Cisco Wireless Explorer
Learning Summary

CISCO STRUCTURED WIRELESS-AWARE NETWORK (SWAN)

The Cisco Structured Wireless-Aware Network (SWAN) provides the framework to integrate and extend wired and wireless networks to deliver the lowest possible total cost of ownership for companies deploying wireless LANs (WLANs). Cisco SWAN extends "wireless awareness" into important elements of the network infrastructure, providing the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations have come to expect from their wired LANs.

There are five components to the framework:

CiscoWorks Wireless LAN Solution Engine

CiscoWorks Wireless LAN Solution Engine (WLSE) is a centralized, systems-level solution for managing the entire Cisco® Aironet® wireless LAN (WLAN) infrastructure. The advanced radio frequency (RF) and device-management features of CiscoWorks WLSE simplify the everyday operation of WLANs, help to ensure smooth deployment, enhance security, and maximize network availability, while reducing deployment and operating expense. The CiscoWorks WLSE is a core component of the Cisco Structured Wireless-Aware Network (SWAN) autonomous access-point solution.

Cisco Aironet® Series WLAN access points running Cisco IOS® Software

Cisco Aironet access points are required. These access points offer secure, manageable, and reliable wireless connectivity with exceptional range and performance, as well as integrated radio frequency (RF) management.

Management and security servers

The CiscoWorks Wireless LAN Solution Engine (WLSE) and an IEEE 802.1X authentication server, such as Cisco Secure Access Control Server (ACS), are required to manage and secure the wireless network. These products simplify the deployment and management of the WLAN infrastructure and implement an enterprise-class security solution.

WLAN client devices

Wi-Fi Certified or IEEE 802.11 clients are required. Using Cisco Aironet or Cisco Compatible client devices provides additional benefits, including advanced enterprise-class security, extended air/RF radio management, and enhanced interoperability.

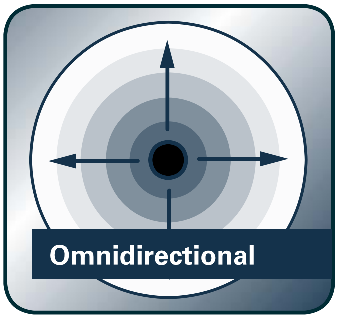
Infrastructure devices

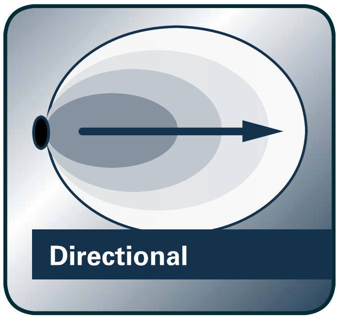
As Cisco incorporates wireless capabilities into its switches and routers, customers receive a unified network system that extends to wireless traffic all of the enterprise-class scalability, security, reliability, and simplified manageability of the wired infrastructure. The result of this wired and wireless integration is a lower overall total cost of ownership-existing routers and switches are used for WLAN support, obviating the need for unfamiliar and unproven WLAN point products.

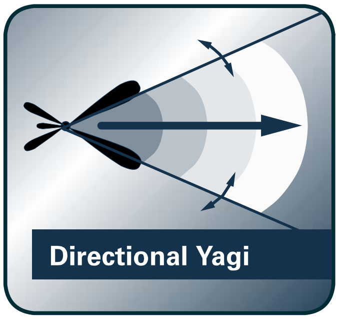
Cisco Systems®

Cisco Wireless Explorer
Learning Summary

CISCO STRUCTURED WIRELESS-AWARE NETWORK (SWAN)







Types of antennas::

Omni-directional Antennas

An omni-directional antenna is designed to provide a 360-degree radiation pattern. This type of antenna is used when coverage in all directions from the antenna is required. The standard 2.14dBi "Rubber Duck" is one style of omni-directional antenna.

Directional Antennas

Directional antennas come in many different styles and shapes. An antenna does not offer any added power to the signal; it simply redirects the energy it receives from the transmitter. By redirecting this energy, it has the effect of providing more energy in one direction, and less energy in all other directions. As the gain of a directional antenna increases, the angle of radiation usually decreases, providing a greater coverage distance, but with a reduced coverage angle. Directional antennas include yagi antennas, patch antennas, and parabolic dishes.

Securing a WLAN:

Open Access

All Wi-Fi certified wireless LAN products, such as Cisco Aironet Series products, are shipped in "open-access" mode, with their security features turned off. While open access or no security may be appropriate and acceptable for public hot spots such as coffee shops, college campuses, airports, or other public locations, it is not an option for an enterprise organization. Security needs to be enabled on wireless devices during their installation in enterprise environments. Some companies are not turning on their WLAN security features. These companies are exposing their networks to serious risk.

Static WEP

A static WEP key is a key composed of either 40 or 128 bits that is statically defined by the network administrator on the access point and all clients that communicate with the access point. When static WEP keys are used, a network administrator must perform the time-consuming task of entering the same keys on every device in the WLAN. If a device that uses static WEP keys is lost or stolen, the possessor of the stolen device can access the WLAN. An administrator will not be able to detect that an unauthorized user has infiltrated the WLAN until and unless the theft is reported. Static WEP is not considered secure and should only be used when there is no other option (such as, to support legacy clients).

Cisco Wireless Explorer
Learning Summary

CISCO STRUCTURED WIRELESS-AWARE NETWORK (SWAN)

Securing a WLAN (continued):

802.1X/EAP

An alternative WLAN security approach focuses on developing a framework for providing centralized authentication and dynamic key distribution. This approach is based on the IEEE 802.11 Task Group "i" end-to-end framework using 802.1X and the Extensible Authentication Protocol (EAP) to provide this enhanced functionality. Cisco has incorporated 802.1X and EAP into its WLAN security solution—the Cisco Wireless Security Suite. The three main elements of an 802.1X and EAP approach follow:

- Mutual authentication between client and authentication (Remote Access Dial-In User Service [RADIUS]) server
- Encryption keys dynamically derived after authentication
- Centralized policy control, where session time-out triggers reauthentication and new encryption key generation

When these features are implemented, a wireless client that associates with an access point cannot gain access to the network until the user performs a network logon.

Additional hardware:

Repeater

A repeater access point is not connected to the wired LAN; it is placed within radio range of an access point connected to the wired LAN to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. When you configure an access point as a repeater, the access point's Ethernet port does not forward traffic.

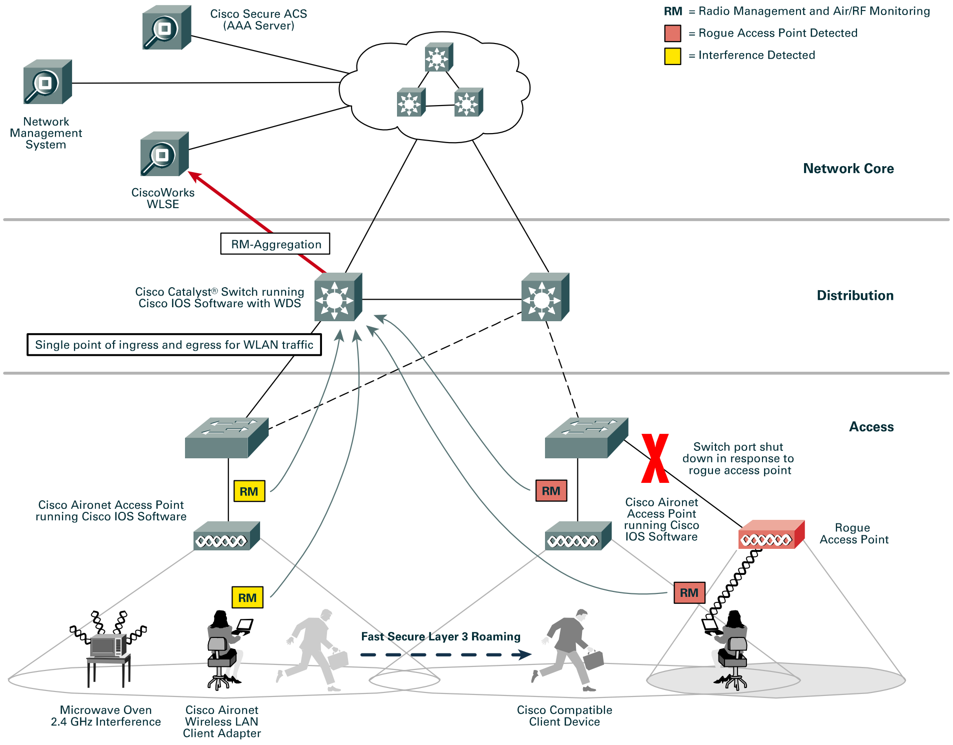
Bridge

Cisco Aironet Series wireless bridges provide high speed and cost effective wireless connectivity between multiple fixed or mobile networks and clients. Building a metropolitan area wireless infrastructure with Cisco Aironet Series wireless bridges provides deployment personnel with a flexible, easy to use solution that meets the security requirements of wide area networking professionals.

Cisco Wireless Explorer
Learning Summary

CISCO STRUCTURED WIRELESS-AWARE NETWORK (SWAN)

Cisco SWAN Framework



RM = Radio Management and Air/RF Monitoring
🟥 = Rogue Access Point Detected
🟨 = Interference Detected
Cisco Secure ACS (AAA Server)
Network Management System
CiscoWorks WLSE
Network Core
RM-Aggregation
Cisco Catalyst® Switch running Cisco IOS Software with WDS
Distribution
Single point of ingress and egress for WLAN traffic
Access
Switch port shut down in response to rogue access point
RM
RM
Cisco Aironet Access Point running Cisco IOS Software
Cisco Aironet Access Point running Cisco IOS Software
Rogue Access Point
RM
RM
Fast Secure Layer 3 Roaming
Microwave Oven 2.4 GHz Interference
Cisco Aironet Wireless LAN Client Adapter
Cisco Compatible Client Device

1. Clients and Access Points (AP) send their Radio Management (RM) date to the Cisco AP, switch or router running wireless-aware Cisco IOS Software with Wireless Domain Services (WDS).

2. Cisco AP, switch or router running wireless-aware Cisco IOS Software with WDS uses RM-Aggregation to remove redundant RM data received from the access points and client devices. The WDS device then forwards the aggregated data to the CiscoWorks WLSE.

3. Cisco SWAN minimizes the total cost of ownership and maximizes wireless network uptime by delivering an enterprise-class WLAN Intrusion Detection System (IDS) and optimizing the following deployment, management and security features:

- Fast secure layer 3 roaming
- Air/RF scanning and monitoring
- Assisted site surveys
- Interference detection
- Enhanced troubleshooting and diagnostic tools
- Rogue access point detection
- Security policy monitoring and alerts
- Auto-configuration of new access points
- WAN link remote site survivability
- Mass configuration and firmware updates
- Self-healing WLANs
- Cisco Wireless Security Suite
- Wi-Fi Protected Access (WPA) and WPA2
- High availability and resiliency
- Ad-hoc network detection

Cisco Systems