CWSP Guide to Wireless Security

Managing the Wireless Network

Objectives

- Describe the functions of a WLAN management system
- List the different types of probes that are used in monitoring the RF
- Explain how a wireless intrusion prevention system differs from a wireless intrusion detection system
- List the features of a WIPS

WLAN Management Systems

- Monitor the network
  - Used to be an important task
  - Network equipment has become:
    - More powerful, intelligent, significantly less expensive, and even self-monitoring
- Wireless network monitoring
  - Remains critical
  - Enables the network administrator or manager to:
    - Identify security threats
    - Verify compliance

WLAN Management Systems (continued)

- Wireless network monitoring (continued)
  - Enables the network administrator or manager to:
    - Monitor scarce bandwidth
    - Administer the shared wireless resource
    - Adjust for unpredictable wireless behavior
- Monitoring a WLAN can be accomplished via:
  - A standard network management protocol
  - A system specifically designed for wireless networks

WLAN Management Systems (continued)

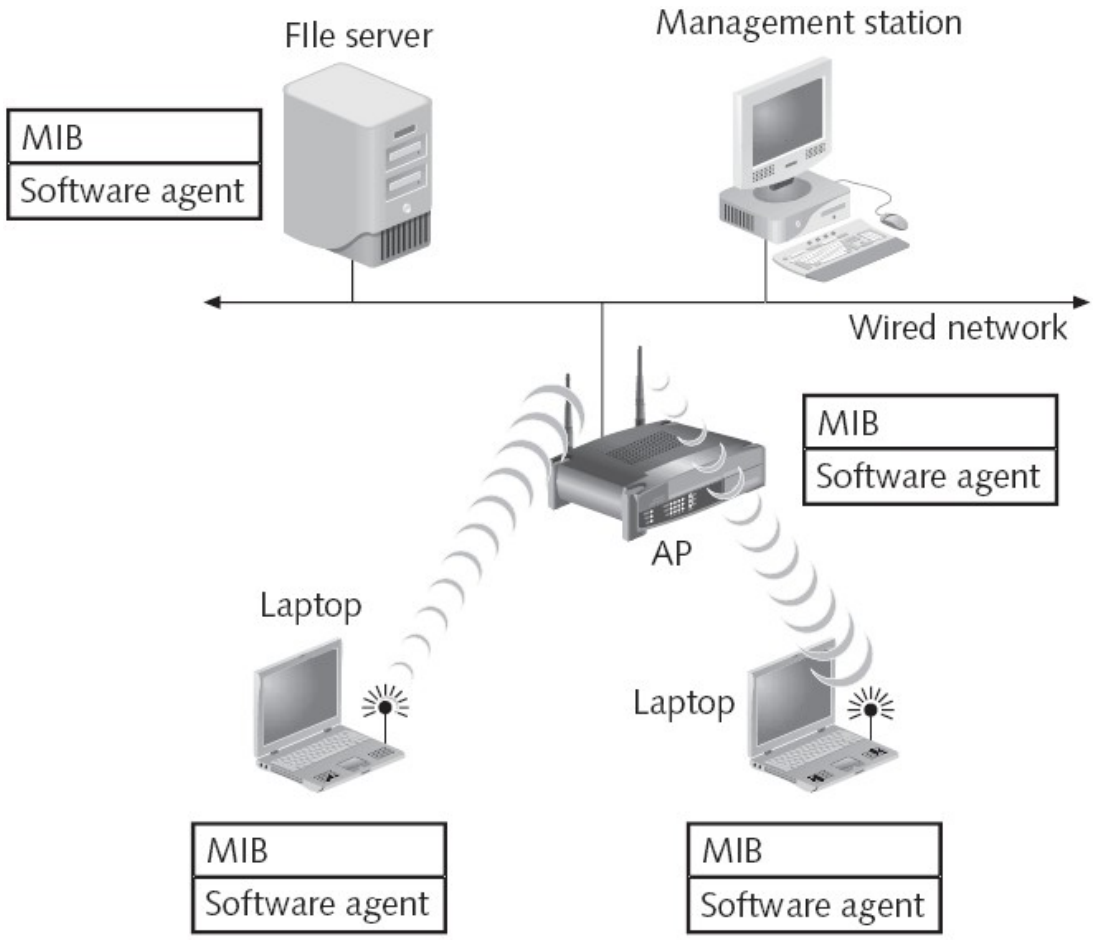

Figure 10-1 WLAN using SNMP

WLAN Management Systems (continued)

- Advantages of using SNMP for WLAN management
  - Ability to support a variety of different types of devices
  - Increased flexibility
  - Ease of expanding the network
  - Widespread popularity
- SNMP shortcomings
  - Wasting bandwidth by sending needless information
  - Complicated encoding rules
  - SNMP may not be quick enough

Discovery

- Identifies wireless devices that comprise the network
- Wireless device discovery
  - SNMP can send a request similar to a PING (Packet Internet Groper)
  - Software then listens for the response and logs that entry into the MIB
  - MIB can be queried to determine if that wireless device is part of the WLAN
  - Unapproved devices would not respond to SNMP requests

Discovery

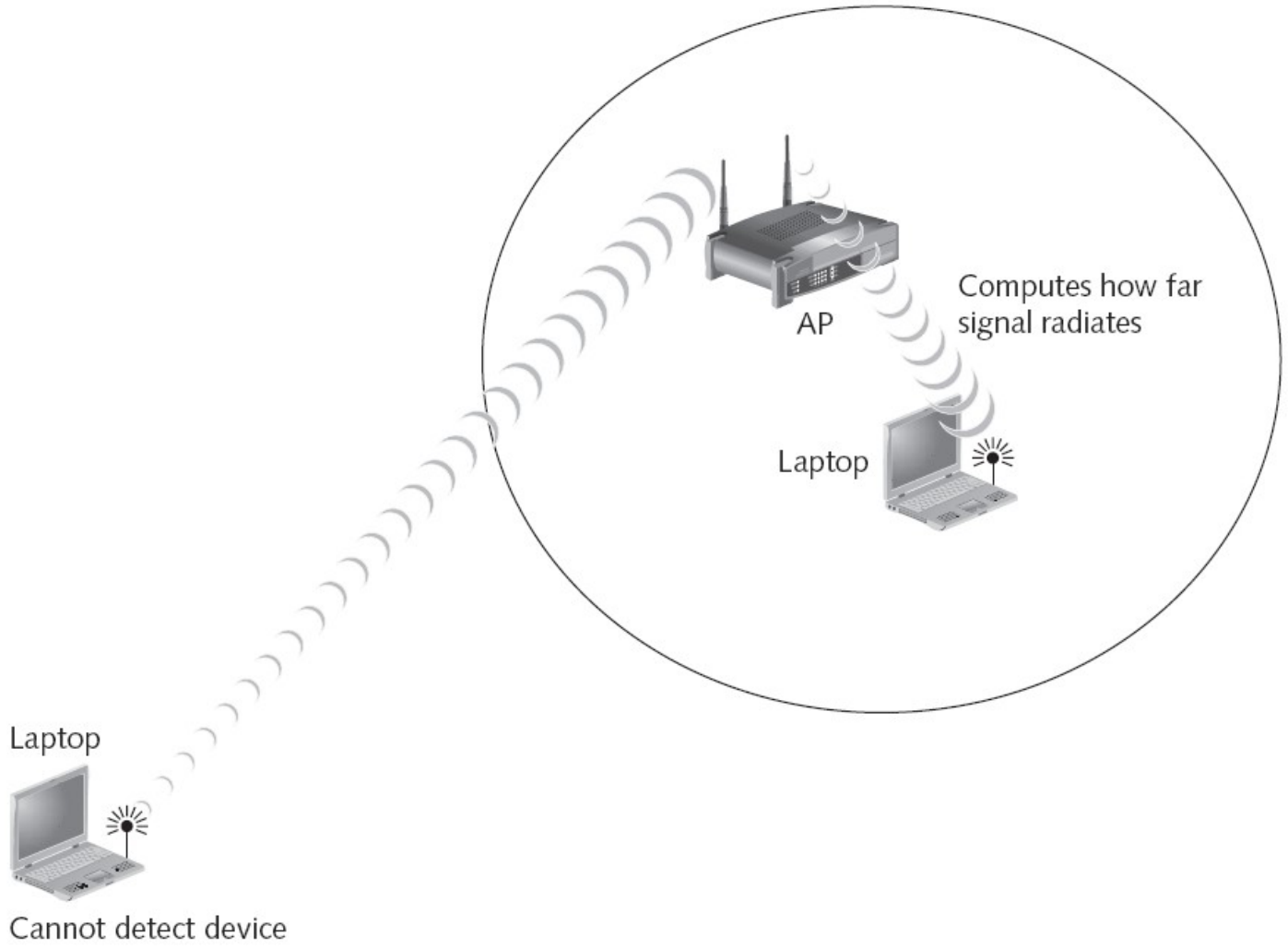

Figure 10-2 Nearest sensor method

Discovery (continued)

- Wireless device discovery (continued)
  - Nearest sensor method
    - Simplest and least precise method
    - First determines the access point to which a wireless device is associated
    - Assumes that this is the sensor closest to that device
    - Computes how far the RF signal radiates from that access point
    - Can locate a client to within a 900-meter area

Discovery (continued)

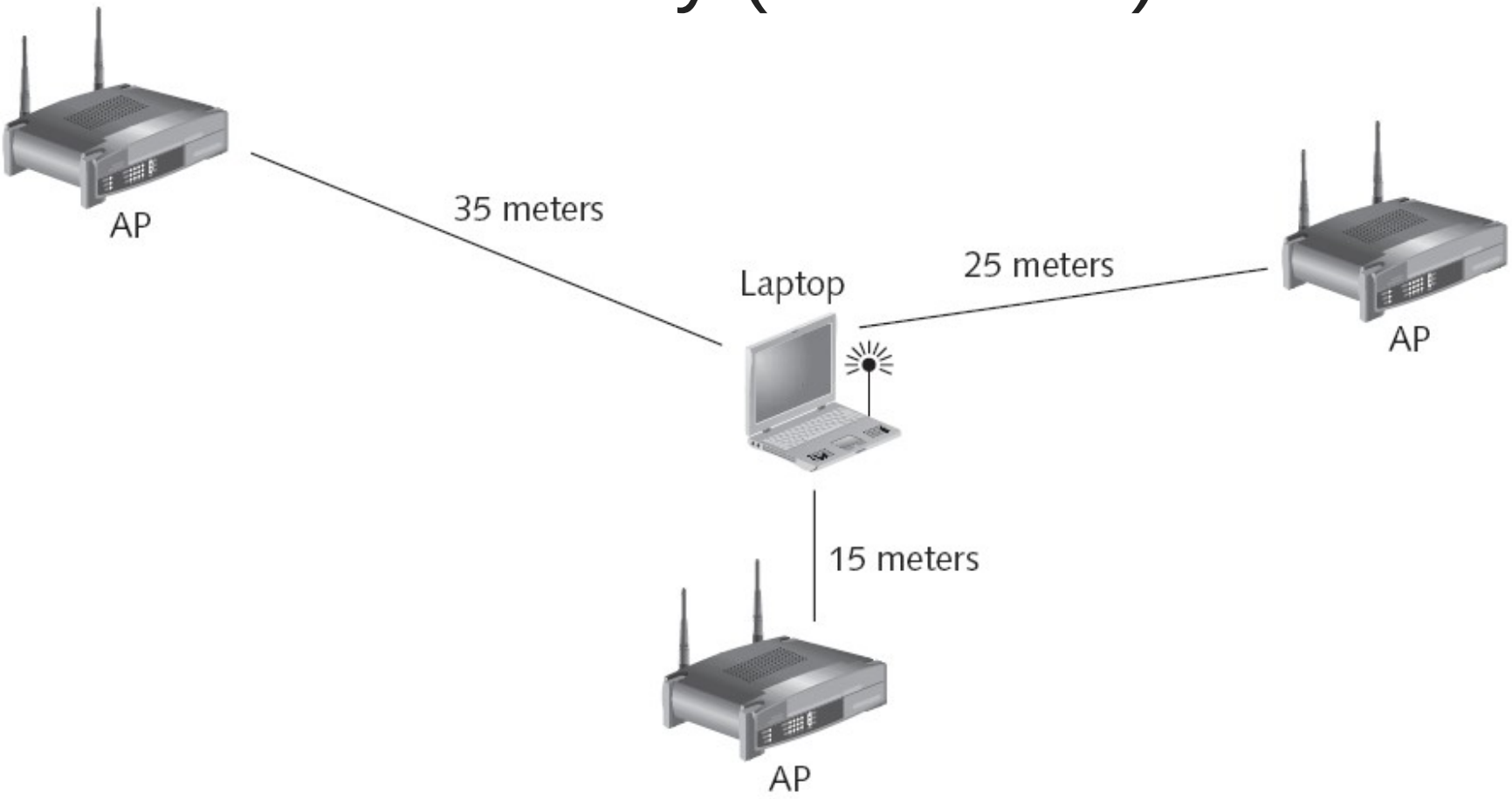

Figure 10-3 Trilateration

Discovery (continued)

- Wireless device discovery (continued)
  - Triangulation/trilateration methods
    - Combine measurements from various APs
    - Triangulation
      - Measures angles between three or more nearby APs
      - Where the measurements intersect, this can be used to calculate the location of the device
    - Trilateration
      - Measures the distance between three or more APs

Discovery (continued)

- Wireless device discovery (continued)
  - RF fingerprinting method
    - Uses intelligent algorithms to improve precision
      - By accounting for the environmental effects on the wireless signal itself (for example):
  - Received Signal Strength Indication (RSSI)
    - Signal that tells strength of incoming (received) signal
    - Can be used to measure the RF power loss between transmitter and receiver
      - To calculate the distance from the transmitting device to the receiver

Discovery (continued)

- Rogue access point discovery
  - Mobile sniffing audits
    - "Manually" audit the airwaves by using a wireless sniffer
      - Such as NetStumbler or AirMagnet
  - Wireless probes
    - Devices that can monitor the airwaves for traffic

Discovery (continued)

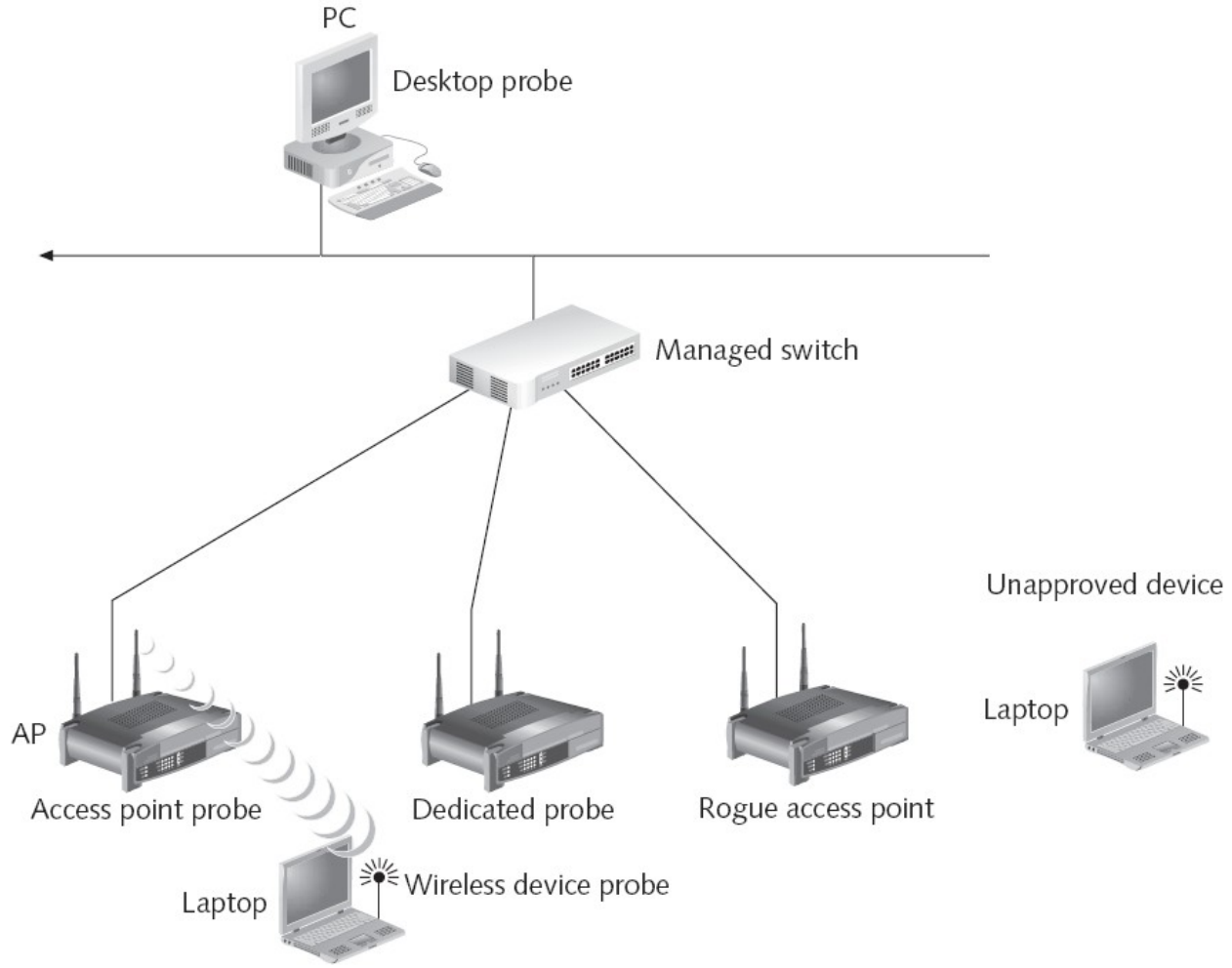

Figure 10-4 Wireless probes

Discovery (continued)

- Rogue access point discovery (continued)
  - Wireless probes (continued)
    - Wireless device probe
    - Desktop probe
    - Access point probe
    - Dedicated probe
  - Suspicious wireless signal information is sent to a centralized database
  - WLAN management system software compares it to a list of approved APs

Discovery (continued)

- Rogue access point discovery (continued)
  - Network management tools
    - Extend “wireless awareness” into key elements of the wired network
    - Example: Cisco Structured Wireless-Aware Network (SWAN)

Monitoring

- If SNMP is being used:
  - Monitoring focuses upon network performance
- Bandwidth utilization can be determined by:
  - Collecting statistics on the amount of data traffic that passes through an access point
- Performance monitoring can assess how often and quickly the device responds to a request
- SNMP trap
  - Spike in a network's bandwidth or a decrease in the time to respond to a request

Monitoring (continued)

- SNMP trap (continued)
  - Considered unreliable because the receiver does not send acknowledgments
- SNMP inform request
  - Acknowledges the message with an SNMP response
- Dedicated WLAN management systems
  - Provide similar capabilities
  - Designed to report specific wireless information
    - Traffic and utilization, data rates, channel usage, and errors rates

Configuration

- SNMP and WLAN management systems allow for configuration of the wireless APs
  - Through the network without the necessity of "touching" each device
- SNMP is only capable of a small number of configuration settings
- You can also "bulk" configure a group of access points with the same configurations
- Another aspect of configuration is upgrading the firmware of access points

Configuration (continued)

Table 10-1 Remote AP configuration settings

Access Point Setting	Description
SSID	Service set identifier for the access point
Allow broadcast SSID	Enable or disable AP to broadcast the SSID
Allow auto channel select	Enable or disable AP to auto select the channel
Channel	Specify the channel number at which the AP transmits
Name	Name of the access point
Use DHCP	Enable or disable DHCP mode
LAN IP	Set IP address of AP
Subnet Mask	Set network mask value
DNS server IP	Set IP address of the DNS server
WEP	Enable or disable WEP data encryption
802.1x	Enables user authentication with RADIUS server
WPA	Enable or disable WPA data encryption and authentication
Beacon period	Set rate for beacon frames
Receive Antenna Left Right Diversity	Set configuration for AP antennas

Wireless Intrusion Prevention System (WIPS)

- Integrates several layers of protection to detect and prevent malicious attacks

Intrusion Systems

- Intrusion system
  - Security management system
  - Compiles information from a computer network or individual computer
  - Analyzes to identify security vulnerabilities and attacks
  - Similar in nature to a firewall
  - Watches for systematic attacks and then takes specified action
  - Can also watch for any attacks that may originate from inside the network

Intrusion Systems (continued)

- Wireless intrusion detection system (WIDS)
  - Constantly monitors the radio frequency (using wireless probes) for attacks
  - If an attack is detected:
    - WIDS sends information but does not take any action
  - Technologies for WIDS
    - Signature detection
      - Compares the information to large databases of attack signatures
    - Anomaly detection
      - Monitors the normal activity of the wireless LAN and "learns" its normal characteristics

Intrusion Systems (continued)

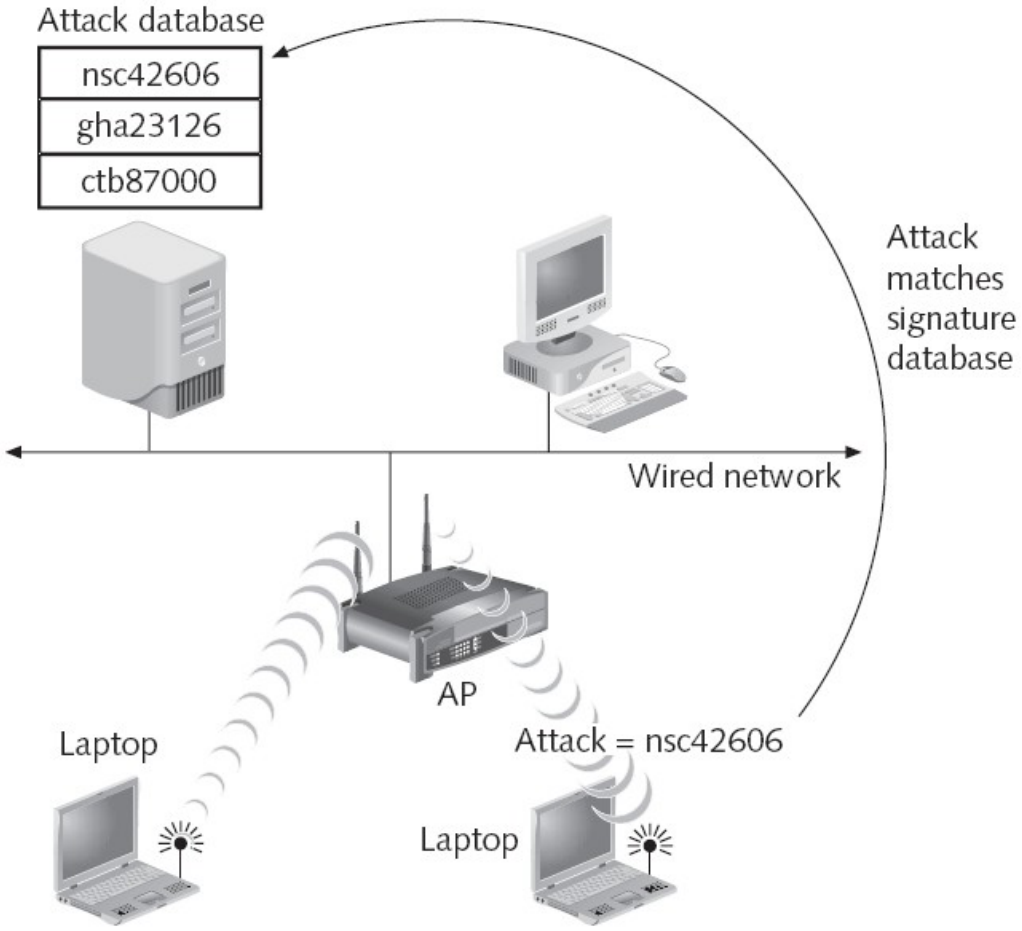

Figure 10-5 Signature detection WIDS

Intrusion Systems (continued)

- Wireless intrusion detection system (WIDS) (continued)
  - Anomaly detection
    - Security administrator defines baseline (normal state)
    - When creating the baseline observe the following tasks:
      - Measure the performance parameters under normal network conditions
      - Configure system to recognize all access points in the area as either authorized, monitored, or known
      - Be aware of any common false positives that may exist for a specific network configuration
    - Looks for variation (from the baseline)

Intrusion Systems (continued)

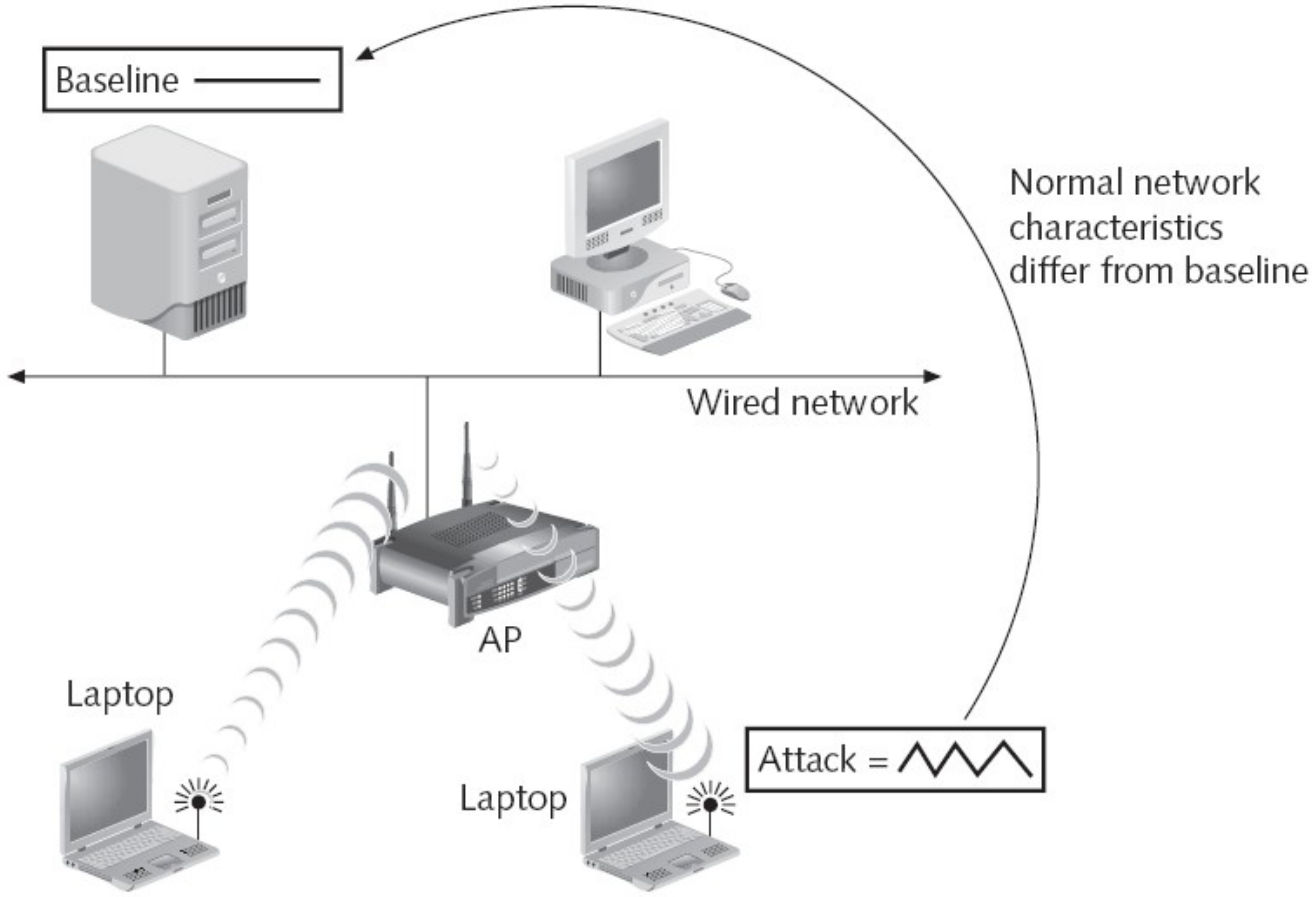

Figure 10-6 Anomaly detection WIDS

Intrusion Systems (continued)

- Wireless intrusion detection system (WIDS) (continued)
  - Disadvantages
    - Only issue alert
    - Alert after attack has started
    - Dependent upon signatures
    - High number of false positives
- Wireless intrusion prevention system (WIPS)
  - More proactive approach
  - Attempts to uncover and prevent an attack before it harms the WLAN

Intrusion Systems (continued)

- Wireless intrusion prevention system (WIPS) (continued)
  - Detects categories of attacks using predictable or deterministic techniques
    - May involve a combination of different approaches
  - Signatures are only used to provide additional details about the attack itself
- WIDS/WIPS Probes
  - Types of probes
    - Integrated
    - Overlay

Intrusion Systems (continued)

- WIDS/WIPS Probes (continued)
  - Integrated probes
    - Also called an access point probe or embedded probe
    - Use existing access points to monitor the RF
    - Drawbacks
      - Can negatively impact throughput
      - AP is not dedicated to watching for attacks
      - IEEE 802.11b/g AP cannot monitor IEEE 802.11a channels

Intrusion Systems (continued)

- WIDS/WIPS Probes (continued)
  - Overlay probe
    - Uses dedicated probes for scanning the RF for attacks
    - Results in higher costs
    - Does not impact WLAN throughput

Intrusion Systems (continued)

- WIDS/WIPS Probes (continued)
  - Overlay probe (continued)
    - Can scan more frequencies
    - Provides broader coverage
    - Detects more attacks
    - Can also be used to troubleshoot WLAN performance issues
    - Drawbacks
      - Requires additional user interfaces, consoles, and databases
      - Must have a list of authorized access points

WIPS Features

- AP identification and categorization
  - Ability to learn about the other access points that are in the area and classify those APs
  - Next, the APs can be tagged as to their status
    - Authorized AP
    - Known AP
    - Monitored AP
    - Rogue AP
- Device tracking
  - Involves the simultaneous tracking of all wireless devices within the WLAN

WIPS Features (continued)

- Device tracking (continued)
  - Used to identify unauthorized device
  - Other uses
    - Asset tracking of wireless equipment
    - Troubleshooting sources of wireless network interference
    - Conducting a site survey
    - Determining a wireless user's availability status based on location &
    - Finding an emergency Voice over WLAN (VoWLAN) telephone caller

WIPS Features (continued)

- Event action and notification
  - WIPS that identifies an attack must immediately and automatically block any malicious wireless activity
  - Once an attack is detected, the WIPS must notify security administrators
- RF scanning
  - All of the radio frequency spectrum must be scanned for potential attacks
- Protocol analysis
  - WIPS products offer remote packet capture and decode capabilities

WIPS Features (continued)

- Protocol analysis (continued)
  - WIPS can view WLAN network traffic to determine exactly what is happening on the network
    - And help determine what actions need to be taken

WIPS Features (continued)

Table 10-2 Features of WIPS

Attribute	Description
AP identification and categorization	All access points should be detected and automatically classified.
Device tracking	WIPS must provides tracking of all wireless devices that are associated with the WLAN.
Event actions and notification	An attack must automatically be stopped and security personnel notified immediately.
RF scanning	The entire spectrum (2.4 GHz for IEEE 802.11b/g and 5 GHz for 802.11a) should be scanned by probes.
Protocol analysis	An integrated packet sniffer and decoder can reveal what is happening on the WLAN.

Summary

- Wireless LAN management systems are important tools for maintaining wireless networks
- A WIDS constantly monitors the radio frequency (using wireless probes) for attacks
- A WIPS attempts to uncover and prevent an attack before it harms the WLAN