14-34](#)).

Related Topics

- [Understanding Switch Port Tracing and Suppression, page 14-30](#)

Setting the Automatic Rogue AP Suppression Policy

Use **IDS > Manage Network-Wide IDS Settings** to enable or disable automatic rogue access point suppression and to view currently suppressed ports.

Typical Scenarios and FAQs

- I want (or no longer want) to suppress the switch port and enable the automatic suppression of switch ports.
- I want to see a list of the currently suppressed switch ports.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage Network-Wide IDS Settings**.

Step 2 Select **Rogue AP Detection**.

**Note**

The switch port suppression settings appear below the rogue AP settings.

Step 3 Complete the following:

Field	Description
Enable	Click Enable to enable automatic rogue AP suppression.
CDP Hop Count	The number of CDP hops made during the rogue discovery process. <ul style="list-style-type: none"> • When the hop count=1, only the seed device and any directly connected neighbor devices are discovered. • The seed devices are the APs that reported the rogue.
Skip Criterion:	
• Gigabit Ethernet Port	If a port is a Gig port, skip.
• Managed AP Port	If CDP neighbor of a port is a managed AP, skip.
• Port Channeling Port	If a port is part of channeling ports, skip.
• Port Grouping Port	If a port is part of port grouping, skip.
• Non-AP CDP Neighbor	If CDP neighbor of a port is a non-AP Cisco device, skip.



Note If a hub is connected to a switch port and the hub connects a managed AP and a rogue AP on its downlink, the port will not be suppressed.

Step 4 Click **Apply** to set the new entry.

Step 5 To view the currently suppressed switch ports, click **View current suppression**. The following information is displayed:

Field	Description
Switch IP	The IP address of the switch to which the rogue AP is connected.
Switch Port	The port to which the rogue AP is connected.
Suppressed AP	The MAC address of the rogue AP.
Timestamp	The time, based on the client browser, the rogue AP switch port was detected (see Understanding WLSE Time Displays, page 1-10).

Step 6 To turn on the port, select **Unshut Port**.

Step 7 Click your browser's **Back** button to return to the network-wide setting window.

Related Topics

- [Tracing Switch Ports and Monitoring Automatic Rogue AP Suppression, page 14-34](#)
- [Setting the Rogue AP Detection Policy, page 14-16](#)

Tracing Switch Ports and Monitoring Automatic Rogue AP Suppression

Use **IDS > Faults** to view information about the switch port to which a rogue AP is connected.

**Note**

Catalyst Operating System (CatOS) software is not supported for switch port tracing.

Typical Scenarios and FAQs

- I want to find the switch port to which a rogue AP is connected.
- I suspect that a rogue AP was moved and connected to a different port. How do I locate it again?

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the switch port detection and suppression prerequisites (see [Guidelines for Detecting and Suppressing Switch Ports, page 14-31](#)).

Procedure

-
- Step 1** Select **IDS > Faults**. The Faults Summary window appears.
- Step 2** Click the Description or Timestamp fields in the Fault Summary table for the device in question.
- In addition to the rogue AP information, the Unknown AP Details window also contains information about the switch to which the rogue AP is connected.

Figure 14-3 Sample Switch Port Tracing Details

1

WLSE Unknown AP Detail - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Help

Rogue Access Point Details

BSSID	State	Vendor	
000c305baf32	Rogue Access Point	Cisco	<input type="button" value="Change to Friendly"/> <input type="button" value="Delete"/>

Beacon Information

SSID	Beacon Interval	Channel	PHY	Data Rates
"tsunami"	100	64	802.11a	Basic: 6.0Mbps, 9.0Mbps, Basic: 12.0Mbps, 18.0Mbps, Basic: 24.0Mbps, 36.0Mbps, 48.0Mbps, 54.0Mbps

Location Estimation

Location	Timestamp	
Location could not be determined. Reporting AP location was not specified.	Wed Nov 03 20:56:51 GMT+00:00 2004	<input type="button" value="View in Location Manager"/>

Switch Port Tracing

Switch IP	Switch Port	Traced MAC Address	Timestamp	
unknown			-	<input type="button" value="Re-Trace"/>

Reporting APs

Reporting AP IP Address	Reporting AP BSSID	RSSI	Reporting AP Location
12.10.10.212	000e3870ba80	-66	
12.10.10.215	000c305baf34	-75	

Associated Clients

Client MAC Address

Fault History

State	Severity	Description	Change	Timestamp	By
Active	P1	Device state is rogue access point	Device state is rogue access point	12:56:51 11/03/2004	

120860

The Switch Port Tracing table contains the following information about the switch to which the rogue AP is connected:

Table 14-11 Switch Port Tracing Table

Column	Description
Switch IP	The IP address of the switch to which the rogue AP is connected.
Switch Port	The port of the switch to which the rogue AP is connected.
Traced MAC Address	The MAC address of the rogue AP or the associated client.
Timestamp	The time, based on the client browser, the rogue AP switch port was detected (see Understanding WLSE Time Displays, page 1-10).
Re-Trace	<p>Click Re-Trace to locate the switch port again. This is useful when you suspect that the rogue AP was moved and connected to a different port.</p> <p>The Re-Trace Switchport window allows you to enter additional seed devices. Using CDP discovery, the Switch Port Location feature uses these seed devices to find the neighboring switches, and then tries to locate the rogue or associated client Ethernet MAC on these switches by querying the MAC address table (see Understanding Switch Port Tracing and Suppression, page 14-30).</p>

- Step 3** To locate a switch port (for example, when you suspect that the rogue AP was moved and connected to a different port):
- a. Click **Re-Trace**. The Re-Trace Switchport window appears.

Figure 14-4 Sample Re-Trace Switchport Window

- b. To add additional seed addresses, enter the IP addresses in the text window and click **Add**. Each new seed address will appear in the Seed IP Addresses list box.
- c. To delete an address, select the address in the list box and click **Delete**.
- d. To start the retrace, click **Trace**.

A log of the switch port tracing progress is displayed in a separate window. This log shows you the detailed state of the fault, including whether a switch port trace is in progress and which switches have already been searched.



Note Refreshing this window while tracing is in progress will *restart* the trace.

- e. The log will be updated when the switch port tracing process is complete. You can then print the log and close the window.

Related Topic

- [Understanding Switch Port Tracing and Suppression, page 14-30](#)
- [Managing Rogue APs, page 14-24](#)

Detecting Ad-Hoc Networks

The following sections will help you understand how and where to use the ad-hoc network detection feature:

- [Understanding Ad-Hoc Network Detection, page 14-37](#)
- [Guidelines for Detecting Ad-Hoc Networks, page 14-37](#)
- [Setting the Ad-Hoc Network Detection Policy, page 14-38](#)
- [Displaying Ad-Hoc Network Faults, page 14-39](#)
- [Viewing Ad-Hoc Network Reports, page 14-41](#)

Understanding Ad-Hoc Network Detection

When setting up a wireless local area network (WLAN), nodes are typically set up as access points to act as bridges to a wired network. The 802.11 standard also specifies an ad-hoc mode for client radio network interface cards (NIC). In this way clients can set up a local network in which participants communicate directly with each other (stations without access points). This is known as an independent basic service set network configuration (IBSS), also known as an ad-hoc network.

Computer manufacturers, specifically laptop manufacturers, are supplying radio NIC's as standard components. The likelihood of having ad-hoc networks created inside an infrastructure WLAN is expected to increase. Ad-hoc networks formed inside a LAN or an infrastructure WLAN are considered a security risk. A member of a wired or infrastructure WLAN that participates in an ad-hoc network could potentially provide unwilling and unwanted access to a wired network. Security conscious customers would like to identify when and where an ad-hoc network is created within their management domain.

When creating an ad-hoc network, the participants issue beacons that synchronize their communication. APs deployed in an infrastructure WLAN can detect these beacons, and therefore the WLSE can detect ad-hoc network creation using this beacon information.

**Note**

The WLSE does not classify IBSS beacons as interference data because it only identifies energy as interference when it cannot interpret the signal data. Because the IBSS beacons are 802.11 data, it *does* interpret these signals and handles them as rogue intrusions.

Guidelines for Detecting Ad-Hoc Networks

Prerequisites

Before you can detect ad-hoc networks, you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management, page 11-5](#)).

**Note**

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

- Be sure Radio Monitoring is enabled on all APs (for both serving and non-serving channels) on the specified floor (see [Starting Radio Monitoring, page 12-4](#)).



Note Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it.

- Set network-wide policies to enable ad-hoc network detection and assign a severity level to the fault that is generated when an ad-hoc network is detected. See [Setting the Ad-Hoc Network Detection Policy, page 14-38](#).

Tips

- If you disable the ad-hoc network fault notification, only the notification is removed; the ad-hoc network detection still occurs.

Related Topics

- [Understanding Ad-Hoc Network Detection, page 14-37](#)

Setting the Ad-Hoc Network Detection Policy

Use **IDS > Manage Network-Wide IDS Settings** to enable ad-hoc network detection and to assign a severity level to the fault that is generated when an ad-hoc network is detected. When an ad-hoc network is detected, a fault is generated and can be viewed under **IDS > Summary**, **IDS > Faults**, or **IDS > Reports**.

Typical Scenarios and FAQs

- I want (or no longer want) to be notified when an ad hoc network is detected.
- I want to specify the severity of an ad hoc network detection notification.
- I want to view the current ad-hoc network faults associated with the current [P1...P5] setting.



Note Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage Network-Wide IDS Settings**.

Step 2 Select **Ad-Hoc Network Detection**.

Step 3 Complete the following:

Field	Description
Enable	Click Enable to enable ad-hoc network detection. This policy is enabled by default. Note If you disable ad-hoc network detection, only the fault notification is removed; the ad-hoc network detection still occurs. The Location Manager displays all rogue stations (ad-hoc networks) in the system regardless of the fault detection setting.
Priority	From the dropdown list, select the severity level to assign the fault when an ad-hoc network is detected.

- Step 4** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 5** To see the faults associated with this setting, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Ad-Hoc Networks Detected**.
-

Related Topics

[Detecting Ad-Hoc Networks, page 14-37](#)

Displaying Ad-Hoc Network Faults

Use **IDS > Summary** to view the fault that is generated when an ad-hoc network is detected. This window allows you to:

- View a list of APs that have reported the ad-hoc network and, if available, the building and floor the AP is in.
- View a list of clients that are associated with the ad-hoc network (if available). The grouping is based upon the SSID used in the ad-hoc network.

Typical Scenarios and FAQs

- I have just been notified of an ad hoc network. What part of my network has detected this? Where is it physically in my network?
- I have just been notified of an ad hoc network. What other NICs are participating in this network?
- I have just been notified of an ad hoc network and I have determined it is no longer a problem. How do I clear the fault?



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the ad-hoc network detection prerequisites (see [Guidelines for Detecting Ad-Hoc Networks, page 14-37](#)).

Procedure

- Step 1** Select **IDS > Summary**. The Intrusion Detection Summary window appears.
- Step 2** Select **Ad-Hoc Networks Detected**. The Faults for Ad-Hoc Networks Detected window appears.
- Step 3** Select the Description or Timestamp fields for the fault. The Fault Details window displays the information about the fault for the selected device (see [Viewing Fault Details, page 3-7](#)).

Step 4 The Unknown AP Detail window for ad-hoc networks contains the following information:

Figure 14-5 Sample Unknown AP Detail Window For Ad-hoc Networks

The screenshot shows a web browser window titled "WSE Unknown AP Detail - Microsoft Internet Explorer provided by Cisco Systems, Inc.". The page content is organized into several sections:

- Rogue Ad-hoc Network Details:** A table with columns BSSID, State, and Vendor. A single row shows BSSID "e611ae029e02", State "Rogue Ad-hoc Network", and Vendor "unknown". There are buttons for "Change to Friendly" and "Delete".
- Beacon Information:** A table with columns SSID, Beacon Interval, Channel, PHY, and Data Rates. A row shows SSID "adhocmysid", Beacon Interval "100", Channel "1", PHY "802.11b", and Data Rates "Basic: 1.0Mbps, Basic: 2.0Mbps, Basic: 5.5Mbps, Basic: 11.0Mbps".
- Location Estimation:** A table with columns Location and Timestamp. A row shows Location "Location could not be determined. Reporting AP location was not specified." and Timestamp "Fri Jan 07 22:30:34 GMT+00:00 2005".
- Reporting APs:** A table with columns Reporting AP IP Address, Reporting AP BSSID, RSSI, and Reporting AP Location. A row shows IP "12.10.80.20", BSSID "00028a0e33b0", and RSSI "-70".
- Participating Clients (if Available):** A table with columns MacAddress, Last Known Ip Address, Last Known EAP Name, and Last Known Client Name. A row shows MacAddress "0009e862993a" and all other fields as "Unavailable".

Three callouts are present: '1' points to the 'Reporting APs' table, '2' points to the 'Rogue Ad-hoc Network Details' table, and '3' points to the 'Participating Clients' table.

1	A list of the APs that have reported the ad-hoc network and, if available, the approximate location (building and floor) of each reporting AP.
2	The approximate location of the ad-hoc participant.
3	A list of the other NICs that are participating in this network. This list is a “best effort” given the beacon information. The source MAC address in the beacon is used to identify each NIC. The ad-hoc network is identified based on the BSSID and the SSID combination used in the network.

Step 5 To clear a fault that is generated when an ad-hoc network is detected, see [Clearing Summary Table Faults](#), page 3-6.



Note Because only the *creation* of a network can be detected, this is the only means of clearing an ad-hoc network detection fault.

Related Topics

- [Understanding Ad-Hoc Network Detection](#), page 14-37
- [Setting the Rogue AP Detection Policy](#), page 14-16

- [Viewing Ad-Hoc Network Reports, page 14-41](#)
- [Using the Faults Subtab, page 14-4](#)

Viewing Ad-Hoc Network Reports

The Ad-hoc Networks report allows you to view a history of the APs within buildings and floors that have reported ad-hoc networks.



Note The NICs participating in an ad-hoc network will be a *best effort* given the beacon information.

Typical Scenarios and FAQs

- How can I see any ad-hoc networks and their participating clients?



Note Your login determines whether you can use this option.

Before You Begin

Satisfy the ad-hoc network detection prerequisites (see [Guidelines for Detecting Ad-Hoc Networks, page 14-37](#)).

Procedure

- Step 1** Select **IDS > Reports**.
- Step 2** From the Report Name list, select **Ad-hoc Network Report**.
- Step 3** To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).



Note To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.

- Step 4** To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.
- Step 5** To narrow the search criteria:
- Select **Participant MAC Address**, **Participant IP Address**, **Participant EAP User Name**, or **Network BSSID** from the dropdown list.
 - Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
 - Click **Search**.
- The data that satisfies the search criteria is displayed below the Search field. The Ad-Hoc Network report, which appears to the right of this list, displays the information for the first entry in the list.
- Click any other entry in the list to display its corresponding report.

The Ad-Hoc Network report contains the following information:

Column	Description
Client MAC Address	The MAC address of each client radio (that WLSE knows of) that is participating in the network (there could be more). The source MAC address in the beacon is used to identify each NIC.
BSSID	Basic Service Set Identifier—The unique identifier for the ad-hoc network.
Last SSID	The last Service Set Identifier. The SSID is an identifier that client devices use to associate with the access point. Note When an AP is configured to not broadcast its SSID, this field will either be blank or contain hex zeros. (When a Cisco AP is configured to not broadcast its SSID, that AP sends null characters (hex zeros) in place of the SSID in the beacon.)
Last Known IP Address	Last known IP address of the client when it was associated with any AP managed by the WLSE. Note This information might not be available or it might not be current.
Last Known EAP Name	The RADIUS username of the client. (User names are not available for non-EAP authentications.) The RADIUS username is generally available in all EAP authentication cases, except for PEAP and EAP-TTLS. In these instances, the availability of the information is dependent on vendor support. Note This information might not be available or it might not be current.
Last Known Client Name	Last known client name. Note This information might not be available or it might not be current.
Last Association With	The last AP managed by WLSE with which the client was associated. Note This information might not be available or it might not be current.
PHY	The type of 802.11 radio the client is using (11a or 11b/11g/11n).
Estimated Location	The estimated location of the client (uses the same location algorithm as rogue AP detection).
Reported By Client	Y = A client detected the network. N = An infrastructure AP detected the network.
First Seen	The time WLSE first heard one of the ad-hoc network beacons that was transported to WLSE via the WDS setup. For more information, see Understanding WLSE Time Displays, page 1-10 .

Step 6 Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Understanding Ad-Hoc Network Detection, page 14-37](#)
- [Using the Basic Report Features, page 10-1](#)

- [Using the IDS Reports Subtab, page 14-5](#)

Detecting Interference

Radio Monitoring continuously monitors your WLAN radio environment to discover the presence of any interference.

**Note**

Interference information is collected only from access points that are on the Radio Monitoring list and the clients associated with these access points.

The following sections will help you understand how and where to use the interference detection feature:

- [Understanding Interference Detection, page 14-43](#)
- [Guidelines for Detecting Interference, page 14-44](#)
- [Setting the Interference Detection Policy, page 14-45](#)
- [Displaying Interference Faults, page 14-46](#)

Understanding Interference Detection

This feature allows you to start interference detection and choose what level of signal strength and duration of signal is required to detect interference. Only access points in the Radio Monitoring list and clients associated with these APs can participate in interference detection.

**Note**

Radio Monitoring is enabled by default. *If you disable Radio Monitoring, you will not be able to detect non-802.11 interference.*

How It Works

The Radio Monitoring feature uses the radio measurement capabilities to discover any new interference. The WLSE defines interference as a non-802.11 signal. An interference fault, therefore, reports signals that cannot be decoded by the access point; that is, energy that cannot be decoded as a valid 802.11 signal.

The WLSE can tell if a signal is from an 802.11 device (such as another access point or client) or a non-802.11 device (such as a microwave oven or cordless phone) as long as the signal is strong enough to be demodulated. When access points are close enough to each other, the access point can tell that the signal is from another access point and will not generate an interference report. If the access point is not known to the WLSE, it flags it as an unknown radio and lets the user make the disposition decision.

If the signal is too weak to be demodulated, or the signal is garbled, or the signal is coming from a non-802.11 device, it presents itself as energy. The access point then reports the detection of such energy levels to the WLSE, which uses the appropriate interference fault profile parameter to decide whether to generate a fault.

If a signal can be decoded as 802.11, then it is a contending signal, not interference. While this neighboring 802.11 signal may interfere with the operation of the access point, it is not causing any radio interference. However, because the access point can actually decode the signal, the two access points will be contending for the channel. Neither one will be allowed to transmit at the same time because they

are following the MAC rules. In other words, they never cause each other any radio interference. You can use the Location Manager to see the interaction of 802.11 signals and determine the amount of overlap between neighboring access points.

Data Produced

When Radio Monitoring detects interference, a new fault is generated. To view details about an interference fault:

1. Select **IDS > Summary > Interference Detected**.
2. Click the link in the Description or Timestamp fields to view the Fault Details window (see [Viewing Fault Details](#), page 3-7).

Related Topics

- [Using Radio Monitoring to Collect RM Data](#), page 12-1

Guidelines for Detecting Interference

Prerequisites

Before you can detect non-802.11 interference, you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management](#), page 11-5).



Note If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab](#), page 14-11). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults](#), page 11-4.

2. Be sure Radio Monitoring is enabled on all APs (for both serving and non-serving channels) on the specified floor (see [Starting Radio Monitoring](#), page 12-4).



Note Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it.

3. Set the threshold condition for interference detection (see [Setting the Interference Detection Policy](#), page 14-45).
4. Define the location elements (buildings and floors) and place the APs on the floor images. This step is optional, but will help you get the best results from the Location Manager displays. For more information, see:
 - [Entering Building Information](#), page 13-4
 - [Adding Floors to Location Manager](#), page 13-9
 - [Adding Devices to Floors](#), page 13-14

Tips

- To detect interference, Radio Monitoring must be running.
- When the signal from a friendly AP is strong enough to cause an interference fault but not strong enough to see the signal as a valid 802.11 signal, there is no way to exclude the transmission from this device. If WLSE can decode the signal as 802.11, then it will not classify it as interference; if it cannot decode the signal, it does not know it comes from a friendly device.

Therefore, if you see “Non-802.11 Interference Detected” fault messages from a friendly AP, you should raise the level at which interference is faulted (see [Setting the Interference Detection Policy, page 14-45](#)).

Related Topics

- [Understanding Interference Detection, page 14-43](#)

Setting the Interference Detection Policy

Use **IDS > Manage Network-Wide IDS Settings** to enable radio frequency interference detection and to assign a severity level to the fault that is generated when interference is detected. When interference is detected, a fault is generated and can be viewed under **IDS > Faults**.

**Note**

Applying new settings will clear all existing non-802.11 interference faults.

Typical Scenarios and FAQs

- I want (or no longer want) to be notified when the interference level for a radio type exceeds a certain level for a specified time.
- I want to choose what level of signal strength and duration of signal is required to detect interference.
- I want to choose at what level of signal strength and duration of signal an interference fault is automatically cleared.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage Network-Wide IDS Settings**.

Step 2 Select **Interference Detection**.

Step 3 Complete the following:

Field	Description
Interference Fault Severity	Select the severity level to associate with this setting. For more information about fault severity levels, see Displaying Faults, page 3-4 .

Field	Description
Enable 802.11b/g Interface Settings - and - Enable 802.11a Interface Settings	Select to enable the policy.
Degraded	Select the criteria that identifies an interference fault: <ul style="list-style-type: none"> • The minimum interference level (in dB) • The percentage of time the interference level exceeds the minimum interference level during each measurement interval • The time interval
Up	Select the time interval after which, if the interference level falls below the minimum interference level for a percentage of time, the interference fault for that device is cleared.



Caution Applying new settings will clear all existing non-802.11 interference faults.

Step 4 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 5 To see the faults associated with this setting, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary > Interference Detected**.

Related Topics

- [Understanding Interference Detection, page 14-43](#)

Displaying Interference Faults

Use **IDS > Summary > Interference Detected** to view a summary of the devices that have detected non-802.11 interference. This window allows you to:

- View a list of APs that have reported the interference and, if available, the building and floor in which the AP is located.
- View a history of the interference faults for the selected device.
- Clear a fault that is generated when radio frequency interference is detected.

Typical Scenarios and FAQs

- How can I see a history of radio frequency interference in my network?

- I have just been notified of radio interference and I have determined it is no longer a problem. How do I clear the fault?

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the interference detection prerequisites (see [Guidelines for Detecting Interference, page 14-44](#)).

Procedure

- Step 1** Select **IDS > Summary**. The Intrusion Detection Summary window appears.
- Step 2** Select **Interference Detected**. The Faults for Interference Detected window appears.
- Step 3** Select the Description or Timestamp fields for the fault. The Fault Details window displays the information about the fault for the selected device (see [Viewing Fault Details, page 3-7](#)).
- Step 4** To clear an interference fault, see [Clearing Summary Table Faults, page 3-6](#).

Related Topics

[Understanding Interference Detection, page 14-43](#)

Detecting Excessive Management Frame Transmissions

Radio Monitoring continuously monitors your WLAN radio environment to discover the presence of any Excessive Management Frame (EMF) transmissions.

**Note**

EMF information is collected only from access points that are on the Radio Monitoring list and the clients associated with these APs.

The following sections will help you understand how and where to use the EMF detection feature:

- [Understanding Excessive Management Frame Detection, page 14-47](#)
- [Guidelines for Using Excessive Management Frame Detection, page 14-48](#)
- [Setting the Excessive Management Frame Detection Policy, page 14-49](#)
- [Displaying EMF Detection Faults, page 14-50](#)
- [Viewing EMF Detection Reports, page 14-50](#)

Understanding Excessive Management Frame Detection

APs must provide a means of determining that normal WLAN management and control frames have exceeded a default threshold. In a DOS attack, an attacker can broadcast so many management frames that the APs become overwhelmed while trying to process the frames and throughput is affected. As part of the WLSE IDS feature set, scanning-only APs can monitor radio frequency signals, detect excessive management frame transmission, and raise a fault when a user-defined threshold is crossed.

There are two types of EMF faults:

- **Per Station:** A station can be a laptop, an access point, a PDA, or any device. The station is identified by the radio MAC address, which is the BSSID.
- **Per Channel:** For channel faults, frames from all stations are aggregated, so it doesn't matter which station is generating the fault.

You can use Excessive Management Frame (EMF) detection to detect transmissions of the following frames:

- Association requests and responses
- Reassociation requests and responses
- Probe requests and responses
- Disassociation
- Authentication
- Deauthentication
- Action Frames

You can specify the duration and count of each type of management frame.

Guidelines for Using Excessive Management Frame Detection

Prerequisites

Before you can use Excessive Management Frame detection, you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management, page 11-5](#)).



Note

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

2. Be sure Radio Monitoring is enabled (see [Starting Radio Monitoring, page 12-4](#)).



Note

Radio Monitoring is enabled by default; if it has been disabled, you must re-enable it.

3. Enable Excessive Management Frame detection mode on selected scanning-only APs (see [Configuring Frame Monitoring, page 12-20](#)).
4. Set the threshold condition for EMF detection (see [Setting the Excessive Management Frame Detection Policy, page 14-49](#)).

Related Topics

[Understanding Excessive Management Frame Detection, page 14-47](#)

Setting the Excessive Management Frame Detection Policy

Use **IDS > Manage IDS Settings** to enable EMF detection, assign thresholds, and assign a severity level to the fault that is generated when an EMF is exceeded. When an EMF threshold is exceeded, a fault is generated and can be viewed under **IDS > Faults** or **IDS > Summary**.

Typical Scenarios and FAQs

- I want to specify the severity and threshold levels for frame management request counts.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.

Step 2 Select an existing IDS fault profile and click **Edit**.

Step 3 Select **Excessive Management Frame Detection**.

Step 4 Complete the following:

Field	Description
Severity	From the dropdown list, select the severity level to assign the fault.
Per Channel Settings and Per Station Settings	
Enabled	For each frame type, select to enable the policy.
Frame Count	The threshold for generating the EMF fault. If the number of frames seen during the observation time exceed the frame count, then that EMF fault is raised.
Observation Time	A sliding window of time over which the number of frames is monitored (that is, “if x frames have been seen in the last y ms, generate a fault”).

Step 5 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 6 To see the faults associated with this threshold, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser’s **Back** button to return to the network-wide setting window.
- Select **IDS > Summary > Excessive Management Frames**.

Step 7 To assign this profile to a device or group of devices, click **Assign Devices** (see [Assigning Devices to an IDS Fault Profile, page 14-9](#)).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Detecting Excessive Management Frame Transmissions, page 14-47](#)

Displaying EMF Detection Faults

Use **IDS > Summary** to view a summary of the devices that have detected excessive management frame transmissions. This window allows you to:

- View a list of APs that have reported the EMF transmission and, if available, the building and floor in which the AP is located.
- View a history of the EMF transmission faults for the selected device.
- Clear a fault that is generated when an EMF transmission is detected.



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting excessive management frame transmissions (see [Guidelines for Using Excessive Management Frame Detection, page 14-48](#)).

Procedure

-
- Step 1** Select **IDS > Summary**. The Intrusion Detection Summary window appears.
- Step 2** Select **Excessive Management Frames**. The Faults for Excessive Management Frames window appears.
- Step 3** Select the Description or Timestamp fields for the fault. The Fault Details window displays the information about the fault for the selected device (see [Viewing Fault Details, page 3-7](#)).
- Step 4** To clear an EMF fault, see [Clearing Summary Table Faults, page 3-6](#).
-

Related Topics

- [Viewing EMF Detection Reports, page 14-50](#)
- [Understanding Excessive Management Frame Detection, page 14-47](#)

Viewing EMF Detection Reports

The EMF Detection Report displays the collected Excessive Management Frame (EMF) statistics.

Typical Scenarios and FAQs

- How do I view the EMF statistics?



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting excessive management frame transmissions (see [Guidelines for Using Excessive Management Frame Detection, page 14-48](#)).

Procedure

- Step 1** Select **IDS > Reports**.
- Step 2** From the Report Name list, select **EMF Detection Report**.
- Step 3** To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).



Note To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.

- Step 4** To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.
- Step 5** To narrow the search criteria:
- Select **Reported From, Frame Type, Network BSSID, or Transmit Address** from the **Filter By** dropdown list.
 - Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
 - Click **Search**.

The data that satisfies the search criteria is displayed below the Search field. The Excessive Management Frame report, which appears to the right of this list, displays the information for the first entry in the list.

- Click any other entry in the list to display its corresponding report.

The Excessive Management Frame report displays the following information:

Table 14-12 Excessive Management Frame Report

Column	Description
Reported From	The station that reported the attack.
BSSID	The radio interface of the reporting AP. Note This column is meaningful only for Station faults (see Understanding Excessive Management Frame Detection, page 14-47).
AP Name	For channel faults, the name of the scanning-only AP that detected excessive management frame transmissions.
Channel	The channel that is performing EMF detection.

Table 14-12 Excessive Management Frame Report (continued)

Column	Description
Frame Type	The frame types that are being monitored: <ul style="list-style-type: none"> • Associated • ReAssociated • DisAssociated • Authenticated • DeAuthenticated • Probe • Action Frame
Observed Frame Count	The total number of frames detected during the observation interval.
Observation Time	The duration (200 to 5000 milliseconds) during which measurements were taken.
Threshold Frame Count	The number of frames that must be seen in the Observation Time period to generate a fault.
Transmit Address	For Station faults, the address of the station that is sending the excessive management packets. For Channel faults, the transmit address is just one of the stations.
Detection Time	The time, based on the client browser, that the scanning-only AP detected excessive management frame transmissions (see Understanding WLSE Time Displays, page 1-10).

Step 6 Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Using the IDS Reports Subtab, page 14-5](#)

Detecting Management Frame Protection Faults

The following sections describe how to use the Management Frame Protection (MFP) feature:

- [Understanding Management Frame Protection, page 14-53](#)
- [Setting the Management Frame Protection Policy, page 14-54](#)
- [Displaying Management Frame Protection Faults, page 14-55](#)
- [Viewing MFP Capabilities Reports, page 14-56](#)
- [Viewing MFP Events Reports, page 14-57](#)
- [Viewing MFP-Client Events Reports, page 14-58](#)

Understanding Management Frame Protection

Although the data frames passing through an 802.11 network are considered to have excellent authentication and privacy through the protocol enhancements of 802.11i, control and management frames are still extremely vulnerable in a strictly 802.11-standard network. Because control and management frames are unauthenticated, any rogue device can, for example, mimic an access point and tell 802.11 client devices that they are no longer associated to that AP.

Management Frame Protection (MFP) inserts secure authentication information into 802.11 management frames to prevent this type of attack. This feature allows network infrastructure devices (APs and their related servers) to be MFP generators and detectors, essentially cross-checking each other during network operations. The primary network-level management takes place at the Wireless Domain Server (WDS) level, and the managed APs provide both generation and detection capabilities. The WLSE functions as a reporting mechanism by logging alerts, sending email to administrators, and so on.

When MFP is enabled for a network, each MFP-capable detector AP queries the WDS when it first observes a management frame from a given generator AP. The WDS tells the detector whether the generator should be producing MFP frames, and, if so, what its AAA keys should be. If the WDS's expectation of the MFP state of the generator AP is violated, the detector AP sends the WDS an MFP report. As all generator APs' AAA keys are rotated, the WDS informs all detector APs ahead of time to avoid false alarms.

Anomalies are reported by a detector AP when the AP receives an 802.11 management frame with one of the following packet states:

MFP State	802.11 Packet States
Enabled	Invalid MIC Invalid NTP/Sequence Counter No MIC in packet
Disabled	MIC was found when none was expected

Guidelines for Using Management Frame Protection

Prerequisites

Before you can run Management Frame Protection (MFP), you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management, page 11-5](#)).



Note

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

2. Enable the Management Frame Protection network-wide setting (see [Setting the Management Frame Protection Policy, page 14-54](#)).

- Configure the access points and WDSs within your network to make use of a Simple Network Time Protocol (SNTP) server. Without time synchronization of the access points and WDSs to an SNTP server, the strength of MFP to protect the network is substantially weakened.

Setting the Management Frame Protection Policy

Use **IDS > Manage Network-Wide IDS Settings** to enable Management Frame Protection (MFP) and to assign a severity level to MFP faults.

Typical Scenarios and FAQs

- I want (or no longer want) to be notified when a Management Frame Protection fault is detected.
- I want to specify the severity of Management Frame Protection detection notifications.
- I want to view the current Management Frame Protection faults associated with the current [P1...P5] setting.

Before You Begin

Satisfy the Management Frame Protection prerequisites (see [Guidelines for Using Management Frame Protection](#), page 14-53).



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage Network-Wide IDS Settings**.

Step 2 Select **Management Frame Protection**.

Step 3 Complete the following:

Field	Description
MFP Configuration	
Enable	Click Enable to start Management Frame Protection fault detection. This policy is not enabled by default.
MFP Violation	Select the severity level to assign the fault when a Management Frame Protection fault is detected.
MFP Configuration Mismatch	Select the severity level to assign the fault when an access point's MFP configuration is not as expected.
MFP Time Sync Error	Select the severity level to assign the fault when an access point's MFP timebase is not synchronized.
MFP-Client Configuration	
Click See detail for information on how to configure this option.	
Client MFP Violation	Select the severity level to assign the fault when a client Management Frame Protection fault is detected.

Step 4 To view the current faults for Management Frame Protection, click **View current faults for this setting**.

- Step 5** Click **Apply** to set the new entries.
- Step 6** To view the MFP Violation faults associated with this profile, click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window. You can also use these options to display MFP faults:
- To view all other faults in addition to the MFP faults, select **IDS > Faults**.
 - To view only the MFP Violation faults, select **IDS > Reports > MFP Events**.
-

Related Topics

[Understanding Management Frame Protection, page 14-53](#)

Displaying Management Frame Protection Faults

You can use **IDS > Summary > MFP Errors** to:

- View a list of APs that are *generating* MFP violations (*not* detecting them).
- View a history of the MFP faults for the selected device.
- Clear a fault that is generated when an MFP violation is detected.



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting Management Frame Protection (MFP) violations (see [Guidelines for Using Management Frame Protection, page 14-53](#)).

Procedure

- Step 1** Select **IDS > Summary**. The Intrusion Detection Summary window appears.
- Step 2** Select **MFP Errors**. The Faults for MFP Errors window appears.



Note

The Management Frame Protection Anomaly Category panel, located below the **MFP Errors** link, summarizes the number of MFP reports that are reporting different MFP errors.

- Step 3** Select the Description or Timestamp fields for the fault. The Fault Details window displays the information about the fault for the selected device (see [Viewing Fault Details, page 3-7](#)).
- Step 4** To clear an MFP fault, see [Clearing Summary Table Faults, page 3-6](#).
-

Related Topics

- [Understanding Management Frame Protection, page 14-53](#)
- [Setting the Management Frame Protection Policy, page 14-54](#)

Viewing MFP Capabilities Reports

The MFP Capabilities Report displays the Management Frame Protection (MFP) capabilities of the WLSE's managed APs.


Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting Management Frame Protection (MFP) transmissions (see [Guidelines for Using Management Frame Protection, page 14-53](#)).

Procedure

-
- Step 1** Select **IDS > Reports**.
- Step 2** From the Report Name list, select **MFP Capabilities Report**.
- Step 3** To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).


Note

To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.

- Step 4** To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.
- Step 5** To narrow the search criteria:
- Select **AP Name**, **BSSID**, **PHYType**, or **Software Version** from the **Filter By** dropdown list.
 - Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
 - Click **Search**.

The data that satisfies the search criteria is displayed below the Search field. The Management Frame Protection Capabilities report, which appears to the right of this list, displays the information for the first entry in the list.

- Click any other entry in the list to display its corresponding report.

The Management Frame Protection Capabilities report displays the following information:

Table 14-13 Management Frame Protection Capabilities Report

Column	Description
AP Name	The name of the managed AP.
BSSID	The radio interface of the managed AP.
PHY	The physical interface type (11a, 11b, or 11g) of the managed AP's radio interface.
Software Version	The software version running on the device.

Table 14-13 Management Frame Protection Capabilities Report (continued)

Column	Description
Generator Capability	The generator capability of the managed AP: None, Full, Non-Beacon/Non-Probe Response.
Detector Capability	The detector capability of the managed AP: None, Full.

Step 6 Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Guidelines for Using Management Frame Protection, page 14-53](#)

Viewing MFP Events Reports

The MFP Events Report displays details about the Management Frame Protection (MFP) events reported by the WLSE's managed APs.

Multiple reports are combined together as a single MFP event when the reports are received:

- From the same Detector AP
- About the same Generator AP
- In the same Anomaly Category
- Less than two minutes apart from each other

This information is used to compute the First Event and Latest Event times (see [Table 14-14](#)).



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting Management Frame Protection (MFP) transmissions (see [Guidelines for Using Management Frame Protection, page 14-53](#)).

Procedure

Step 1 Select **IDS > Reports**.

Step 2 From the Report Name list, select **MFP Events Report**.

Step 3 To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).



Note

To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.

Step 4 To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.

Step 5 To narrow the search criteria:

- a. Select **Generator AP Name**, **Generator BSSID**, **Detector AP Name**, **Detector BSSID**, **Generator PHY Type**, or **Category of Anomaly** from the dropdown list.
- b. Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
- c. Click **Search**.

The data that satisfies the search criteria is displayed below the Search field. The Management Frame Protection Events report, which appears to the right of this list, displays the information for the first entry in the list.

- d. Click any other entry in the list to display its corresponding report.

The Management Frame Protection Events report displays the following information:

Table 14-14 Management Frame Protection Events Report

Column	Description
Generator AP Name	The name of the generator AP.
Generator BSSID	The radio interface of the generator AP.
Detector AP Name	The name of the detector AP.
Detector BSSID	The radio interface of the detector AP.
Generator PHY	The physical interface type (11a, 11b, or 11g) of the generator AP's radio interface.
First Event	The time of the first report of this event during the time interval.
Latest Event	The time of the most recent report of this event during the time interval.
Category of Anomaly	The type of anomaly reported by the detector AP (see Understanding Management Frame Protection, page 14-53).
Number of Anomalies	The total number of anomalies of this event during the time interval.
Packet Types	The type of 802.11 packets in which the anomaly was observed.

Step 6 Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Guidelines for Using Management Frame Protection, page 14-53](#)

Viewing MFP-Client Events Reports

The MFP-Client Events Report displays details about the MFP-Client events reported by the WLSE's managed APs.

Multiple reports are combined together as a single MFP-Client event when the reports are received:

- From the same Detector AP
- In the same Anomaly Category

- Less than two minutes apart from each other

This information is used to compute the First Event and Latest Event times (see [Table 14-15](#)).

**Note**

Your login determines whether you can use this option.

Before You Begin

Satisfy the prerequisites for detecting MFP-Client transmissions (see [Guidelines for Using Management Frame Protection, page 14-53](#)).

Procedure

Step 1 Select **IDS > Reports**.

Step 2 From the Report Name list, select **MFP-Client Events Report**.

Step 3 To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).

**Note**

To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.

Step 4 To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.

Step 5 To narrow the search criteria:

- Select **Client MAC**, **Detector AP Name**, **Detector BSSID**, or **Category of Anomaly** from the dropdown list.
- Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
- Click **Search**.

The data that satisfies the search criteria is displayed below the Search field. The MFP-Client Events report, which appears to the right of this list, displays the information for the first entry in the list.

- Click any other entry in the list to display its corresponding report.

The Management Frame Protection Events report displays the following information:

Table 14-15 Management Frame Protection Events Report

Column	Description
Client MAC	The MAC address of the MFP-Client.
Detector AP Name	The name of the detector access point.
Detector BSSID	The radio interface of the detector access point.
First Event	The time of the first report of this event during the time interval.
Latest Event	The time of the most recent report of this event during the time interval.
Category of Anomaly	The type of anomaly reported by the detector access point (see Understanding Management Frame Protection, page 14-53).

Table 14-15 Management Frame Protection Events Report (continued)

Column	Description
Number of Anomalies	The total number of anomalies of this event during the time interval.
Packet Types	The type of 802.11 packets in which the anomaly was observed.

- Step 6** Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Guidelines for Using Management Frame Protection, page 14-53](#)

Detecting Unregistered Clients

The following sections describe how to use the Unregistered Client detection feature:

- [Understanding Unregistered Client Detection, page 14-60](#)
- [Guidelines for Using Unregistered Client Detection, page 14-60](#)
- [Enabling Unregistered Client Detection, page 14-61](#)
- [Displaying Unregistered Client Faults, page 14-62](#)
- [Viewing Unregistered Client Reports, page 14-63](#)

Understanding Unregistered Client Detection

Unregistered clients are clients that are:

- Unsuccessfully attempting to authenticate with the APs during the observation interval and the number of failed attempts crosses the threshold defined by the administrator.
- Sending probe requests.

When you enable the Unregistered Client feature, the WLSE will command all clients (CCX V2 or later with radio management capability) to perform the same radio measurements both on- and off-channels. The clients will then scan other channels in a similar manner to the APs that are performing Radio Monitoring.



Note Clients that participate in Radio Monitoring *do not* increase the coverage area of the network.

Guidelines for Using Unregistered Client Detection

Prerequisites

Before you can use detect unregistered clients, you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management, page 11-5](#)).



Note If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

2. Configure access points that will be checking for unregistered clients to run in scanning-only mode.
3. Set the threshold condition for unregistered client detection (see [Enabling Unregistered Client Detection, page 14-61](#)).

Tips

- The Unregistered Client option is applicable only for an AP in *scanning* mode. When an AP is in scanning mode, it monitors the radio environment by looking for rogue APs and unassociated clients; it does not accept client associations.

Enabling Unregistered Client Detection

Use this option to enable unregistered client detection and set the threshold condition and fault priority level.



Note Your login determines whether you can use this option.

Typical Scenarios and FAQs

- I want (or no longer want) to be notified when an unregistered client has been detected.
- I want to specify the severity of an unregistered client detection notification.

Before You Begin

Satisfy the unregistered client detection prerequisites (see [Guidelines for Using Unregistered Client Detection, page 14-60](#)).

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **Unregistered Client**.



Note The Unregistered Client option is applicable only for an AP in *scanning* mode.

- Step 4** Complete the following:

Field	Description
Enable	Click Enable to enable unregistered client detection. This setting is enabled by default.

Field	Description
Priority	From the dropdown list, select the severity level to assign the fault.
Client Registration Request Count	Enter the minimum value that, when exceeded during a period of 15 minutes, will generate a fault.

- Step 5** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Unregistered Clients Detected**.
- Step 6** Click **Apply** to set the new entries.
- Step 7** To assign this profile to a device or group of devices, click **Assign Devices** (see [Assigning Devices to an IDS Fault Profile, page 14-9](#)).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Viewing Unregistered Client Reports, page 14-63](#)

Displaying Unregistered Client Faults

Use **IDS > Summary > Unregistered Clients Detected** to view a summary of the unregistered clients.

Typical Scenarios and FAQs

- I have just been notified of an unregistered client. What part of my network has detected this?
- I have just been notified of an unregistered client and I have determined it is no longer a problem. How do I clear the fault?



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the unregistered client detection prerequisites (see [Guidelines for Using Unregistered Client Detection, page 14-60](#)).

Procedure

- Step 1** Select **IDS > Summary**. The Intrusion Detection Summary window appears.
- Step 2** Select **Unregistered Clients Detected**. The Faults for Unregistered Clients Detected window appears.
- Step 3** To view information about a specific fault, select the Description or Timestamp fields for that fault. The Fault Details window displays the fault information (see [Viewing Fault Details, page 3-7](#)).
- Step 4** To clear an unregistered client fault, see [Clearing Summary Table Faults, page 3-6](#).

Related Topics

[Understanding Unregistered Client Detection, page 14-60](#)

Viewing Unregistered Client Reports

The Unregistered Client Report displays any unregistered clients that are present in the wireless network.

Typical Scenarios and FAQs

- I want to view the unregistered clients that are present in my network.

**Note**

Your login determines whether you can use this option.


Before You Begin

Satisfy the unregistered client detection prerequisites (see [Guidelines for Using Unregistered Client Detection, page 14-60](#)).

**Note**

This report is only available from APs in scanning-only mode.

Procedure

-
- Step 1** Select **IDS > Reports**.
- Step 2** From the Report Name list, select **Unregistered Client Report**.
- Step 3** To view all records, click **View** (located to the right of the Report Name, Start Date, and End Date dropdown lists).
-  **Note** To see all records *after* a filtering selection has been entered, select another report, then return to this one and click **View**.
-
- Step 4** To view the information for a longer time period (the default is one day), select **Start Date** and **End Date** values from the pulldown lists and click **View**.
- Step 5** To narrow the search criteria:
- a. Select **Scanning AP Name** or **Client MAC Address** from the dropdown list.
 - b. Enter any filtering criteria in the text box. You can use an asterisk (*) as a wild card to denote numbers and letters.
 - c. Click **Search**.
- The data that satisfies the search criteria is displayed below the Search field. The Unregistered Clients report, which appears to the right of this list, displays the information for the first entry in the list.
- d. Click any other entry in the list to display its corresponding report.

The Unregistered Clients report displays the following information:

Table 14-16 *Unregistered Clients Report*

Column	Description
Scanner AP	The IP address of the reporting AP.
Client MAC	The MAC address of the unregistered client.
Probe Request	The probe request from the unregistered client.
Association Request	The association request from the unregistered client.
Last Seen Time	Indicates the time, based on the client browser, that a scan was run and the unregistered client was detected.

Step 6 Use the buttons to the right of the Report Name, Start Date, and End Date lists to export or email this report.

Related Topics

- [Using the IDS Reports Subtab, page 14-5](#)
- [Detecting Unregistered Clients, page 14-60](#)

Detecting Authentication and Protection Attacks

The following sections describe how to use the Authentication and Protection Attack detection features:

- [Understanding Authentication and Protection Attack Detection, page 14-65](#)
- [Guidelines for Using Authentication and Protection Detection, page 14-66](#)
- [Enabling Authentication and Protection Attack Detection, page 14-67](#)
- [Displaying Authentication and Protection Attack Faults, page 14-81](#)

Understanding Authentication and Protection Attack Detection

The WLSE provides several methods of authentication and protection attack detection:

- [MIC/Encryption Failures, page 14-65](#)
- [MAC Spoofing, page 14-65](#)
- [EAPOL Flooding, page 14-66](#)

MIC/Encryption Failures

After a client successfully authenticates with an AP, it can begin protecting data frames sent to and from the AP. Several failures that can be identified during this protection phase can broadly be categorized as decrypt errors, MIC failures or replay failures. In all cases, when the AP detects a given failure, it updates the appropriate MIB counter.

In addition, the Michael MIC employed in TKIP is known to be weak and requires some additional counter measures to ensure protection. The counter measure involves disabling the interface whenever the MIC has been deemed to be compromised. Each time a counter measure is enforced a MIB variable is incremented.

The WLSE periodically polls the MIB counters described above and compares against a pre-defined threshold to determine when a failure has occurred. When a failure takes place, the WLSE generates a fault.

MAC Spoofing

When a client roams from one AP to another, the switches connected to the AP must update the forwarding tables so that the client's layer 2 frames are properly forwarded to the new AP. However, it is possible for a client to authenticate with a new AP using another client's MAC address, causing the frames for the valid client to be sent to the spoofing client.

The WDS, however, is in a position to detect when a valid client has had its MAC address spoofed. The WDS maintains a mapping of user ID to client MAC address based on WLCCP registrations. When there is another authentication request from the same MAC address with a different user ID it is flagged as a MAC spoofing.

When the Wireless Client MAC Spoofing IDS fault is enabled on the WLSE, it polls the MIB `ciscoWdsIdsMacSpoofClient` at the configured polling interval. (The default polling interval is 5 minutes.)

The WLSE generates faults for all clients identified by the MIB `ciscoWdsIdsMacSpoofClient`. The MIB retains the history of all spoofed MAC addresses. An entry from the WDS MIB is cleared when:

- The WDS AP reaches the maximum number of events to hold for a reporting non-WDS AP. The maximum number is determined by the MIBS `ciscoWdsIdsMaxMacAddresses` and `ciscoWdsIdsMaxEntriesPerMac`.
- When the WDS is not configured. Because the AP maintains a history, the WLSE raises the MAC spoofing fault on the next polling cycle even after clearing the fault on the WLSE.

EAPOL Flooding

The vast majority of wireless LANs deployed today employ some form of 802.1X authentication. In these networks a client can only transmit data packets after it successfully authenticates with an AP. The 802.1X authentication that takes place between the client and the AP triggers a series of messages between the AP, the authenticator, and an authentication server using EAPOL (Extensive Authentication Protocol over LAN) messaging. The authentication server, typically a RADIUS server, can quickly become overwhelmed if there are too many authentication attempts. If not regulated, a single client can trigger enough authentication requests to launch a DoS attack on the rest of the network.

Currently Cisco APs provide rate limiting functionality that prevents these types of attacks. If any single user makes more than three 802.1X authentication attempts within 30 seconds the client is placed on a black list for a configurable period of time (default of 60 seconds). Once blacklisted, the client's subsequent 802.1X authentication attempts are rejected. For this existing rate limiting feature the detection threshold is not configurable.

This rate limiting functionality now provides general detection of the EAPOL flood attacks. An administrator-controlled number of 802.1X authentication attempts per unit of time can be entered via the CLI on an AP or via the WLSE GUI. The parameters apply to the entire radio interface. When the threshold is crossed, the AP indicates the event by recording a MIB variable indicating that the failure occurred and the MAC address of the client with the largest number of attempts.

The WLSE periodically polls these MIB variables to determine when an EAPOL flooding failure occurred. The WLSE generates a fault when it finds a record of this event.

Guidelines for Using Authentication and Protection Detection

Prerequisites

Before you can use detect the Authentication and Protection Attack detection features, you must:

1. Configure your network for radio management (see [Configuring Your Network for Radio Management, page 11-5](#)).



Note

If you choose to disable radio management, only one Intrusion Detection System subtab, **Manage Remaining IDS Settings**, is displayed (see [Using the Manage Remaining IDS Settings Subtab, page 14-11](#)). For information about the faults that will not be generated when Radio Management is disabled, see [Disabled Radio Management Related Faults, page 11-4](#).

2. Set the threshold condition for Authentication and Protection Attack detection features (see [Enabling Authentication and Protection Attack Detection, page 14-67](#)).

Enabling Authentication and Protection Attack Detection

The following sections describe how to set the authentication and protection attack fault settings. When the thresholds are exceeded, faults are generated and can be viewed under **Faults > Display Faults** or **IDS > Faults**.

- MIC/encryption failure thresholds:
 - [Setting the TkipReplayClient Policy](#), page 14-67
 - [Setting the TkipLocalMicFailureClient Policy](#), page 14-68
 - [Setting the TkipRemoteMicFailureClient Policy](#), page 14-69
 - [Setting the CcmpReplaysClient Policy](#), page 14-70
 - [Setting the CcmpDecryptErrorsClient Policy](#), page 14-71
- MAC spoofing threshold:
 - [Setting MAC Spoofing Policy](#), page 14-72
- EAPOL flooding thresholds:
 - [Setting EAPOL Settings \(IOS\) Policy](#), page 14-73
 - [Setting the EAPOL Detection \(IOS\) Policy](#), page 14-74
- Radio interface thresholds:
 - [Setting the Association Error Rate Policy](#), page 14-75
 - [Setting the TKIP Local MIC Failures Policy](#), page 14-76
 - [Setting the TKIP Remote MIC Failures Policy](#), page 14-77
 - [Setting the TKIP Counter Measure Invoked Policy](#), page 14-78
 - [Setting the TKIP Replays Detected Policy](#), page 14-79
 - [Setting the CCMP Replays Discarded Policy](#), page 14-80

Setting the TkipReplayClient Policy

Use this policy to check **TKIP** replay errors. A fault is generated when the counter value increases from the last polled value. By default, polling is every 5 minutes. This setting can be applied to IOS devices only.

**Note**

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **TkipReplayClient[IOS]**.

Step 4 Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault.

Step 5 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 6 To see the faults associated with this threshold, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary**, then select the fault type.

Step 7 To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Understanding Authentication and Protection Attack Detection, page 14-65](#)

Setting the TkipLocalMicFailureClient Policy

Use this policy to check local **TKIP** MIC failure errors. A fault is generated when the counter value increases from the last polled value. By default, polling is every 5 minutes.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.

Step 2 Select an existing IDS fault profile and click **Edit**.

Step 3 Select **TkipLocalMicFailureClient**.

Step 4 Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault.

Step 5 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 6 To see the faults associated with this threshold, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary**, then select the fault type.

Step 7 To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Understanding Authentication and Protection Attack Detection, page 14-65](#)

Setting the TkipRemoteMicFailureClient Policy

Use this policy to check remote **TKIP** MIC failure errors. A fault is generated when the counter value increases from the last polled value. By default, polling is every 5 minutes.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.

Step 2 Select an existing IDS fault profile and click **Edit**.

Step 3 Select **TkipRemoteMicFailureClient**.

Step 4 Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault.

Step 5 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 6 To see the faults associated with this threshold, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary**, then select the fault type.

Step 7 To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Understanding Authentication and Protection Attack Detection, page 14-65](#)

Setting the CcmpReplaysClient Policy

Use this policy to check the number of unicast fragments received by the **CCMP** play mechanism on the interface. A fault will be generated when the counter value increases from the last polled counter value. By default, the polling is every 5 minutes.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.

Step 2 Select an existing IDS fault profile and click **Edit**.

Step 3 Select **CcmpReplaysClient**.

Step 4 Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault.

Step 5 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 6 To see the faults associated with this threshold, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary**, then select the fault type.

Step 7 To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Understanding Authentication and Protection Attack Detection, page 14-65](#)

Setting the CcmpDecryptErrorsClient Policy

Use this policy to check the number of decryption errors detected by the **CCMP** play mechanism on the interface. A fault will be generated when the counter value increases from the last polled counter value. By default, the polling is every 5 minutes.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **CcmpDecryptErrorsClient**.

Step 4 Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault.

Step 5 Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

Step 6 To see the faults associated with this threshold, you can:

- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
- Select **IDS > Summary**, then select the fault type.

Step 7 To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

- [Using the Manage IDS Settings Subtab, page 14-6](#)
- [Understanding Authentication and Protection Attack Detection, page 14-65](#)

Setting MAC Spoofing Policy

This policy counts the number of times a valid client has had its MAC address spoofed. A fault will be generated when the counter value increases from the last polled counter value. By default, the polling is every 5 minutes.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.

Step 2 Select an existing IDS fault profile and click **Edit**.

Step 3 Select **Wireless Client MAC Spoofing**.

Step 4 Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault when Wireless Client MAC Spoofing is detected.

- Step 5** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 6** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Wireless Client MAC Spoofing**.
- Step 7** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting EAPOL Settings (IOS) Policy

This policy sets the threshold settings for **EAPOL** flood attacks. A fault will be generated when the counter value increases from the last polled counter value.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **EAPOL Settings**.
- Step 4** Complete the following:

Field	Description
Enable	Select to enable the policy.

Field	Description
EAP Attempts [1-512]	Number of allowed EAP attempts during a polling interval before a fault is raised.
Interval [1-60]	The polling interval (in seconds).

- Step 5** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 6** To assign this profile to a device or group of devices, click **Assign Devices** from the IDS Fault Settings window (see [Assigning Devices to an IDS Fault Profile, page 14-9](#)).
- Step 7** Go to [Setting the EAPOL Detection \(IOS\) Policy, page 14-74](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting the EAPOL Detection (IOS) Policy

Use this policy to count the number of [EAPOL](#) flood attacks that have been attempted on a valid client. A fault will be generated when the counter value increases from the last polled counter value. By default, the polling is every 10 minutes.



Note

This setting is applicable to the *access point*; it is not set per radio interface type and is not reported by interface type on the Faults page.



Note

Your login determines whether you can use this option.

Before You Begin

Set the EAPOL Settings (see [Setting EAPOL Settings \(IOS\) Policy, page 14-73](#)).

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **EAPOL Detection**.
- Step 4** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from the list.
Detect	Select the severity level to be assigned to the fault when an excessive number of EAPOL flooding faults are detected (see Setting EAPOL Settings (IOS) Policy, page 14-73).

- Step 5** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 6** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > EAPOL Flood Detection**.
- Step 7** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting the Association Error Rate Policy

Use this policy to check the number of association errors detected on the interface. A fault is generated when the counter value increases from the last polled counter value. By default, polling is every 5 minutes.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **IDS-802.11x** (where x = a, b, or g).
- Step 4** Select **Association Error Rate**.
- Step 5** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from each list.
Overloaded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Overloaded.
Degraded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Degraded.
OK	Select the number of consecutive polling cycles after which, when the error rate falls below the minimum per-minute error rate for the Degraded state, the status is OK.

- Step 6** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 7** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Authentication Failures**.
- Step 8** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting the TKIP Local MIC Failures Policy

Use this policy to check the number of **TKIP** local MIC failures detected on the interface. A fault is generated when the counter value increases from the last polled counter value. This setting can be applied to IOS devices only.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **IDS-802.11x** (where x = a, b, or g).
- Step 4** Select **TKIP Local MIC failures [IOS]**.
- Step 5** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from each list.
Overloaded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Overloaded.
Degraded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Degraded.
OK	Select the number of consecutive polling cycles after which, when the error rate falls below the minimum per-minute error rate for the Degraded state, the status is OK.

- Step 6** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 7** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Authentication Failures**.
- Step 8** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting the TKIP Remote MIC Failures Policy

Use this policy to check the number of **TKIP** remote MIC failures detected on the interface. A fault is generated when the counter value increases from the last polled counter value. This setting can be applied to IOS devices only.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **IDS-802.11x** (where x = a, b, or g).
- Step 4** Select **TKIP Remote MIC failures [IOS]**.
- Step 5** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from each list.
Overloaded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Overloaded.
Degraded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Degraded.
OK	Select the number of consecutive polling cycles after which, when the error rate falls below the minimum per-minute error rate for the Degraded state, the status is OK.

- Step 6** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 7** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Authentication Failures**.
- Step 8** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting the TKIP Counter Measure Invoked Policy

Use this policy to check the number of **TKIP** counter measures invoked on the interface. A fault is generated when the counter value increases from the last polled counter value. This setting can be applied to IOS devices only.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **IDS-802.11x** (where x = a, b, or g).
- Step 4** Select **TKIP Counter Measure Invoked [IOS]**.
- Step 5** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from each list.
Overloaded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Overloaded.
Degraded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Degraded.
OK	Select the number of consecutive polling cycles after which, when the error rate falls below the minimum per-minute error rate for the Degraded state, the status is OK.

- Step 6** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.
- Step 7** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Authentication Failures**.
- Step 8** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting the TKIP Replays Detected Policy

Use this policy to check **TKIP** replay errors. A fault is generated when the counter value increases from the last polled value. This setting can be applied to IOS devices only.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **IDS-802.11x** (where x = a, b, or g).
- Step 4** Select **TKIP Replays Detected [IOS]**.
- Step 5** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from each list.
Overloaded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Overloaded.
Degraded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Degraded.
OK	Select the number of consecutive polling cycles after which, when the error rate falls below the minimum per-minute error rate for the Degraded state, the status is OK.

- Step 6** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

- Step 7** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Authentication Failures**.
- Step 8** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Setting the CCMP Replays Discarded Policy

Use this policy to check the number of received unicast fragments discarded by the **CCMP** play mechanism on the interface. A fault will be generated when the counter value increases from the last polled counter value. This setting can be applied to IOS devices only.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **IDS > Manage IDS Settings**. The IDS Fault Settings window appears.
- Step 2** Select an existing IDS fault profile and click **Edit**.
- Step 3** Select **IDS-802.11x** (where x = a, b, or g).
- Step 4** Select **CCMP Replays Discarded [IOS]**.
- Step 5** Complete the following:

Field	Description
Enable	Select to enable the policy.
Poll Interval	Select the polling interval from each list.
Overloaded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Overloaded.
Degraded	Select the priority level to be assigned to the fault, the minimum per-minute error rate, and the number of consecutive polling cycles before the status is set to Degraded.
OK	Select the number of consecutive polling cycles after which, when the error rate falls below the minimum per-minute error rate for the Degraded state, the status is OK.

- Step 6** Click **Apply** to set the new entries, or click **Reset** to refresh any fields you have changed but want to restore.

- Step 7** To see the faults associated with this threshold, you can:
- Click **View current faults for this setting** (see [Viewing Current Faults, page 3-51](#)). Click your browser's **Back** button to return to the network-wide setting window.
 - Select **IDS > Summary > Authentication Failures**.
- Step 8** To assign this profile to one or more devices, click **Assign Devices to [profile name]**. The window refreshes with the device selector in the left pane. For more information about assigning an IDS fault profile to the devices in your network, see [Assigning Devices to an IDS Fault Profile, page 14-9](#).
-

Related Topics

[Using the Manage IDS Settings Subtab, page 14-6](#)

Displaying Authentication and Protection Attack Faults

Use **IDS > Summary** to view a summary of the various authentication and protection attack faults.



Note

Your login determines whether you can use this option.

Before You Begin

Satisfy the authentication and protection detection prerequisites (see [Guidelines for Using Authentication and Protection Detection, page 14-66](#)).

Procedure

- Step 1** Select **IDS > Summary**. The Intrusion Detection Summary window appears.
- Step 2** Select one of the following fault types:
- **Association Error Rate**
 - **Authentication Failures**
 - **Wireless Client MAC Spoofing**
 - **EAPOL Flood Detection**
- The Fault Summary window for the selected fault type appears.
- Step 3** To view information about a specific fault, select the Description or Timestamp fields for that fault. The Fault Details window displays the fault information (see [Viewing Fault Details, page 3-7](#)).
- Step 4** To clear a fault, see [Clearing Summary Table Faults, page 3-6](#).
-

Related Topics

[Understanding Authentication and Protection Attack Detection, page 14-65](#)

