Cisco Adaptive Wireless Intrusion Prevention Service Configuration Guide Release 5.2

December 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-18279-01

CONTENTS

Preface

This section describes the objectives, audience, organization, and conventions of the *Cisco Wireless Intrusion Prevention Service Configuration Guide*.

Objectives

This publication explains the steps for using Cisco Wireless Control System (WCS) for configuring and managing the Cisco 3310 Mobility Services Engine and the Cisco Adaptive Wireless Intrusion Prevention Service (wIPS) which resides on the mobility services engine.

Audience

This publication is for the person configuring and managing wIPS. The user should be familiar with network structures, terms, and concepts.

Conventions

This publication uses the following conventions to convey instructions and information:

- Commands and keywords are in **boldface** type.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix “Translated Safety Warnings.”)**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico’s en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel “Translated Safety Warnings” (Vertalingen van veiligheidsvoorschriften) raadplegen.)**

Varoitus **Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)**

Attention **Ce symbole d’avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d’accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l’annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel “Translated Safety Warnings” (Übersetzung der Warnhinweise).)**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell’appendice, “Translated Safety Warnings” (Traduzione delle avvertenze di sicurezza).**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice “Translated Safety Warnings” - “Traduções dos Avisos de Segurança”).**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)**

Related Publications

Refer to the *Cisco 3310 Mobility Services Engine Getting Started Guide*, which describes how to install and set up mobility services engines.

This document is available on the Cisco.com website at the following URL:

http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Overview

This chapter describes the role of the Cisco 3310 Mobility Services Engine and one of its services, the Cisco Adaptive Wireless Intrusion Prevention Service (wIPS) within the overall Cisco Unified Wireless Network (CUWN).

This chapter contains the following sections:

- "Overview of wIPS" section on page 1-2
- "Differences Between Controller IDS and Adaptive wIPS" section on page 1-6
- "Configuration Guide Overview" section on page 1-12

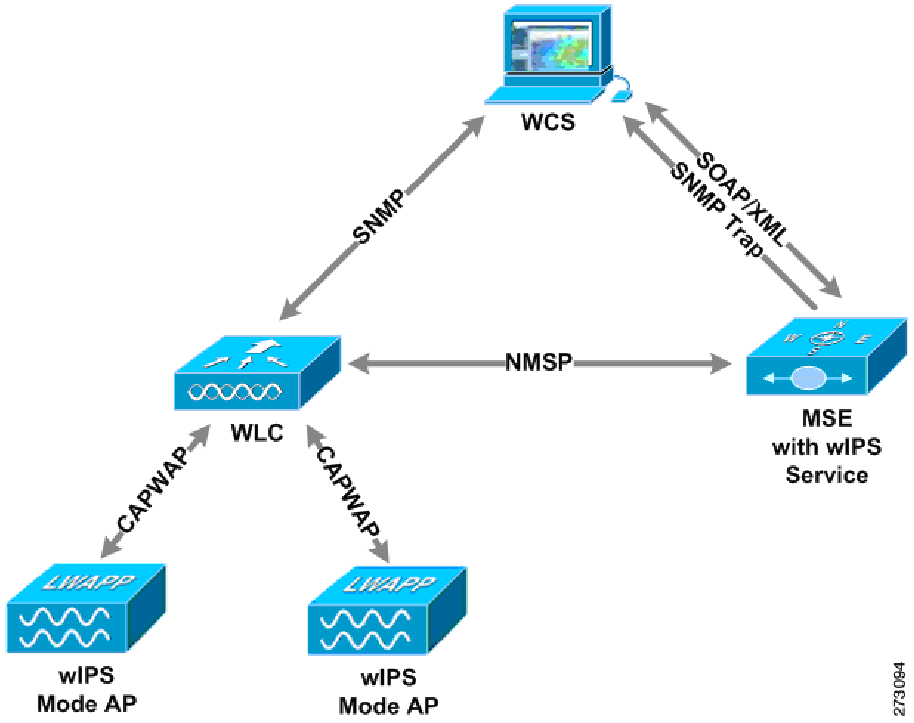
Overview of wIPS

Cisco Adaptive Wireless Intrusion Prevention Service (wIPS) performs rogue access point, rogue client, and ad-hoc connection detection and mitigation, over-the-air wireless hacking and threat detection, security vulnerability monitoring, performance monitoring and self-optimization, network hardening for proactive prevention of threats and complete wireless security management and reporting.

Built on Cisco Unified Wireless Network (CUWN) and leveraging the efficiencies of Cisco Motion, wIPS is deployment-hardened and enterprise-ready. Cisco's wIPS is made up of the following components that work together to provide a unified security monitoring solution.

- A mobility services engine (MSE) running wIPS software–Serves as the central point of alarm aggregation for all controllers and their respective wIPS monitor mode access points. Alarm information and forensic files are stored on the mobility services engine for archival purposes.
- An wIPS monitor mode access point–Provides constant channel scanning with attack detection and forensics (packet capture) capabilities.
- Local mode access point–Provides wireless service to clients in addition to time-sliced rogue scanning.
- Wireless LAN Controller–Forwards attack information received from wIPS monitor mode access points to the mobility services engine and distributes configuration parameters to access points.
- Wireless Control System–Provides a centralized management platform for the administrator to configure the wIPS Service on the mobility services engine, push wIPS configurations to the controller, and configure access points in wIPS monitor mode. WCS is also used to view wIPS alarms, forensics, reporting, and to access the attack encyclopedia.

Figure 1-1 Wireless Intrusion Prevention Service



Communication among the system components involves the following protocols:

- Control and Provisioning of Wireless Access Points (CAPWAP)–This protocol is the successor to LWAPP and is used for communication between access points and controllers. It provides a bi-directional tunnel in which alarm information is sent to the controller and configuration information is sent to the access point.
- Network Mobility Services Protocol (NMSP)–The protocol handles communication between controllers and the mobility services engine. In an wIPS deployment, this protocol provides a pathway for alarm information to be aggregated from controllers and forwarded to the mobility services engine and for wIPS configuration information to be pushed to the controller. This protocol is encrypted.
  - Controller TCP Port: 16113
- Simple Object Access Protocol (SOAP/XML)–The method of communication between the mobility services engine and WCS. This protocol is used to distribute configuration parameters to the wIPS service running on the mobility services engine.
  - MSE TCP Port: 443
- Simple Network Management Protocol (SNMP)–This protocol is used to forward wIPS alarm information from the mobility services engine to the WCS. It is also employed to communicate rogue access point information from the controller to WCS.

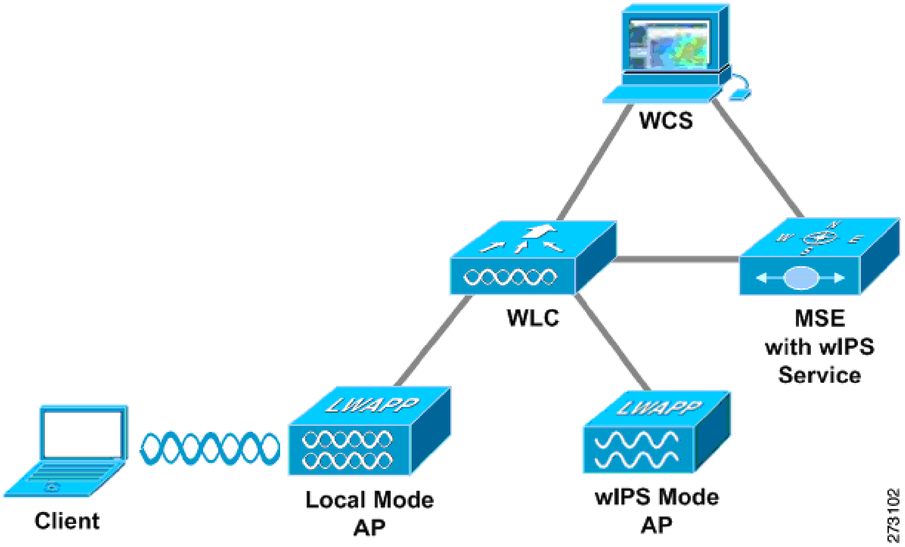
wIPS in a Cisco Unified Wireless Network

You can integrate wIPS within the CUWN infrastructure or overlay wIPS on the CUWN or Cisco autonomous wireless network (or third party wireless network). A summary of each deployment and its uses is summarized in this section.

wIPS Integrated Within a Cisco Unified Wireless Network

An integrated wIPS deployment is a system design in which both *local* mode and wIPS *monitor mode* access points are intermixed on the same controller, and managed by the same Cisco WCS. Cisco recommends this configuration as it allows the tightest integration between the client serving and monitoring infrastructure (Figure 1-2).

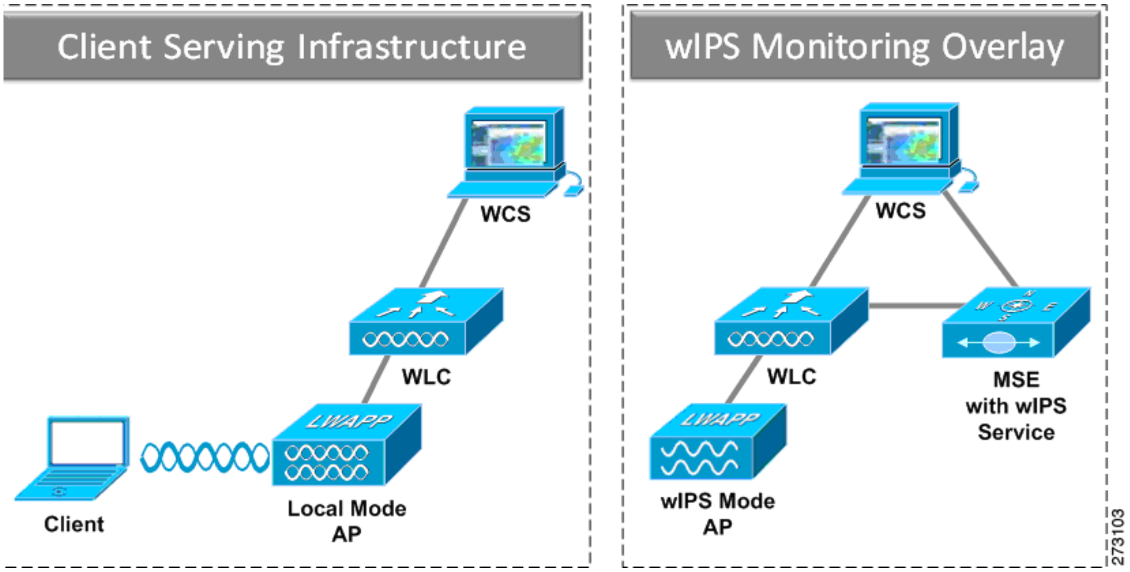
Figure 1-2 wIPS Integrated Within CUWN



wIPS Overlay Deployment in a Cisco Unified Wireless Network

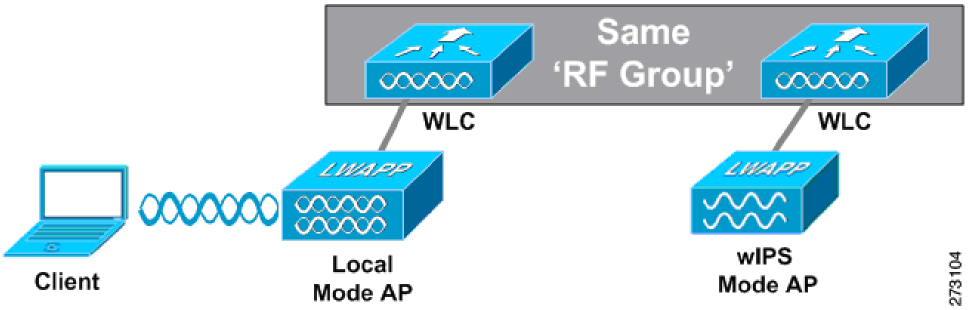
In a wIPS Overlay deployment, the wIPS monitoring infrastructure is completely separate from the client serving infrastructure. Each distinct system has its own set of controllers, access points and Cisco WCS. The reason for selecting this deployment model often stems from business mandates that require distinct network infrastructure and security infrastructure systems with separate management consoles (Figure 1-3). This deployment model is also used when the total number of access points (wIPS monitor and local mode) exceed the 3000 access point limit contained in WCS.

Figure 1-3 wIPS Overlay Monitoring Network Deployment in CUWN



In order to configure the wIPS Overlay Monitoring network to provide security assessment of the client serving infrastructure, specific configuration items must be completed. The wIPS system operates on the assumption that only attacks against trusted devices must be logged. In order for an overlay system to view a separate Cisco Unified WLAN infrastructure as trusted, the controllers must be in the same RF Group (Figure 1-4).

Figure 1-4 Controllers in Same RF Group for wIPS Overlay Deployment



As a result of separating the client serving infrastructure from the wIPS monitoring overlay infrastructure, several monitoring caveats arise:

- wIPS alarms are only shown on the wIPS Overlay WCS instance
- Management Frame Protection (MFP) alarms are only shown on the client infrastructure WCS instance
- Rogue alarms are shown in both WCS instances
- Rogue location accuracy is greater on the client serving infrastructure Cisco WCS because this deployment employs a greater density of access points than the wIPS overlay deployment
- Over-the-air rogue mitigation is more scalable in an integrated wIPS model, as the local-mode access points are employed in mitigation actions
- The security monitoring dashboard is incomplete on both Cisco WCS instances because some events such as wIPS only exist on the wIPS Overlay WCS
  - To monitor the comprehensive security of the wireless network, both security dashboard instances must be observed

Table 1-1 summarizes some of the key differences between client serving and overlay deployments.

Table 1-1 wIPS Client Serving and wIPS Monitoring Overlay Comparison

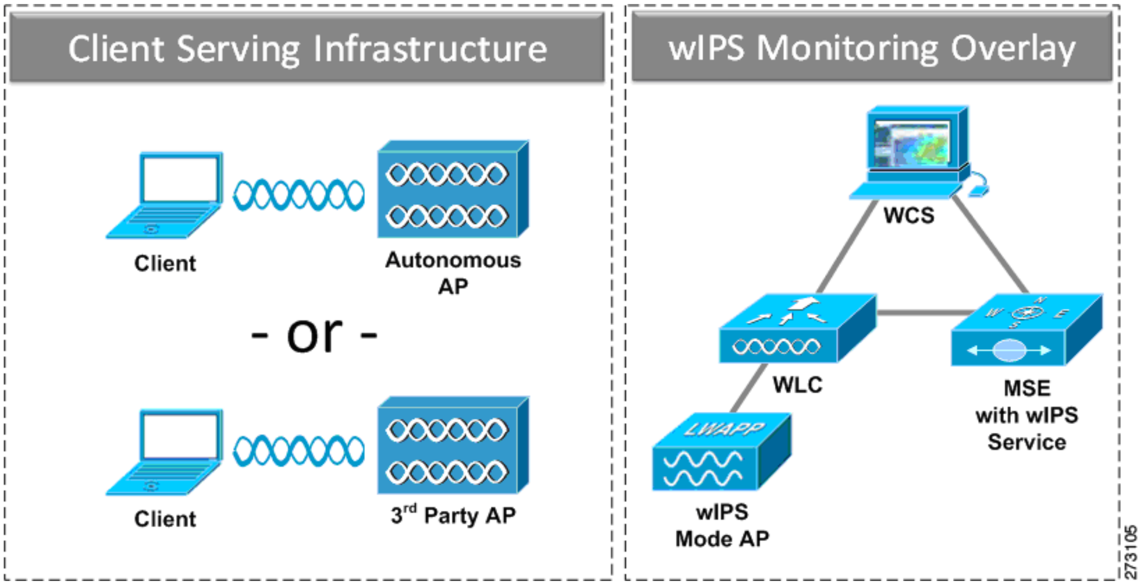
	Client Serving Infrastructure WCS	wIPS Monitoring Overlay WCS
wIPS alarms	No	Yes
MFP alarms	Yes	No
Rogue alarms	Yes	Yes
Rogue location	High accuracy	Low accuracy
Rogue containment	Yes	Yes, but scalable

One challenge of the overlay solution is the possibility of lightweight access points on either the client serving infrastructure or wIPS monitoring overlay associating to the wrong controller. Association with the wrong controller can be addressed by specifying the primary, secondary and tertiary controller names for each access point (both local and wIPS monitor mode). In addition, Cisco recommends that the controllers for each respective solution have separate management VLANs for communication with their respective access points and that access control lists (ACLs) are used to prevent CAPWAP traffic from crossing these VLAN boundaries.

wIPS Overlay in Autonomous or Other Wireless Network

The Adaptive wIPS solution is also capable of performing security monitoring over an existing WLAN infrastructure other than CUWN. In this case, the client serving infrastructure is completely separate and uncoordinated with the wIPS overlay. The application for this deployment is security monitoring of either Cisco autonomous access points or third-party access points (Figure 1-5).

Figure 1-5 wIPS Overlay in Autonomous



Differences Between Controller IDS and Adaptive wIPS

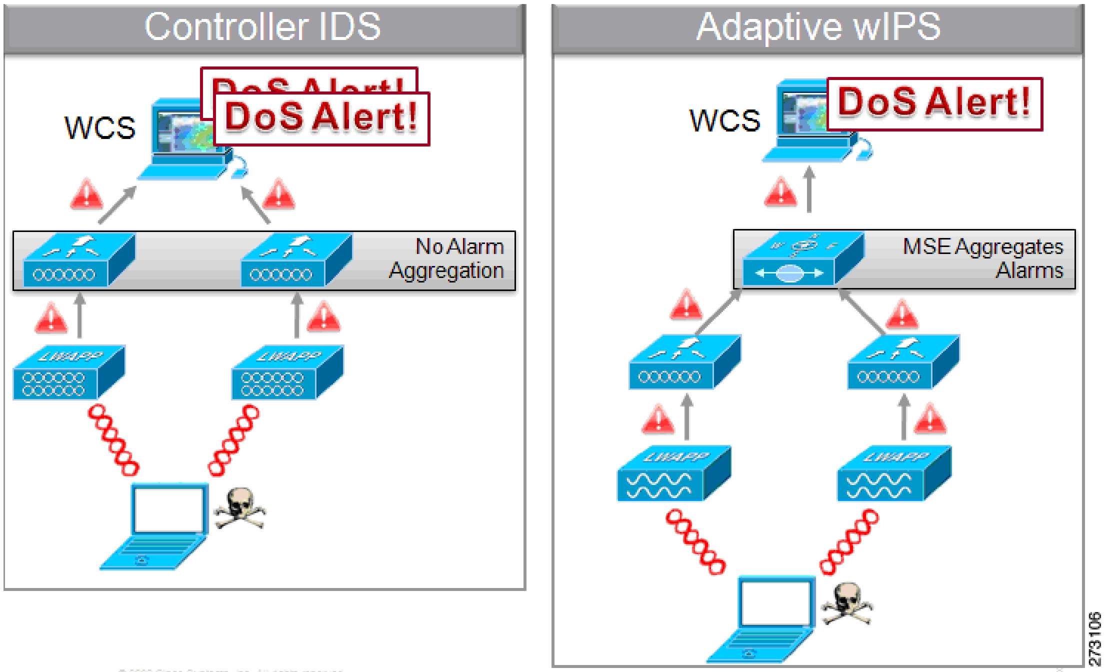
Reduction in False Positives

Cisco wIPS facilitates a reduction in false positives with respect to security monitoring of the wireless network. In contrast to Cisco's controller-based solution, which triggers an alarm when it detects a number of management frames over the air, wIPS only triggers an alarm when it detects a number of management frames over the air that are causing damage to the wireless infrastructure network. This a result of the wIPS system being able to dynamically identify the state and validity of access points and clients present in the wireless infrastructure. Only when attacks are launched against the infrastructure are alarms raised.

Alarm Aggregation

One major differentiation between Cisco's existing controller-based IDS system and its wIPS system is the unique attacks seen over the air are correlated and aggregated into a single alarm. This is accomplished by the wIPS system automatically assigning a unique hash key to each particular attack the first time it is identified. If the attack is received by multiple wIPS access points, it will only be forwarded to the WCS once because alarm aggregation takes place on the mobility services engine. The existing controller-based IDS system does not aggregate alarms (Figure 1-6).

Figure 1-6 Alarm Aggregation Using Cisco's Controller-based IDS versus Adaptive wIPS



Another major differentiation between the controller-based IDS and wIPS is the number of attacks that each system can detect. As described in the sub-sections and showcased in the tables below, wIPS can detect a multitude of attacks and attack tools. These attacks include both denial of service (DoS) attacks and security penetration attacks.

DoS Attacks

A DoS attack involves mechanisms which are designed to prohibit or slow successful communication within a wireless network. These often incorporate a number of spoofed frames which are designed to drop or falter legitimate connections within the wireless network. Although a DoS attack can be devastating to a wireless networks ability to deliver reliable services, they do not result in a data breach and their negative consequences are often over once the attack has stopped. Table 1-2 compares the DoS attacks detected by the controller-based IDS and wIPS service.

Table 1-2 DoS Attack Detection By Controller IDS and wIPS

Alarm Name	Detected by Controller IDS	Detected by wIPS
Association flood	X	X
Association table overflow		X
Authentication flood	X	X
EAPOL-Start attack	X	X
PS-Poll flood		X
Unauthenticated Association		X
CTS Flood		X
Queensland University of Technology Exploit		X
RF jamming attack		X
RTS flood		X
Virtual carrier attack	X	X
Authentication-failure attack		X
Deauthentication broadcast attack	X	X
Deauthentication flood attack	X	X
Disassociation broadcast attack		X
Disassociation flood attack	X	X
EAPOL-logoff attack	X	X
FATA-jack tool detected		X
Premature EAP-failure attack		X
Premature EAP-success attack		X

Security Penetration Attacks

Arguably the more harmful of the two attack types threatening wireless networks, a security penetration is designed to capture or expose information such as sensitive data or encryption keys that can later be used for exposing confidential data. A security penetration attack can involve targeted queries against the infrastructure or replay attacks that aim to break cryptographic keys. Security Penetration attacks can also be harmful to the client by which an attempt to lure the client onto a fake access point such as a Honeypot. Table 1-3 compares the security penetration attacks detected by the controller-based IDS and wIPS service.

Table 1-3 Security Penetration Attack Detection By Controller IDS and wIPS

Alarm Name	Detected by Controller IDS	Detected by wIPS
Airsnarf attack		X
ChopChop Attack		X
Day-zero attack by WLAN security anomaly		X
Day-zero attack by device security anomaly		X

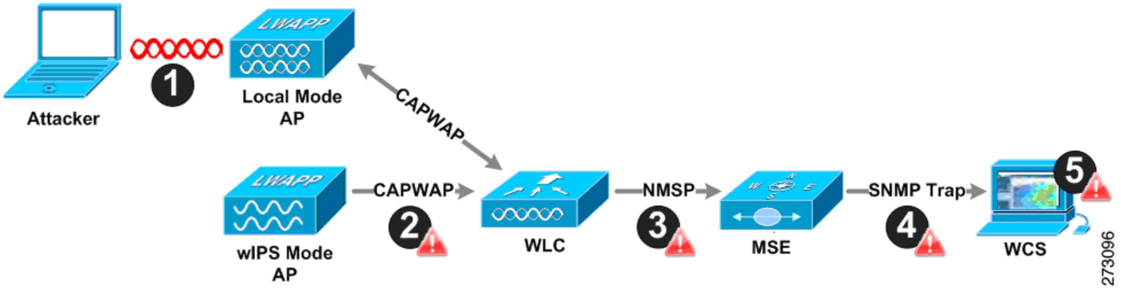
Table 1-3 Security Penetration Attack Detection By Controller IDS and wIPS (continued)

Alarm Name	Detected by Controller IDS	Detected by wIPS
Device probing for access points		X
Dictionary attack on EAP methods		X
EAP attack against 802.1x authentication		X
Fake access points detected	X	X
Fake DHCP server detected		X
Fast WEP crack detected		X
Fragmentation Attack		X
Hotspotter tool detected		X
Malformed 802.11 packets detected		X
Man in the middle attack detected		X
NetStumbler detected	X	X
PSPF violation		X
ASLEAP attack detected		X
Honey pot access point detected	X	X
Soft access point or Host access point detected		X
Spoofed MAC address detected		X
Suspicious after-hours traffic		X
Unauthorized association by vendor list		X
Unauthorized association detected		X
Wellenreiter detected	X	X

wIPS Alarm Flow

The Adaptive wIPS system follows a linear chain of communication to propagate attack information obtained from initially scanning the airwaves to forwarding information to Cisco WCS.

Figure 1-7 Alarm Flow Within Network



1. In order for an alarm to be triggered on the wIPS system, an attack must be launched against a legitimate access point or client. Legitimate access points and clients are discovered automatically in a CUWN by trusting devices broadcasting the same RF-Group name. In this configuration, the

system dynamically maintains a list of local-mode access points and their associated clients. The system can also be configured to trust devices by SSID using the SSID Groups feature. Only attacks which are considered harmful to the WLAN infrastructure are propagated upwards to the rest of the system.

2. Once an attack is identified by the wIPS monitor mode access point, an alarm update is sent to the controller and is encapsulated inside the CAPWAP control tunnel.
3. The controller transparently forwards the alarm update from the access point to the wIPS service running on the mobility services engine. The protocol used for this communication is Network Mobility Service Protocol (NMSP).
4. Once received by the wIPS service on the mobility services engine, the alarm update is added to the alarm database for archival and attack tracking. An SNMP trap is forwarded to WCS. The SNMP trap contains the attack information. If multiple alarm updates are received referencing the same attack (for example, if multiple access points hear the same attack) only one SNMP trap is sent to WCS.
5. The SNMP trap containing the alarm information is received and displayed by WCS.

Forensics

Cisco's Adaptive wIPS system provides the ability to capture attack forensics for further investigation and troubleshooting purposes. At a base level, the forensics capability is a toggle-based packet capture facility which logs and retrieves a set of wireless frames. This feature is enabled on a per attack basis within a wIPS profile. wIPS profiles are configured on WCS.

Once enabled, the forensics feature is triggered when a specific attack alarm is seen over the airwaves. The forensic file created is based on the packets contained within the buffer of the wIPS monitor mode access point that triggered the original alarm. This file is transferred to the controller via CAPWAP, which then forwards the forensic file via NMSP to the wIPS Service running on the mobility services engine. The file is stored within the forensic archive on the mobility services engine until the user configured disk space limit for forensics is reached. By default, this limit is 20 Gigabytes, which when reached, causes the oldest forensic files to be removed. Access to the forensic file is obtained by opening the alarm in WCS which contains a hyperlink to the forensic file. The files are stored in a *.CAP* file format which is accessed by either WildPacket *Omnipeek*, AirMagnet *WiFi Analyzer*, *Wireshark* or any other packet capture program which supports this format. Wireshark is available at http://www.wireshark.org.

Note Cisco recommends that the forensics capability of wIPS system be used sparingly and disabled after the desired information is captured. This primarily because it places an intensive load on the access point as well as interrupts scheduled channel scanning. A wIPS access point cannot simultaneously perform channel scanning and produce a forensic file. While the forensic file is being dumped, channel scanning is delayed.

Rogue Detection

An access point in wIPS-optimized monitor mode performs rogue threat assessment and mitigation using the same logic as current CUWN implementations. This allows a wIPS mode access point to scan, detect and contain rogue access points and ad-hoc networks. Once discovered, this information regarding rogue wireless devices is reported to WCS where rogue alarm aggregation takes place.

However, with this functionality comes the caveat that if a containment attack is launched using a wIPS mode access point, its ability to perform methodical attack-focused channel scanning is interrupted for the duration of the containment.

Attack Encyclopedia

The integrated attack encyclopedia provides a visual and textural description of each attack detected by the system. This attack encyclopedia is available from any wIPS alarm by clicking the Help hyperlink or by browsing through a wIPS profile configuration screen. This integrated encyclopedia provides the administrator information as to how the attack is undertaken, what tools might be used to launch it and potential mitigation strategies. Refer to Chapter A, “wIPS Policy Alarm Encyclopedia” for a summary of the integrated attack alarms.

Anomaly Detection

wIPS includes specific alarms pertaining to anomalies in attack patterns or device characteristics captured. The anomaly detection system takes into account the historic attack log and device history contained within the mobility services engine to baseline the typical characteristics of the wireless network. The anomaly detection engine is triggered when events or attacks on the system undergo a measurable change as compared to historical data kept on the mobility services engine. For example, if the system regularly captures a few MAC spoofing events each day, and then on another day MAC spoofing events are up 200%, an anomaly alarm is triggered on the mobility services engine. This alarm is then sent to WCS to inform the administrator that something else is going on in the wireless network beyond traditional attacks that they system may encounter. The anomaly detection alarm can also be employed to detect day-zero attacks that might not have a preexisting signature in the wIPS system.

Default Configuration Profiles

To simplify the configuration tuning for each specific WLAN security deployment, wIPS includes a number of default profiles tailored to meet the security needs of specific industries or deployments. The templates summarize the differing risk profiles and requirements for security monitoring of varying deployments. The specific profiles include Education, Enterprise (Best), Enterprise (Rogue), Financial, Healthcare, Hotspot (Open Security), Hotspot (802.1x Security), Military, Retail, Tradeshow, and Warehouse. The profiles can be further customized to address the specific needs of the prospective deployment.

Integration into Release 5.1 Features

wIPS tightly integrates into an existing CUWN to leverage the security features introduced in previous releases. On the security dashboard, wIPS events display under their own category.

Configuration Guide Overview

This configuration guide addresses the configuration of wIPS and mobility services engine. A summary of the configuration items is noted below.

Adding and Deleting Mobility Services Engine

You can use Cisco WCS to add and delete mobility services engine within the network. You are also able to define the service supported on the mobility services engine. Refer to Chapter 2, "Adding and Deleting Systems" for configuration details.

Editing Mobility Services Engine Properties

You can use Cisco WCS to configure the following parameters on the mobility services engine. Refer to Chapter 4, "Configuring and Viewing System Properties" for configuration details.

- General Properties: Enables you to assign a contact name, username, password, and HTTP for the mobility services engine.
- NMSP Parameters: Enables you to modify Network Mobility Services Protocol (NMSP) parameters such as echo and neighbor dead intervals as well as response and retransmit periods. NMSP is the protocol that manages communication between the mobility services engine and the controller.
- Active Sessions: Enables you to view active user sessions on the mobility services engine.
- Trap Destinations: Enables you to specify which Cisco WCS or Cisco Security Monitoring, Analysis and Response System (CS-MARS) network management platform is the recipient of SNMP traps generated by the mobility services engine.
- Advanced Parameters: Enables you to set the number of days events are kept, set session time out values, set an absent data interval cleanup interval, and enable or disable Advanced Debug.

Managing Users and Groups

You can use Cisco WCS to add, delete, and edit user session and user group parameters as well as add and delete host access records. Refer to Chapter 5, "Managing Users and Groups" for configuration details.

Mobility Services Engine Synchronization

Cisco WCS pushes wIPS information to the mobility services engine to maintain accurate information between the mobility services engine and controller. Cisco WCS provides you with two ways to synchronize: manual and automatic (auto-sync). Refer to Chapter 3, "Synchronizing Mobility Services Engines" for specifics.

Configuring wIPS and Profile Management

You can use Cisco WCS to configure the Cisco Adaptive wIPS service.

Refer to Chapter 6, "Configuring wIPS and Profiles" for specifics.

Monitoring Capability

You can use Cisco WCS to monitor alarms, events, and logs generated by mobility services engine. You can also monitor the status of mobility services engines, clients, and tagged assets. Additionally, you can generate a utilization report for the mobility services engine to determine CPU and memory utilization as well as counts for clients, tags and rogue access points and clients. Refer to Chapter 7, "Monitoring the System and Services" for specifics.

Maintenance Operations

You can use Cisco WCS to recover a password, back up mobility services engine data to a predefined FTP folder on Cisco WCS at defined intervals, and restore the mobility services engine data from that Cisco WCS. Other mobility services engine maintenance operations that you can perform include: downloading new software images to all associated mobility services engines from any Cisco WCS station, defragmenting the mobility services engine database, restarting a mobility services engine, shutting down a mobility services engine and clearing mobility services engine configurations. Refer to Chapter 8, "Performing Maintenance Operations" for specifics.

System Compatibility

Note Refer to the *Cisco 3300 Mobility Services Engine Release Note* for the latest system (controller, WCS, mobility services engine) compatibility information, feature support, and operational notes for your current release at: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.htm

CHAPTER 2

Adding and Deleting Systems

This chapter describes how to add and delete a mobility services engine from Cisco WCS.

This chapter contains the following sections:

- "Adding a Mobility Services Engine to Cisco WCS" section on page 2-2
- "Deleting a Mobility Services Engine from the Cisco WCS" section on page 2-3

Adding a Mobility Services Engine to Cisco WCS

To add a Cisco 3300 Series Mobility Services Engine to Cisco WCS, log into WCS and follow these steps:

Step 1 Verify that you can ping the mobility service engine that you want to add from Cisco WCS.

Step 2 Click **Mobility > Mobility Services** to display the Mobility Services window.

Step 3 From the Select a command drop-down menu, select **Add Mobility Services Engine** and click **GO**.

Step 4 In the Device Name field, enter a name for the mobility services engine.

Step 5 In the IP Address field, enter the mobility services engine's IP address.

Step 6 (Optional) In the Contact Name field, enter the name of the mobility services engine administrator.

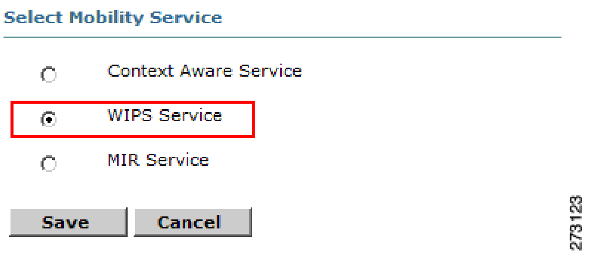
Step 7 In the User Name and Password fields, enter the username and password for the mobility services engine.

The default username and password are both *admin*.

Note If you changed the username and password during the automatic installation script, enter those values here. If you did not change the default passwords, Cisco strongly recommends that you rerun the automatic installation script and change the username and password.

Step 8 Click **Next**. The Select Mobility Service window appears (Figure 2-1).

Figure 2-1 Mobility Services Engine > Select Mobility Service



Select Mobility Service

○ Context Aware Service

● WIPS Service

○ MIR Service

Step 9 To enable one service on the mobility services engine, click the circle next to that service.

Note A mobility services engine can only be configured to support a single service at a time.

Step 10 Click **Save**.

Note After adding a new mobility services engine, you can synchronize network designs (campus, building, and outdoor maps) and event groups on the local mobility services engine with Cisco WCS. You can also choose to synchronize the mobility services engine with a specific controller. You can do this synchronization immediately after adding a new mobility services engine or at a later time. To synchronize the local and Cisco WCS databases, continue to the "Synchronizing Cisco WCS and a Mobility Services Engine" section on page 3-2.

Deleting a Mobility Services Engine from the Cisco WCS

To delete a mobility services engine from the Cisco WCS database, follow these steps:

Step 1 Click **Mobility > Mobility Services** to display the Mobility Services window.

Step 2 Select the mobility services engine(s) to be deleted by checking the corresponding check box(es).

Step 3 From the Select a command drop-down menu, select **Delete Service(s)** and click **GO**.

Step 4 Click **OK** to confirm that you want to delete the selected mobility services engine from the WCS database.

Step 5 Click **Cancel** to stop deletion.

CHAPTER 3

Synchronizing Mobility Services Engines

This chapter describes how to synchronize Cisco wireless LAN controllers and Cisco WCS with mobility services engines.

This chapter contains the following sections:

- "Keeping Mobility Services Engines Synchronized" section on page 3-2
- "Viewing Synchronization Information" section on page 3-5

Keeping Mobility Services Engines Synchronized

This section describes how to synchronize Cisco WCS and mobility services engines manually and automatically.

After adding a mobility services engine to Cisco WCS, you can synchronize network designs (campus, building, and outdoor maps), event groups or controller information (name and IP address) with the mobility services engine.

Note Be sure to verify software compatibility between the controller, Cisco WCS and the mobility services engine before synchronizing. Refer to the latest mobility services engine release note at the following link: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

Note Communication between the mobility services engine and Cisco WCS and the controller is in universal time code (UTC). Configuring NTP on each system provides devices with the UTC time. The mobility services engine and its associated controllers must be mapped to the same NTP server and the same Cisco WCS server. An NTP server is required to automatically synchronize time between the controller, Cisco WCS, and the mobility services engine.

Synchronizing Cisco WCS and a Mobility Services Engine

To synchronize Cisco WCS network designs, a controller or event groups with the mobility services engine, follow these steps:

Step 1 Click **Mobility > Synchronize Services** to display the Mobility Services > Synchronize WCS and MSE(s) window. A three-tabbed window appears.

Note The Devices column lists the system name of the mobility services engine and the active service on that device. Services are noted in parenthesis next to the device name. Services supported are Context-Aware Software (C), and Wireless Intrusion Prevention Service (W).

Step 2 Select the appropriate tab (network designs, controllers, or event groups).

a. To assign a network design to a mobility services engine, click its corresponding **Assign** link.

Note A network design might comprise a large campus with several buildings, each monitored by a different mobility services engine. Therefore, you might need to assign a single network design to multiple mobility services engines.

In the Network Designs panel that appears, check the check box of each network design that you want to apply to the mobility services engine. Click **OK** when the selection is complete.

A red asterisk (*) appears next to the Assign link. To undo assignments, click **Reset**. To go back to the Synchronize WCS and MSE(s) window without making any changes, click **Cancel**.

b. To associate a mobility services engine with a controller, click the **Assign** link for that mobility services engine.

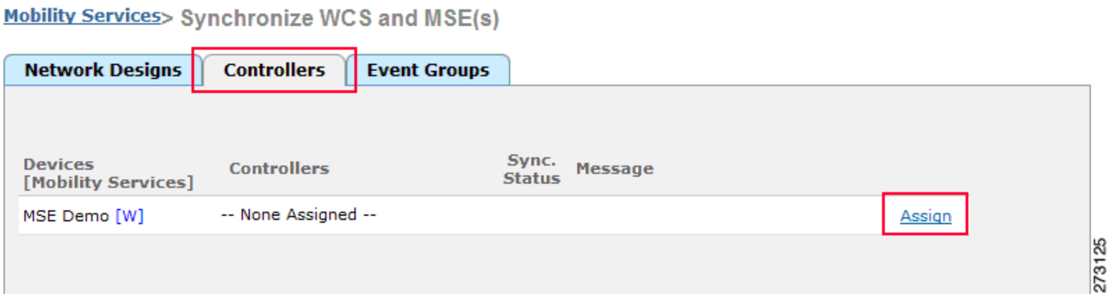
In the Controllers panel that appears, check the check box next to each controller to which you want the mobility services engine associated. Click **OK** (Figure 3-1).

Note The controller must support the service that is configured on the mobility services engine (as noted in the supported services column). If not, when you click **OK**, a warning message appears noting that the service is not supported on that controller.

Note Controller names must be unique for synchronizing with a mobility services engine. If you have two controllers with the same name, only one controller synchronizes.

A red asterisk (*) appears next to the Assign link. To undo assignments, click **Reset**. To go back to the Synchronize WCS and MSE(s) window without making any changes, click **Cancel**.

Figure 3-1 Assign > Controllers



Devices [Mobility Services]	Controllers	Sync. Status	Message	
MSE Demo [W]	-- None Assigned --			Assign

c. To assign an event group to a mobility services engine, click its corresponding **Assign** link.

In the Event Groups panel that appears, check the check box for each event group that you want to assign to the mobility services engine. Click **OK**.

A red asterisk (*) appears next to the Assign link. To undo assignments, click **Reset**. To go back to the Synchronize WCS and Server(s) window without making any changes, click **Cancel**.

Step 3 Click **Synchronize** to update the mobility services engine database.

When items are synchronized, a green two-arrow icon appears in the Sync. Status column for each synchronized entry.

Note To unassign a network design, controller or event group from a mobility services engine, click the **Assign** link next to the system. In the panel that appears, uncheck the check box for the corresponding network design, controller or event group. Click **OK.** Then, click **Synchronize**. The name of the removed network design, controller or event group is replaced with *None Assigned*.

Configuring Automatic Database Synchronization and Out of Sync Alerts

Manual synchronization of Cisco WCS and mobility services engine databases is immediate. However, future deployment changes (such as changes to maps and access point positions) can yield incorrect information until resynchronization reoccurs.

To prevent out-of-sync conditions, use Cisco WCS to enable automatic synchronization. This policy ensures that synchronization between Cisco WCS and mobility services engine databases is triggered periodically and any related alarms are cleared.

To configure automatic synchronization, follow these steps:

Step 1 In Cisco WCS, choose **Administration > Background Tasks**.

Step 2 Check the **Mobility Service Synchronization** check box. Select **Enable Task** from the Select a command drop-down menu if not already enabled. Click **GO**.

Step 3 Click the **Mobility Service Synchronization** link and the Task > Mobility Service Synchronization window appears.

Step 4 To set the mobility services engine to send out-of-sync alerts, check the Out of Sync Alerts **Enabled** check box. By default, out-of-sync alarms are enabled.

Note Uncheck the Out of Sync Alerts **Enabled** check box to disable forwarding of out-of-sync alarms.

Note For a summary of out of sync alerts that are sent, refer to the "Out-of-Sync Alarms" section on page 3-4.

Step 5 To enable automatic synchronization, check the Auto Synchronization **Enabled** check box.

Note Automatic synchronization does not apply to network designs, controllers, or event groups that have not yet been assigned to a mobility services engine. However, out-of-sync alarms will still be generated for these unassigned elements. For automatic synchronization to apply to network designs, controllers, or event groups, you need to manually assign them to a mobility services engine.

Step 6 Enter the time interval in hours that the automatic synchronization is to be performed.

By default, auto-sync is disabled.

Step 7 Click **Submit**. You are returned to the **Administration > Background Tasks** screen and the Mobility Service Synchronization task displays an enabled state.

Out-of-Sync Alarms

Out-of-sync alarms are of Minor severity (yellow), and are raised in response to the following conditions:

- Elements are modified in Cisco WCS (the auto-sync policy pushes these elements)
- Elements are modified in the mobility services engine (the auto-sync policy pulls these elements)

- Elements other than controllers exist in the mobility services engine database but not in Cisco WCS (the auto-sync policy pulls these elements)
- Elements are not assigned to any mobility services engine (the auto-sync policy does not apply)

Out-of-sync alarms are cleared when the following occurs:

- Mobility services engine is deleted

Note When you delete a mobility services engine, the out-of-sync alarms for that system are also deleted. In addition, if you delete the last available mobility services engine, the alarms for the following event: *elements not assigned to any server* will also be deleted.

- Elements are synchronized manually or automatically
- User manually clears the alarms (although the alarms may reappear in the future when the scheduled task is next executed)

Viewing Synchronization Information

This section describes how to view synchronization status and history.

Viewing Mobility Services Engine Synchronization Status

You can use the Synchronize Servers command in Cisco WCS to view the status of network design, controller, and event group synchronization with a mobility services engine.

To view synchronization status, follow these steps:

Step 1 In Cisco WCS, choose **Mobility > Synchronize Services**.

Step 2 From the **Synchronize** drop-down menu, select either the **Network Designs**, **Controllers**, or **Event Groups** tab.

In the panel that appears, check the Sync. Status column for the synchronization status. A green two-arrow icon indicates that the mobility services engine is synchronized with the specified network design, controller or event group. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a given server.

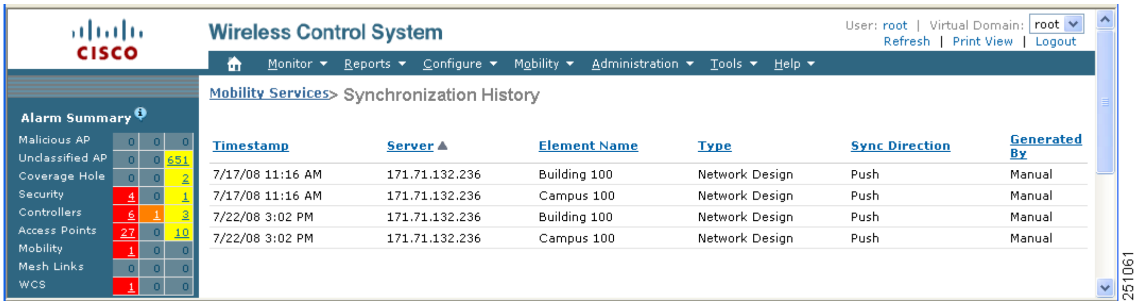
Viewing Synchronization History

You can view the synchronization history for the last 30 days for a mobility services engine. This is especially useful when automatic synchronization is enabled as alarms are automatically cleared. Synchronization history provides a summary of those cleared alarms.

To view synchronization history, follow these steps:

Step 1 In Cisco WCS, choose **Mobility > Synchronization History**. The Synchronization History window appears (.

Figure 3-2 Mobility > Synchronization History


Wireless Control System
User: root | Virtual Domain: root
Refresh | Print View | Logout
Monitor
Reports
Configure
Mobility
Administration
Tools
Help
Mobility Services> Synchronization History
251061

Alarm Summary

Malicious AP	0	0	0
Unclassified AP	0	0	651
Coverage Hole	0	0	2
Security	4	0	1
Controllers	6	1	3
Access Points	27	0	10
Mobility	1	0	0
Mesh Links	0	0	0
WCS	1	0	0

Timestamp	Server ▲	Element Name	Type	Sync Direction	Generated By
7/17/08 11:16 AM	171.71.132.236	Building 100	Network Design	Push	Manual
7/17/08 11:16 AM	171.71.132.236	Campus 100	Network Design	Push	Manual
7/22/08 3:02 PM	171.71.132.236	Building 100	Network Design	Push	Manual
7/22/08 3:02 PM	171.71.132.236	Campus 100	Network Design	Push	Manual

Step 2 Click the column headers to sort the entries. describes the column headings.

In the Synchronization History window, the Sync Direction column indicates whether information is pushed into the mobility services engine or pulled by the mobility services engine. The Generated By column indicates whether the synchronization was manual or automatic.

CHAPTER 4

Configuring and Viewing System Properties

This chapter describes how to configure and view system properties on the mobility services engine.

This chapter contains the following sections:

Configuring General Properties

You can use Cisco WCS to edit the general properties of a mobility services engine such as contact name, user name, password, HTTP and HTTPS.

To edit the general properties of a mobility services engine, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services** to display the Mobility Services window.

Step 2 Click the name of the mobility services engine you want to edit. A two-tabbed panel labeled with General and Performance appears.

Note If the General Properties window does not display by default, select **General Properties** from the **Systems** menu left panel.

Step 3 Modify the parameters as appropriate in the **General** panel. Table 4-1 describes each parameter.

Table 4-1 General Properties

Parameter	Configuration Options
Contact Name	Enter a contact name for the mobility services engine.
User Name	Enter the login user name for the Cisco WCS server that manages the mobility services engine.
Password	Enter the login password for the Cisco WCS server that manages the mobility services engine.
Port	8001
HTTP	Check the **Enable** check box to enable HTTP. By default, HTTPS is enabled. **Note** HTTP is primarily enabled to allow third-party applications to communicate with the mobility services engine. **Note** Cisco WCS always communicates through HTTPS.
Legacy Port	Enter the mobility services port number that supports HTTPS communication. The Legacy HTTPS option must also be enabled.
Legacy HTTPS	This parameter does not apply to mobility services engines. It applies only to location appliances.
Mobility Services	To enable a service on a mobility services engine, select the button next to the desired service. Once selected, the service displays as active (UP). **Note** Only one service can operate on a mobility services engine at a time. Operation of multiple services on a mobility services engine is not supported. All inactive services are noted as (DOWN) on the selected (current) system and on the network.

Step 4 Click **Save** to update the Cisco WCS and mobility services engine databases.

Modifying NMSP Parameters

Network Mobility Services Protocol (NMSP) is the protocol that manages communication between the mobility services engine and the controller. Transport of telemetry, emergency, and chokepoint information between the mobility services engine and the controller is managed by this protocol.

Note No change in the default parameter values is recommended unless the network is experiencing slow response or excessive latency.

- Telemetry, emergency and chokepoint information is only seen on controllers and Cisco WCS installed with release 4.1 software or later.
- The TCP port (16113) that the controller and mobility services engine communicate over MUST be open (not blocked) on any farewell that exists between the controller and mobility services engine for NMSP to function.

To configure NMSP parameters, follow these steps:

Step 1 In Cisco WCS, click **Mobility> Mobility Services.**

Step 2 Click the name of the mobility services engine whose properties you want to edit.

Step 3 From the **System** menu (left panel), select **NMSP Parameters**. The configuration options appear.

Step 4 Modify the NMSP parameters as appropriate. Table 4-2 describes each parameter.

Table 4-2 NMSP Parameters

Parameter	Description
Echo Interval	Defines how frequently an echo request is sent from a mobility services engine to a controller. The default value is 15 seconds. Allowed values range from 1 to 120 seconds. **Note** If a network is experiencing slow response, you can increase the values of the echo interval, neighbor dead interval and the response timeout values to limit the number of failed echo acknowledgements.
Neighbor Dead Interval	The number of seconds that the mobility services engine waits for a successful echo response from the controller before declaring the neighbor dead. This timer begins when the echo request is sent. The default values is 30 seconds. Allowed values range from 1 to 240 seconds. **Note** This value must be at least two times the echo interval value.
Response Timeout	Indicates how long the mobility services engine waits before considering the pending request as timed out. The default value is 1 second. Minimum value is one (1). There is no maximum value.

Table 4-2 NMSP Parameters (continued)

Parameter	Description
Retransmit Interval	Interval of time that the mobility services engine waits between notification of a response time out and initiation of a request retransmission. The default setting is 3 seconds. Allowed values range from 1 to 120 seconds.
Maximum Retransmits	Defines the maximum number of retransmits that are sent in the absence of a response to any request. The default setting is 5. Allowed minimum value is zero (0). There is no maximum value.

Step 5 Click **Save** to update the Cisco WCS and mobility services engine databases.

Viewing Active Sessions on a System

You can view active user sessions on the mobility services engine.

For every session, Cisco WCS displays the following information:

- Session identifier
- IP address from which the mobility services engine is accessed
- Surname of the connected user
- Date and time when the session started
- Date and time when the mobility services engine was last accessed
- How long the session was idle since it was last accessed

To view active user sessions, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine on which you want to view active sessions.

Step 3 Click **System > Active Sessions**.

Adding and Deleting Trap Destinations

You can specify which Cisco WCS or Cisco Security Monitoring, Analysis and Response System (CS-MARS) network management platform is the recipient of SNMP traps generated by the mobility services engine.

When a user adds a mobility services engine using Cisco WCS, that WCS platform automatically establishes itself as the default trap destination. If a redundant Cisco WCS configuration exists, the backup WCS is not listed as the default trap destination unless the primary WCS fails and the back system takes over. Only an active Cisco WCS is listed as a trap destination.

Adding Trap Destinations

To add a trap destination, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine for which you want to define a new SNMP trap destination server.

Step 3 Click **System > Trap Destinations**.

Step 4 Select **Add Trap Destination** from the Select a command drop-down menu. Click **GO**.

Step 5 Enter IP address of destination SNMP server.

Step 6 Port number default of **162** is auto-populated. You can modify this as needed.

Step 7 Community default value of **public** is auto-populated. You can modify this as needed.

Step 8 Destination default value of *other* auto-populates.

Note All trap destinations are identified as *other* except for the automatically created *default* trap destination.

Step 9 Click **Save** to save settings.

You are returned to the trap destinations summary window and the newly-defined trap is listed.

Deleting Trap Destinations

To delete a trap destination, follow these steps;

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine for which you want to delete a SNMP trap destination server.

Step 3 Click **System > Trap Destinations**.

Step 4 Check the check box next to the trap destination entry that you want to delete.

Step 5 Select **Delete Trap Destination** from the Select a command drop-down menu. Click **GO**.

Step 6 In the message box that appears, click **OK** to confirm deletion.

Viewing and Configuring Advanced Parameters

In Cisco WCS, at the Advanced Parameters window (Figure 4-1) you can both view general system level settings of the mobility services engine, and configure monitoring parameters.

- Refer to the“Viewing Advanced Parameters Settings” section on page 4-6 to review current system level settings of the advanced parameters.

- Refer to the "Configuring Advanced Parameters" section on page 4-7 to modify the current system level settings of the advanced parameters.

Note You can also initiate advanced commands such as a system reboot, a system shutdown, clearing the configuration file, and defragment the system database. Refer to the "Initiating Advanced Commands" section on page 4-8 for information on these commands and when they should be used

Viewing Advanced Parameters Settings

To view the advanced parameter settings of the mobility services engine, follow these steps:

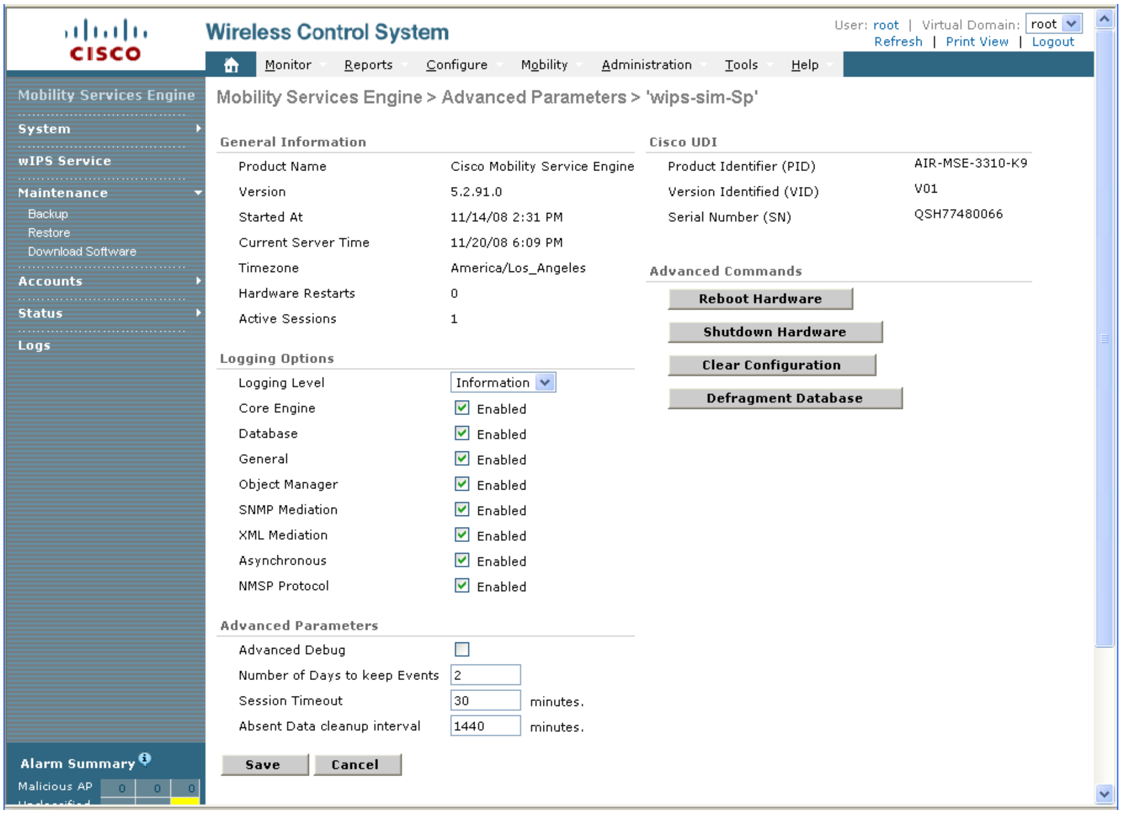
Step 1 In Cisco WCS, click **Mobility > Mobility Services.**

Step 2 Click the name of a mobility services engine to view its status.

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.The following window appears (Figure 4-1).

Figure 4-1 System > Advanced Parameters



Mobility Services Engine > Advanced Parameters > 'wips-sim-Sp'

General Information

Product Name	Cisco Mobility Service Engine
Version	5.2.91.0
Started At	11/14/08 2:31 PM
Current Server Time	11/20/08 6:09 PM
Timezone	America/Los_Angeles
Hardware Restarts	0
Active Sessions	1

Cisco UDI

Product Identifier (PID)	AIR-MSE-3310-K9
Version Identified (VID)	V01
Serial Number (SN)	QSH77480066

Advanced Commands

Logging Options

Logging Level	Information
Core Engine	☑ Enabled
Database	☑ Enabled
General	☑ Enabled
Object Manager	☑ Enabled
SNMP Mediation	☑ Enabled
XML Mediation	☑ Enabled
Asynchronous	☑ Enabled
NMSP Protocol	☑ Enabled

Advanced Parameters

Advanced Debug	☐
Number of Days to keep Events	2
Session Timeout	30 minutes.
Absent Data cleanup interval	1440 minutes.

273618

Configuring Advanced Parameters

On the Advanced Parameters window, you can use Cisco WCS:

- To specify the logging level and types of messages to log.

  Refer to the "Configuring Logging Options" section on page 4-7.

- To set how long events are kept, how long before a session time-outs, interval between data clean ups and enable or disable advanced debug level messages in the logs.

  Refer to the "Configuring Advanced Parameters" section on page 4-7.

Configuring Logging Options

You can use Cisco WCS to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to configure.

Step 3 From the System menu (left panel) click **Advanced Parameters**. The advanced parameters for the selected mobility services engine appears.

Step 4 Scroll down to the Logging Options section and choose the appropriate option from the Logging Level drop-down menu.

There are four logging options: **Off**, **Error**, **Information**, and **Trace**.

Caution Use **Error** and **Trace** only when directed to do so by Cisco Technical Assistance Center (TAC) personnel.

Step 5 Check the **Enabled** check box next to each item listed in that section to begin logging of its events.

Step 6 Click **Save** to apply your changes.

Configuring Advanced Parameters

You can use Cisco WCS to set how long events are kept, how long before a session time-outs, interval between data clean ups and enable or disable advanced debug level messages in the logs.

To configure advanced parameters, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to configure.

Step 3 From the System menu (left panel) click **Advanced Parameters**. The advanced parameters for the selected mobility services engine appears.

Step 4 Scroll down to the Advanced Parameters and make the appropriate changes. Table 4-3 describes the parameters.

Table 4-3 Advanced Parameters

Parameter	Configuration Options
Advanced debug	Check the check box to enable advanced debug. This enables reporting of advanced debug level messages to the log files.
Number of days to keep events	Enter the number of days that events are kept in the event table. Default value is 2.
Session time-out (minutes)	Enter the number of minutes a Cisco WCS or client session can remain inactive before it times out. Default value is 30.
Absent data cleanup interval (minutes)	Enter the number of minutes that data for *absent* mobile stations is kept. An *absent* mobile station is one that was discovered but does not appear in the network. Default value is 1440.

Initiating Advanced Commands

You can initiate a system reboot or shutdown, clear the system configuration or defragment a database by clicking the appropriate button on the Advanced Parameters page.

Reboot or Shutdown a System

To reboot or shutdown a mobility services engine, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services.**

Step 2 Click the name of a mobility services engine you want to reboot or shutdown

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands section of the window (right), click the appropriate button (**Reboot Hardware** or **Shutdown Hardware**).

Click **OK** in the confirmation pop-up window to initiate either the reboot or shutdown process. Click **Cancel** to stop the process.

Clear a Configuration File

To clear a configuration file of a mobility services engine, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services.**

Step 2 Click the name of a mobility services engine for which you want to clear its configuration file.

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands section of the window (right), click the **Clear Configuration** button.

Click **OK** in the confirmation pop-up window to initiate the process. Click **Cancel** to stop the process.

Defragment Database

To clear a configuration file of a mobility services engine, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services.**

Step 2 Click the name of a mobility services engine for which you want to clear its configuration file.

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands section of the window (right), click the **Clear Configuration** button.

Click **OK** in the confirmation pop-up window to initiate the process. Click **Cancel** to stop the process.

CHAPTER 5

Managing Users and Groups

This chapter describes how to configure and manage users, groups, and host access on the mobility services engine.

This chapter contains the following sections:

- "Managing Groups" section on page 5-2
- "Managing Users" section on page 5-3

Managing Groups

This section describes how to add, delete, and edit user groups.

User groups allow you to define and different access privileges to users.

Caution Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with read access permission, that user will not be able to configure mobility services engine settings.

Adding User Groups

To add a user group to a mobility services engine, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine to which you want to add a user group.

Step 3 Click **Accounts** (left).

Step 4 Click **Groups**.

Step 5 Select **Add Group** from the Select a command drop-down menu and click **GO**.

Step 6 Enter the name of the group in the Group Name field.

Step 7 Select a permission level from the Permission drop-down menu.

There are three permissions levels to select from:

- Read Access
- Write Access
- Full Access (required for Cisco WCS to access mobility services engines)

Step 8 Click **Save** to add the new group to the mobility services engine.

Deleting User Groups

To delete user groups from a mobility services engine, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine from which you want to delete a user group.

Step 3 Click **Accounts** (left).

Step 4 Click **Groups**.

Step 5 Check the check boxes of the groups that you want to delete.

Step 6 Select **Delete Group** from the Select a command drop-down menu and click **GO**.

Step 7 Click **OK** to confirm that you want to delete the selected groups.

Changing User Group Permissions

To change user group permissions, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine you want to edit.

Step 3 Click **Accounts** (left).

Step 4 Click **Groups**.

Step 5 Click the name of the group you want to edit.

Step 6 Select a permission level from the Permission drop-down menu.

Step 7 Click **Save** to apply your change.

Caution Group permissions override individual user permissions. For example, if you give a user permission for full access and add that user to a group with read access, that user will not be able to configure mobility services engine settings.

Managing Users

This section describes how to add, delete, and edit users to a mobility services engine. It also describes how to view active user sessions.

Adding Users

To add a users to a mobility services engine, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine to which you want to add users.

Step 3 Click **Accounts** (left).

Step 4 Click **Users**.

Step 5 Select **Add User** from the Select a command drop-down menu and click **GO**.

Step 6 Enter the username in the Username field.

Step 7 Enter a password in the Password field.

Step 8 Enter the name of the group to which the user belongs in the Group Name field.

Step 9 Select a permission level from the Permission drop-down menu.

There are three permission levels to select from: Read Access, Write Access, and Full Access (required for Cisco WCS to access a mobility services engine).

Caution Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with read access, that user will not be able to configure mobility services engine settings.

Step 10 Click **Save** to add the new user to the mobility services engine.

Deleting Users

To delete a user from a mobility services engine, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine from which you want to delete a user.

Step 3 Click **Accounts** (left).

Step 4 Click **Users**.

Step 5 Check the check boxes of the users that you want to delete.

Step 6 Select **Delete User** from the Select a command drop-down menu and click **GO**.

Step 7 Click **OK** to confirm that you want to delete the selected users.

Changing User Properties

To change user properties, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine you want to edit.

Step 3 Click **Accounts** (left).

Step 4 Click **Users**.

Step 5 Click the name of the group that you want to edit.

Step 6 Make the required changes to the Password, Group Name, and Permission fields.

Step 7 Click **Save** to apply your change.

CHAPTER 6

Configuring wIPS and Profiles

This chapter describes how to configure wIPS profiles and those items that must be configured in conjunction to operate wIPS.

This chapter contains the following sections:

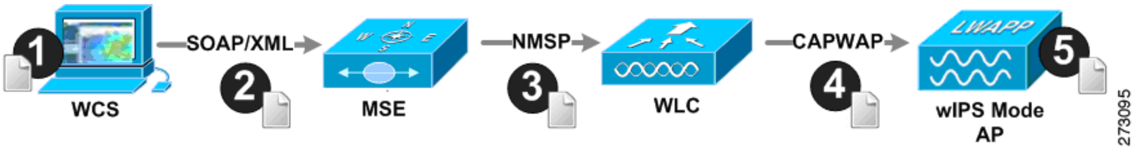
- "Configuring Access Points for wIPS Monitor Mode" section on page 6-3
- "Configuring wIPS Profiles" section on page 6-4

Overview of wIPS Configuration and Profile Management

Configuration of wIPS profiles follows a chained hierarchy starting with WCS which is used for profile viewing and modification. The actual profiles are stored within the wIPS service running on the mobility services engine (MSE).

From the wIPS service on the mobility services engine, profiles are propagated to specific controllers which in turn communicate this profile transparently to wIPS mode access points associated to that respective controller.

Figure 6-1 Configuration and Update of wIPS Profiles



When a configuration change to a wIPS profile is made at WCS and applied to a set of mobility services engines and controllers, the following occurs:

1. The configuration profile is modified on WCS and version information is updated.
2. An XML-based profile is pushed to the wIPS engine running on the mobility services engine. This update occurs over the SOAP/XML protocol.
3. The wIPS engine on the mobility services engine updates each controller associated with that profile by pushing out the configuration profile over NMSP.

Note A controller is associated to a single configuration profile. All wIPS mode access points connected to that controller share the same wIPS configuration.

4. The controller receives the updated wIPS profile, stores it into NVRAM (replacing any previous revision of the profile) and propagates the updated profile to its associated wIPS access points using CAPWAP control messages.
5. A wIPS mode access point receives the updated profile from the controller and applies the modifications to its wIPS software engine.

Note The mobility services engine can only be configured from one Cisco WCS.

Before you can configure wIPS profiles you must do the following:

1. Install a mobility services engine (if one is not already operating in the network). Refer to the *Cisco 3350 Mobility Services Engine Getting Started Guide* or *Cisco 3350 Mobility Services Engine Getting Started Guide* at:
   http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html
2. Add the mobility services engine to Cisco WCS (if not already added). Refer to Chapter 2, "Adding and Deleting Systems"
3. Configure access points to operate in wIPS monitor mode. Refer to "Configuring Access Points for wIPS Monitor Mode" section on page 6-3.
4. Configure wIPS profiles. Refer to "Configuring wIPS Profiles" section on page 6-4.

Configuring Access Points for wIPS Monitor Mode

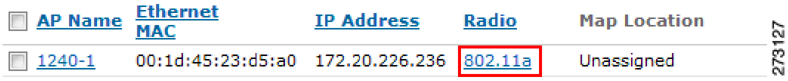
Note Only Cisco Aironet 1130, 1140, 1240 and 1250 Series Access Points support wIPS monitor mode.

To configure an access point to operate in wIPS monitor mode, follow these steps:

Step 1 In Cisco WCS, click **Configure > Access Points**.

Step 2 Click on the 802.11a or 802.11b/g radio. (Figure 6-2).

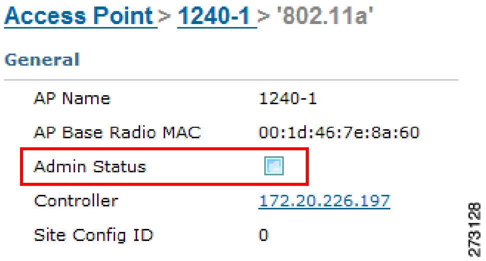
Figure 6-2 Configure > Access Points > Radio



☐	AP Name	Ethernet MAC	IP Address	Radio	Map Location
☐	1240-1	00:1d:45:23:d5:a0	172.20.226.236	802.11a	Unassigned

Step 3 On the access point window, uncheck **Admin Status** to disable the radio.

Figure 6-3 Access Points > Radio



Access Point > 1240-1 > '802.11a'

General

AP Name	1240-1
AP Base Radio MAC	00:1d:46:7e:8a:60
Admin Status	☐
Controller	172.20.226.197
Site Config ID	0

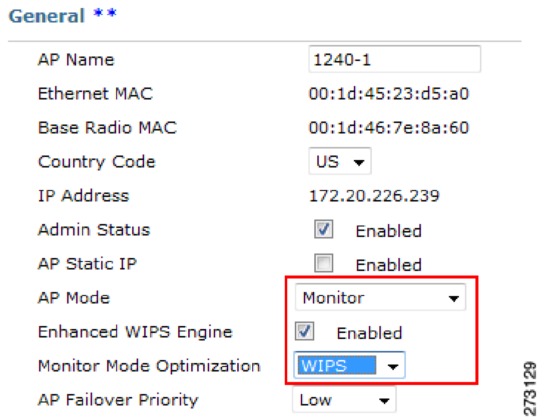
Step 4 Click **Save** (bottom).

Note Repeat these steps for each and every radio on an access point that is to be configured for wIPS monitor mode. For example, an Aironet 1130 requires this step to be performed on both its 802.11a and 802.11b/g radios.

Step 5 Once the radios are disabled, click **Configure > Access Points** and then click on the name of the access point whose radio you just disabled.

Step 6 At the access point configuration window, select **Monitor Mode** from the AP Mode drop-down menu. (Figure 6-4)

Figure 6-4 Configure > Access Points > AP Name



General **

AP Name	1240-1
Ethernet MAC	00:1d:45:23:d5:a0
Base Radio MAC	00:1d:46:7e:8a:60
Country Code	US
IP Address	172.20.226.239
Admin Status	☑ Enabled
AP Static IP	□ Enabled
AP Mode	Monitor
Enhanced WIPS Engine	☑ Enabled
Monitor Mode Optimization	WIPS
AP Failover Priority	Low

Step 7 Check the **Enabled** check box for the Enhanced WIPS Engine.

Step 8 Select **WIPS** from the Monitor Mode Optimization drop-down menu.

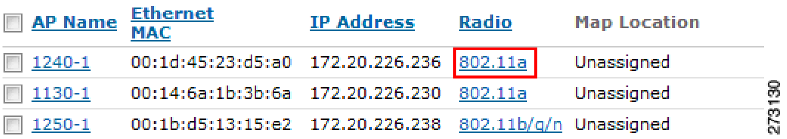
Step 9 Click **Save**.

Step 10 Click **OK** when prompted to reboot the access point.

Step 11 To reenable the access point radio, click **Configure > Access Points**.

Step 12 Click on the appropriate access point radio.

Figure 6-5 Configure > Access Points > Radio



□	AP Name	Ethernet MAC	IP Address	Radio	Map Location
□	1240-1	00:1d:45:23:d5:a0	172.20.226.236	802.11a	Unassigned
□	1130-1	00:14:6a:1b:3b:6a	172.20.226.230	802.11a	Unassigned
□	1250-1	00:1b:d5:13:15:e2	172.20.226.238	802.11b/g/n	Unassigned

Step 13 At the radio configuration panel, check the Admin Status **Enabled** check box.

Step 14 Click **Save**.

Repeat this for each access point and each respective radio configured for wIPS monitor mode.

Configuring wIPS Profiles

By default, the MSE and corresponding wIPS access points inherit the default wIPS profile from WCS. This profile comes pre-tuned with a majority of attack alarms enabled by default and will monitor attacks against access points within the same RF-Group as the wIPS access points. In this manner, the system comes pre-setup to monitor attacks against a deployment model that utilizes an integrated solution in which both the WLAN infrastructure and wIPS access points are intermixed on the same controller.

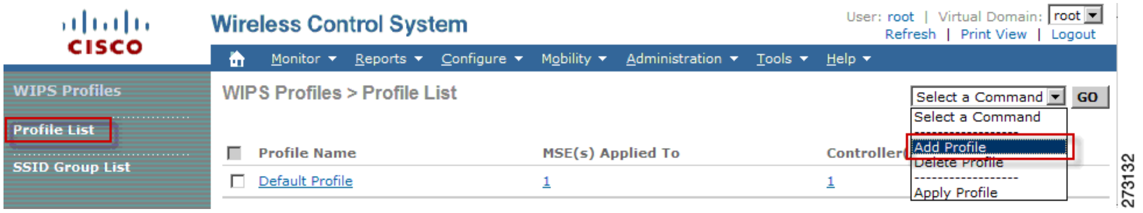
Note Some of the configuration steps that follow are marked as *Overlay-Only* and are only to be undertaken when deploying the Adaptive wIPS solution to monitor an existing WLAN Infrastructure such as an autonomous or completely separate controller-based WLAN.

To configure wIPS profiles, follow these steps:

Step 1 In Cisco WCS, click **Configure > WIPS Profiles**.

Step 2 In the window that appears (Figure 6-6), select **Profile List** (left panel).

Figure 6-6 WIPS Profiles > Profile List



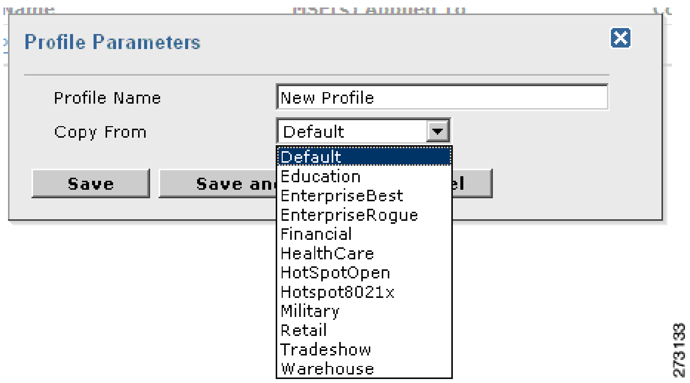
Profile Name	MSE(s) Applied To	Controller
Default Profile	1	1

Step 3 Select **Add Profile** from the Select a command drop-down menu.

Step 4 At the profile parameters panel, select a profile template from the Copy From drop-down menu. (Figure 6-7)

Note Cisco's Adaptive wIPS comes with a pre-defined set of profile templates from which customers can choose from or use as a basis for their own custom profiles. Each profile is tailored to either a specific business or application as are the specific alarms enabled on that profile.

Figure 6-7 Profile Parameters Configuration Panel



Profile Name: New Profile

Copy From: Default

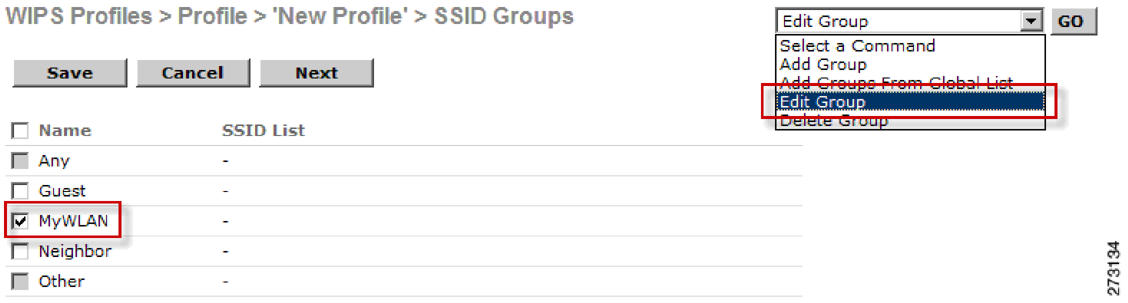
Step 5 After selecting a profile and entering a profile name, click **Save and Edit**.

Step 6 (Optional) Configure the SSIDs to Monitor.

By default, the system monitors attacks launched against the local Wireless LAN Infrastructure (as defined by APs which have the same 'RF Group' name). If the system should also be required to monitor attacks against another network, such as when deployed in an overlay deployment model, the SSID groups feature must be utilized.

Note If this step is not required, simply click **Next**.

Figure 6-8 SSID Groups Summary Panel


WIPS Profiles > Profile > 'New Profile' > SSID Groups
Save
Cancel
Next
Edit Group
GO
Select a Command
Add Group
Add Groups From Global List
Edit Group
Delete Group
273134

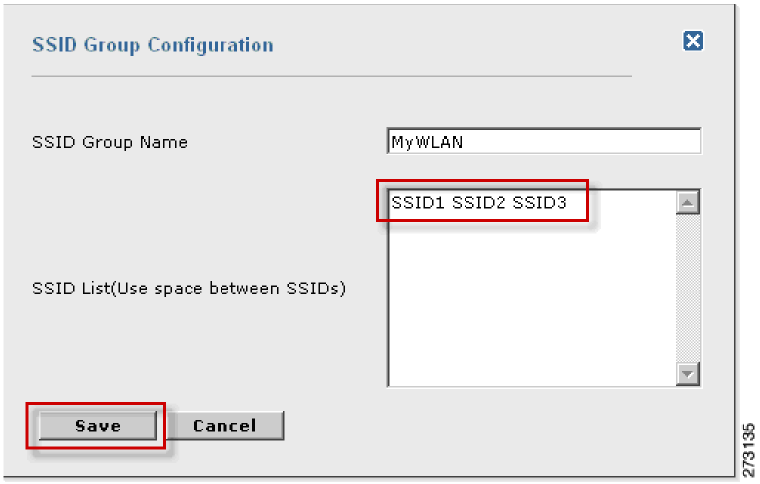
□ Name	SSID List
□ Any	-
□ Guest	-
☑ MyWLAN	-
□ Neighbor	-
□ Other	-

a. Check the box next to **MyWLAN** and select **Edit Group** from the drop down in the upper right hand corner then click **GO.**

b. Enter SSIDs to Monitor.

c. Enter the SSID name (separate multiple entries by a single space) and click **Save**.

Figure 6-9 SSID Group Configuration Panel

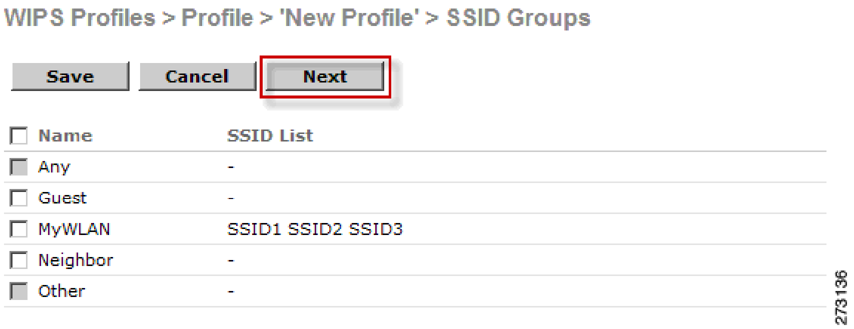


SSID Group Name: MyWLAN

SSID List(Use space between SSIDs): SSID1 SSID2 SSID3

The SSID Groups page appears confirming the SSID are added successfully. (Figure 6-10).

Figure 6-10 New Profile > SSID Groups Window

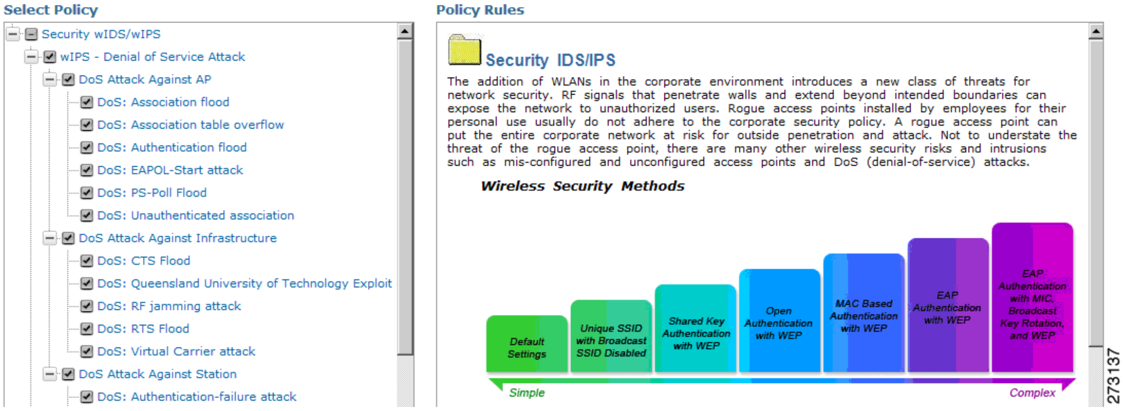


□ Name	SSID List
□ Any	-
□ Guest	-
□ MyWLAN	SSID1 SSID2 SSID3
□ Neighbor	-
□ Other	-

d. Click **Next**.

The Select Policy and Policy Rules summary window appears (Figure 6-11).

Figure 6-11 Next > Select Policy Summary Window



Select Policy

- ☐ Security wIDS/wIPS
  - ☑ wIPS - Denial of Service Attack
    - ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow
      - ☑ DoS: Authentication flood
      - ☑ DoS: EAPOL-Start attack
      - ☑ DoS: PS-Poll Flood
      - ☑ DoS: Unauthenticated association
    - ☑ DoS Attack Against Infrastructure
      - ☑ DoS: CTS Flood
      - ☑ DoS: Queensland University of Technology Exploit
      - ☑ DoS: RF jamming attack
      - ☑ DoS: RTS Flood
      - ☑ DoS: Virtual Carrier attack
    - ☑ DoS Attack Against Station
      - ☑ DoS: Authentication-failure attack

Policy Rules

Security IDS/IPS

The addition of WLANs in the corporate environment introduces a new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured and unconfigured access points and DoS (denial-of-service) attacks.

Wireless Security Methods

Default Settings
Unique SSID with Broadcast SSID Disabled
Shared Key Authentication with WEP
Open Authentication with WEP
MAC Based Authentication with WEP
EAP Authentication with WEP
EAP Authentication with MIC, Broadcast Key Rotation, and WEP
Simple
Complex
273137

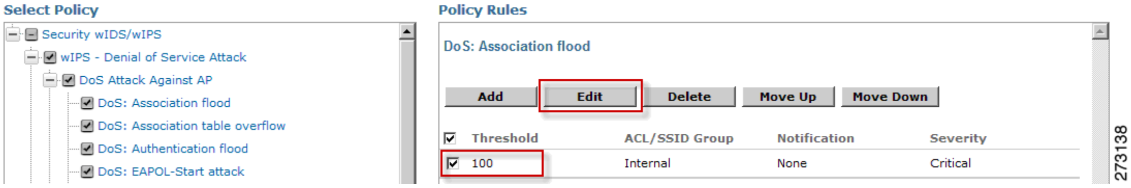
Note At the policy window (Figure 6-11), you can enable or disable attacks to be detected and reported. You can also edit specific thresholds for alarms and turn on forensics.

Step 7 To enable or disable attacks to be detected and reported, check the check box next to the specific attack type in question (left panel).

Step 8 To edit the profile, click on the name of the attack type (such as DoS: Association Flood).

The configuration panel for that attack type appears in the right panel above the policy rule description (Figure 6-12).

Figure 6-12 Policy Rules Panel



Select Policy

- ☐ Security wIDS/wIPS
  - ☑ wIPS - Denial of Service Attack
    - ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow
      - ☑ DoS: Authentication flood
      - ☑ DoS: EAPOL-Start attack

Policy Rules

DoS: Association flood

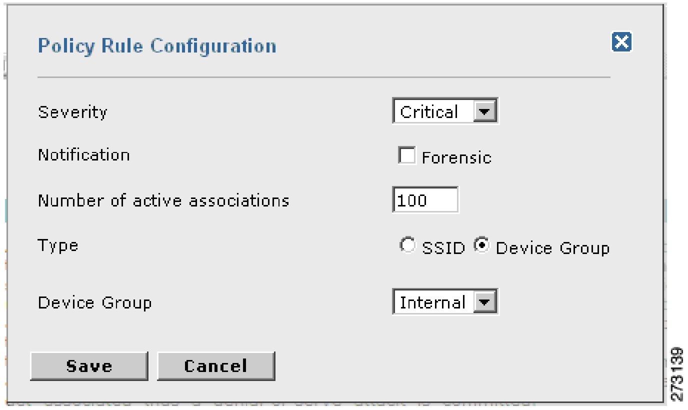
☑	Threshold	ACL/SSID Group	Notification	Severity
☑	100	Internal	None	Critical

Step 9 To modify a policy rule do the following:

a. Check the check box next to the policy rule and click **Edit**.

The Policy Rule Configuration window appears. (Figure 6-13)

Figure 6-13 Policy Rule Configuration Panel



Policy Rule Configuration

Severity	Critical
Notification	□ Forensic
Number of active associations	100
Type	○ SSID ● Device Group
Device Group	Internal

Save Cancel

b. Select the severity of the alarm.

c. Check the forensic check box if you want to capture packets for this alarm.

d. Modify the number of active associations, if desired. (This value varies by alarm type).

e. Select the type of WLAN infrastructure (SSID or Device Group) that the system will monitor for attacks.

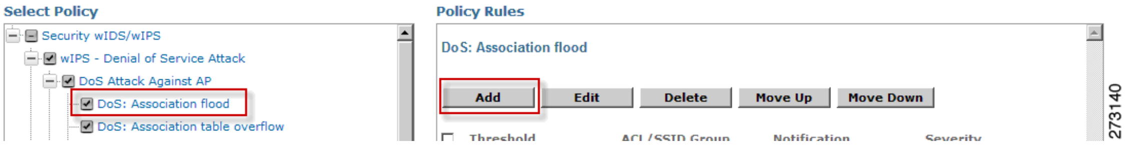
1. If you select SSID, continue with Step 10.
2. If you select Device Group, continue with Step 11.

Note **Device Group** (Type) and **Internal** are the defaults. *Internal* indicates all access points within the same RF Group. Selecting SSID as the type, allows you to monitor a separate network which is typical of an overlay deployment.

Step 10 (Optional, overlay deployments only) To add a policy rule for an SSID, do the following:

a. To add a policy rule, click **Add**. (Figure 6-14)

Figure 6-14 Adding a Policy Rule



Select Policy

- ☑ Security wIDS/wIPS
  - ☑ wIPS - Denial of Service Attack
    - ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow

Policy Rules

DoS: Association flood

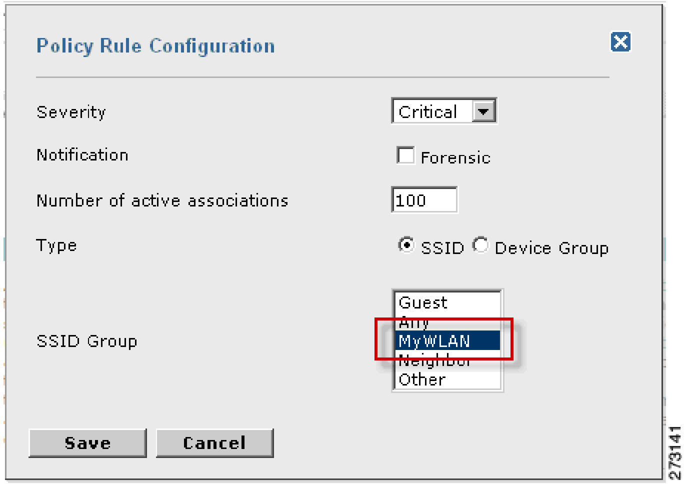
Add Edit Delete Move Up Move Down

□	Threshold	ACL/SSID Group	Notification	Severity

b. In the policy rule configuration panel that appears, select **MyWLAN** from the SSID Group pull-down menu. (Figure 6-15)

Note SSID is already selected as the type.

Figure 6-15 Policy Configuration Panel for SSIDs



Policy Rule Configuration

Severity	Critical ▾
Notification	□ Forensic
Number of active associations	100
Type	● SSID ○ Device Group
SSID Group	Guest Any MyWLAN Neighbor Other

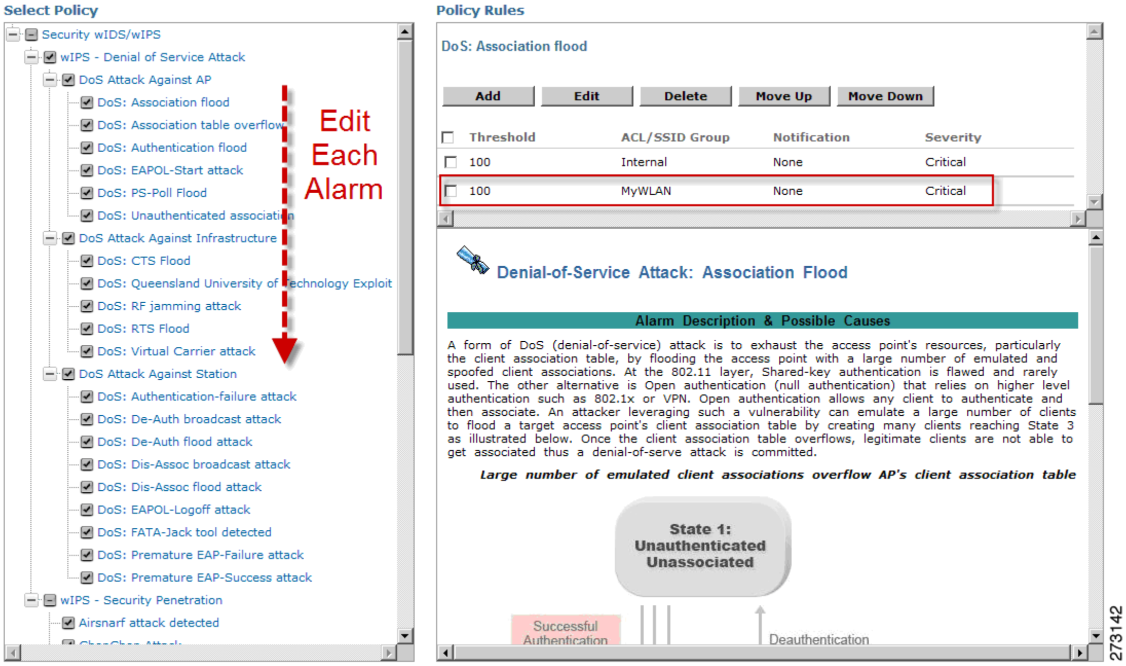
Save Cancel

c. Click **Save** after all changes are complete.

d. Modify each policy rule.Continue to Step 11 when all edits are complete.

Note When you configure a system to monitor another WLAN infrastructure by SSID, changes must be made for each and every policy rule to monitor by SSID. You must create a policy rule under each separate alarm which defines the system to monitor attacks against the SSID Group created earlier.

Figure 6-16 Edit Policy Rules for SSID Monitoring



Select Policy

- ☐ Security wIDS/wIPS
  - ☑ wIPS - Denial of Service Attack
    - ☑ DoS Attack Against AP
      - ☑ DoS: Association flood
      - ☑ DoS: Association table overflow
      - ☑ DoS: Authentication flood
      - ☑ DoS: EAPOL-Start attack
      - ☑ DoS: PS-Poll Flood
      - ☑ DoS: Unauthenticated association
    - ☑ DoS Attack Against Infrastructure
      - ☑ DoS: CTS Flood
      - ☑ DoS: Queensland University of Technology Exploit
      - ☑ DoS: RF jamming attack
      - ☑ DoS: RTS Flood
      - ☑ DoS: Virtual Carrier attack
    - ☑ DoS Attack Against Station
      - ☑ DoS: Authentication-failure attack
      - ☑ DoS: De-Auth broadcast attack
      - ☑ DoS: De-Auth flood attack
      - ☑ DoS: Dis-Assoc broadcast attack
      - ☑ DoS: Dis-Assoc flood attack
      - ☑ DoS: EAPOL-Logoff attack
      - ☑ DoS: FATA-Jack tool detected
      - ☑ DoS: Premature EAP-Failure attack
      - ☑ DoS: Premature EAP-Success attack
  - ☐ wIPS - Security Penetration
    - ☑ Airsnarf attack detected
    - ☑ ChopChop Attack

Policy Rules

DoS: Association flood

Add Edit Delete Move Up Move Down

□	Threshold	ACL/SSID Group	Notification	Severity
□	100	Internal	None	Critical
□	100	MyWLAN	None	Critical

Denial-of-Service Attack: Association Flood

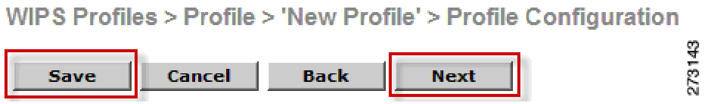
Alarm Description & Possible Causes

A form of DoS (denial-of-service) attack is to exhaust the access point's resources, particularly the client association table, by flooding the access point with a large number of emulated and spoofed client associations. At the 802.11 layer, Shared-key authentication is flawed and rarely used. The other alternative is Open authentication (null authentication) that relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker leveraging such a vulnerability can emulate a large number of clients to flood a target access point's client association table by creating many clients reaching State 3 as illustrated below. Once the client association table overflows, legitimate clients are not able to get associated thus a denial-of-serve attack is committed.

Large number of emulated client associations overflow AP's client association table

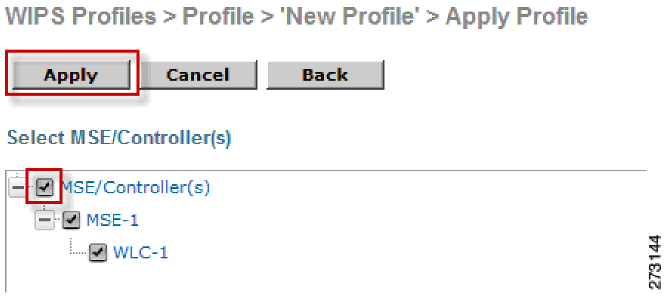
Step 11 Click **Save** to save the Profile (SSID or Device Group). Click **Next**. (Figure 6-17)

Figure 6-17 Saving Profile Configuration


WIPS Profiles > Profile > 'New Profile' > Profile Configuration
Save
Cancel
Back
Next
273143

Step 12 Select the MSE/Controller combinations to apply the profile to and then click **Apply**. (Figure 6-18)

Figure 6-18 Applying Profile Configuration.



☑ MSE/Controller(s)
- ☑ MSE-1
  - ☑ WLC-1

CHAPTER 7

Monitoring the System and Services

This chapter describes how to monitor the mobility services engine by configuring and viewing alarms, events, and logs as well as how to generate reports on system utilization and security.

This chapter contains the following sections:

- "Working with Alarms" section on page 7-2
- "Working with Events" section on page 7-5
- "Working with Logs" section on page 7-6
- "Generating Reports" section on page 7-7
- "Security Reports" section on page 7-10

Working with Alarms

This section describes how to view, assign, and clear alarms and events on a mobility services engine using Cisco WCS. Details on how to have email notifications for alarms sent to you is described as well as how to define those types (all, critical, major, minor, warning) of alarm notifications that are sent to you.

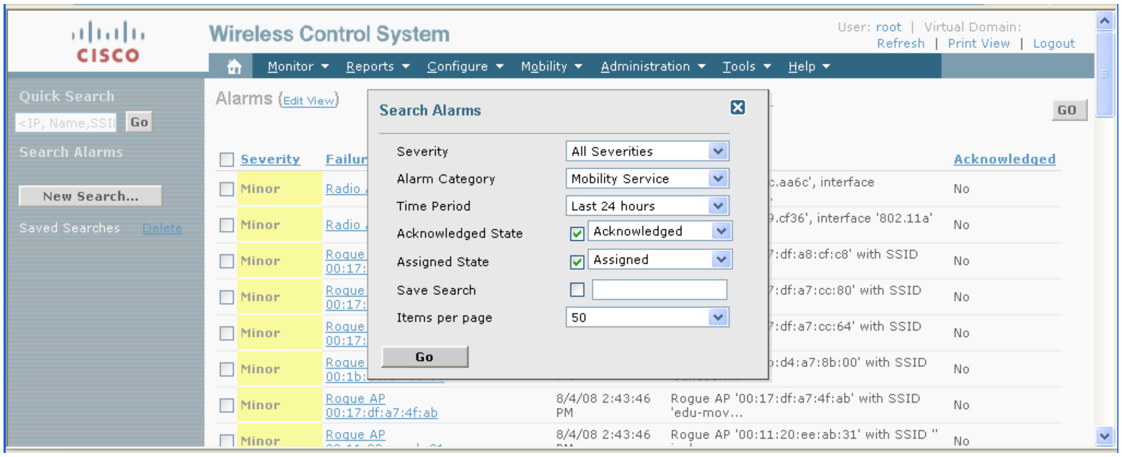
Viewing Alarms

To view mobility services engine alarms, follow these steps:

Step 1 In Cisco WCS, click **Monitor > Alarms**.

Step 2 Click **New Search**. A configurable search panel for alarms appears (Figure 7-1).

Figure 7-1 Search Alarm Panel



Search Alarms

Severity	All Severities
Alarm Category	Mobility Service
Time Period	Last 24 hours
Acknowledged State	☑ Acknowledged
Assigned State	☑ Assigned
Save Search	□
Items per page	50

Go

Step 3 Select the Severity of Alarms to display. Options are All Severities, Critical, Major, Minor or Warning.

Step 4 Select **Mobility Service** from the Alarm Category.

Options are: All Types, Access Points, Controller, Coverage Hole, Config Audit, Mobility Service Location Notifications, Interference, Mesh Links, Rogue AP, Rogue Adhoc**,** Security and WCS.

Step 5 Select the time frame for which you want to review alarms by selecting the appropriate option from the Time Period drop-down menu.

Options range from minutes (5, 15 and 30) to hours (1 and 8) to days (1 and 7). To display all select **Any time**.

Step 6 Check the **Acknowledged State** check box to exclude the acknowledged alarms and their count from the Alarm Summary window.

Step 7 Check the **Assigned Stat**e check box to exclude the assigned alarms and their count from the Alarm Summary window.

Step 8 To save the search criteria for later use, check the **Save Search** box and enter a name for the search.

Note The search is then accessible from the Saved Searches drop-down menu (left-panel) of the Monitor > Alarms window.

Step 9 Select the number of alarms to display on each window from the Items per page drop-down menu.

Step 10 Click **GO**. Alarms summary panel appears with search results.

Note Click the column headings (Severity, Failure Object, Owner, Date/Time and Message) to sort alarms.

Step 11 Repeat Step 2 to Step 10 to see notifications for the mobility services engine by entering **Location Notifications** as the alarm category in Step 4.

Assigning and Unassigning Alarms

To assign and unassign an alarm to yourself, follow these steps:

Step 1 Display the Alarms window as described in the "Viewing Alarms" section on page 7-2.

Step 2 Select the alarms that you want to assign to yourself by checking their corresponding check boxes.

Note To unassign an alarm assigned to you, uncheck the box next to the appropriate alarm. You cannot unassign alarms assigned to others.

Step 3 From the Select a command drop-down menu, choose **Assign to Me** (or **Unassign**) and click **GO**.

If you choose **Assign to Me**, your username appears in the Owner column. If you choose **Unassign**, the username column becomes empty.

Deleting and Clearing Alarms

To delete or clear an alarm from a mobility services engine, follow these steps:

Step 1 Display the Alarms window as described in the "Viewing Alarms" section on page 7-2.

Step 2 Select the alarms that you want to delete or clear by checking their corresponding check boxes.

Note If you delete an alarm, Cisco WCS removes it from its database. If you clear an alarm, it remains in the Cisco WCS database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.

Step 3 From the Select a command drop-down menu, choose **Delete** or **Clear**, and click **GO**.

Emailing Alarm Notifications

Cisco WCS lets you send alarm notifications to a specific email address. Sending notifications through email enables you to take prompt action when needed.

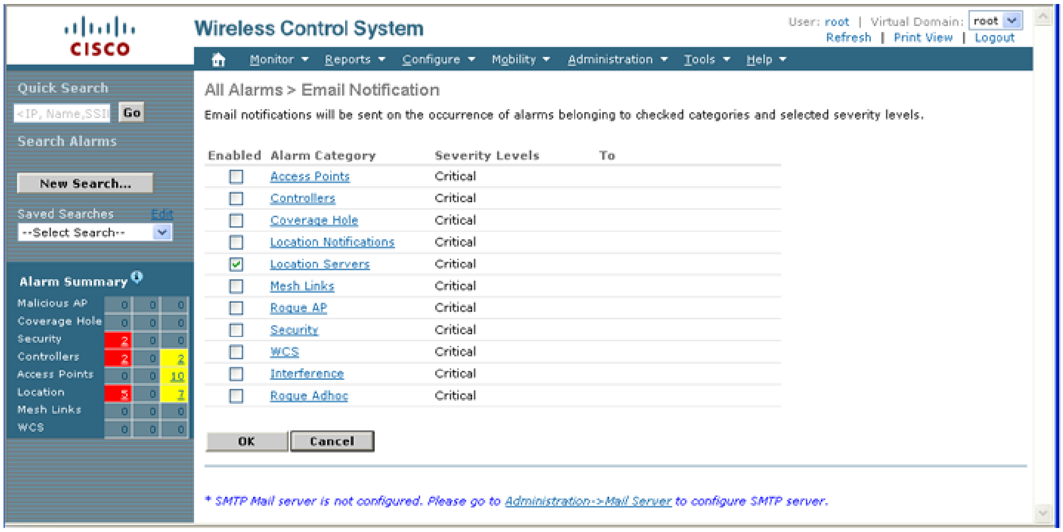
You can select the alarm severity types (critical, major, minor and warning) that are emailed to you.

To send alarm notifications, follow these steps:

Step 1 Display the Alarms window as described in the "Viewing Alarms" section on page 7-2.

Step 2 From the Select a commands drop-down menu, choose **Email Notification**, and click **GO**. The Email Notification window appears.

Figure 7-2 All Alarms > Email Notification Window



Malicious AP	0	0	0
Coverage Hole	0	0	0
Security	2	0	0
Controllers	2	0	2
Access Points	0	0	10
Location	5	0	7
Mesh Links	0	0	0
WCS	0	0	0

All Alarms > Email Notification

Email notifications will be sent on the occurrence of alarms belonging to checked categories and selected severity levels.

Enabled	Alarm Category	Severity Levels	To
□	Access Points	Critical	
□	Controllers	Critical	
□	Coverage Hole	Critical	
□	Location Notifications	Critical	
☑	Location Servers	Critical	
□	Mesh Links	Critical	
□	Rogue AP	Critical	
□	Security	Critical	
□	WCS	Critical	
□	Interference	Critical	
□	Rogue Adhoc	Critical	

* SMTP Mail server is not configured. Please go to Administration->Mail Server to configure SMTP server.

281000

Note A SMTP Mail Server must be defined prior to entry of target email addresses for email notification. Choose **Administraton** > **Settings** > **Mail Server** to enter the appropriate information. You can also select the Administration > Mail Server link, if displayed, on the Email Notification window noted above.

Step 3 Click the **Enabled** box next to the **Location Servers**.

Note Enabling the Location Servers alarm category sends all alarms related to location services and the mobility services engine system to the defined email address.

Step 4 Click the **Location Servers** link. The panel for configuring the alarm severity types (critical, major, minor and warning) that are reported for the mobility services engine appears.

Step 5 Check the check box next to all the alarm severity types for which you want email notifications sent.

Step 6 In the To field, enter the email address or addresses to which you want the email notifications sent. Email addresess are separated by commas.

Step 7 Click **OK**.

You are returned to the Alarms > Notification window. The changes to the reported alarm severity levels and the recipient email address for email notifications are displayed.

Working with Events

You can use Cisco WCS to view mobility services engine and location notification events. You can search and display events based on their severity (critical, major, minor, warning, clear, info) and event category.

You can search by the following event categories:

- By network coverage: coverage holes and interference
- By link: mesh links
- By notifications: location notifications
- By product type: access points (rogue and non-rogue), clients, controllers, and mobility service

Note The product type: mobility service reports events for mobility services engines.

- By security

Additionally, you can search for an element's events by its IP address, MAC address or name.

A successful event search displays the event severity, failure object, date and time of the event, and any messages for each event.

To display events, follow these steps:

Step 1 In Cisco WCS, click **Monitor > Events**.

Step 2 In the Events window:

- If you want to display the events for a specific element and you know its IP address, MAC address, or Name, enter that value in the Quick Search field (left panel). Click **GO**.
- To display events by severity and category, select the appropriate options from the Severity and Event Category drop-down menus (left panel). Click **Search**.

Step 3 If Cisco WCS finds events that match the search criteria, it displays a list of these events.

Note For more information about an event, click the failure object associated with the event. Additionally, you can sort the events summary by each of the column headings.

Working with Logs

This section describes how to configure logging options and how to download log files.

Configuring Logging Options

You can use Cisco WCS to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to configure.

Step 3 From the System menu (left panel) click **Advanced Parameters**. The advanced parameters for the selected mobility services engine appears.

Step 4 Scroll down to the Logging Options section and choose the appropriate option from the Logging Level drop-down menu.

There are four logging options: **Off**, **Error**, **Information**, and **Trace**.

Caution Use **Error** and **Trace** only when directed to do so by Cisco Technical Assistance Center (TAC) personnel.

Step 5 Check the **Enabled** check box next to each element listed in that section to begin logging of its events.

Step 6 Click **Save** to apply your changes.

Downloading Location Server Log Files

If you need to analyze mobility services engine log files, you can use Cisco WCS to download them to your system. Cisco WCS downloads a zip file containing the log files.

To download a zip file containing the log files, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine to view its status.

Step 3 Click **Logs** (left panel).

Step 4 Click **Download Logs**.

Step 5 Follow the instructions in the File Download dialog box to open the file or save the zip file to your system.

Generating Reports

In Cisco WCS, you can generate a utilization report for a mobility services engine. By default, reports are stored on the Cisco WCS server.

The location utilization report summarizes and charts the following information in two separate charts for a prescribed period of time:

- Chart 1 summarizes and graphs CPU and memory utilization
- Chart 2 summarizes and graphs client count, tag count, rouge client count, rogue access point count, and ad hoc rogue count

You can generate a utilization report for a mobility services engine. Once defined, the report can be saved for future diagnostic use and run on either an ad hoc or scheduled basis.

You can define the following in a utilization report:

- What mobility services engine or mobility services engines are monitored
- How often the report is generated
- How the data is graphed on the charts
- Whether the report is emailed or exported to a file

Creating a System Utilization Report

To create a utilization report for the mobility services engine, follow these steps:

Step 1 In Cisco WCS, click **Reports > Performance Reports.**

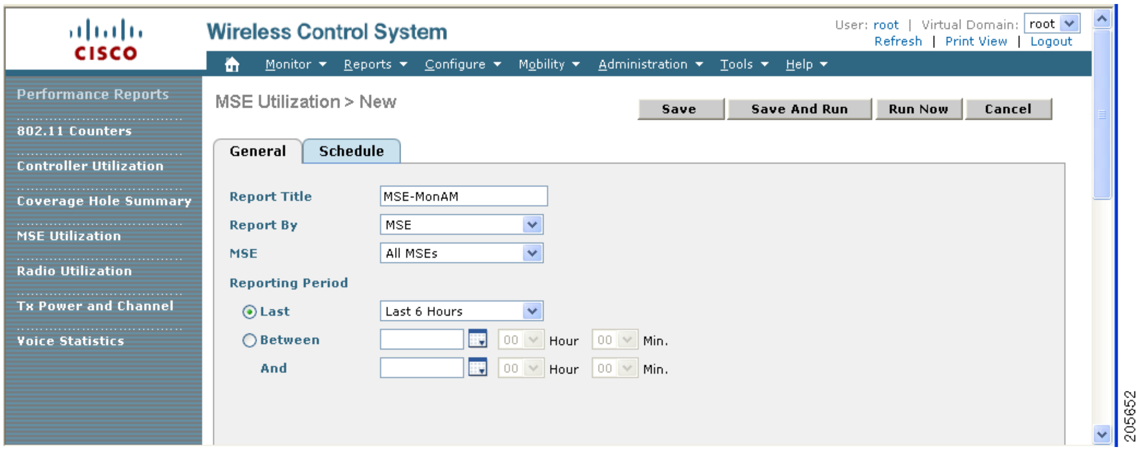
Step 2 Select **MSE Utilization** from the listing under the Performance Reports heading (left panel).

The MSE summary window appears.

Step 3 Select **New** from the Select a command drop-down menu. Click **GO**.

A tabbed panel appears (see Figure 7-3).

Figure 7-3 Reports > Performance Reports > MSE Utilization



Report Title: MSE-MonAM

Report By: MSE

MSE: All MSEs

Reporting Period

● Last: Last 6 Hours

○ Between: 00 Hour 00 Min.

And: 00 Hour 00 Min.

Step 4 Enter a report title.

Step 5 The Report By selection is always MSE.

Step 6 Select either a specific mobility services engine or **All MSEs** from the drop-down MSE menu.

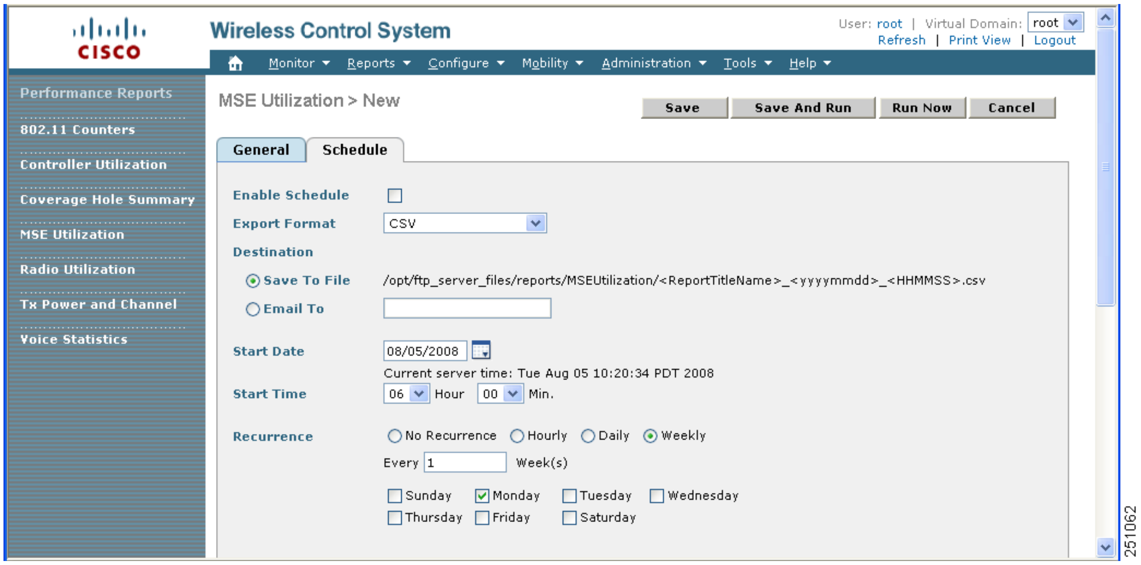
Step 7 Enter the reporting period for the report. You can define the report to collect data on either an hourly or weekly basis or at a specific date and time. The selected reporting period type will display on the x-axis. Select the **Schedule** tab when complete.

> **Note** The reporting period uses a 24-hour rather than a 12-hour clock. For example, select hour 13 for 1:00 PM.

Step 8 At the Schedule window, check the **Enable Schedule** check box.

Step 9 Select the report format (CSV or PDF) from the Export Report drop-down menu.

Figure 7-4 MSE Utilization > New > Schedule Tab



MSE Utilization > New

Enable Schedule □

Export Format CSV

Destination

● Save To File /opt/ftp_server_files/reports/MSEUtilization/<ReportTitleName>_<yyyymmdd>_<HHMMSS>.csv

○ Email To

Start Date 08/05/2008

Current server time: Tue Aug 05 10:20:34 PDT 2008

Start Time 06 Hour 00 Min.

Recurrence ○ No Recurrence ○ Hourly ○ Daily ● Weekly

Every 1 Week(s)

□ Sunday ☑ Monday □ Tuesday □ Wednesday
□ Thursday □ Friday □ Saturday

Step 10 Select either the **Save To File** or the **Email To** option as the destination of the report.

- If you select the Save To File option, a destination path must first be defined at the **Administration > Settings** > *Report* window. Enter the destination path for the files in the Repository Path field.
- If you select the Email To option, an SMTP Mail Server must be defined prior to entry of target email address. Choose **Administrator > Settings >** *Mail Server* to enter the appropriate information.

Step 11 Enter a start date (MM:DD:YYYY) or click the calendar icon to select a date.

Step 12 Specify a start time using the hour and minute drop-down menus.

Step 13 Click one of the Recurrence buttons to select how often the report is run.

> **Note** The days of the week appear only on the screen when the weekly option is chosen.

Step 14 When complete with all of the above steps, do one of the following:

- Click **Save** to save edits. The report is run at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule tab.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any scheduled time associated with the report and is viewable in the **Results** tab. Additionally, the report is run at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule tab.
  - At the results window, you can cancel or delete the report.
- Click **Run Now** if you want to run the report immediately and review the results in the WCS window The report runs regardless of any scheduled time associated with the report and is viewable in the **Results** tab. If the report is too large to display in the WCS window, you are referred to the history tab to download the file for viewing. Click **Save** if you want to save the report scenario you entered.

Note You can also use the **Run Now** command to check a report scenario before saving it or to run reports as necessary.

Viewing a Defined System Utilization Report

To view results of a defined report, follow these steps:

Step 1 In Cisco WCS, click **Reports > Performance Reports**.

Step 2 Select **MSE Utilization** from the listing under the Performance Reports heading.

The MSE Utilization summary window appears. Any pre-defined reports, previously created and saved, are listed.

Note You can select one of the listed reports or you can define a new report. For details on creating a new report, see the "Creating a System Utilization Report" section on page 7-7.

Step 3 Click the listed report's link to review its settings. The two-tabbed window appears.

Step 4 Review or modify the report parameters on the General tab window. When finished, select the **Schedule** tab.

Step 5 Check the **Enable Schedule** check box to enable the report, if not already checked.

Step 6 Review and edit other parameters, as necessary. When you are finished with your review or edit, do one of the following:

- Click **Save** to save edits. The report is run at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule tab.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any scheduled time associated with the report and is viewable in the **Results** tab. Additionally, the report is run at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule tab.
  - At the results window, you can cancel or delete the report.

- Click **Run Now** if you want to run the report immediately and review the results in the WCS window. The report runs regardless of any scheduled time associated with the report. If the report is too large to display in the WCS window, you are referred to the history tab to download the file for viewing. Click **Save** if you want to save the report scenario you entered. You can also delete or cancel the report.

Note You can also use the **Run Now** command to check a report scenario before saving it or to run reports as necessary.

Security Reports

In the left sidebar menu (**Reports > Security**), all of the security report options are listed. The security reports display information about the security of the wireless network.

Note Security reports do not show the status of autonomous access points.

The choices are as follows:

- New Rogue APs—Displays, in tabular form, all rogues detected in a selected timeframe. It provides which new rogues were detected within a selected time. The created time indicates the time at which the rogue was first detected.
- New Rogue AP Count—Displays, in graphical form, all rogues detected in a selected timeframe.
- Rogue APs—Displays all rogues that are active in your network and have been updated in the selected timeframe. WCS receives updated events for rogues that are detected
- Rogue APs Event—Displays all the events received by WCS. The controller sends updates of detected rogues if any of the attributes change or new rogues are detected.

Note This report was formally called the Rogue Detected by AP.

- Rogue Adhocs—Displays all adhocs that have been updated in the selected timeframe.
- Rogue Adhocs Event—Displays all adhoc events that WCS has received in the selected timeframe.
- Security Summary Report— Shows the number of association failures, rogues access points, ad hocs, and access point connections or disconnections over one month.

Viewing or Modifying Security Reports

Follow these steps to view or modify existing security reports.

Step 1 Click **Reports > Security Reports**. The Security Reports page appears.

Step 2 Select the Security Report type from the left panel.

Step 3 Define (or modify) the conditions for the report in the General panel. Select the **Schedule** tab when complete.

Step 4 Check the **Enable Schedule** check box to enable the report, if not already checked.

Step 5 Review and edit other parameters, as necessary. When you are finished with your review or edit, do one of the following:

- Click **Save** to save edits. The report is run at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule tab.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any scheduled time associated with the report and is viewable in the **Results** tab. Additionally, the report is run at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule tab.
  - At the results window, you can cancel or delete the report.
- Click **Run Now** if you want to run the report immediately and review the results in the WCS window. The report runs regardless of any scheduled time associated with the report. If the report is too large to display in the WCS window, you are referred to the history tab to download the file for viewing. Click **Save** if you want to save the report scenario you entered. You can also delete or cancel the report.

Note You can also use the **Run Now** command to check a report scenario before saving it or to run reports as necessary.

Step 6 Click the History tab if you want to review details of the current and past runs of the report.

Creating a New Security Report

To create a new security report, follow these steps:

Note Some of these steps or options are not required for every report.

Step 1 Click **Reports > Security Reports**. The Security Reports page appears.

Step 2 Click on one of the report types summarized under Security Reports (left-side).

Step 3 Select **New** from the Select a command drop-down menu and click **GO**. The two-tabbed entry panel appears.

Step 4 Specify a report title.

Step 5 Specify if you want the report listed by controller, floor area, outdoor area, AP by floor, AP by outdoor area, or SSID. The floor area and outdoor area report generates the report on an area basis while the AP by floor or AP by outdoor area generates the report on a per-access point basis.

Step 6 If you chose controller, you need to enter a controller IP address.
If you chose floor area or AP by floor area, you need to enter the campus, building, and floor location.
If you chose outdoor area or AP by outdoor area, you need to enter the campus and outdoor area.

Step 7 If necessary, enter which access points or location server to include in the report.

Step 8 Enter the reporting period for the report. You can define the report to collect data for an hourly or weekly period or choose a specific date and time range for reporting.

Step 9 Click the Schedule tab to complete the scheduling process.

Step 10 Check the **Enable Schedule** check box to enable the report.

Step 11 Review and edit other parameters, as necessary. When you are finished with your review or edit, do one of the following:

- Click **Save** to save edits. The report is run at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule tab.
- Click **Save and Run** to save the changes and run the report now. The report runs regardless of any scheduled time associated with the report and is viewable in the **Results** tab. Additionally, the report is run at the designated time and the results are either emailed or saved to a designated file as defined in the Schedule tab.
  - At the results window, you can cancel or delete the report.
- Click **Run Now** if you want to run the report immediately and review the results in the WCS window. The report runs regardless of any scheduled time associated with the report. If the report is too large to display in the WCS window, you are referred to the history tab to download the file for viewing. Click **Save** if you want to save the report scenario you entered. You can also delete or cancel the report.

Note You can also use the **Run Now** command to check a report scenario before saving it or to run reports as necessary.

Step 12 Click the History tab if you want to review details of the current and past runs of the report.

CHAPTER 8

Performing Maintenance Operations

This chapter describes how to back up and restore mobility services engine data and how to update the mobility services engine software. It also describes other maintenance operations.

This chapter contains the following sections:

Recovering a Lost Password

To recover a lost or forgotten password for a mobility services engine, follow these steps:

Step 1 When the GRUB screen comes up, press **Esc** to enter the boot menu.

Step 2 Press **e** to edit.

Step 3 Navigate to the line beginning with *kernel* and press **e.**

At the end of the line put a space, followed by the number one (**1**). Press **Enter** to save this change.

Step 4 Press **b** to begin boot.

The boot sequence will commence and at the end the user will be given a shell prompt.

Step 5 The user may change the root password by invoking the **passwd** command.

Step 6 Enter and confirm the new password.

Step 7 Reboot the machine.

Recovering a Lost Root Password

To recover a lost or forgotten root password for a mobility services engine, follow these steps:

Step 1 When the GRUB screen comes up, press **Esc** to enter the boot menu.

Step 2 Press **e** to edit.

Step 3 Navigate to the line beginning with *kernel* and press **e.**

At the end of the line enter a space and the number one (**1**). Press **Enter** to save this change.

Step 4 Press **b** to begin boot sequence.

At the end of the boot sequence, a shell prompt appears.

Note The shell prompt does not appear if you have setup a single user mode password.

Step 5 You can change the root password by entering the **passwd** command.

Step 6 Enter and confirm the new password.

Step 7 Restart the machine.

Backing Up and Restoring Mobility Services Engine Data

This information describes how to back up and restore mobility services engine data. It also describes how to enable automatic backup.

Backing Up Mobility Services Engine Historical Data

Cisco WCS includes functionality for backing up mobility services engine data.

To back up mobility services engine data, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services.**

Step 2 Click the name of the mobility services engine that you want to back up.

Step 3 Click **Maintenance** (left).

Step 4 Click **Backup**.

Step 5 Enter the name of the backup.

Step 6 Enter the time in seconds after which the backup times out.

Step 7 Click **Submit** to back up the historical data to the hard drive of the server running Cisco WCS.

Status of the backup can be seen on the screen while the backup is in process. Three items will display on the screen during the backup process: (1) Last Status field provides messages noting the status of the backup; (2) Progress field shows what percentage of the backup is complete; and (3) Started at field shows when the backup began noting date and time.

Note You can run the backup process in the background while working on other mobility services engine operations in other Cisco WCS windows.

Note Backups are stored in the FTP directory you specify during the Cisco WCS installation.

Restoring Mobility Services Engine Historical Data

You can use Cisco WCS to restore backed-up historical data.

To restore mobility services engine data, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to restore.

Step 3 Click **Maintenance** (left panel).

Step 4 Click **Restore**.

Step 5 Choose the file to restore from the drop-down menu.

Step 6 Enter the time in seconds after which restoration times out.

Step 7 Click **Submit** to start the restoration process.

Step 8 Click **OK** to confirm that you want to restore the data from the Cisco WCS server hard drive.

When restoration is completed, Cisco WCS displays a message to that effect.

Note You can run the restore process in the background while working on other mobility service engine operations in other Cisco WCS windows.

Enabling Automatic Location Data Backup

You can configure Cisco WCS to perform automatic backups of location data on a regular basis.

To enable automatic backup of location data on a mobility services engine, follow these steps:

Step 1 In Cisco WCS, click **Administration > Background Tasks**.

Step 2 Check the **Mobility Service Backup** check box.

Step 3 Select **Enable Task** from the Select a command drop-down menu. Click **GO**.

The backups are stored in the FTP directory that you specify during the Cisco WCS installation.

Downloading Software to Mobility Services Engines

To download software to a mobility services engine, follow these steps:

Step 1 Verify that you can ping the mobility services engine from the Cisco WCS server or an external FTP server, whichever you are going to use for the application code download.

Step 2 In Cisco WCS, click **Mobility > Mobility Services.**

Step 3 Click the name of the mobility services engine to which you want to download software.

Step 4 Click **Maintenance** (left panel).

Step 5 Click **Download Software**.

Step 6 To download software, do one of the following:

- To download software listed in the Cisco WCS directory, select **Select from uploaded images to transfer into the Server**. Then, choose a binary image from the drop-down menu.

  Cisco WCS downloads the binary images listed in the drop-down menu into the FTP server directory you have specified during the Cisco WCS installation.

- To use downloaded software available locally or over the network, select the **Browse a new software image to transfer into the Server** and click **Browse**. Locate the file and click **Open**.

Step 7 Enter the time in seconds (between 1 and1800) after which software download times out.

Step 8 Click **Download** to send the software to the /opt/installers directory on the mobility services engine.

Step 9 After the image is transferred to the mobility services engine, log in to the mobility services engine CLI.

Step 10 Run the installer image from the */opt/installers* directory by entering the following command **./.bin** *mse image*. This installs the software.

Step 11 To run the software enter **/etc/init.d/msed start**.

Note To stop the software, enter **/etc/init.d/msed stop**, and to check status enter **/etc/init.d/msed status**.

Manually Downloading Software

If you do not want to automatically update the mobility services engine software using Cisco WCS, follow these steps to upgrade the software manually using a local (console) or remote (SSH) connection.

Step 1 Transfer the new mobility services engine image onto the hard drive.

a. Log in as root, and use the binary setting to send the image from an external FTP server root directory. The release note format is similar to the following and changes with each release: *CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz*.

Note The mobility services engine image is compressed at this point.

Note The default login name for the FTP server is *ftp-user*.

Your entries should look like this example:

```
# cd /opt/installers
# ftp <FTP Server IP address>
Name: <login>
Password: <password>
binary
get CISCO-MSE-L-K9-x-x-x-x-0-64bit.bin.gz
<CTRL-Z>
#
```

b. Verify that the image (*CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz*) is in the mobility services engine /opt/installers directory.

c. To decompress (unzip) the image file enter the following command:

gunzip *CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz*

The decompression yields a *bin* file.

d. Make sure that the *CISCO-MSE-L-K9-x-x-x-x.bin* file has execute permissions for the root user. If not, enter **chmod 755** *CISCO-MSE-L-K9-x-x-x-x.bin*.

Step 2 Manually stop the mobility services engine.

a. Log in as root and enter **/etc/init.d/msed stop**.

Step 3 Enter **/opt/installers/***CISCO-MSE-L-K9-x-x-x-x.bin* to install the new mobility services engine image.

Step 4 Start the new mobility services engine software by entering the following command:

/etc/init.d/msed start

Caution Only complete the next step that uninstalls the script files, if the system instructs you to do so. Removing the files unnecessarily erases your historical data.

Step 5 Enter **/opt/mse/uninstall** to uninstall the mobility services engine's script files.

Configuring NTP Server

You can configure NTP servers to set up the time and date of the mobility services engine.

Note

- You are automatically prompted to enable NTP and enter NTP server IP addresses as part of the automatic installation script for the mobility services engine. For more details on the automatic installation script, refer to the *Cisco 3310 Mobility Services Engine Getting Started Guide* at the following link: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html
- If you need to add or change an NTP server installation after a mobility services engine install, rerun the automatic installation script. You can configure the NTP server without adjusting the other values by just tabbing through the script.

Note For more information on NTP server configuration, consult the Linux configuration guides.

Defragmenting the Mobility Services Engine Database

Over time, the mobility services engine's database might get fragmented, which might lead to a decrease in the system's performance. To fix this problem, use Cisco WCS to defragment the database.

To defragment the mobility services engine database, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to defragment its database.

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands section, click **Defragment Database**.

Step 6 Click **OK** to confirm that you want to defragment the mobility services engine's database.

Rebooting the Mobility Services Engine Hardware

If you need to restart a mobility services engine, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services.**

Step 2 Click the name of the mobility services engine that you want to reboot.

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands section (right), click **Reboot Hardware**.

Step 6 Click **OK** to confirm that you want to reboot the mobility services engine hardware.

The rebooting process takes a few minutes to complete.

Shutting Down the Mobility Services Engine Hardware

If you need to shutdown a mobility services engine, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine that you want to shutdown.

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands section (right), click **Shutdown Hardware**.

Step 6 Click **OK** to confirm that you want to shutdown the mobility services engine.

Clearing Mobility Services Engine Configurations

To clear a mobility services engine configuration and restore its factory defaults, follow these steps:

Step 1 In Cisco WCS, click **Mobility > Mobility Services**.

Step 2 Click the name of the mobility services engine you want to configure.

Step 3 Click **System** (left panel).

Step 4 Click **Advanced Parameters**.

Step 5 In the Advanced Commands section (right), click **Clear Configuration**.

Note Using this command also clears the system's database.

Step 6 Click **OK** to clear the mobility services engine configurations.

APPENDIX A

wIPS Policy Alarm Encyclopedia

This appendix provides an overview of the types on threats that wIPS addresses.

- "Security IDS/IPS Overview" section on page A-B
- "Intrusion Detection—Denial-of-Service Attack" section on page A-C

Security IDS/IPS Overview

The addition of WLANs to the corporate environment introduces a new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured and unconfigured access points and DoS (denial-of-service) attacks.

The Cisco Adaptive Wireless IPS is designed to help manage against security threats by validating proper security configurations and detecting possible intrusions. With the comprehensive suite of security monitoring technologies, the Cisco Adaptive Wireless IPS alerts the user on more than 100 different threat conditions in the following categories:

- User authentication and traffic encryption
- Rogue and ad-hoc mode devices.
- Configuration vulnerabilities
- Intrusion detection on security penetration
- Intrusion detection on DoS attacks

To maximize the power of the Cisco Adaptive Wireless IPS, security alarms can be customized to best match your security deployment policy. For example, if your WLAN deployment includes access points made by a specific vendor, the product can be customized to generate the rogue access point alarm when an access point made by another vendor is detected by the access point or sensor.

Pre-configured profiles for various WLAN environments

During installation, the user can select an appropriate profile based on the WLAN network implemented.

The Cisco Adaptive Wireless IPS provides separate profiles for:

- Enterprise best practice
- Enterprise rogue detection only
- Financial (Gramm-Leach-Bliley Act compliant)
- HealthCare (Health Insurance Portability and Accountability Act compliant)
- Hotspot implementing 802.1x security
- Hotspot implementing NO security
- Tradeshow environment
- Warehouse/manufacturing environment
- Government/Military (8100.2 directive compliant)
- Retail environment

When the administrator selects the appropriate profile, the Cisco Adaptive Wireless IPS will enable or disable alarms from the policy profile that are appropriate for that WLAN environment. For example, health care institutions can select the Healthcare profile and all alarms that are necessary to be HIPAA compliant will be enabled. The administrator still has the option after installation to enable or disable any alarm or change the threshold values as per individual preferences.

The Cisco Adaptive Wireless IPS system not only is an IDS (Intrusion Detection System), but also is an IPS (Intrusion Prevention System).

Cisco Adaptive Wireless IPS policies are included in two security subcategories: wIPS—Denial of Service (DoS) Attacks and wIPS—Security Penetration.

- Intrusion Detection—Denial-of-Service Attack
- Intrusion Detection—Security Penetration

Intrusion Detection—Denial-of-Service Attack

Wireless DoS (denial-of-service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLAN at layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example RF jamming attack with high power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

The nature and protocol standards for wireless are subject to some of these attacks. Cisco has developed Management Frame Protection, the basis of 802.11i, to proactively prevent many of these attacks. (For more information on MFP, refer to the Cisco WCS online help.) The Cisco Adaptive Wireless IPS contributes to this solution by an early detection system where the attack signatures are matched. The Cisco Adaptive Wireless IPS's DoS detection focuses on WLAN layer one (physical layer) and two (data link layer, 802.11, 802.1x). When strong WLAN authentication and encryption mechanisms are used, higher layer (IP layer and above) DoS attacks are difficult to execute. The wIPS server tightens your WLAN defense by validating strong authentication and encryption policies. In addition, the Cisco Adaptive Wireless IPS's Intrusion Detection on Denial-of-Service attacks and security penetration provides 24 X 7 air tight monitoring on potential wireless attacks.

Denial-of-Service Attacks include the following three subcategories:

- Denial-of-Service Attack Against Access Points
- Denial-of-Service Attack Against Infrastructure
- DoS Attacks Against Client Station

Denial-of-Service Attack Against Access Points

DoS attacks against access points are typically carried out on the basis of the following assumptions:

- Access points have limited resources. For example, the per-client association state table.
- WLAN management frames and authentication protocols 802.11 and 802.1x have no encryption mechanisms.

Wireless intruders can exhaust access point resources, most importantly the client association table, by emulating large number of wireless clients with spoofed MAC addresses. Each one of these emulated clients attempts association and authentication with the target access point but leaves the protocol transaction mid-way. When the access point's resources and the client association table is filled up with these emulated clients and their incomplete authentication states, legitimate clients can no longer be serviced by the attacked access point. This creates a denial of service attack.

The Cisco Adaptive Wireless IPS tracks the client authentication process and identifies DoS attack signatures against the access point. Incomplete authentication and association transactions trigger the attack detection and statistical signature matching process. Detected DoS attack results in setting off wIPS alarms which includes the usual alarm detail description and target device information.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing. For more information on MFP, refer to the Cisco WCS online help.

DoS attacks against access points include:

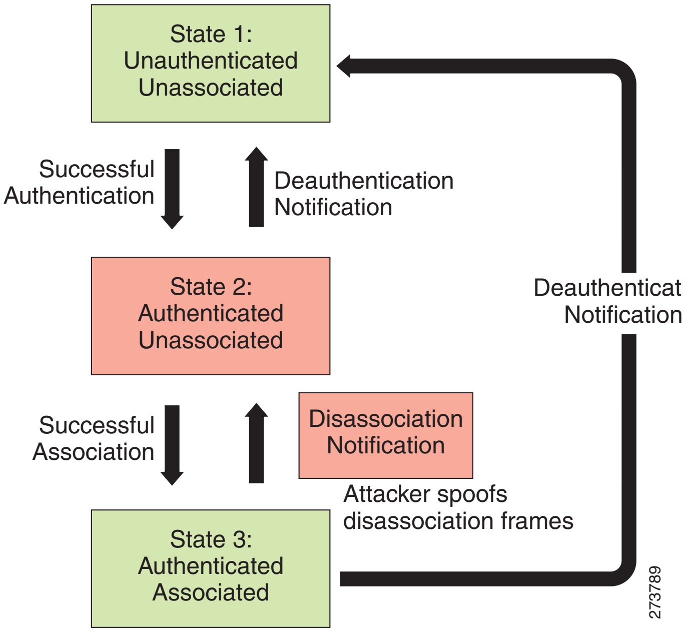
- Denial-of-Service Attack: Association Flood
- Denial-of-Service Attack: Association Table Overflow
- Denial-of-Service Attack: Authentication Flood
- Denial-of-Service Attack: EAPOL-Start Attack
- Denial-of-Service Attack: PS Poll Flood Attack
- Denial-of-Service Attack: Unauthenticated Association

Denial-of-Service Attack: Association Flood

Alarm Description and Possible Causes

This DoS attack exhausts the access point's resources, particularly the client association table, by flooding the access point with a large number of spoofed client associations. At the 802.11 layer, shared-key authentication is flawed and rarely used. The other alternative is open authentication (null authentication) that relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker using such a vulnerability can emulate a large number of clients to flood a target access point's client association table by creating many clients. When the client association table overflows, legitimate clients cannot get associated; therefore, a DoS attack is committed.

Figure A-1 Association Flood



wIPS Solution

The Cisco Adaptive Wireless IPS detects spoofed MAC addresses and tracks the 802.1x actions and data communication after a successful client association to detect this form of DoS attack. After this attack is reported by the Cisco Adaptive Wireless IPS, you may log onto this access point to inspect its association table for the number of client associations.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide* or the Cisco WCS online help.

Denial-of-Service Attack: Association Table Overflow

Alarm Description and Possible Causes

Wireless intruders can exhaust access point resources, most importantly the client association table, by imitating a large number of wireless clients with spoofed MAC addresses. Each one of these imitated clients attempts association and authentication with the target access point. The 802.11 authentication typically completes because most deployments use 802.11 open system authentication, which is a null authentication process. Association with these imitated clients follows the authentication process. These imitated clients do not, however, follow up with higher level authentication such as 802.1x or VPN, which leaves the protocol transaction half-finished. At this point, the attacked access point maintains a state in the client association table for each imitated client. When the access point's resources and client association table is filled with these imitated clients and their state information, legitimate clients can no longer be serviced by the attacked access point. This creates a DoS (denial of service) attack.

wIPS Solution

The Cisco Adaptive Wireless IPS tracks the client authentication process and identifies a DoS attack signature against an access point. Incomplete authentication and association transactions trigger the Cisco Adaptive Wireless IPS's attack detection and statistical signature matching process.

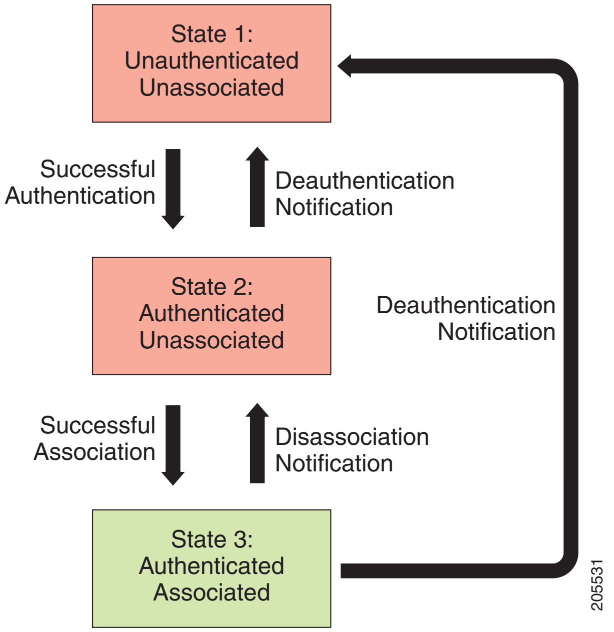
Denial-of-Service Attack: Authentication Flood

Attack tool: Void11

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement such a state machine according to the IEEE standard (see Figure A-2). On the access point, each client has a state recorded in the access point's client table (association table). This recorded state has a size limit that can either be a hard-coded number or a number based on the physical memory constraint.

Figure A-2 Authentication Flood



A form of DoS attack floods the access point's client state table (association table) by imitating many client stations (MAC address spoofing) sending authentication requests to the access point. Upon receipt of each individual authentication request, the target access point creates a client entry in State 1 of the association table. If open system authentication is used for the access point, the access point returns an *authentication success* frame and moves the client to State 2. If shared-key authentication is used for the access point, the access point sends an *authentication challenge* to the attacker's imitated client, which does not respond. In this case, the access point keeps the client in State 1. In either case, the access point contains multiple clients hanging in either State 1 or State 2 which fills up the access point association table. When the table reaches its limit, legitimate clients cannot authenticate and associate with this access point. This results in a DoS attack.

wIPS Solution

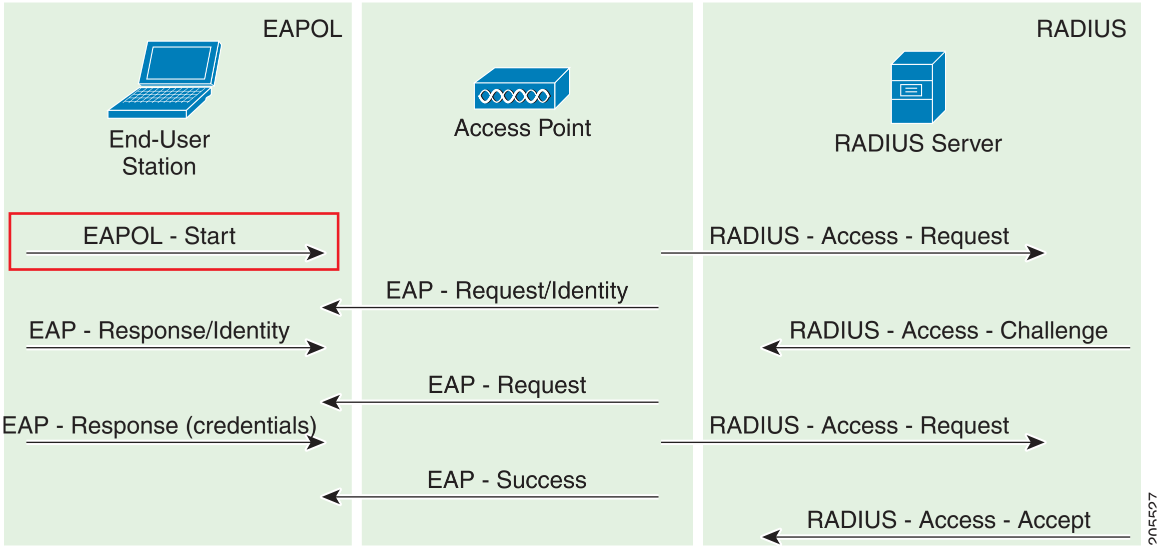
The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security analyst can log onto the access point to check the current association table status.

Denial-of-Service Attack: EAPOL-Start Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP over LANs (EAPOL). The 802.1x protocol starts with an EAPOL-Start frame sent by the client station to begin the authentication transaction. The access point responds to an EAPOL-start frame with a EAP-identity-request and some internal resource allocation.

Figure A-3 EAPOL-Start Protocol and EAPOL-Start Attack



An attacker attempts to disrupt an access point by flooding it with EAPOL-start frames to exhaust the access point internal resources.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking the 802.1x authentication state transition and particular attack signature.

Denial-of-Service Attack: PS Poll Flood Attack

Alarm Description and Possible Causes

Power management is probably one of the most critical features of wireless LAN devices. Power management helps to conserve power by enabling stations to remain in power saving state mode for longer periods of time and to receive data from the access point only at specified intervals.

The wireless client device must inform the access point of the length of time that it will be in the sleep mode (power save mode). At the end of the time period, the client wakes up and checks for waiting data frames. After it completes a handshake with the access point, it receives the data frames. The beacons from the access point also include the Delivery Traffic Indication Map (DTIM) to inform the client when it needs to wake up to accept multicast traffic.

The access point continues to buffer data frames for the sleeping wireless clients. Using the Traffic Indication Map (TIM), the access point notifies the wireless client that it has buffered data buffered. Multicast frames are sent after the beacon that announces the DTIM.

The client requests the delivery of the buffered frames using PS-Poll frames to the access point. For every PS-Poll frame, the access point responds with a data frame. If there are more frames buffered for the wireless client, the access point sets the data bit in the frame response. The client then sends another PS-Poll frame to get the next data frame. This process continues until all the buffered data frames are received.

A potential hacker could spoof the MAC address of the wireless client and send out a flood of PS-Poll frames. The access point then sends out the buffered data frames to the wireless client. In reality, the client could be in the power safe mode and would miss the data frames.

wIPS Solution

The Cisco Adaptive Wireless IPS can detect this DoS attack that can cause the wireless client to lose legitimate data. Locate and remove the device from the wireless environment.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide* or the Cisco WCS online help.

Denial-of-Service Attack: Unauthenticated Association

Alarm Description and Possible Causes

A form of DoS attack is to exhaust the access point's resources, particularly the client association table, by flooding the access point with a large number of spoofed client associations. At the 802.11 layer, shared-key authentication is flawed and rarely used. The other alternative is open authentication (null authentication) which relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker using such a vulnerability can imitate a large number of clients to flood a target access point's client association table by creating many clients. When the client association table overflows, legitimate clients cannot get associated causing a DoS attack.

wIPS Solution

The Cisco Adaptive Wireless IPS detects spoofed MAC addresses and tracks 802.1x actions and data communication after a successful client association to detect this form of DoS attack. After this attack is reported by the Cisco Adaptive Wireless IPS, you may log onto this access point to inspect its association table for the number of client associations.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide* or the Cisco WCS online help.

Denial-of-Service Attack Against Infrastructure

In addition to attacking access points or client stations, the wireless intruder may target the RF spectrum or the back-end authentication RADIUS server for DoS (denial-of-service) attacks. The RF spectrum can be easily disrupted by injecting RF noise generated by a high power antenna from a distance. Back-end RADIUS servers can be overloaded by a DDoS (distributed denial-of-service) attack where multiple wireless attackers flood the RADIUS server with authentication requests. This attack does not require a successful authentication to perform the attack.

DoS attacks against infrastructure include:

- Denial-of-Service Attack: CTS Flood
- Denial-of-Service Attack: Queensland University of Technology Exploit

- Denial-of-Service attack: RF Jamming Attack
- Denial of Service: RTS Flood
- Denial-of-Service Attack: Virtual Carrier Attack

Denial-of-Service Attack: CTS Flood

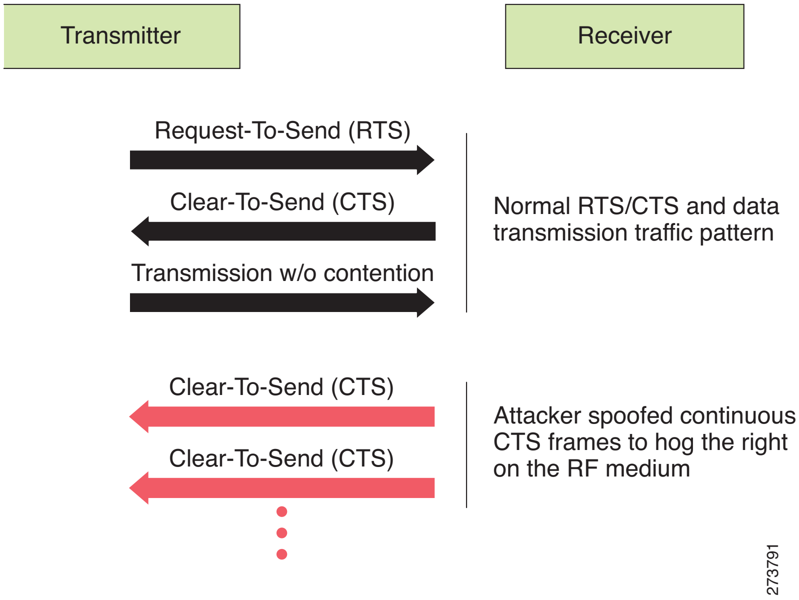
Attack tool: CTS Jack

Alarm Description and Possible Causes

As an optional feature, the IEEE 802.11 standard includes the RTS/CTS (request-to-send/clear-to-send) functionality to control the station access to the RF medium. The wireless device ready for transmission sends a RTS frame in order to acquire the right to the RF medium for a specified time duration. The receiver grants the right to the RF medium to the transmitter by sending a CTS frame of the same time duration. All wireless devices observing the CTS frame should yield the media to the transmitter for transmission without contention.

A wireless DoS attacker might take advantage of the privilege granted to the CTS frame to reserve the RF medium for transmission. By transmitting back-to-back CTS frames, an attacker can force other wireless devices sharing the RF medium to hold back their transmission until the attacker stops transmitting the CTS frames.

Figure A-4 CTS Spoof and Challenge to RF Control


Transmitter
Receiver
Request-To-Send (RTS)
Clear-To-Send (CTS)
Transmission w/o contention
Normal RTS/CTS and data transmission traffic pattern
Clear-To-Send (CTS)
Clear-To-Send (CTS)
Attacker spoofed continuous CTS frames to hog the right on the RF medium
273791

wIPS Solution

The Cisco Adaptive Wireless IPS detects the abuse of CTS frames for a DoS attack.

Denial-of-Service Attack: Queensland University of Technology Exploit

Denial of Service Vulnerability in IEEE 802.11 Wireless Devices: US-CERT VU#106678 & Aus-CERT AA-2004.02

Alarm Description and Possible Causes

802.11 WLAN devices use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the basic access mechanism in which the WLAN device listens to the medium before starting any transmission and backs-off when it detects any existing transmission taking place. Collision avoidance combines the physical sensing mechanism and the virtual sense mechanism that includes the Network Allocation Vector (NAV), the time before which the medium is available for transmission. Clear Channel Assessment (CCA) in the DSSS protocol determines whether a WLAN channel is clear so an 802.11b device can transmit on it.

Mark Looi, Christian Wullems, Kevin Tham and Jason Smith from the Information Security Research Centre, Queensland University of Technology, Brisbane, Australia, have recently discovered a flaw in the 802.11b protocol standard that could potentially make it vulnerable to DoS radio frequency jamming attacks.

This attack specifically attacks the CCA functionality. According to the AusCERT bulletin, "an attack against this vulnerability exploits the CCA function at the physical layer and causes all WLAN nodes within range, both clients and access points, to defer transmission of data for the duration of the attack. When under attack, the device behaves as if the channel is always busy, preventing the transmission of any data over the wireless network."

This DoS attack affects DSSS WLAN devices including IEEE 802.11, 802.11b, and low-speed (below 20Mbps) 802.11g wireless devices. IEEE 802.11a (using OFDM), high-speed (above 20Mbps using OFDM) 802.11g wireless devices are not affected by this attack. Devices that use FHSS are also not affected.

Any attacker using a PDA or a laptop equipped with a WLAN card can launch this attack on SOHO and enterprise WLANs. Switching to the 802.11a protocol is the only solution or known protection against this DoS attack.

For more information on this DoS attack refer to:

- www.isrc.qut.edu.au
- www.isrc.qut.edu.au/wireless
- http://www.auscert.org.au/render.html?it=4091
- http://www.kb.cert.org/vuls/id/106678

wIPS Solution

The Cisco Adaptive Wireless IPS detects this DoS attack and sets off the alarm. Locate and remove the responsible device from the wireless environment.

Denial-of-Service attack: RF Jamming Attack

Alarm Description and Possible Causes

WLAN reliability and efficiency depend on the quality of the radio frequency (RF) media. Each RF is susceptible to RF noise impact. An attacker using this WLAN vulnerability can perform two types of DoS attacks:

- **Disrupt WLAN service—**At the 2.4 GHz unlicensed spectrum, the attack may be unintentional. A cordless phone, Bluetooth devices, microwave, wireless surveillance video camera, or baby monitor can all emit RF energy to disrupt WLAN service. Malicious attacks can manipulate the RF power at 2.4 GHz or 5 GHz spectrum with a high-gain directional antenna to amplify the attack impact from a distance. With free-space and indoor attenuation, a 1-kW jammer 300 feet away from a building can jam 50 to 100 feet into the office area. The same 1-kW jammer located inside a building can jam 180 feet into the office area. During the attack, WLAN devices in the target area are out of wireless service.
- **Physically damage AP hardware—**An attacker using a high-output transmitter with directional high gain antenna 30 yards away from an access point can pulse enough RF power to damage electronics in the access point putting it being permanently out of service. Such High Energy RF (HERF) guns are effective and are inexpensive to build.

wIPS Solution

The Cisco Adaptive Wireless IPS detects continuous RF noise over a certain threshold for a potential RF jamming attack.

Cisco Spectrum Intelligence also provides specific detection of non-802.11 jamming devices. For more information on Cisco Spectrum Intelligence, refer to the *Cisco Wireless Control System Configuration Guide* or the Cisco WCS online help.

Denial of Service: RTS Flood

Alarm Description and Possible Causes

As an optional feature, the IEEE 802.11 standard includes the RTS/CTS (Request-To-Send/Clear-To-Send) functionality to control access to the RF medium by stations. The wireless device ready for transmission sends an RTS frame in order to acquire the right to the RF medium for a specified duration. The receiver grants the right to the RF medium to the transmitter by sending a CTS frame of the same duration. All wireless devices observing the CTS frame should yield the RF medium to the transmitter for transmission without contention.

A wireless denial-of-service attacker may take advantage of the privilege granted to the CTS frame to reserve the RF medium for transmission. By transmitting back-to-back RTS frames with a large transmission duration field, an attacker reserves the wireless medium and force other wireless devices sharing the RF medium to hold back their transmissions.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the abuse of RTS frames for denial-of-service attacks.

Denial-of-Service Attack: Virtual Carrier Attack

Alarm Description and Possible Causes

The virtual carrier-sense attack is implemented by modifying the 802.11 MAC layer implementation to allow random duration values to be sent periodically. This attack can be carried out on the ACK, data, RTS, and CTS frame types by using large duration values. By doing this the attacker can prevent channel access to legitimate users.

Under normal circumstances, the only time a ACK frame carries a large duration value is when the ACK is part of a fragmented packet sequence. A data frame legitimately carries a large duration value only when it is a sub-frame in a fragmented packet exchange.

One approach to deal with this attack is to place a limit on the duration values accepted by nodes. Any packet containing a larger duration value is truncated to the maximum allowed value. Low cap and high cap values can be used. The low cap has a value equal to the amount of time required to send an ACK frame, plus media access backoffs for that frame. The low cap is used when the only packet that can follow the observed packet is an ACK or CTS. This includes RTS and all management (such as association) frames. The high cap is used when it is valid for a data packet to follow the observed frame. The limit in this case needs to include the time required to send the largest data frame, plus the media access backoffs for that frame. The high cap must be used in two places: when observing an ACK (because the ACK my be part of a MAC level fragmented packet) and when observing a CTS.

A station that receives an RTS frame also receives the data frame. The IEEE 802.11 standard specifies the exact times for the subsequent CTS and data frames. The duration value of RTS is respected until the following data frame is received or not received. Either the observed CTS is unsolicited or the observing node is a hidden terminal. If this CTS is addressed to a valid in-range station, the valid station can nullify this by sending a zero duration null function frame. If this CTS is addressed to an out-of-range station, one method of defense is to introduce authenticated CTS frames containing cryptographically signed copies of the preceding RTS. With this method, there is a possibility of overhead and feasibility issues.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this DoS attack. Locate the device and take appropriate steps to remove it from the wireless environment.

DoS Attacks Against Client Station

DoS attacks against wireless client station are typically carried out based upon the fact that 802.11 management frames and 802.1x authentication protocols have no encryption mechanism and thus can be spoofed. For example, wireless intruders can disrupt the service to a client station by continuously spoofing a 802.11 disassociation or deauthentication frame from the access point to the client station.

Besides the 802.11 authentication and association state attack, there are similar attack scenarios for 802.1x authentication. For example, 802.1x EAP-Failure or EAP-logoff messages are not encrypted and can be spoofed to disrupt the 802.1x authenticated state to disrupt wireless service.

Cisco Adaptive Wireless IPS tracks the client authentication process and identifies DoS attack signatures. Incomplete authentication and association transactions trigger the attack detection and statistical signature matching process. Detected DoS attack results in setting off wIPS alarms that include the usual alarm detail description and target device information.

DoS attacks against client station include:

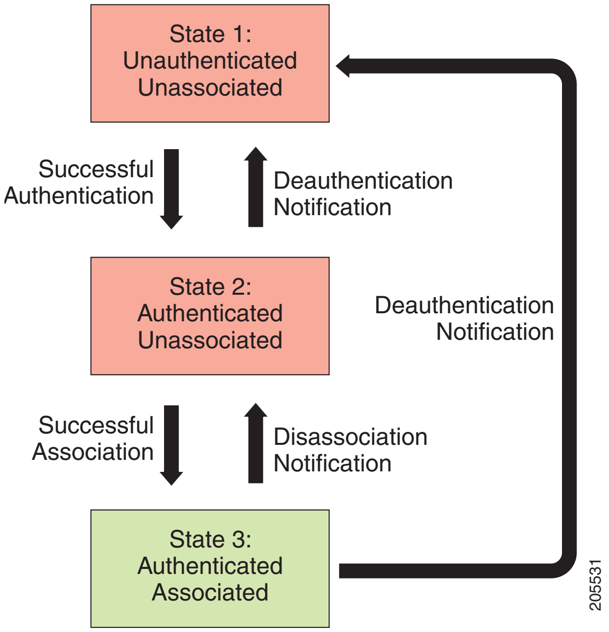
- "Denial-of-Service Attack: Authentication Failure Attack" section on page A-M
- "Denial-of-Service Attack: Deauthentication Broadcast" section on page A-N
- "Denial-of-Service Attack: Disassociation Flood" section on page A-Q
- "Denial-of-Service Attack: EAPOL Logoff Attack" section on page A-R
- "Denial-of-Service Attack: FATA Jack Tool Detected" section on page A-S
- "Denial-of-Service Attack: Premature EAP Failure Attack" section on page A-U
- "Denial-of-Service Attack: Premature EAP Success Attack" section on page A-V

Denial-of-Service Attack: Authentication Failure Attack

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this client state machine based on the IEEE standard (see illustration below). A successfully associated client remains in State 3 in order to continue wireless communication. A client in State 1 and in State 2 cannot participate in the WLAN data communication process until it is authenticated and associated to State 3. IEEE 802.11 defines two authentication services: open system authentication and shared key authentication. Wireless clients go through one of these authentication processes to associate with an access point. (see Figure A-5).

Figure A-5 Authentication Failure Attack



A denial-of-service (DoS) attack spoofs invalid authentication request frames (with bad authentication service and status codes) being sent from an associated client in State 3 to an access point. Upon receipt of the invalid authentication requests, the access point updates the client to State 1, which disconnects client's wireless service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of a DoS attack by monitoring for spoofed MAC addresses and authentication failures. This alarm may also indicate an intrusion attempt. When a wireless client fails too many times in authenticating with an access point, the server raises this alarm to indicate a potential intruder's attempt to breach security.

Note This alarm focuses on IEEE 802.11 authentication methods, such as open system and shared key. EAP and 802.1x based authentications are monitored by other alarms.

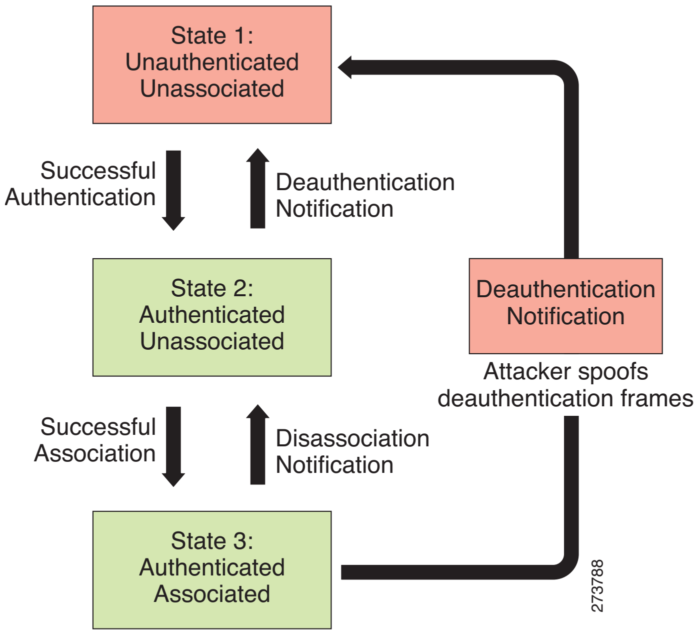
Denial-of-Service Attack: Deauthentication Broadcast

Attack tool: WLAN Jack, Void11, Hunter Killer

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client remains in State 3 to continue wireless communication. A client in State 1 and State 2 cannot participate in WLAN data communication until it is authenticated and associated to State 3.

Figure A-6 Deauthentication Broadcast Attack



A form of DoS attack sends all clients of an access point to the unassociated or unauthenticated State 1 by spoofing deauthentication frames from the access point to the broadcast address. With current client adapter implementation, this form of attack is very effective and immediate in disrupting wireless services against multiple clients. Typically, client stations reassociate and reauthenticate to regain service until the attacker sends another deauthentication frame.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed deauthentication frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security analyst can log onto the access point to verify the current association table status.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide* or the Cisco WCS online help.

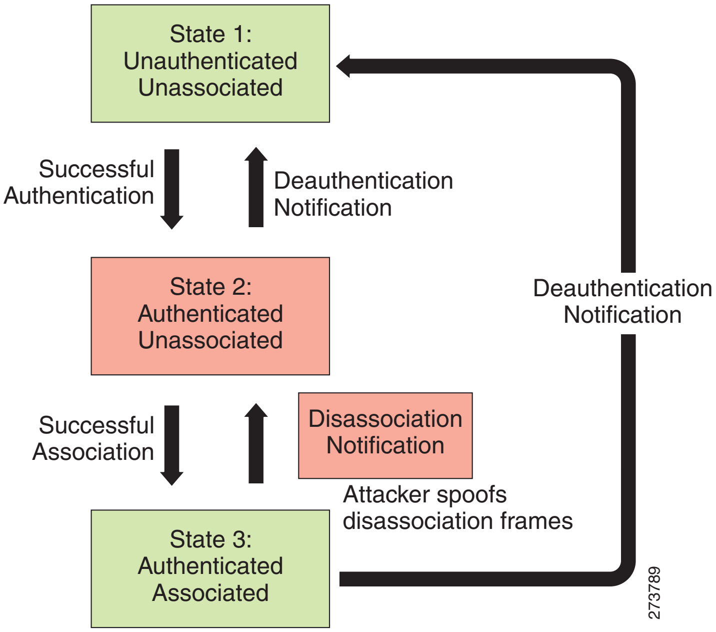
Denial-of-Service Attack: Deauthentication Flood

Attack tool: WLAN Jack, Void11

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client stays in State 3 in order to continue wireless communication. A client in State 1 and State 2 cannot participate in WLAN data communication until it is authenticated and associated to State 3.

Figure A-7 Deauthentication Flood Attack



A form of DoS attack aims to send an access point's client to the unassociated or unauthenticated State 1 by spoofing deauthentication frames from the access point to the client unicast address. With current client adapter implementations, this form of attack is very effective and immediate for disrupting wireless services against the client. Typically, client stations reassociate and reauthenticate to regain service until the attacker sends another deauthentication frame. An attacker repeatedly spoofs the deauthentication frames to keep all clients out of service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed deauthentication frames and tracking client authentication and association states. When the alarm is triggered, the access point and client under attack are identified. The WLAN security officer can log onto the access point to check the current association table status.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide* or the Cisco WCS online help.

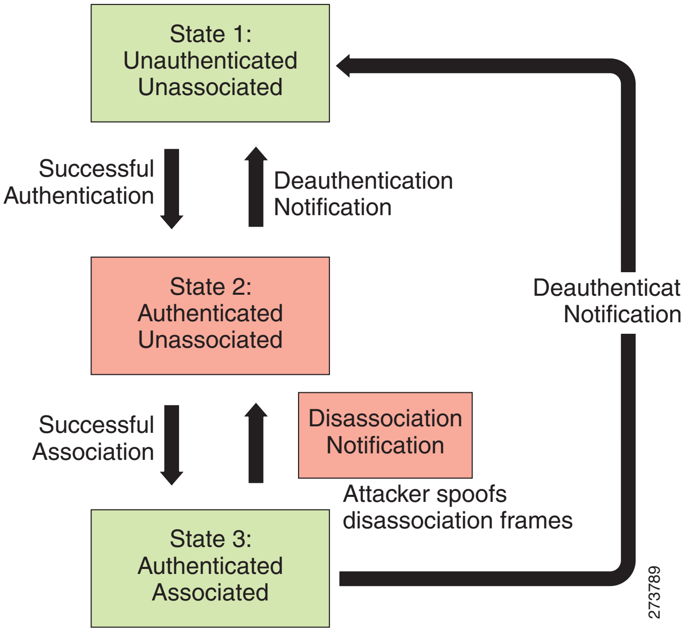
Denial-of-Service Attack: Disassociation Broadcast

Attack tool: ESSID Jack

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client station stays in State 3 in order to continue wireless communication. A client station in State 1 and State 2 can not participate in WLAN data communication until it is authenticated and associated to State 3.

Figure A-8 Disassociation Broadcast Attack



A form of DoS attack aims to send an access point's client to the unassociated or unauthenticated State 2 by spoofing disassociation frames from the access point to the broadcast address (all clients). With current client adapter implementations, this form of attack is effective and immediate for disrupting wireless services against multiple clients. Typically, client stations reassociate to regain service until the attacker sends another disassociation frame. An attacker repeatedly spoofs the disassociation frames to keep all clients out of service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed disassociation frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log onto the access point to check the current association table status.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide* or the Cisco WCS online help.

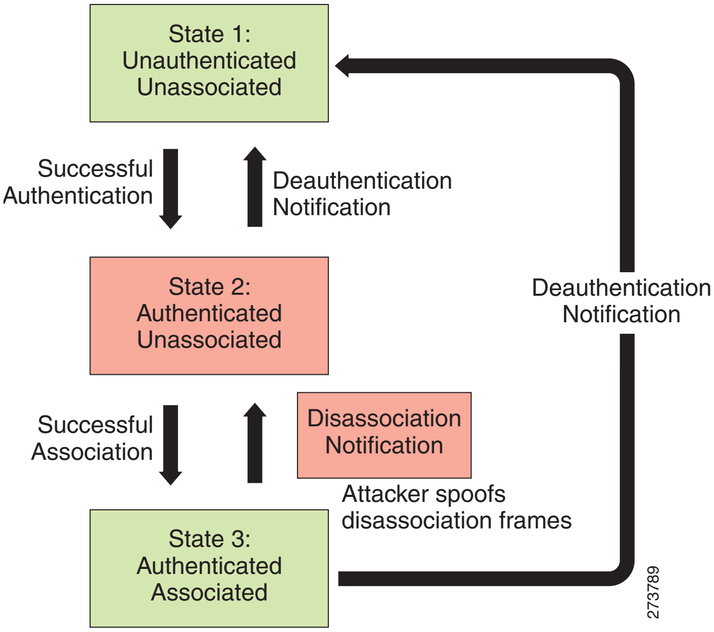
Denial-of-Service Attack: Disassociation Flood

Attack tool: ESSID Jack

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client stays in State 3 in order to continue wireless communication. A client in State 1 and State 2 cannot participate in WLAN data communication until it is authenticated and associated to State 3.

Figure A-9 Disassociation Flood Attack



A form of DoS attack aims to send an access point to the unassociated or unauthenticated State 2 by spoofing disassociation frames from the access point to a client. With client adapter implementations, this form of attack is effective and immediate for disrupting wireless services against this client. Typically, client stations reassociate to regain service until the attacker sends another disassociation frame. An attacker repeatedly spoofs the disassociation frames to keep the client out of service.

wIPS Solution

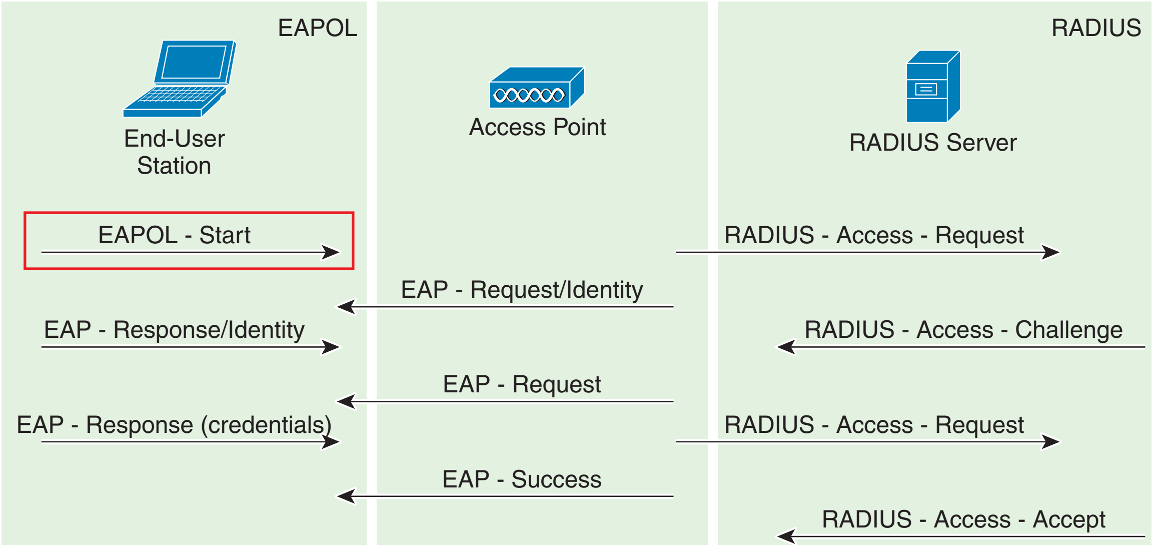
The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed disassociation frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log onto the access point to check the current association table status.

Denial-of-Service Attack: EAPOL Logoff Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using Extensible Authentication Protocol (EAP) over LANs or EAPOL. The 802.1x protocol starts with a EAPOL-start frame to begin the authentication transaction. At the end of an authenticated session when a client station logs off, the client station sends an 802.1x EAPOL-logoff frame to terminate the session with the access point.

Figure A-10 EAPOL Logoff Attack



Because the EAPOL-logoff frame is not authenticated, an attacker can potentially spoof this frame and log the user off the access point, thus committing a DoS attack. The fact that the client is logged off from the access point is not obvious until it attempts communication through the WLAN. Typically, the disruption is discovered and the client re-associates and authenticates automatically to regain the wireless connection. The attacker can continuously transmit the spoofed EAPOL-logoff frames to be effective on this attack.

wIPS Solution

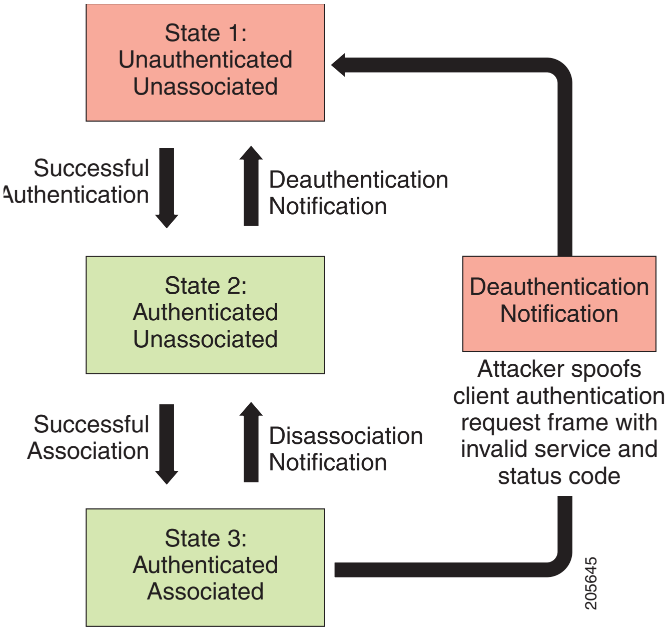
The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking 802.1x authentication states. When the alarm is triggered, the client and access point under attack are identified. The WLAN security officer logs onto the access point to check the current association table status.

Denial-of-Service Attack: FATA Jack Tool Detected

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this state machine based on the IEEE standard. A successfully associated client station stays in State 3 in order to continue wireless communication. A client station in State 1 and in State 2 cannot participate in the WLAN data communication process until it is authenticated and associated to State 3. IEEE 802.11 defines two authentication services: open system and shared key. Wireless clients go through one of these authentication processes to associate with an access point.

Figure A-11 Invalid Authentication Request Spoof



A form of DoS attack spoofs invalid authentication request frames (with bad authentication service and status codes) from an associated client in State 3 to an access point. Upon reception of the invalid authentication requests, the access point updates the client to State 1, which disconnects its wireless service.

FATA-jack is one of the commonly used tools to run a similar attack. It is a modified version of WLAN-jack and it sends authentication-failed packets along with the reason code of the previous authentication failure to the wireless station. This occurs after it spoofs the MAC address of the access point. FATA-jack closes most active connections and at times forces the user to reboot the station to continue normal activities.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the use of FATA-jack by monitoring on spoofed MAC addresses and authentication failures. This alarm may also indicate an intrusion attempt. When a wireless client fails too many times in authenticating with an access point, the Cisco Adaptive Wireless IPS raises this alarm to indicate a potential intruder's attempt to breach security.

Note This alarm focuses on 802.11 authentication methods (such as open system and shared key). EAP and 802.1x based authentications are monitored by other alarms.

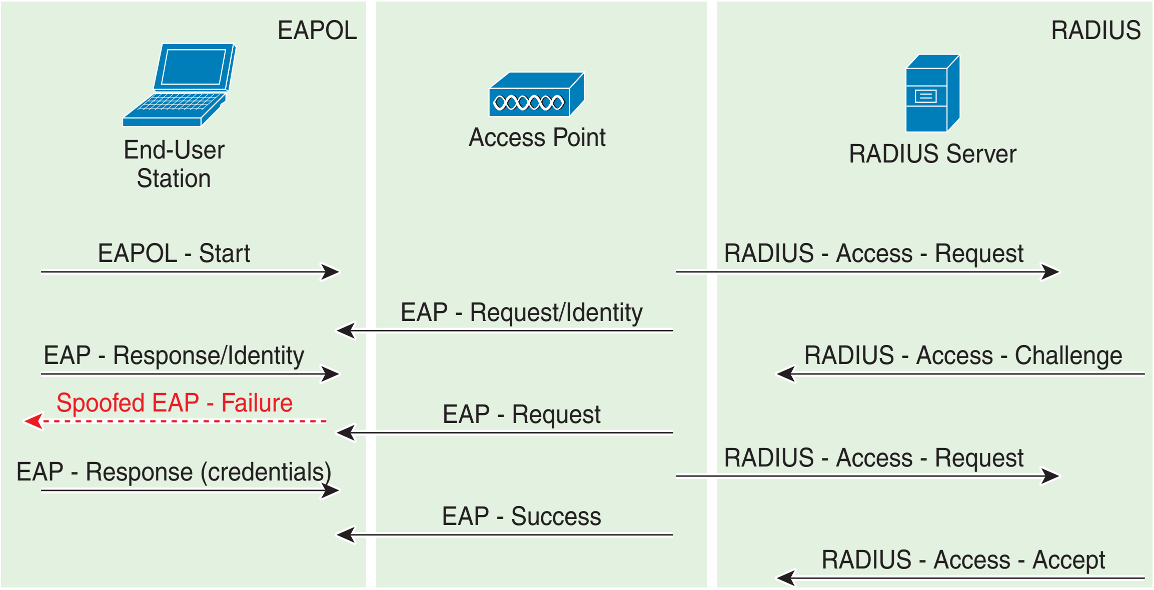
Cisco Management Frame Protection also provides complete proactive protection against frame and device spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide* or the Cisco WCS online help.

Denial-of-Service Attack: Premature EAP Failure Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using Extensible Authentication Protocol over LANs or EAPOL. The 802.1x protocol starts with an EAPOL-Start frame to begin the authentication transaction. When the 802.1x authentication packet exchange is complete with the back-end RADIUS server, the access point sends an EAP-success or EAP-failure frame to the client to indicate authentication success or failure.

Figure A-12 Premature EAP Failure Attack



The IEEE 802.1X specification prohibits a client from displaying its interface when the required mutual authentication is not complete. This enables a well-implemented 802.1x client station to avoid being fooled by a fake access point sending premature EAP-success packets.

An attacker keeps the client interface from appearing by continuously spoofing pre-mature EAP-failure frames from the access point to the client to disrupt the authentication state on the client.

wIPS Solution

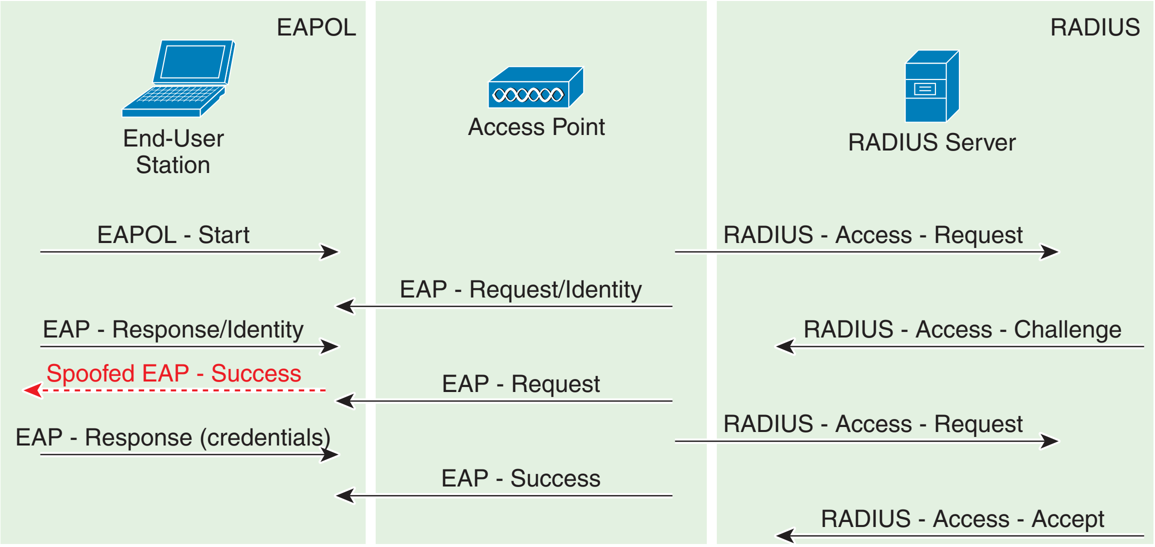
The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking the spoofed premature EAP-failure frames and the 802.1x authentication states for each client station and access point. Find the device and remove it from the wireless environment.

Denial-of-Service Attack: Premature EAP Success Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using Extensible Authentication Protocol over LANs or EAPOL. The 802.1x protocol starts with an EAPOL-start frame to begin the authentication transaction. When the 802.1x authentication packet exchange is completed with the back-end RADIUS server, the access point sends an EAP-success frame to the client to indicate a successful authentication.

Figure A-13 EAP Success Attack



The IEEE 802.1X specification prohibits a client from displaying its interface when the required mutual authentication has not been completed. This enables a well-implemented 802.1x client station to avoid being fooled by a fake access point sending premature EAP-success packets to bypass the mutual authentication process.

An attacker keeps the client interface from appearing by continuously spoofing premature EAP-success frames from the access point to the client to disrupt the authentication state.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking spoofed premature EAP-success frames and the 802.1x authentication states for each client station and access point. Find the device and remove it from the wireless environment.

Intrusion Detection—Security Penetration

A form of wireless intrusion is to breach the WLAN authentication mechanism in order to gain access to the wired network or the wireless devices. Dictionary attacks on the authentication method is a common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked access point attack on a unsuspicious wireless client may fool the client into associating with faked access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.

These security threats can be prevented if mutual authentication and strong encryption techniques are used. The Cisco Adaptive Wireless IPS looks for weak security deployment practices as well as any penetration attack attempts. The Cisco Adaptive Wireless IPS ensures a strong wireless security umbrella by validating the best security policy implementation as well as detecting intrusion attempts. If such vulnerabilities or attack attempts are detected, the Cisco Adaptive Wireless IPS generates alarms to bring these intrusion attempts to the administrator's notice.

Security penetration attacks include:

- Airsnarf Attack Detected
- Potential Chopchop Attack in Progress
- Day-0 Attack by WLAN Performance Anomaly
- Day-0 Attack by WLAN Security Anomaly
- Day-0 Attack by Device Performance Anomaly
- Day-0 Attack by Device Security Anomaly
- Device Probing for Access Points
- Dictionary Attack on EAP Methods
- EAP Attack Against 802.1x Authentication
- Fake Access Points Detected
- Fake DHCP Server Detected (Potential wireless phishing)
- Fast WEP Crack (ARP Replay) Detected
- Potential Fragmentation Attack in Progress
- Hot-Spotter Tool Detected (Potential Wireless Phishing)
- Malformed 802.11 Packets Detected
- Man-in-the-Middle Attack Detected
- Monitored Device Detected
- NetStumbler Detected
- NetStumbler Victim Detected
- Publicly Secure Packet Forwarding (PSPF) Violation
- Potential ASLEAP Attack Detected
- Potential Honey Pot AP Detected
- Soft AP or Host AP Detected
- Spoofed MAC Address Detected
- Suspicious After-Hours Traffic Detected
- Unauthorized Association by Vendor List
- Unauthorized Association Detected
- Wellenreiter Detected

Airsnarf Attack Detected

Alarm Description and Possible Causes

A hotspot is any location where Wi-Fi network access is made available for the general public. Hotspots are found in airports, hotels, coffee shops, and other places where business people tend to congregate. They are important network access services for business travelers.

Customers are able to connect to the legitimate access point and receive service using a wireless-enabled laptop or handheld. Most hotspots do not require the user to have any advanced authentication mechanism to connect to the access point other than popping up a web page for the user to log in. The criterion for entry is dependent only on whether or not the subscriber has paid the subscription fees. In a wireless hotspot environment, no one should be trusted. Due to current security concerns, some WLAN hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user.

The four components of a basic hotspot network include:

- Hotspot Subscribers—Valid users with a wireless-enabled laptop or handheld and valid login for accessing the hotspot network.
- WLAN Access Points—Can be small office or home office (SOHO) gateways or enterprise-level access points depending upon the hotspot implementation.
- Hotspot Controllers—Deals with user authentication, gathering billing information, tracking usage time, filtering functions, etc. This can be an independent machine or incorporated in the access point itself.
- Authentication Server—Contains the login credentials for the subscribers. Most hotspot controllers verify subscribers' credentials with the authentication server.

Airsnarf is a wireless access point setup utility that shows how a hacker can steal username and password credentials from public wireless hotspots.

Airsnarf, a shell script-based tool, creates a hotspot complete with a captive portal where the users enter their login information. Important values such as local network information, gateway IP address, and SSID can be configured within the airsnarf configuration file. This tool initially broadcasts a very strong signal that disassociates the hotspot wireless clients from the authorized access point connected to the Internet. The wireless clients assume that they are temporarily disconnected from the Internet due to some unknown issue and they try to log in again. Wireless clients that associate to the Airsnarf access point receive the IP address, DNS address, and gateway IP address from the rogue Airsnarf access point instead of the legitimate access point installed by the hotspot operator. A web page requests a username and password and the DNS queries are resolved by the rogue Airsnarf access point. The username and password entered are collected by the hacker.

The username and password can be used in any other hotspot location of the same provider anywhere in the nation without the user realizing the misuse. The only case where it could have lesser impact is if the hotspot user is connected using a pay-per-minute usage scheme.

The Airsnarf tool can also penetrate the laptop clients that are unknowingly connected to the Airsnarf access point. The AirSnarf tool can be downloaded by hackers from http://airsnarf.shmoo.com/

wIPS Solution

The Cisco Adaptive Wireless IPS detects the wireless device running the AirSnarf tool. Appropriate action must be taken by the administrator to remove the AirSnarf tool from the WLAN environment.

Potential Chopchop Attack in Progress

Alarm Description and Possible Causes

It is well publicized that a WLAN device using a static WEP key for encryption is vulnerable to various WEP cracking attacks. Refer to *Weaknesses in the Key Scheduling Algorithm of RC4 - I* by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information.

A cracked WEP secret key offers no encryption protection for data to be transmitted, leading to compromised data privacy. The WEP key, which is in most cases 64-bit or 128-bit (some vendors also offer 152-bit encryption), is a secret key specified by the user, linked with the 24-bit IV (Initialization Vector). The chopchop tool was written for the Linux operating system by Korek to exploit a weakness in WEP and decrypt the WEP data packet. However, the chopchop tool only reveals the plaintext. The attacker uses the packet capture file of a previously injected packet during the initial phase and decrypts the packet by retransmitting modified packets to the attacked network. When the attack is completed, the chopchop tool produces an unencrypted packet capture file and another file with Pseudo Random Generation Algorithm (PRGA) information determined during the decryption process. The PGRA is then XORed with the cyphertext to obtain the plaintext.

Example commands that indicate a chopchop attack:

```
aireplay-ng -4 -h XX:XX:XX:XX:XX:XX -b YY:YY:YY:YY:YY:YY ath0
```

where

4: Indicates a chopchop attack

-h XX:XX:XX:XX:XX:XX: Identifies a MAC address of an associated client

-b YY:YY:YY:YY:YY:YY: Identifies the MAC address of the access point

ath0: Identifies the wireless interface name

Access points that drop data packets shorter than 60 bytes may not be vulnerable to this kind of attack. If an access point drops packets shorter than 42 bytes, aireplay will try to guess the rest of the missing data, as far as the headers are predictable. If an IP packet is captured, it additionally checks if the checksum of the header is correct after guessing the missing parts of it. This attack requires at least one WEP data packet. A chopchop attack also works against dynamic WEP configurations. The Cisco Adaptive Wireless IPS is able to detect potential attacks using the chopchop tool.

wIPS Solution

The Cisco Adaptive Wireless IPS activates an alert when a potential chopchop attack is in progress. WEP should not be used in the corporate environment and appropriate measures should be taken to avoid any security holes in the network and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard.

Day-0 Attack by WLAN Performance Anomaly

Alarm Description and Possible Causes

WLAN performance efficiency is constantly challenged by the dynamics of the RF environment and the mobility of client devices. A closely monitored and well tuned WLAN system can achieve a higher throughput than a poorly managed one. Radio Resource Management (RRM) built into the Cisco Unified

Wireless Network monitors and dynamically corrects performance issues found in the RF environment. Further performance anomaly monitoring may be done via the Wireless IPS system. For more information on RRM, refer to the Cisco WCS online help.

The Cisco Adaptive Wireless IPS ensures WLAN performance and efficiency by monitoring the WLAN on a continued basis and alerting the wireless administrator on early warning signs for trouble. Performance alarms are generated and classified in the following categories in the event of any performance degradation:

- **RF Management—**The Cisco Adaptive Wireless IPS monitors the physical RF environment that is dynamic and very often the source of WLAN performance problems. While monitoring on the RF environment, the server characterizes the following WLAN fundamentals and reports problems accordingly:
  - Channel interference and channel allocation problems
  - Channel noise and non-802.11 signals
  - WLAN RF service under-coverage area
  - Classic RF hidden-node syndrome
- **Problematic traffic pattern—**Many WLAN performance problems including the RF multi-path problem manifest themselves in the MAC layer protocol transactions and statistics. By tracking and analyzing the wireless traffic, the Cisco Adaptive Wireless IPS is able to spot performance inefficiencies and degradations early on. In many cases, the Cisco Adaptive Wireless IPS can determine the cause of the detected performance problem and suggest counter measures. The Cisco Adaptive Wireless IPS tracks MAC layer protocol characteristics including the following:
  - Frame CRC error
  - Frame re-transmission
  - Frame speed (1, 2, 5.5, 11, ... Mbps) usage and distribution
  - Layer 2 frame fragmentation
  - Access point and station association, reassociation and disassociation relationship
  - Roaming hand-off
- **Channel or device overloaded—**The Cisco Adaptive Wireless IPS monitors and tracks the load to ensure smooth operation with both channel bandwidth limitation or the WLAN device resource capacity. In the event of unsatisfactory performance by the WLAN due to under-provisioning or over-growth, the Cisco Adaptive Wireless IPS raises alarms and offers specific details. RF has no boundaries that could lead to your WLAN channel utilization to increase significantly even when your neighbor installs new WLAN devices in an adjoining channel. The Cisco Adaptive Wireless IPS monitors your WLAN to ensure proper bandwidth and resource provisioning.
- **Deployment and operation error—**The Cisco Adaptive Wireless IPS scans the airwaves for configuration and operation errors. The following specific areas are continuously monitored:
  - Inconsistent configuration among access points servicing the same SSID
  - Configuration against the principles of best practice
  - Connection problems caused by client/access point mismatch configuration
  - WLAN infrastructure device down or reset
  - Flaws in WLAN device implementation
- **IEEE 802.11e and VoWLAN issues—**The IEEE 802.11e standard adds quality-of-service (QoS) features and multimedia support to the existing 802.11 a/b/g wireless standard. This is done while maintaining full backward compatibility with these standards. The QoS feature is critical to voice and

video applications. Wireless LAN has limited bandwidth and high overheads as compared to the traditional wired Ethernet. The throughput is reduced for a variety of reasons including the RTS/CTS mechanism, packet fragmentation, packet retransmission, acknowledgements, and collisions.

wIPS Solution

The Cisco Adaptive Wireless IPS has detected a single Performance Intrusion policy violation on a large number of devices in the wireless network. Either the number of devices violating the specific policy in the time period specified are observed or there is a sudden percentage increase in the number of devices as specified in the threshold settings for the alarm. Depending on the Performance Intrusion violation, it is suggested that the devices be monitored and located to carry out further analysis.

For example:

- If the *AP overloaded by stations alarm* is generated by a large number of devices, it may indicate that a hacker has generated thousands of stations and forcing them to associate to the corporate access point. If this occurs, legitimate corporate clients cannot connect to the access point.
- *Excessive frame retries* on the wireless devices may indicate such things as noise, interference, packet collisions, multi-path, and hidden node syndrome.

Day-0 Attack by WLAN Security Anomaly

Alarm Description and Possible Causes

The addition of WLANs in the corporate environment introduces a whole new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk of outside penetration and attack. Besides rogue access points, there are many other wireless security vulnerabilities which compromise the wireless network such as misconfigured and unconfigured access points. There can also be DoS (denial-of-service) attacks from various sources against the corporate network.

Cisco WCS provides automated security vulnerability assessment within the wireless infrastructure that proactively reports any security vulnerabilities or mis-configurations. Further assessment may be done over-the-air via the Wireless IPS system. With the comprehensive suite of security monitoring technologies, the Cisco Adaptive Wireless IPS alerts the user on more than 100 different threat conditions in the following categories:

- **User authentication and traffic encryption (Static WEP encryption, VPN, Fortress, Cranite, 802.11i and 802.1x)—**Common security violations in this category (authentication and encryption) include mis-configurations, out-of-date software or firmware, and suboptimal choice of corporate security policy.
- **Rogue, monitored, and ad-hoc mode devices—**Rogue devices must be detected and removed immediately in order to protect the integrity of the wireless and wired enterprise network.
- **Configuration vulnerabilities—**Implementing a strong deployment policy is fundamental to a secure WLAN. However, enforcing the policy requires constant monitoring to catch violations caused by mis-configuration or equipment vendor implementation errors. With the increased trend on laptops with built-in Wi-Fi capabilities, the complexity of WLAN configuration extends beyond access points to the user laptops. WLAN device configuration management products can make the configuration process easier, but the need for validation persists especially in laptops with built-in but unused and unconfigured Wi-Fi.

- **Intrusion detection on security penetration—**A form of wireless intrusion includes breaching the WLAN authentication mechanism in order to gain access to the wired network or the wireless devices. A Dictionary attack on the authentication method is a very common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked AP attack on a unsuspicious wireless client may fool the client into associating with a fake access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.
- **Intrusion detection on denial-of-service attacks—**Wireless DoS (denial-of-service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLAN at layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example, RF jamming attack with high power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

wIPS Solution

The Cisco Adaptive Wireless IPS has detected a single Security IDS/IPS policy violation on a large number of devices in the wireless network. Either the number of devices violating the specific policy in the time period specified are observed or there is a sudden percentage increase in the number of devices as specified in the threshold settings for the alarm. Depending on the Security IDS/IPS violation, it is suggested that the devices are monitored and located to carry out further analysis to check if they are compromising the Enterprise wireless network in any way (attack or vulnerability). If this is an increase in the number of rogue devices, it may indicate an attack against the network. The WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find it.

If there is a sudden increase in the number of client devices with encryption disabled, it may be necessary to revisit the Corporate Security Policy and enforce users to use the highest level of encryption and authentication according to the policy rules.

Day-0 Attack by Device Performance Anomaly

Alarm Description and Possible Causes

WLAN performance efficiency is constantly challenged by the dynamics of the RF environment and the mobility of client devices. A closely monitored and well tuned WLAN system can achieve a higher throughput than a poorly managed one. Radio Resource Management built into the Cisco Unified Wireless Network monitors and dynamically corrects performance issues found in the RF environment. Further performance anomaly monitoring may be done via the Wireless IPS system. For more information on RRM, refer to the Cisco WCS online help.

The Cisco Adaptive Wireless IPS ensures WLAN performance and efficiency by monitoring the WLAN on a continued basis and alerting the wireless administrator on early warning signs for trouble. Performance alarms are generated and classified in the following categories in the event of any performance degradation:

- **RF Management—**The Cisco Adaptive Wireless IPS monitors the physical RF environment that is dynamic and very often the source of WLAN performance problems. While monitoring on the RF environment, the server characterizes the following WLAN fundamentals and reports problems accordingly:

  - Channel interference and channel allocation problems
  - Channel noise and non-802.11 signals
  - WLAN RF service under-coverage area
  - Classic RF hidden-node syndrome
- **Problematic traffic pattern—**Many WLAN performance problems including the RF multi-path problem manifest themselves in the MAC layer protocol transactions and statistics. By tracking and analyzing the wireless traffic, the Cisco Adaptive Wireless IPS is able to spot performance inefficiencies and degradations early on. In many cases, the Cisco Adaptive Wireless IPS can determine the cause of the detected performance problem and suggest counter measures. The Cisco Adaptive Wireless IPS tracks MAC layer protocol characteristics including the following:
  - Frame CRC error
  - Frame re-transmission
  - Frame speed (1, 2, 5.5, 11, ... Mbps) usage and distribution
  - Layer 2 frame fragmentation
  - Access point and station association/reassociation/disassociation relationship
  - Roaming hand-off
- **Channel or device overloaded—**The Cisco Adaptive Wireless IPS monitors and tracks the load to ensure smooth operation with both channel bandwidth limitation or the WLAN device resource capacity. In the event of unsatisfactory performance by the WLAN due to under-provisioning or over-growth, the Cisco Adaptive Wireless IPS raises alarms and offers specific details. RF has no boundaries that could lead to your WLAN channel utilization to increase significantly even when your neighbor installs new WLAN devices in an adjoining channel. The Cisco Adaptive Wireless IPS monitors your WLAN to ensure proper bandwidth and resource provisioning.
- **Deployment and operation error—**The Cisco Adaptive Wireless IPS scans the airwaves for configuration and operation errors. The following specific areas are continuously monitored:
  - Inconsistent configuration among access points servicing the same SSID
  - Configuration against the principles of best practice
  - Connection problems caused by client/access point mismatch configuration
  - WLAN infrastructure device down or reset
  - Flaws in WLAN device implementation
- **IEEE 802.11e and VoWLAN issues—**The IEEE 802.11e standard adds QoS (quality-of-service) features and multimedia support to the existing 802.11 a/b/g wireless standard. This is done while maintaining full backward compatibility with these standards. The QoS feature is critical to voice and video applications. Wireless LAN has limited bandwidth and high overheads as compared to the traditional wired Ethernet. The throughput is reduced for a variety of reasons including the RTS/CTS mechanism, packet fragmentation, packet retransmission, acknowledgements, and collisions.

To maximize the power of the Cisco Adaptive Wireless IPS, performance alarms can be customized to best match your WLAN deployment specification. For example, if your WLAN is designed for all users to use 5.5 and 11 Mb/s speed only, customize the threshold for performance alarm 'Low speed tx rate exceeded' to reflect such an expectation.

wIPS Solution

The Cisco Adaptive Wireless IPS detects a device violating a large number of performance intrusion policies. This device has either generated a large number of performance intrusion violations in the time period specified or there is a sudden percentage increase as specified in the threshold settings for the various alarms. It is suggested that the device is monitored and located to carry out further analysis to check if this device is causing any issues in the overall performance of the network.

For example, if there is a device which has caused an increase in the number of "access points overloaded by stations" and "access points overloaded by utilization" alarms, this could indicate that the access point cannot handle the stations. The administrator may need to reconsider re-deployment of the access points.

Day-0 Attack by Device Security Anomaly

Alarm Description and Possible Causes

The addition of WLANs in the corporate environment introduces a new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. Rogue access points can put the entire corporate network at risk for outside penetration and attack. Besides rogue access points, there are many other wireless security vulnerabilities which compromise the wireless network such as misconfigured and unconfigured access points. There can also be DoS attacks from various sources against the corporate network.

Cisco WCS provides automated security vulnerability assessment within the wireless infrastructure that proactively reports any security vulnerabilities or mis-configurations. Further assessment may be done over-the-air via the Wireless IPS system. With the comprehensive suite of security monitoring technologies, the Cisco Adaptive Wireless IPS alerts the user on more than 100 different threat conditions in the following categories:

- **User authentication and traffic encryption (Static WEP encryption, VPN, Fortress, Cranite, 802.11i and 802.1x)—**Common security violations in this category (authentication and encryption) include mis-configurations, out-of-date software or firmware, and suboptimal choice of corporate security policy.
- **Rogue, monitored, and ad-hoc mode devices—**Rogue devices must be detected and removed immediately in order to protect the integrity of the wireless and wired enterprise network.
- **Configuration vulnerabilities—**Implementing a strong deployment policy is fundamental to a secure WLAN. However, enforcing the policy requires constant monitoring to catch violations caused by mis-configuration or equipment vendor implementation errors. With the increased trend on laptops with built-in Wi-Fi capabilities, the complexity of WLAN configuration extends beyond access points to the user laptops. WLAN device configuration management products can make the configuration process easier, but the need for validation persists especially in laptops with built-in but unused and unconfigured Wi-Fi.
- **Intrusion detection on security penetration—**A form of wireless intrusion includes breaching the WLAN authentication mechanism in order to gain access to the wired network or the wireless devices. A Dictionary attack on the authentication method is a very common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked AP attack on a unsuspicious wireless client may fool the client into associating with a fake access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.

- **Intrusion detection on DoS attacks—**Wireless DoS (denial-of-service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLAN at layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example, RF jamming attack with high power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

wIPS Solution

The Cisco Adaptive Wireless IPS detects a device violating a large number of Security IDS/IPS policies. This device has either generated a number of Security IDS/IPS violations in the time period specified or there is a sudden percentage increase as specified in the threshold settings for the various alarms. The device should be monitored and located to carry out further analysis to check if this device is compromising the Enterprise Wireless Network in any way (attack or vulnerability). If this is a rogue device, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find it.

Device Probing for Access Points

Some commonly used scan tools include: NetStumbler (newer versions), MiniStumbler (newer versions), MACStumbler, WaveStumbler, PrismStumbler, dStumbler, iStumbler, Aerosol, Boingo™ Scans, WiNc™, AP Hopper, NetChaser, Microsoft Windows XP scans.

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects wireless devices probing the WLAN and attempting association (such as association request for an access point with any SSID).

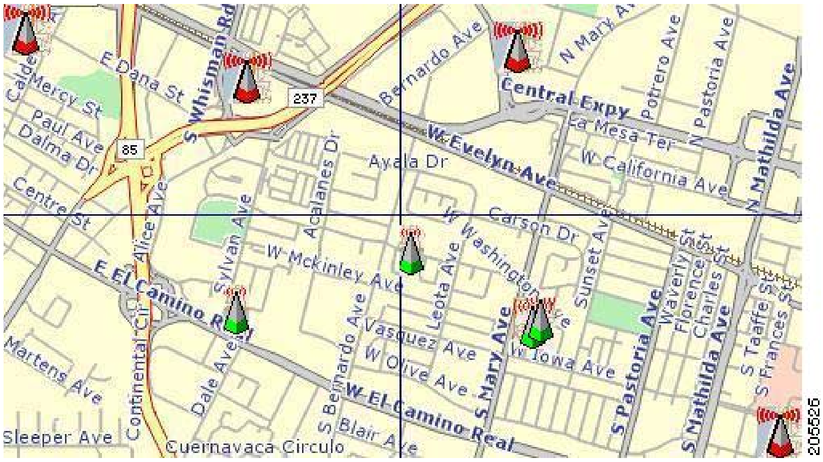
Such devices could pose potential security threats in one of the following ways:

- War-driving, WiLDing (Wireless LAN Discovery), war-chalking, war-walking, war cycling, war-lightrailing, war-busing, and war-flying.
- Legitimate wireless client attempting risky promiscuous association.

War-driving, war-chalking, war-walking, and war-flying activities include:

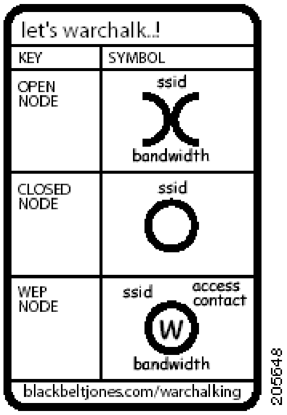
- **War-driving—**A wireless hacker uses war-driving tools to discover access points and publishes information such as MAC address, SSID, and security implemented on the Internet with the access points' geographical location information (see Figure A-14).

Figure A-14 Access Point Locations Posted on the Internet



- **War-chalking—**War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols (see below).

Figure A-15 War Chalker Universal Symbols



- **War-walking—**War-walking is similar to war-driving, but the hacker is on foot instead of a car.
- **War-flying—**War-flying refers to sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet relay chat sessions from an altitude of 1,500 feet on a war-flying trip.

Legitimate Wireless Client Attempting Risky Association

The second potential security threat for this alarm may be more damaging. Some of these alarms could be from legitimate and authorized wireless clients on your WLAN who are attempting to associate with any available access point including your neighbor's access point or the more damage-causing rogue access point. This potential security threat can be from a Microsoft Windows XP laptop with a built-in Wi-Fi card or laptops using wireless connectivity tools such as the Boingo™ client utility and the WiNc™ client utility. When associated, this client station can be accessed by an intruder leading to a major security breach. Even worse, the client station may bridge the unintended access point with your company's wired LAN. Typically, laptops are equipped with built-in Wi-Fi cards and, at the same, are physically attached to your company WLAN for network connectivity. Your wired network is exposed if the Windows bridging service is enabled on that Windows laptop. To be secure, configure all client stations with specific SSIDs to avoid associating with an unintended access point. Also consider mutual authentication such as 802.1x and various EAP methods.

The Cisco Adaptive Wireless IPS also detects a wireless client station probing the WLAN for an anonymous association such as an association request for an access point with any SSID) using the NetStumbler tool. The device probing for access point alarm is generated when hackers use the latest versions of the NetStumbler tool. For older versions, the NetStumbler detected alarm is triggered.

NetStumbler is the most widely used tool for war-driving and war-chalking. The NetStumbler web site (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or more recent operating systems. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to search shopping malls and retail stores.

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure the access points to not broadcast SSIDs. Use the Cisco Adaptive Wireless IPS to determine which access points are broadcasting (announcing) their SSID in the beacons.

Dictionary Attack on EAP Methods

Alarm Description and Possible Causes

EEE 802.1x provides an EAP framework for wired or wireless LAN authentication. An EAP framework allows flexible authentication protocol implementation. Some implementations of 802.1x or WPA use authentication protocols such as LEAP, MD5, OTP (one-time-password), TLS, and TTLS. Some of these authentication protocols are based upon the username and password mechanism in which the username is transmitted without encryption and the password is used to answer authentication challenges.

Most password-based authentication algorithms are susceptible to dictionary attacks. During a dictionary attack, an attacker gains the username from the unencrypted 802.1x identifier protocol exchange. The attacker then tries to guess a user's password to gain network access by using every word in a dictionary of common passwords or possible combinations of passwords. A dictionary attack relies on a password being a common word, name, or combination of both with a minor modification such as a trailing digit or two.

A dictionary attack can take place actively online, where an attacker repeatedly tries all the possible password combinations. Online dictionary attacks can be prevented using lock-out mechanisms available on the authentication server (RADIUS servers) to lock out the user after a certain number of invalid login attempts. A dictionary attack can also take place offline, where an attacker captures a successful authentication challenge protocol exchange and then tries to match the challenge response with all possible password combinations. Unlike online attacks, offline attacks are not easily detected. Using a strong password policy and periodically expiring user passwords significantly reduces an offline attack tool's success.

wIPS Solution

The Cisco Adaptive Wireless IPS detects online dictionary attacks by tracking 802.1x authentication protocol exchange and the user identifier usages. When a dictionary attack is detected, the alarm message identifies the username and attacking station's MAC address.

The Cisco Adaptive Wireless IPS advises switching username and password based authentication methods to encrypted tunnel based authentication methods such as PEAP and EAP-FAST, which are supported by many vendors including Cisco.

EAP Attack Against 802.1x Authentication

Alarm Description and Possible Causes

IEEE 802.1x provides an Extensible Authentication Protocol (EAP) framework for wired or wireless LAN authentication. An EAP framework allows flexible authentication protocol implementation. Some implementations of 802.1x or WPA use authentication protocols such as LEAP, MD5, OTP (one-time-password), TLS, TTLS, and EAP-FAST. Some of these authentication protocols are based upon the username and password mechanism, where the username is transmitted clear without encryption and the password is used to answer authentication challenges.

Most password-based authentication algorithms are susceptible to dictionary attacks. During a dictionary attack, an attacker gains the username from the unencrypted 802.1x identifier protocol exchange. The attacker attempts to guess a user's password and gain network access by using every "word" in a dictionary of common passwords or possible combinations of passwords. A dictionary attack relies on the fact that a password is often a common word, name, or combination of words or names with a minor modification such as a trailing digit or two.

Intruders with the legitimate 802.1x user identity and password combination (or valid certificate) can penetrate the 802.1x authentication process without the proper knowledge of the exact EAP-type. The intruder tries different EAP-types such as TLS, TTLS, LEAP, EAP-FAST, or PEAP to successfully log onto the network. This is a trial and error effort because there are only a handful of EAP-types for the intruder to try and manage to get authenticated to the network.

wIPS Solution

The Cisco Adaptive Wireless IPS detects an attempt by an intruder to gain access to the network using different 802.1x authentication types. Take appropriate steps to locate the device and remove it from the wireless environment.

Fake Access Points Detected

Alarm Description and Possible Causes

The Fake AP tool is meant to protect your WLAN acting as a decoy to confuse war-drivers using NetStumbler, Wellenreiter, MiniStumbler, Kismet, and so on. The tool generates beacon frames imitating thousands of counterfeit 802.11b access points. War-drivers encountering a large number of access points cannot identify the real access points deployed by the user. This tool, although very effective in fending off war-drivers, poses other disadvantages such as bandwidth consumption, misleading legitimate client stations, and interference with the WLAN management tools. Running the Fake AP tool in your WLAN is not recommended.

wIPS Solution

The administrator should locate the device running the Fake AP tool and remove it from the wireless environment.

Fake DHCP Server Detected (Potential wireless phishing)

Alarm Description and Possible Causes

Dynamic Host Configuration Protocol (DHCP) is used for assigning dynamic IP addresses to devices on a network.

DHCP address assignment takes place as follows:

Step 1 The client NIC sends out a DHCP discover packet, indicating that it requires a IP address from a DHCP server.

Step 2 The server sends a DHCP offer packet with the IP address.

Step 3 The client NIC sends a DHCP request, informing the DHCP server that it wants to be assigned the IP address sent by the servers offer.

Step 4 The server returns a DHCP ACK, acknowledging that the NIC has sent a request for a specific IP address.

Step 5 The client's interface assigns or binds the initially offered IP address from the DHCP server.

The DHCP server should be a dedicated machine and part of the enterprise wired network or it could be a wireless/wired gateway. Other wireless devices can have the DHCP service running innocently or maliciously so as to disrupt the WLAN IP service. Wireless clients that are requesting an IP address from the DHCP server may then connect to these fake DHCP servers to get their IP address because the clients do not have any means to authenticate the server. These fake DHCP servers may give the clients non-functional network configurations or divert all the client's traffic through them. The hackers can then eavesdrop on every packet sent by the client. With the aid of rogue DNS servers, the hacker could also send the users to fake web page logins to get username and password credentials. It could also give out non-functional and non-routable IP addresses to achieve a DoS attack. This sort of attack is generally against a WLAN without encryption such as hotspots or trade show networks.

wIPS Solution

The Cisco Adaptive Wireless IPS detects such wireless STAs running the DHCP service and providing IP addresses to unaware users.

When the client is identified and reported, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the device.

Fast WEP Crack (ARP Replay) Detected

Alarm Description and Possible Causes

It is well publicized that WLAN devices using static WEP key for encryption are vulnerable to WEP key cracking attack (Refer to *Weaknesses in the Key Scheduling Algorithm of RC4* - I by Scott Fluhrer, Itsik Mantin, and Adi Shamir).

The WEP secret key that has been cracked by any intruder results in no encryption protection, thus leading to compromised data privacy. The WEP key that is in most cases 64-bit or 128-bit (few vendors also offer 152-bit encryption) consists of the secret key specified by the user linked with the 24-bit IV (Initialization Vector). The IV that is determined by the transmitting station can be reused frequently or in consecutive frames, thus increasing the possibility of the secret key to be recovered by wireless intruders.

The most important factor in any attack against the WEP key is the key size. For 64-bit WEP keys, around 150K unique IVs and for 128-bit WEP keys around 500k to a million unique IVs should be enough. With insufficient traffic, hackers have created a unique way of generating sufficient traffic to perform such an attack. This is called the replay attack based on arp-request packets. Such packets have a fixed length and can be spotted easily. By capturing one legitimate arp-request packet and resending them repeatedly, the other host responds with encrypted replies, providing new and possibly weak IVs.

wIPS Solution

The Cisco Adaptive Wireless IPS alerts on weak WEP implementations and recommends a device firmware upgrade if available from the device vendor to correct the IV usage problem. Ideally, enterprise WLAN networks can protect against WEP vulnerability by using the TKIP (Temporal Key Integrity Protocol) encryption mechanism, which is now supported by most enterprise level wireless equipment. TKIP enabled devices are not subject to any such WEP key attacks.

Cisco WCS also provides automated security vulnerability scanning that proactively reports any access points configured to utilize weak encryption or authentication. For more information on automated security vulnerability scanning, refer to the Cisco WCS online help.

Potential Fragmentation Attack in Progress

Alarm Description and Possible Causes

It is well publicized that a WLAN device using a static WEP key for encryption is vulnerable to various WEP cracking attacks. Refer to *Weaknesses in the Key Scheduling Algorithm of RC4 - I* by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information.

A cracked WEP secret key offers no encryption protection for data to be transmitted which leadw to compromised data privacy. The WEP key, which is in most cases 64-bit or 128-bit (few vendors also offer 152-bit encryption), is the secret key specified by the user and linked with the 24-bit IV (Initialization Vector).

According to **http://www.aircrack-ng.org/doku.php?id=fragmentation&s=fragmentation**, the aircrack program obtains a small amount of keying material from the packet and then attempts to send ARP and/or LLC packets with known information to an access point. If the packet gets successfully echoed back by the access point, then a larger amount of keying information can be obtained from the returned packet. This cycle is repeated several times until 1500 bytes (less in some cases) of PRGA are obtained.

This attack does not recover the WEP key itself, but merely obtains the PRGA. The PRGA can then be used to generate packets with *packetforge-ng* which can be used for various injection attacks.

Example commands that indicate a fragmentation attack:

```
aireplay-ng -5 -h XX:XX:XX:XX:XX:XX -b YY:YY:YY:YY:YY:YY ath0
```

where

5: Indicates a fragmentation attack

-h XX:XX:XX:XX:XX:XX: Identifies a MAC address of an associated client

-b YY:YY:YY:YY:YY:YY: Identifies the MAC address of the access point

ath0: Identifies the wireless interface name

wIPS Solution

The Cisco Adaptive Wireless IPS detects potential fragmentation attacks in progress against the Wi-Fi network. Further, wIPS and recommends that WEP not be used in the corporate environment and that appropriate measures be taken to avoid any security holes in the network, and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard.

Hot-Spotter Tool Detected (Potential Wireless Phishing)

Alarm Description and Possible Causes

A hotspot is any location where Wi-Fi network access available for the general public. Hotspots are often found in airports, hotels, coffee shops, and other places where business people tend to congregate. It is currently one of the most important network access service for business travelers. The customer requires a wireless-enabled laptop or handheld to connect to the legitimate access point and to receive service. Most hotspots do not require the user to have an advanced authentication mechanism to connect to the access point, other than using a web page to log in. The criterion for entry is only dependent on whether or not the subscriber has paid subscription fees. In a wireless hotspot environment, no one should trust anyone else. Due to current security concerns, some WLAN hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user.

Basic components of a WLAN Hotspot network

The four components of a basic hotspot network are:

- Hotspot Subscribers—Valid users with a wireless enabled laptop or handheld and valid login for accessing the hotspot network.
- WLAN Access Points—SOHO gateways or enterprise level access points depending upon the hotspot implementation.
- Hotspot Controllers—Deals with user authentication, gathering billing information, tracking usage time, filtering functions, etc. This can be an independent machine or can be incorporated in the access point itself.
- Authentication Server—Contains the login credentials for the subscribers. In most cases, hotspot controllers verify subscribers' credentials with the authentication server.

Hotspotter automates a method of penetration against wireless clients, independent of the encryption mechanism used. Using the Hotspotter tool, the intruder can passively monitor the wireless network for probe request frames to identify the SSIDs of the networks of the Windows XP clients.

After it acquires the preferred network information, the intruder compares the network name (SSID) to a supplied list of commonly used hotspot network names. When a match is found, the Hotspotter client acts as an access point. The clients then authenticate and associate unknowingly to this fake access point.

When the client gets associated, the Hotspotter tool can be configured to run a command such as a script to kick off a DHCP daemon and other scanning against the new victim.

Clients are also susceptible to this kind of attack when they are operating in different environments (home and office) while they are still configured to include the hotspot SSID in the Windows XP wireless connection settings. The clients send out probe requests using that SSID and make themselves vulnerable to the tool.

wIPS Solution

When the rogue access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

Malformed 802.11 Packets Detected

Alarm Description and Possible Causes

Hackers using illegal packets (malformed non-standard 802.11 frames) can force wireless devices to behave in an unusual manner. Illegal packets can cause the firmware of a few vendor's wireless NICs to crash.

Examples of such vulnerability includes NULL probe response frame (null SSID in the probe response frame) and oversized information elements in the management frames. These ill-formed frames can be broadcasted to cause multiple wireless clients to crash.

wIPS Solution

The Cisco Adaptive Wireless IPS can detect these illegal packets that may cause some NICs to lock up and crash. Also, wireless clients experiencing blue screen or lock-up problem during the attack period should consider upgrading the WLAN NIC driver or the firmware.

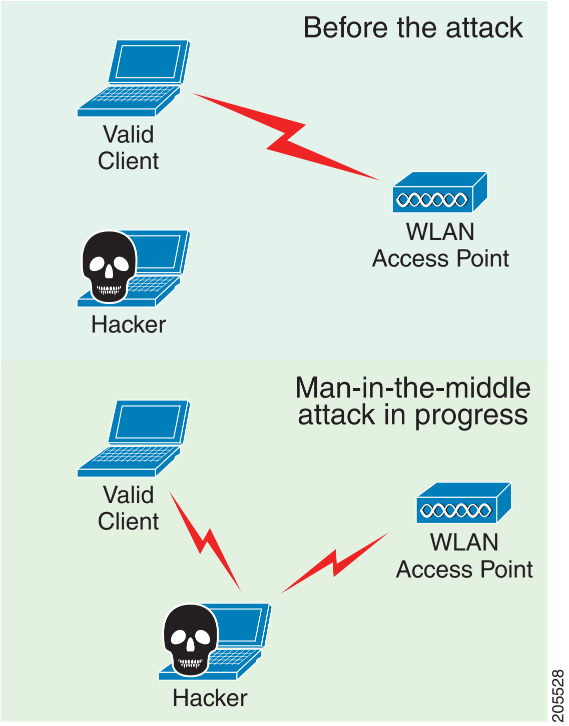
When the client is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use the device locator to locate it.

Man-in-the-Middle Attack Detected

Alarm Description and Possible Causes

Man-in-the-middle (MITM) attack is one of the most common 802.11 attacks that can lead to confidential corporate and private information being leaked to hackers. In a MITM attack, the hacker can use a 802.11 wireless analyzer and monitor 802.11 frames sent over the WLAN. By capturing the wireless frames during the association phase, the hacker gets IP and MAC address information about the wireless client card and access point, association ID for the client, and the SSID of the wireless network.

Figure A-16 Man-in-the-Middle Attack



A common MITM attack involves the hacker sending spoofed disassociation or deauthentication frames. The hacker station then spoofs the MAC address of the client to continue an association with the access point. At the same time, the hacker sets up a spoofed access point in another channel to keep the client associated. All traffic between the valid client and access point then passes through the hacker's station.

One of the most commonly used MITM attack tools is Monkey-Jack.

wIPS Solution

The Cisco Adaptive Wireless IPS recommends the use of strong encryption and authentication mechanisms to thwart any MITM attacks by hackers. One way to avoid such an attack is to prevent MAC address spoofing by using MAC address exclusion lists and monitoring the RF channel environment.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MITM attacks. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide* or the Cisco WCS online help.

Monitored Device Detected

Alarm Description and Possible Causes

There are some cases in which the access points and STAs activity must be continuously monitored:

- Malicious intruders attempting to hack into the enterprise wired network must be monitored. It is important to keep track of these access points and STAs to help avoid repeated rogue-related and intrusion attempt problems.

- Lost enterprise wireless equipment must be located.
- Vulnerable devices with previous security violations must be monitored.
- Devices used by ex-employees who may have not returned all their wireless equipment must be monitored.

These nodes may be added to the monitor list to alert the wireless administrator the next time the access point or STA shows up in the RF environment.

wIPS Solution

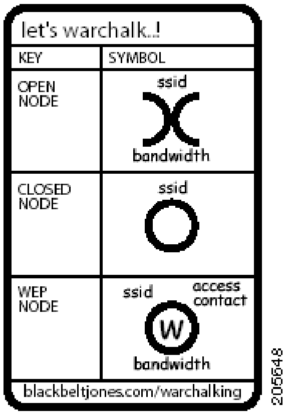
The wireless administrator can add the access point or STA to the monitor list by identifying it as a monitored device on the Cisco Adaptive Wireless IPS.

NetStumbler Detected

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (such as an association request for an access point with any SSID) using the NetStumbler tool. The *Device probing for Access Point* alarm is generated when hackers use recent versions of the NetStumbler tool. For older versions, the Cisco Adaptive Wireless IPS generates the *NetStumbler detected* alarm.

Figure A-17 War-Chalker Universal Symbols



NetStumbler is the most widely used tool for war-driving and war-chalking. A wireless hacker uses war-driving tools to discover access points and to publish their information (MAC address, SSID, security implemented, etc.) on the Internet with the access points' geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similar to war-driving, but the hacker is on foot instead of a car. The NetStumbler web site (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or later versions. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas.

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which of your access points is broadcasting an SSID in the beacons.

Cisco WCS also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, refer to the Cisco WCS online help.

NetStumbler Victim Detected

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (such as association request for an access point with any SSID) using the NetStumbler tool. The Device probing for access point alarm is generated when hackers more recent versions of the NetStumbler tool. For older versions, the Cisco Adaptive Wireless IPS generates the NetStumbler detected alarm.

NetStumbler is the most widely used tool for war-driving, war-walking, and war-chalking. A wireless hacker uses war-driving tools to discover access points and publish their information (MAC address, SSID, security implemented, etc.) on the Internet with the access points' geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similar to war-driving, but the hacker conducts the illegal operation on foot instead of by car. The NetStumbler web site (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or later. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers typically use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used, but from a low-flying private plane with high-power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.

wIPS Solution

The Cisco Adaptive Wireless IPS alerts the user when it observes that a station running Netstumbler is associated to a corporate access point. To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which access point is broadcasting its SSID in the beacons.

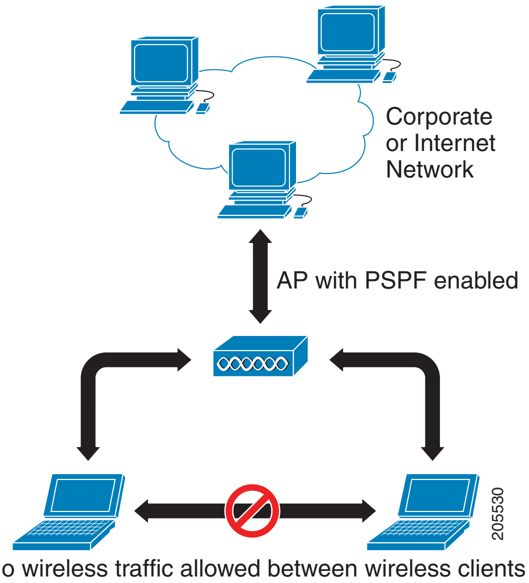
Publicly Secure Packet Forwarding (PSPF) Violation

Alarm Description and Possible Causes

Publicly Secure Packet Forwarding (PSPF) is a feature implemented on WLAN access points to block wireless clients from communicating with other wireless clients. With PSPF enabled, client devices cannot communicate with other client devices on the wireless network.

For most WLAN environments, wireless clients communicate only with devices such as web servers on the wired network. By enabling PSPF it protects wireless clients from being hacked by a wireless intruder. PSPF is effective in protecting wireless clients especially at wireless public networks (hotspots) such as airports, hotels, coffee shops, and college campuses where authentication is null and anyone can associate with the access points. The PSPF feature prevents client devices from inadvertently sharing files with other client devices on the wireless network.

Figure A-18 PSPF Enabled On The Network



wIPS Solution

The Cisco Adaptive Wireless IPS detects PSPF violations. If a wireless client attempts to communicate with another wireless client, the Cisco Adaptive Wireless IPS raises an alarm for a potential intrusion attack. This alarm does not apply if your WLAN deploys wireless printers or VoWLAN applications because these applications rely on wireless client-to-client communication.

Potential ASLEAP Attack Detected

Alarm Description and Possible Causes

WLAN devices using static WEP key for encryption are vulnerable to the WEP key cracking attack (See *Weaknesses in the Key Scheduling Algorithm of RC4-I* by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information).

Cisco Systems introduced LEAP (Lightweight Extensible Authentication Protocol) to leverage the existing 802.1x framework to avoid such WEP key attacks. The Cisco LEAP solution provides mutual authentication, dynamic per session and per user keys, and configurable WEP session key time out. The LEAP solution was considered a stable security solution and is easy to configure.

There are hacking tools that compromise wireless LAN networks running LEAP by using off-line dictionary attacks to break LEAP passwords After detecting WLAN networks that use LEAP, this tool de-authenticates users which forces them to reconnect and provide their username and password credentials. The hacker captures packets of legitimate users trying to re-access the network. The attacker can then analyze the traffic off-line and guess the password by testing values from a dictionary.

The main features of the ASLEAP tool include:

- Reading live from any wireless interface in RFMON mode with libpcap.
- Monitoring a single channel or performing channel hopping to look for target networks running LEAP.
- Actively deauthenticating users on LEAP networks, forcing them to reauthenticate. This allows quick LEAP password captures.
- Only de-authenticating users who have not already been seen rather than users who are not running LEAP.
- Reading from stored libpcap files.
- Using a dynamic database table and index to allow quick lookups on large files. This reduces the worst-case search time to .0015% as opposed to lookups in a flat file.
- Writing only the LEAP exchange information to a libpcap file.

This could be used to capture LEAP credentials with a device short on disk space (like an iPaq); the LEAP credentials are then stored in the libpcap file on a system with more storage resources to mount the dictionary attack.

The source and Win32 binary distribution for the tool are available at http://asleap.sourceforge.net.

Cisco Systems has developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol which stops these dictionary attacks. EAP-FAST helps prevent man-in-the-middle attacks, dictionary attacks, and packet and authentication forgery attacks. In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is then authenticated using the user-name and password credentials.

Some advantages of EAP-FAST include:

- It is not proprietary.
- It is compliant with the IEEE 802.11i standard.
- It supports TKIP and WPA.
- It does not use certificates and avoids complex PKI infrastructures.
- It supports multiple Operating Systems on PCs and Pocket PCs.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the deauthentication signature of the ASLEAP tool. When detected, the server alerts the wireless administrator. The user of the attacked station should reset the password. The best solution to counter the ASLEAP tool is to replace LEAP with EAP-FAST in the corporate WLAN environment.

Cisco WCS also provides automated security vulnerability scanning that proactively reports any access points configured to utilize weak encryption or authentication. For more information on automated security vulnerability scanning, refer to Cisco WCS online help.

Potential Honey Pot AP Detected

Alarm Description and Possible Causes

The addition of WLANs in the corporate environment introduces a whole new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured access points, unconfigured access points, and DoS (denial-of-service) attacks.

One of the most effective attacks facing enterprise networks implementing wireless is the use of a honey pot access point. An intruder uses tools such as NetStumbler, Wellenreiter, and MiniStumbler to discover the SSID of the corporate access point. Then the intruder sets up an access point outside the building premises or, if possible, within the premises and broadcasts the discovered corporate SSID. An unsuspecting client then connects to this honey pot access point with a higher signal strength. When associated, the intruder performs attacks against the client station because traffic is diverted through the honey pot access point.

wIPS Solution

When a honey pot access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

Soft AP or Host AP Detected

Host AP tools: Cqure AP

Alarm Description and Possible Causes

A host-based access point (desktop or a laptop computer serving as a wireless access point) represents two potential threats to enterprise security. First, host based access points are not typically part of the enterprise wireless infrastructure and are likely to be rogue devices which do not conform to the corporate security policy. Second, host-based access points are used by wireless attackers as a convenient platform to implement various known intrusions such as man-in-the-middle, honey-pot access point, access point impersonation, and DoS (denial-of-service) attacks. Since software tools for turning a desktop or laptop into an access point can be easily downloaded from the Internet, host-based access points are more than just a theoretical threat.

Some laptops are shipped with the HostAP software pre-loaded and activated. When the laptops connect to the enterprise wireless network, they expose the wireless network to the hackers.

wIPS Solution

The Cisco Adaptive Wireless IPS's detected soft access point should be treated as a rogue access point as well as a potential intrusion attempt. When the soft access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

Spoofed MAC Address Detected

Spoofing tools may include the following: SMAC, macchanger, and SirMACsAlot.

Alarm Description and Possible Causes

A wireless intruder can disrupt a wireless network using a wide range of available attack tools, many of which are available as free downloads from the Internet. Most of these tools rely on a spoofed MAC address which masquerades as an authorized wireless access point or as an authorized client. By using these tools, an attacker can launch various denial of service (DoS) attacks, bypass access control mechanisms, or falsely advertise services to wireless clients.

wIPS Solution

The Cisco Adaptive Wireless IPS detects a spoofed MAC address by following the IEEE authorized OUI (vendor ID) and 802.11 frame sequence number signature.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the *Cisco Wireless Control System Configuration Guide* or the Cisco WCS online help.

Suspicious After-Hours Traffic Detected

Alarm Description and Possible Causes

One way to detect a wireless security penetration attempt is to match wireless usage against the time when there is not supposed to be any wireless traffic. The wIPS server monitors traffic patterns against the office-hours configured for this alarm to generate alerts when an abnormality is found. Specific suspicious wireless usage sought after by the wIPS server during after-office hours includes the following:

- Client station initiating authentication or association requests to the office WLAN that may indicate security breach attempts.
- Wireless data traffic that may indicate suspicious download or upload over the wireless network.

wIPS Solution

For global wIPS deployment, the configurable office-hour range is defined in local time. The access point or sensor can be configured with a time zone to facilitate management. For the office and manufacturing floor mixed WLAN, one can define one set of office hours for the office WLAN SSID and another set for the manufacturing floor WLAN SSID. If this alarm is triggered, the administrator should look for the devices responsible for the suspicious traffic and remove them from the wireless environment.

Unauthorized Association by Vendor List

Alarm Description and Possible Causes

In the enterprise WLAN environment, rogue stations cause security concerns and undermine network performance. They take up air space and compete for network bandwidth. Since an access point can only accommodate a limited number of stations, it rejects association requests from stations when its capacity is reached. An access point laden with rogue stations denies legitimate stations the access to the network. Common problems caused by rogue stations include connectivity problems and degraded performance.

wIPS Solution

The Cisco Adaptive Wireless IPS enables network administrators to include vendor information in a policy profile to allow the system to effectively detect stations in use on the WLAN that are not approved vendor products. An alarm is triggered.

When the alarm has been triggered, the unauthorized station must be identified and actions must be taken to resolve the issue. One way is to block it using the rogue containment.

Unauthorized Association Detected

Alarm Description and Possible Causes

In an enterprise network environment, rogue access points installed by employees do not usually follow the network’s standard deployment practice and therefore compromise the integrity of the network. They are loopholes in network security and make it easy for intruders to hack into the enterprise wired network. One of the major concerns that most wireless network administrators face is unauthorized associations between stations in an ACL and a rogue access point. Since data to and from the stations flows through the rogue access point, it leaves the door open for hackers to obtain sensitive information.

Rogue stations cause security concerns and undermine network performance. They take up air space and compete for bandwidths on the network. Since an access point can only serve a certain number of stations, it rejects association requests from stations once its capacity is reached. An access point laden with rogue stations denies legitimate stations access to the network. Common problems caused by rogue stations include disrupted connections and degraded performance.

wIPS Solution

The Cisco Adaptive Wireless IPS can automatically alert network administrators to any unauthorized access point-station association it has detected on the network through this alarm. When the alarm is triggered, the rogue or unauthorized device must be identified and actions must be taken to resolve the reported issue.

Wellenreiter Detected

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (such as association request for an access point with any SSID) using the Wellenreiter tool.

Wellenreiter is a commonly used tool for war-driving and war-chalking. A wireless hacker uses war-driving tools to discover access points and to publish their information (MAC address, SSID, security implemented, etc.) on the Internet with the access points' geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similar to war-driving, but the hacker is on foot instead of a car. War-walkers like to use Wellenreiter and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used, but from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up email and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.

The tool supports Prism2, Lucent, and Cisco based cards. The tool can discover infrastructure and ad-hoc networks that are broadcasting SSIDs, their WEP capabilities, and can provide vendor information automatically. It also creates an ethereal/tcpdump-compatible dumpfile and an Application savefile. It also has GPS support. Users can download the tool from http://www.wellenreiter.net/index.html

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which of your access points is broadcasting an SSID in the beacons.

Cisco WCS also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, refer to the WCS online help.

APPENDIX B

Rogue Management

This section describes security issues and solutions for rogue access points.

Rogue Access Point Challenges

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

The operating system security solution uses the radio resource management (RRM) function to continuously monitor all nearby access points, automatically discover rogue access points, and locate them as described in the "Rogue Access Point Location, Tagging, and Containment" section.

Rogue Access Point Location, Tagging, and Containment

When the Cisco Unified Wireless Network Solution is monitored using WCS, WCS generates the flags as rogue access point traps and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the access points closest to each rogue access point. The next step is to mark them as Known or Acknowledged rogue access points (no further action), Alert rogue access points (watch for and notify when active), or Contained rogue access points (have between one and four access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

This built-in detection, tagging, monitoring, and containment capability enables system administrators to take appropriate action:

- Locate rogue access points
- Receive new rogue access point notifications, eliminating hallway scans
- Monitor unknown rogue access points until they are eliminated or acknowledged
- Determine the closest authorized access point, making directed scans faster and more effective
- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment can be done for individual rogue access points by MAC address or can be mandated for all rogue access points connected to the enterprise subnet.
- Tag rogue access points:
  - Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or wireless LAN security
  - Accept rogue access points when they do not compromise the LAN or wireless LAN security
  - Tag rogue access points as unknown until they are eliminated or acknowledged
  - Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

Detecting and Locating Rogue Access Points

When the access points on your wireless LAN are powered up and associated with controllers, WCS immediately starts listening for rogue access points. When a controller detects a rogue access point, it immediately notifies WCS, which creates a rogue access point alarm.

When WCS receives a rogue access point message from a controller, an alarm monitor appears in the lower left corner of all WCS user interface pages.

To detect and locate rogue access points, follow these steps:

Step 1 Click the Rogues indicator to display the Rogue AP Alarms page. This page lists the severity of the alarms, the rogue access point MAC addresses, the rogue access point types, the date and time when the rogue access points were first detected, and their SSIDs.

Step 2 Click any Rogue MAC Address link to display the associated Alarms > Rogue - AP MAC Address page. This page shows detailed information about the rogue access point alarm.

Step 3 To modify the alarm, choose one of these commands from the Select a Command drop-down menu and click **GO**.

- Assign to me—Assigns the selected alarm to the current user.
- Unassign—Unassigns the selected alarm.
- Delete—Deletes the selected alarm.
- Clear—Clears the selected alarm.
- Event History—Enables you to view events for rogue alarms.
- Detecting APs (with radio band, location, SSID, channel number, WEP state, short or long preamble, RSSI, and SNR)—Enables you to view the access points that are currently detecting the rogue access point.
- Rogue Clients—Enables you to view the clients associated with this rogue access point.
- Set State to `Unknown - Alert'—Tags the rogue access point as the lowest threat, continues to monitor the rogue access point, and turns off containment.

  Set State to `Known - Internal'—Tags the rogue access point as internal, adds it to the known rogue access points list, and turns off containment.

  Set State to `Known - External'—Tags the rogue access point as external, adds it to the known rogue access points list, and turns off containment.
- 1 AP Containment through 4 AP Containment—When you select level 1 containment, one access point in the vicinity of the rogue unit sends deauthenticate and disassociate messages to the client devices that are associated to the rogue unit. When you select level 2 containment, two access points in the vicinity of the rogue unit send deauthenticate and disassociate messages to the rogue's clients and so on up to level 4.

Step 4 From the Select a Command drop-down menu, choose Map (High Resolution) and click **GO** to display the current calculated rogue access point location on the Maps > Building Name > Floor Name page.

If you are using WCS Location, WCS compares RSSI signal strength from two or more access points to find the most probable location of the rogue access point and places a small skull-and-crossbones indicator at its most likely location. In the case of an underdeployed network for location with only one access point and an omni antenna, the most likely location is somewhere on a ring around the access point, but the center of likelihood is at the access point. If you are using WCS Base, WCS relies on RSSI signal strength from the rogue access point and places a small skull-and-crossbones indicator next to the access point receiving the strongest RSSI signal from the rogue unit.

Monitoring Alarms

- Monitoring Rogue Access Point Alarms
- Monitoring Rogue Access Point Details
- Detecting Access Points
- Monitoring Events
- Monitoring Rogue Clients

Monitoring Rogue Access Point Alarms

Rogue access point radios are unauthorized access points detected by one or more Cisco lightweight access points. This page displays rogue access point alarms based on the severity you clicked in the Alarm Monitor.

To access the Rogue AP Alarms page, do one of the following:

- Choose Monitor > Alarms. From the left sidebar, click New Search and choose Rogue AP from the Alarm Category drop-down menu. Click GO to display the matching alarms.
- Choose Monitor > Security. From the left sidebar, click Rogue APs.
- Click the Malicious AP number link in the Alarm Summary box at the bottom of the left sidebar.

Note If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use the scroll arrows to view additional alarms.

Table B-1 describes the parameters found on the rogue access point alarms page.

Table B-1 Alarm Parameters

Parameter	Description
Check box	Select the alarms on which you want to take action.
Severity	The severity of the alarm: Critical, Major, Minor, Clear. Color coded.
Rogue MAC Address	Media Access Control address of the rogue access points. See Monitor Alarms > Rogue AP Details.
Vendor	Rogue access point vendor name, or Unknown.
Classification Type	Malicious, Friendly, or Unclassified.
Radio Type	Indicates the radio type for this rogue access point.
Strongest AP RSSI	Indicates the strongest received signal strength indicator in dBm.

Table B-1 Alarm Parameters (continued)

Parameter	Description
No. of Rogue Clients	Indicates the number of rogue clients associated to this access point.
Owner	Indicates the `owner' of the rogue access point.
Date/Time	Date and time the alarm occurred.
State	State of the alarm: Alert, Known or Removed.
SSID	Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
Map Location	Indicates the map location for this rogue access point.
Acknowledged	Displays whether or not the alarm is acknowledged by the user.

Note The alarm remains in WCS, and you can search for all Acknowledged alarms using the alarm search functionality.

- The other sections on the Rogue AP Alarms page include the following:
- Unacknowledge—Unacknowledge an already acknowledged alarm.
- E-mail Notification—Takes you to the All Alarms > E-mail Notification page to view and configure e-mail notifications. See Monitor Alarms > E-mail Notification for more information.
- Severity Configuration—Change the severity level for newly-generated alarms. See Monitor Alarms > Severity Configuration for more information.
- Detecting APs—View the Cisco lightweight access points that are currently detecting the rogue access point.
- Map (High Resolution)—Click to display a high-resolution map of the rogue access point location.
- Rogue Clients—Click to view a list of rogue clients associated with this rogue access point. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the rogue access point.
- Set State to `Unclassified - Alert'—Choose this command to tag the rogue access point as the lowest threat, continue monitoring the rogue access point, and to turn off containment.
- Set State to `Malicious - Alert'—Choose this command to tag the rogue access point as Malicious.
- Set State to `Friendly - Internal'—Choose this command to tag the rogue access point as internal, add it to the Known Rogue APs list, and to turn off containment.
- 1 AP Containment—Target the rogue access point for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue access point for containment by two Cisco lightweight access points.
- 3 AP Containment—Target the rogue access point for containment by three Cisco lightweight access points.
- 4 AP Containment—Target the rogue access point for containment by four Cisco lightweight access points. (Highest containment level.)

Caution Attempting to contain a rogue access point may lead to legal consequences. When you select any of the AP Containment commands and click GO, a message "Containing a Rogue AP may have legal consequences. Do you want to continue?" appears. Click **OK** if you are sure or click **Cancel** if you do not wish to contain any access points.

Monitoring Rogue Access Point Details

Alarm event details for each rogue access point are available from the Rogue AP Alarms page.

To view alarm events for a rogue access point radio, follow these steps:

Step 1 From the Rogue AP Alarms page, click an item under Rogue MAC Address.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by Cisco lightweight access points. The following information is available:

- General–
  - Rogue MAC Address—Media Access Control address of the rogue access points.
  - Vendor—Rogue access point vendor name or Unknown.
  - On Network—Indicates whether or not the rogue access point is located on the network.
  - Owner—Indicates the owner or left blank.
  - Acknowledged—Indicates whether or not the alarm is acknowledged by the user.
  - Classification Type—Malicious, Friendly, or Unclassified.
  - State—Indicates the state of the alarm: Alert, Known, or Removed.
  - SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
  - Channel Number—Indicates the channel of the rogue access point.
  - Containment Level—Indicates the containment level of the rogue access point or Unassigned.
  - Radio Type—Indicates the radio type for this rogue access point.
  - Strongest AP RSSI—Indicates the strongest received signal strength indicator in dBm.
  - No. of Rogue Clients—Indicates the number of rogue clients associated to this access point.
  - Created—Indicates when the alarm event was created.
  - Modified—Indicates when the alarm event was modified.
  - Generated By—Indicates how the alarm event was generated.
  - Severity—The severity of the alarm: Critical, Major, Minor, Clear. Color coded.
  - Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear. Color coded
- Annotations—Enter any new notes in this box and click Add to update the alarm.
- Message—Displays descriptive information about the alarm.
- Help—Displays the latest information about the alarm.
- Event History—Click to access the Monitor Alarms > Events page.

- Annotations—Lists existing notes for this alarm.

Detecting Access Points

Click a Rogues alarm square in the Alarm Monitor (lower left-hand side of the screen) to access the Monitor Alarms > *failure object* page. In the Monitor Rogue AP Alarms page, click an item under Rogue MAC Address to access the Monitor Alarms > Rogue AP Details page, from the Select a command drop-down list choose Detecting APs, and click **GO** to access this page.

Choose Monitor > Alarms, then click New Search in the left sidebar. Choose Severity > All Severities and Alarm Category > Rogue AP, and click Go to access Monitor Alarms > *failure object*.

In the Monitor Rogue AP Alarms page, click an item under Rogue MAC Address to access Monitor Alarms > Rogue AP Details. In the Monitor Alarms > Rogue *vendor:MACaddr* page, from the Select a command drop-down list, choose Detecting APs to access this page.

This page enables you to view information about the Cisco lightweight access points that are detecting a rogue access point.

Click a list item to display data about that item:

- AP Name
- Radio
- Map Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio.
- Channel Number—Which channel the rogue access point is broadcasting on.
- WEP—Enabled or disabled.
- WPA—Enabled or disabled.
- Pre-Amble—Long or short.
- RSSI—Received signal strength indicator in dBm.
- SNR—Signal-to-noise ratio.
- Containment Type—Type of containment applied from this access point.

Containment Channels—Channels that this access point is currently containing.

Monitoring Rogue Adhoc Alarms

The Rogue Adhoc Alarms page displays alarm events for rogue adhocs.

To access the Rogue Adhoc Alarms page, do one of the following:

- Choose **Monitor > Alarms**. From the left sidebar, click **New Search** and select **Rogue Adhoc** from the **Alarm Category** drop-down menu. Click **GO** to display the matching alarms.
- Choose **Monitor > Security**. From the left sidebar, click **Rogue Adhocs**.

Note If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

Table B-2 describes the parameters found on the rogue adhoc alarms page.

Table B-2 Rogue Adhoc Alarms

Parameter	Description
Check box	Select the alarms on which you want to take action.
Severity	The severity of the alarm: Critical, Major, Minor, Clear. Color coded.
Rogue Adhoc MAC Address	Media Access Control address of the rogue adhoc.
Vendor	Rogue adhoc vendor name, or Unknown.
Classification Type	Malicious, Friendly, or Unclassified.
Radio Type	Indicates the radio type for this rogue adhoc.
Strongest AP RSSI	Indicates the strongest received signal strength indicator in dBm.
No. of Rogue Clients	Indicates the number of rogue clients associated to this rogue adhoc.
Owner	Indicates the ‘owner’ of the rogue adhoc.
Date/Time	Date and time the alarm occurred.
State	State of the alarm: Alert, Known or Removed.
SSID	Service Set Identifier being broadcast by the rogue adhoc radio. (Blank if SSID is not broadcast.)
Map Location	Indicates the map location for this rogue adhoc.
Acknowledged	Displays whether or not the alarm is acknowledged by the user.

Select a Command

Select one or more alarms by checking their respective check boxes, select one of the following commands from the **Select a Command** drop-down menu, and click **GO**.

- Assign to me—Assign the selected alarm(s) to the current user.
- Unassign—Unassign the selected alarm(s).
- Delete—Delete the selected alarm(s).
- Clear—Clear the selected alarm(s).
- Clear—Clear the selected alarm.
- Acknowledge—Acknowledge the alarm to prevent it from showing up in the Alarm Summary window.

Note The alarm remains in WCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the **All Alarms > Email Notification** page to view and configure email notifications.
- Detecting APs—View the Cisco Aironet 1000 Series lightweight access points that are currently detecting the rogue adhoc. See Detecting Access Points for more information.
- Map (High Resolution)—Click to display a high-resolution map of the rogue adhoc location.

- Rogue Clients—Click to view a list of rogue clients associated with this rogue adhoc. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the Rogue adhoc.
- Set State to ‘Alert’—Choose this command to tag the rogue adhoc as the lowest threat, continue monitoring the rogue access point, and to turn off Containment.
- Set State to ‘Internal’—Choose this command to tag the rogue adhoc as internal, add it to the Known Rogue APs list, and to turn off Containment.
- Set State to ‘External’—Choose this command to tag the rogue adhoc as external, add it to the Known Rogue APs list, and to turn off Containment.
- 1 AP Containment—Target the rogue adhoc for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue adhoc for containment by two Cisco Aironet 1000 Series lightweight access points.
- 3 AP Containment—Target the rogue adhoc for containment by three Cisco Aironet 1000 Series lightweight access points.
- 4 AP Containment—Target the rogue adhoc for containment by four Cisco Aironet 1000 Series lightweight access points. (Highest containment level.)

Caution Attempting to contain a rogue adhoc may lead to legal consequences. When you select any of the AP Containment commands and click GO, a message `“Containing a Rogue AP may have legal consequences. Do you want to continue?”` appears. Click **OK** if you are sure or click **Cancel** if you do not wish to contain any access points.

Monitoring Rogue Adhoc Details

Alarm event details for each Rogue adhoc are available from the Rogue Adhoc Alarms page.

To view alarm events for a rogue adhoc radio, follow these steps:

Step 1 From the Rogue Adhoc Alarms page, click an item under **Rogue MAC Address**.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by Cisco Aironet 1000 Series lightweight access points. The following information is available:

- General—
  - Rogue MAC Address—Media Access Control address of the rogue adhoc.
  - Vendor—Rogue adhoc vendor name or Unknown.
  - On Network—Indicates whether or not the rogue adhoc is located on the network.
  - Owner—Indicates the owner or left blank.
  - Acknowledged—Indicates whether or not the alarm is acknowledged by the user.
  - Classification Type—Malicious, Friendly, or Unclassified.
  - State—Indicates the state of the alarm: Alert, Known, or Removed.
  - SSID—Service Set Identifier being broadcast by the rogue adhoc radio. (Blank if SSID is not broadcast.)
  - Channel Number—Indicates the channel of the rogue adhoc.

  - Containment Level—Indicates the containment level of the rogue adhoc or Unassigned.
  - Radio Type—Indicates the radio type for this rogue adhoc.
  - Strongest AP RSSI—Indicates the strongest received signal strength indicator in dBm.
  - No. of Rogue Clients—Indicates the number of rogue clients associated to this adhoc.
  - Created—Indicates when the alarm event was created.
  - Modified—Indicates when the alarm event was modified.
  - Generated By—Indicates how the alarm event was generated.
  - Severity—The severity of the alarm: Critical, Major, Minor, Clear. Color coded.
  - Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear. Color coded.
- **Annotations—**Enter any new notes in this box and click **Add** to update the alarm.
- **Message—**Displays descriptive information about the alarm.
- **Help—**Displays the latest information about the alarm.
- **Event History—**Click to access the Monitoring Events page.
- **Annotations—**Lists existing notes for this alarm.

Select a Command

Select one or more alarms by checking their respective check boxes, selecting one of the following commands, and clicking **GO**.

- Assign to me—Assign the selected alarm to the current user.
- Unassign—Unassign the selected alarm.
- Delete—Delete the selected alarm.
- Clear—Clear the selected alarm.
- Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary window. The alarm remains in WCS and you can search for all Acknowledged alarms using the alarm search functionality.
- Unacknowledge—You can choose to unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the **All Alarms > Email Notification** page to view and configure email notifications.
- Detecting APs—View the Cisco Aironet 1000 Series lightweight access points that are currently detecting the rogue adhoc. See Detecting Access Points for more information.
- Map (High Resolution)—Click to display a high-resolution map of the rogue adhoc location.
- Rogue Clients—Click to view a list of rogue clients associated with this rogue adhoc. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the Rogue adhoc.
- Set State to 'Alert'—Choose this command to tag the rogue adhoc as the lowest threat, continue monitoring the rogue adhoc, and to turn off Containment.
- Set State to 'Internal'—Choose this command to tag the rogue adhoc as internal, add it to the Known Rogue APs list, and to turn off Containment.

- Set State to 'External'—Choose this command to tag the rogue access point as external, add it to the Known Rogue APs list, and to turn off Containment.
- 1 AP Containment—Target the rogue adhoc for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue adhoc for containment by two Cisco Aironet 1000 Series lightweight access points.
- 3 AP Containment—Target the rogue adhoc for containment by three Cisco Aironet 1000 Series lightweight access points.
- 4 AP Containment—Target the rogue adhoc for containment by four Cisco Aironet 1000 Series lightweight access points. (Highest containment level.)

Monitoring Events

Click a Rogues alarm square in the Alarm Monitor (lower left-hand side of the screen), click a list item under Rogue MAC Addresses, from the Select a command drop-down list choose Event History, and click GO to access this page.

Choose Monitor > Alarms and then click New Search in the left sidebar. Choose Severity > All Severities and Alarm Category > Rogue AP, and click Go to access the Monitor Alarms > *failure object* page. Click an item under the Rogue MAC Address to display the Monitor Alarms > Rogue AP Details page. From the Select a command drop-down list choose Event History, and click GO to access this page.

This page enables you to review information about rogue alarm events. Events list the sequence of occurrences for an element(s) over a period of time.

Click the title of each column to reorder the listings:

- Severity—Color coded display of the severity of the event.
- Rogue MAC Address—Click a list item to display information about the entry.
- Vendor—Name of rogue access point manufacturer.
- Type—AP or AD-HOC.
- On Network—Whether or not the rogue access point is on the same subnet as the associated Port.
- On 802.11a—Whether or not the rogue access point is broadcasting on the 802.11a band.
- On 802.11b—Whether or not the rogue access point is broadcasting on the 802.11b/802.11g band.
- Date/Time—Date and time of the alarm.
- Classification Type—Malicious, Friendly, or Unclassified
- State—State of the alarm, such as Alert and Removed.
- SSID—Service Set Identifier being broadcast by the rogue access point radio.

Monitoring Rogue Clients

Choose Monitor > Alarms and then click New Search in the left sidebar. Choose Severity > All Severities and Alarm Category > Rogue AP, and click GO to access the Monitor Alarms > *failure object* page. Click an item under the Rogue MAC Address to display the Monitor Alarms > Rogue AP Details page. From the Select a command drop-down list, choose Rogue Clients to access this page.

This page enables you to view information about clients that have associated with the rogue access point.

- Client MAC Address—Media Access Control address of the rogue access point client.
- Last Heard—The last time a Cisco access point detected the rogue access point client.
- Status—Status of the rogue access point client.

Configuring Controllers

- Configuring Rogue Policies
- Configuring Rogue AP Rules

Configuring Rogue Policies

This page enables you to set up policies for rogue access points.

To access the Rogue Policies page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address under the IP Address column.

Step 3 From the left sidebar menu, select **Security > Rogue Policies**.

- Rogue Location Discovery Protocol—Enabled, Disabled.
- Rogue APs
  - Expiration Timeout for Rogue AP Entries (seconds)—1 - 3600 seconds (1200 default).
- Rogue Clients
  - Validate rogue clients against AAA (check box)—Enabled, Disabled.
  - Detect and report Adhoc networks (check box)—Enabled, Disabled.

Command Buttons

- **Save**—Save the changes made to the client exclusion policies and return to the previous window.
- **Audit**—Compare the WCS values with those used on the controller.

Configuring Rogue AP Rules

This page enables you to view and edit current Rogue AP Rules.

To access the Rogue AP Rules page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address under the IP Address column.

Step 3 From the left sidebar menu, select **Security > Rogue AP Rules**. The Rogue AP Rules displays the Rogue AP Rules, the rule types (Malicious or Friendly), and the rule sequence.

Step 4 Select a Rogue AP Rule to view or edit its details. See Configuring Rogue AP Rules for more information.

Configuring Controller Templates

- Configuring Rogue Policies
- Configuring Rogue AP Rules
- Configuring Rogue AP Rule Groups

Configuring Rogue Policies

This window enables you to configure the rogue policy template (for access points and clients) applied to the controller.

To view current templates and the number of controllers to which they are applied, choose **Configure > Controller Templates > Security > Rogue Policies**.

To create a new rogue policy template, follow these steps:

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Rogue Policies**.

Step 3 From the **Select a command** drop-down menu, click **Add Template**.

Step 4 Click **GO**.

Note To make modifications to an existing rogue policy template or to apply a current template to controllers, choose **Configure > Controller Templates > Security > Rogue Policies** and click a template name in the **Template Name** column. Make the necessary changes to the template and click **Save** or **Apply to Controllers**.

Step 5 Select the **Rogue Location Discovery Protocol** check box to enable it. Rogue Location Discovery Protocol (RLDP) determines whether or not the rogue is connected to the enterprise wired network.

Note With RLDP, the controller instructs a managed access point to associate with the rogue access point and send a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points that do not have encryption enabled.

Step 6 Set the expiration timeout (in seconds) for rogue access point entries.

Step 7 Check the **Validate rogue clients against AAA** check box to enable the AAA validation of rogue clients.

Step 8 Check the **Detect and report Adhoc networks** check box to enable detection and reporting of rogue clients participating in adhoc networking.

Step 9 Click **Save**.

Command Buttons

- Save—Click to save the current template.
- Apply to Controllers—Click to apply the current template to controllers. From the **Apply to Controllers** screen, select the applicable controllers and click **OK**.
- Delete—Click to delete the current template. If the template is currently applied to controllers, click **OK** to confirm that you want to remove the template from the selected controllers to which it is applied.
- Cancel—Click to cancel the current template creation or changes to the current template.

Configuring Rogue AP Rules

Rogue AP Rules allow you to define rules to automatically classify rogue access points. WCS applies the rogue access point classification rules to the controllers. These rules can limit a rogue's appearance on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

Note Rogue AP Rules also help reduce false alarms.

To view current classification rule templates, rule type, and the number of controllers to which they are applied, choose **Configure > Controller Templates > Security > Rogue AP Rules**.

Note Rogue classes include the following types:
Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category.
Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.
Unclassified Rogue—A detected access point that does not match the Malicious or Friendly rules.

To create a new classification rule template for rogue access points, follow these steps:

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Rogue AP Rules**

Step 3 From the **Select a command** drop-down menu, click **Add Classification Rule**.

Step 4 Click **GO**.

Note To make modifications to an existing Rogue AP Rules template or to apply a current template to controllers, choose **Configure > Controller Templates > Security > Rogue AP Rules** and click a template name in the **Template Name** column. Make the necessary changes to the template and click **Save** or **Apply to Controllers**.

Step 5 Enter the following parameters:

- General–
  - Rule Name—Enter a name for the rule in the text box.
  - Rule Type—Select **Malicious** or **Friendly** from the drop-down menu.

Note Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category.
Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.

  - Match Type—Select **Match All Conditions** or **Match Any Condition** from the drop-down menu.
- Malicious Rogue Classification Rule
  - Open Authentication—Select the check box to enable Open Authentication.
  - Match Managed AP SSID—Select the check box to enable the matching of Managed AP SSID.

Note Managed SSID are the SSIDs configured for the WLAN and is known to the system.

  - Match User Configured SSID—Select the check box to enable the matching of User Configured SSID.

Note User Configured SSID are the SSIDs that are manually added. Enter the User Configured SSIDs (one per line) in the text box below **Match User Configured SSID**.

  - Minimum RSSI—Select the check box to enable the Minimum RSSI threshold limit.

Note Enter the minimum RSSI threshold level (dB) in the text box. The detected access point is classified as malicious if it is detected above the indicated RSSI threshold.

  - Time Duration—Select the check box to enable the Time Duration limit.

Note Enter the time duration limit (in seconds) in the text box. The detected access point is classified as malicious if it is viewed for a longer period of time than the indicated time limit.

  - Minimum Number Rogue Clients—Select the check box to enable the Minimum Number Rogue Clients limit.

Note Enter the minimum number of rogue clients allowed. The detected access point is classified as malicious if the number of clients associated to the detected access point is greater than or equal to the indicated value.

Step 6 Click **Save** to save the Rogue AP Rules template or **Cancel** to exit the screen without saving the template.

Command Buttons

- Save—Click to save the current template.
- Apply to Controllers—Click to apply the current template to controllers. From the **Apply to Controllers** screen, select the applicable controllers and click **OK**.
- Delete—Click to delete the current template. If the template is currently applied to controllers, click **OK** to confirm that you want to remove the template from the selected controllers to which it is applied.
- Cancel—Click to cancel the current template creation or changes to the current template.

Configuring Rogue AP Rule Groups

A Rogue AP Rule Group template allows you to combine more than one rogue AP rule to apply to controllers.

To view current Rogue AP Rule Group templates, choose **Configure > Controller Templates > Security > Rogue AP Rule Groups**.

To create a new Rogue AP Rule Groups template, follow these steps:

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Rogue AP Rule Groups**.

Step 3 From the **Select a command** drop-down menu, click **Add Rogue Rule Group**.

Step 4 Click **GO**.

Note To make modifications to an existing rogue policy template or to apply a current template to controllers, choose **Configure > Controller Templates > Security > Rogue AP Rule Groups** and click a template name in the **Template Name** column. Make the necessary changes to the template and click **Save** or **Apply to Controllers**.

Step 5 Enter the following parameters:

- General
  - Rule Group Name—Enter a name for the rule group in the text box.

Step 6 To add a Rogue AP rule, click to highlight the rule in the left column. Click **Add** to move the rule to the right column.

Note Rogue AP rules can be added from the ***Rogue AP Rules*** section. See Configuring Rogue AP Rules for more information.

Step 7 To remove a Rogue AP rule, click to highlight the rule in the right column. Click **Remove** to move the rule to the left column.

Step 8 Use the **Move Up/Move Down** buttons to specify the order in which the rules apply. Highlight the desired rule and click **Move Up** or **Move Down** to move it higher or lower in the current list.

Step 9 Click **Save** to confirm the Rogue AP rule list.

Step 10 Click **Cancel** to close the window without making any changes to the current list.

Note To view and edit the rules applied to a controller, choose **Configure > Controller** and click the controller name to open the controller.

APPENDIX C

Radio Resource Management

The operating system security solution uses the radio resource management (RRM) function to continuously monitor all nearby access points, automatically discover rogue access points, and locate them.

Radio Resource Management (RRM) is built into the Cisco Unified Wireless Network monitors and dynamically corrects performance issues found in the RF environment.

- "RRM Dashboard" section on page C-2
- "Configuring Controllers" section on page C-5
- "Configuring Controller Templates" section on page C-6

RRM Dashboard

RRM automatically detects and configures new controllers and lightweight access points as they are added to the network. It then automatically adjusts associated and nearby lightweight access points to optimize coverage and capacity.

Lightweight access points can simultaneously scan all valid 802.11a/b/g channels for the country of operation as well as for channels available in other locations. The access points go “off-channel” for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

Note In the presences of voice traffic (in the last 100 ms), the access points defer off-channel measurements and do not change channels.

Each access point spends only 0.2 percent of its time off-channel. This activity is distributed across all access points so that adjacent access points are not scanning at the same time, which could adversely affect wireless LAN performance. In this way, administrators gain the perspective of every access point, thereby increasing network visibility.

Cisco WCS provides a snapshot of Radio Resource Management (RRM) statistics to help identify trouble spots and possible reasons for channel or power level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on grouping the events together (access point performance, configuration mismatch between controllers in the same RF group, coverage holes that were detected by access points based on threshold, coverage holes that were detected by controllers, ratios of access points operating at maximum power, and so on).

Note The RRM dashboard information is only available for CAPWAP access points.

Channel Change Notifications

Two adjacent access points on the same channel can cause either signal contention or signal collision. In the case of a collision, data is simply not received by the access point. This functionality can become a problem, for example, when someone reading e-mail in a cafe affects the performance of the access point in a neighboring business. Even though these are completely separate networks, someone sending traffic to the cafe on channel 1 can disrupt communication in an enterprise using the same channel. Controllers address this problem by dynamically allocating access point channel assignments to avoid conflict and to increase capacity and performance. Channels are “reused” to avoid wasting scarce RF resources. In other words, channel 1 is allocated to a difference access point far from the cafe, which is more effective than not using channel 1 altogether.

The controller’s dynamic channel assignment (DCA) capabilities are also useful in minimizing adjacent channel interference between access points. For example, two overlapping channels in the 802.11b/g band, such as 1 and 2, cannot both simultaneously use 11/54 Mb/s. By effectively reassigning channels, the controller keeps adjacent channels separated, thereby avoiding this problem.

Notifications are sent to the WCS RRM dashboard when a channel change occurs. Channel changes depend on the dynamic channel assignment (DCA) configuration where the mode can be set to auto or on demand. When the mode is *auto*, channel assignment is periodically updated for all CAPWAP access points which permit this operation. When the mode is set to *on demand*, channel assignments are updated based upon request. If the DCA is static, no dynamic channel assignments occur, and values are set to their global default.

DCA supports 802.11n 40-MHz channels in the 5-GHz band. 40-MHz channelization allows radios to achieve higher instantaneous data rates (potentially 2.25 times higher than 20-MHz channels.) You can choose between DCA working at 20 or 40 MHz.

Note Radios using 40-MHz channelization in the 2.4-GHz band are not supported by DCA.

When a channel change trap is received and a channel change had occurred earlier, the event is marked as Channel Revised; otherwise, the event is marked as Channel Changed. Each event for channel change can be caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur. For example, suppose a channel change is caused by signal, interference, or noise. When the reason code is received in the notification, the reason code is refactored across the reasons. If three reasons caused the event to occur, the reason code is refactored to 1/3 or 0.33 per reason. If ten channel change events are received with the same reason code, all of the three reasons are equally factored to determine the cause of the channel change.

Transmission Power Change Notifications

The controller dynamically controls access point transmit power based on real0time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the access points' transmit power according to how the access points are seen by their third strongest neighbor.

The transmit power control algorithm only reduces an access point's power. However, the coverage hole algorithm can increase access point power, thereby filling a coverage hole. For example, if a failed access point is detected, the coverage hole algorithm can automatically increase power on surrounding access points to fill the gap created by the loss in coverage.

Notifications are sent to the WCS RRM dashboard when transmission power changes occur. Each event for transmit power changes is caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur.

RF Grouping Notifications

When RRM is run on the controller, dynamic grouping is done, and a new group leader is chosen. Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs, and each switch optimizes only its own CAPWAP access point parameters. When the grouping is on, switches form groups and elect leaders to perform better dynamic parameter optimization. With grouping on, configured intervals (in seconds) represent the period with which the grouping algorithm is run. (Grouping algorithms also run when the group contents change and automatic grouping is enabled.)

Viewing the RRM Dashboard

The RRM dashboard is accessed by choosing **Monitor > RRM**.

The dashboard is made up of the following parts:

- The RRM Statistics portion shows network-wide statistics
- The Channel Change Reason portion shows why channels changed for all 802.11a/b/g/n radios.
- The Channel Change shows all events complete with causes.
- The Configuration Mismatch portion shows comparisons between the leaders and members.
- The Coverage Hole portion rates how severe the coverage holes are and gives their location.
- The Percent Time at Maximum Power shows what percent of time the access points were at maximum power and gives the location of those access points.

The following statistics are displayed:

- Total Channel Changes—The sum total of channel changes across 802.11a/b/g/n radios, irrespective of whether the channel was updated or revised. The count is split over a 24-hour and 7-day period. If you click the percentages link or the link under the 24-hour column, a screen with details for that access point only appears.
- Total Configuration Mismatches—The total number of configuration mismatches detected over a 24-hour.
- Total Coverage Hole Events—The total number of coverage hole events over a 24-hour and 7-day period.
- Number of RF Groups—The total number of RF groups currently managed by WCS.
- Configuration Mismatch—The configuration mismatch over a 24-hour period by RF group with details on the group leader.
- Percent of APs at MAX Power—The percentage of access points with 802.11a/n radios as a total percentage across all access points which are at maximum power. The maximum power levels are preset and are derived with reference to the present maximum power of the access point.

Note Maximum power is shown in three areas of the RRM dashboard. This maximum power portion shows the current value and is poll driven.

- Channel Change Causes—A graphical bar chart for 802.11a/n radios. The chart is factored based on the reason for channel change. The chart is divided into two parts, each depicting the percentage of weighted reasons causing the event to occur over a 24-hour and 7-day period. Each event for channel change can be caused by multiple reasons, and the weight is equally divided across these reasons. The net reason code is factored and equated to one irrespective of the number of reasons for the event to occur.
- Channel Change APs—Each event for channel change includes the MAC address of the CAPWAP access point. For each reason code, you are given the most channel changes that occurred for the 802.11a/n access point based on the weighted reason for channel events. This count is split over a 24-hour and 7-day period.
- Coverage Hole Events APs—The top five access points filtered by IF Type 11 a/n which triggered a coverage hole event are displayed.
- Aggregated Percent Max Power APs—A graphical progressive chart of the total percentage of 802.11a/n CAPWAP access points which are operating at maximum power to accommodate coverage holes and events. The count is split over a 24-hour and 7-day period.

Note This maximum power portion shows the values from the last 24 hours and is poll driven. The power is polled every 15 minutes or as configured for radio performance.

- Percent Time at Maximum Power—A list of the top five 802.11a/n CAPWAP access points which have been operating at maximum power.

Note This maximum power portion shows the value from the last 24 hours and is only event driven.

Configuring Controllers

Configuring an RRM Threshold Controller (for 802.11a/n or 802.11b/g/n)

To configure an 802.11a/n or 802.11b/g/n RRM threshold controller, follow these steps.

Step 1 Choose **Configure > Controller**.

Step 2 Click the **IP address** of the appropriate controller to open the **Controller Properties** page.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM Thresholds** or **802.11b/g/n > RRM Thresholds**.

Step 4 Make any necessary changes to Coverage Thresholds, Load Thresholds, Other Thresholds, and Noise/Interference/Rogue Monitoring Channels.

Note When the Coverage Thresholds Min SNR Level (dB) parameter is adjusted, the value of the Signal Strength (dB) automatically reflects this change. The Signal Strength (dB) parameter provides information regarding what the target range of coverage thresholds is when adjusting the SNR value.

Step 5 Click **Save**.

Configuring 40-MHz Channel Bonding

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.

Note Choosing a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments.

To configure 802.11 a/n RRM DCA channels for an individual controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM DCA**. The 802.11a/n RRM DCA window appears.

> **Note** You can also configure the channel width on the access point page by choosing **Configure > Access Points** and clicking the **802.11a/n** link in the Radio column. The Current RF Channel Assignment. is provided, and you can choose a Global assignment method or choose Custom to specify a channel.

Step 4 From the Channel Width drop-down menu, choose **20 MHz** or **40 MHz**.

> **Note** Be cautious about deploying a mix of 20-MHz and 40-MHz devices. The 40-MHz devices have slightly different channel access rules which may negatively impact the 20-MHz devices.

> **Note** To view the channel width for an access point's radio, go to **Monitor > Access Points > <name> > Interfaces** tab. You can also view the channel width and antenna selections by choosing **Configure > Access Points** and clicking on the desired radio in the Radio column.

Step 5 Choose the check box(es) for the applicable DCA channel(s). The selected channels are listed in the **Selected DCA channels** text box.

Step 6 Click **Save**.

Configuring Controller Templates

Configuring an RRM Threshold Template for 802.11a/n or 802.11b/g/n

To add a new 802.11a/n or 802.11b/g/n RRM threshold template or make modifications to an existing template, follow these steps:

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **802.11a/n > RRM Thresholds** or **802.11b/g/n > RRM Thresholds**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO.** To make modifications to an existing template, click to select a template name in the Template Name column. The 802.11a/n or 802.11b/g/n RRM Thresholds Template appears and the number of controllers the template is applied to automatically populates.

Step 4 Enter the minimum number of failed clients that are currently associated with the controller.

Step 5 Enter the desired coverage level. When the measured coverage drops by the percentage configured in the coverage exception level, a coverage hole is generated.

Step 6 The Signal Strength (dBm) parameter shows the target range of coverage thresholds.

Step 7 Enter the maximum number of clients currently associated with the controller.

Step 8 At the RF Utilization parameter, enter the percentage of threshold for either 802.11a/n or 802.11b/g/n.

Step 9 Enter an interference threshold.

Step 10 Enter a noise threshold between -127 and 0 dBm. When outside of this threshold, the controller sends an alarm to WCS.

Step 11 Enter the coverage exception level percentage. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole is generated.

Step 12 At the Channel List drop-down menu in the Noise/Interference/Rogue Monitoring Channels section, choose between all channels, country channels, or DCA channels based on the level of monitoring you want. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

Step 13 Click **Save**.

Configuring an RRM Interval Template (for 802.11a/n or 802.11b/g/n)

To add an 802.11a/n or 802.11b/g/n RRM interval template or make modifications to an existing template, follow these steps:

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **802.11a/n > RRM Intervals** or **802.11b/g/n > RRM Intervals**.

Step 3 To add a new template, choose **Add Template** from the Select a command drop-down menu and click **GO**. To make modifications to an existing template, click a template name from the Template Name column.

The 802.11a/n or 802.11b/g/n RRM Threshold Template appears and the number of controllers the template is applied to automatically populates.

Step 4 Enter at which interval you want strength measurements taken for each access point. The default is 300 seconds.

Step 5 Enter at which interval you want noise and interference measurements taken for each access point. The default is 300 seconds.

Step 6 Enter at which interval you want load measurements taken for each access point. The default is 300 seconds.

Step 7 Enter at which interval you want coverage measurements taken for each access point. The default is 300 seconds.

Step 8 Click **Save**.

INDEX