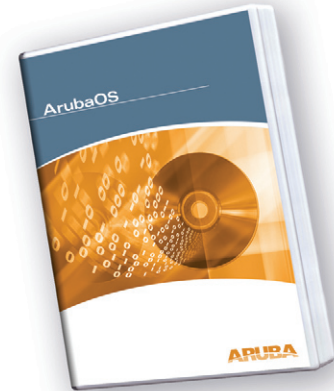


# ArubaOS Wireless Intrusion Protection (WIP)

Aruba's Wireless Intrusion Protection (WIP) module protects the mobile edge of the network against wireless threats to network security. By integrating wireless intrusion protection into the mobile edge infrastructure, the need for a separate system of RF sensors and security appliances is eliminated. The WIP module provides extraordinary capabilities to Aruba's enterprise mobility system, giving administrators visibility into the network, along with the power to thwart malicious wireless attacks, impersonations and unauthorized intrusions.



## ROGUE AP PREVENTION

Rogue AP classification and automatic containment

## DENIAL OF SERVICE (DoS) ATTACK DETECTION

- Management frame floods
- Deauthentication attacks
- Authentication floods
- Probe request floods
- Fake AP floods
- Null probe responses
- EAP handshake floods

## PROBING AND NETWORK DISCOVERY

Detection of NetStumbler and broadcast probes

## CLIENT INTRUSION PREVENTION

- Honeytrap AP protection
- Valid station protection

## NETWORK INTRUSION DETECTION

- Wireless bridges
- ASLEAP attacks

## SURVEILLANCE

Detection of weak encryption implementation

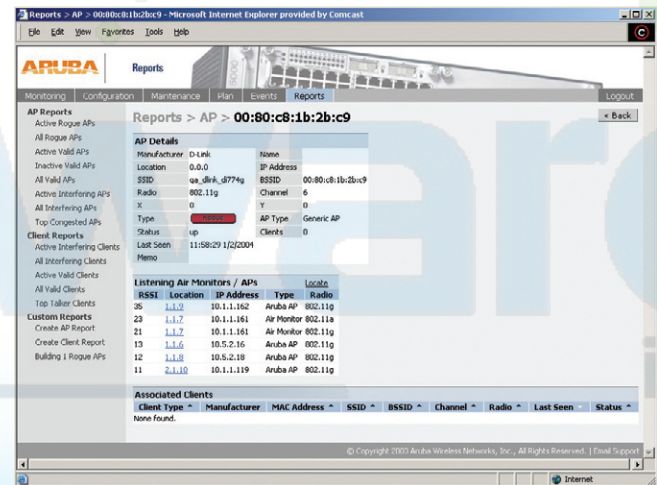
## IMPERSONATION DETECTION AND PREVENTION

- MAC address spoofing
- AP impersonations
- Man-in-the-middle attacks
- Sequence number anomaly detection

Detection alone is only the first step in securing the corporate environment from unwanted wireless access. Without adequate measures to quickly shut down intrusions, detection is almost worthless. Without accurate classification of APs and stations (e.g., valid, rogue, or neighbor), providing an automated response to possible intrusion is impossible.

Aruba access points constantly scan all channels of the RF spectrum, capturing all 802.11 traffic and locally examining the captured data. Only policy violations are sent to the central mobility controller to ensure minimal impact on wired network performance. While scanning the environment, the Aruba system learns about all wireless APs and stations and classifies these devices based on traffic flows seen on the wire and in the air. This traffic is collected and correlated on the mobility controller.

Aruba's WIP module provides both detection and prevention capabilities. Users and devices are detected and classified so administrators can react to both unintentional and malicious WLAN access. No other system on the market provides such capabilities.



Accurately detect and stop rogue access points.

## UNIQUE STATION AND USER CLASSIFICATION

Aruba's patent-pending classification system automatically identifies and classifies all APs and stations connected to the network. The system works by comparing traffic seen in the air with traffic seen on the wire. When a match is found, it is known with certainty that the device belongs to the local network rather than a neighboring network. This avoids false alarms for the administrator, because only true rogue devices are classified as such.

## DETECTING AND DISABLING ROGUE APs

Aruba's classification algorithms allow the system to accurately determine who is a threat and who is not. Once classified as rogue, these APs can be automatically disabled. Administrators are also notified of the presence of rogue devices, along with their precise physical location on a floorplan, so that they may be removed from the network.

## DENIAL OF SERVICE AND IMPERSONATION PROTECTION

Wireless networks, by their nature, make an attractive target for denial of service attacks. Such attacks include software that floods the network with association requests, attacks that make a laptop look like thousands of APs, and deauthentication floods. Aruba mobility controllers equipped with the ArubaOS WIP module maintain signatures of many different wireless attacks and are able to block them so service is not disrupted.

Advanced Denial of Service (DoS) protection keeps enterprises safe against a variety of wireless attacks, including association and de-authentication floods, honeypots and AP and station impersonations. Based on location signatures and client classification, Aruba access points will drop illegal requests and generate alerts to notify administrators of the attack.

## MAN-IN-THE-MIDDLE PROTECTION

One of the common attacks possible in wireless networks is the “man-in-the-middle” attack. During a man-in-the-middle attack, a hacker masquerades as a legitimate AP. Then, acting as a relay point, this man-in-the-middle fools users and other APs into sending data through the unauthorized device. An attacker can then modify or corrupt data or conduct password-cracking routines.

Aruba access points monitor the air to detect other wireless stations masquerading as valid APs. When such masquerading is detected, appropriate defense mechanisms are put into place. Aruba mobility controllers also track unique “signatures” for each wireless client in the network. If a new station is introduced claiming to be a particular client, but without the proper signature, a station impersonation attack is detected.

## POLICY DEFINITION AND ENFORCEMENT

The ArubaOS WIP module provides a number of policies that can be configured to take automatic action when a policy is violated. Examples of wireless policies include weak WEP implementation detection, AP misconfiguration protection, ad-hoc network detection and protection, unauthorized NIC type detection, wireless bridge detection and more.

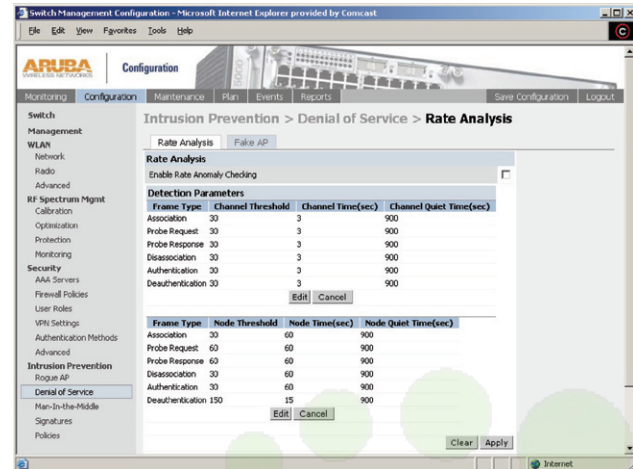
## USING WIRELESS TO PROTECT YOUR WIRED NETWORK

Even if wireless LANs are not sanctioned at this time, no security conscious company can afford to do nothing. Aruba's WIP will keep wireless traffic from working its way into the wired network through rogue APs unknowingly attached to a network port. With Aruba's mobility system equipped with WIP, the enterprise network is protected against wireless security holes. And when the enterprise is ready to deploy wireless LANs, the Aruba system can be easily reconfigured to provide a scalable and secure wireless LAN infrastructure.

## USING WIRELESS TO PROTECT YOUR EXISTING WIRELESS NETWORK

Aruba's mobility system with WIP delivers the detection and protection

necessary to keep your existing wireless network safe from undesirable wireless access. ArubaOS WIP complements and enhances any existing WLAN deployment, including Cisco deployments, by providing advanced RF security and control features not found in first-generation wireless products.



Wireless Intrusion Protection detects entire range of RF threats.

### FEATURE

Complete wireless intrusion detection and protection

Patent-pending wireless classification engine

Real-time remote monitoring and intrusion analysis

Centralized management

Programmable signature analysis

Upgradable and programmable WIP system

Flexible deployment options

### BENEFIT

- Protection against all known wireless threats in a single enterprise-class system.
- Uniquely categorizes wireless threats and enables automatic policy-based response.
- 24 x 7 protection without requiring network security staff at every location.
- WAN friendly - doesn't consume large amounts of bandwidth.
- Configure corporate WLAN policies globally with localized enforcement at each access point.
- Detect and protects against common network probing and attack tools such as Net Stumbler, Wellenreiter and AirJack.
- Quickly deliver protection against new attacks.
- Deploy Aruba WIP as an integrated part of the existing wireless environment or as an overlay to protect against wireless intrusions and rogue APs.