CISCO

Configure a Wireless Router
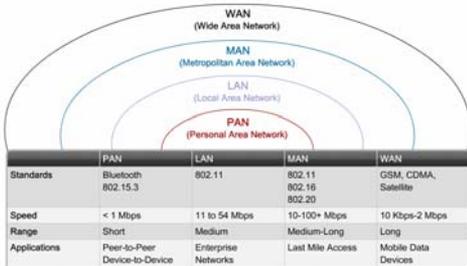
LAN Switching and Wireless – Chapter 7

Objectives

- Describe the components and operations of basic wireless LAN topologies.
- Describe the components and operations of basic wireless LAN security.
- Configure and verify basic wireless LAN access.
- Configure and troubleshoot wireless client access.

Wireless Local Area Networks - WLANs

- Provides mobility for users
- Connects clients to the network through a wireless access point (AP) instead of an Ethernet switch

|	PAN	LAN	MAN	WAN
Standards	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satellite
Speed	< 1 Mbps	11 to 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Last Mile Access	Mobile Data Devices

---

Regulation

- The radio spectrum is considered a natural resource and hence is regulated locally
- The ITU-R designates the 900 MHz, 2.4 GHz, and 5 GHz frequency bands as unlicensed for ISM communities.
- IEEE 802.11 standard for WLANs
- Physical layer:
    Radio frequency (RF) 2.4 GHz and 5 GHz bands
- Wi-Fi Alliance
    Ensures that vendors make devices that are interoperable

IEEE WLAN Standards

	Band GHz	Max B/w Mbs	Modulation	
802.11		1/2		Defunct
802.11a	5.7	54	OFDM	Higher cost
802.11b	2.4	11	DSSS	Prone to interf.
802.11g	2.4	54	DSSS-OFDM	Prone to interf
802.11n	2.4/5?	200+	MIMO-OFDM	Not yet ratified


Data Rates and Range
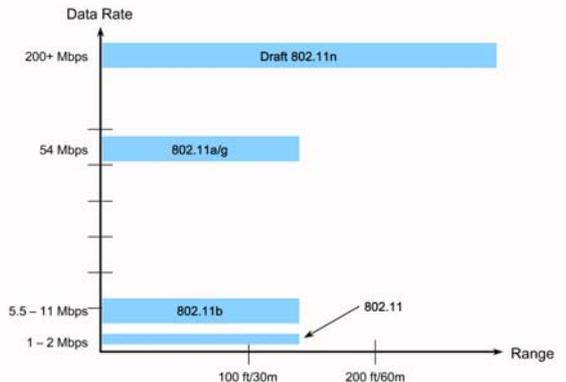
Basic Wireless LAN Components

- Wireless NICs
- In small business, a Wireless Router performs the role of access point, Ethernet switch, and router.

Wireless Access Points (APs)

- A Layer 2 device that functions like an 802.3 Ethernet switch
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- If an AP receives data from a client station, it sends an acknowledgement to the client that the data has been received
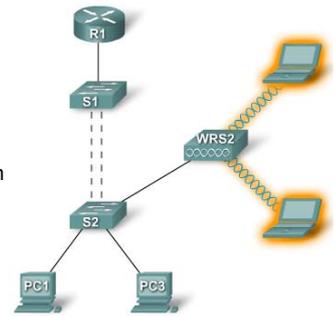
Configurable Parameters for Wireless Clients

## Configurable Parameters for Wireless Clients

- Wireless network mode refers to the WLAN protocols: 802.11a, b, g, or n.
- Mixed mode: 802.11b and 802.11g (backward compatible)
- For an AP to support 802.11a as well as 802.11b/g, it must have a second radio to operate in the different RF band.
- Shared service set identifier (SSID)

    A unique case-sensitive string used to distinguish between multiple wireless networks in the same vicinity.

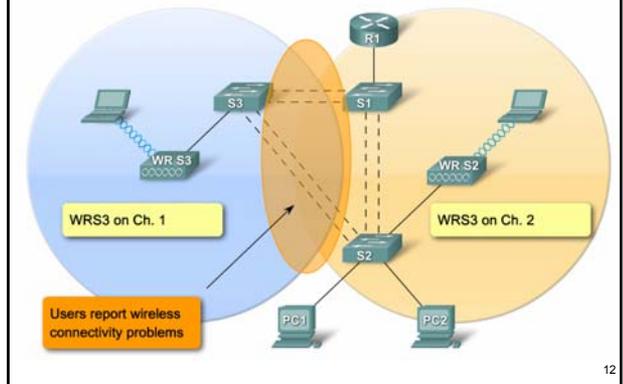   Several access points on a network can share an SSID.

Wireless Channel: 2.4-GHz RF Band
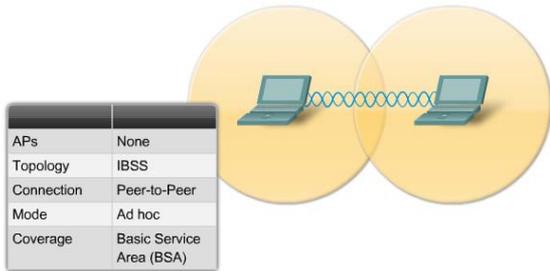

North America: 11 channels
Europe: 13 channels
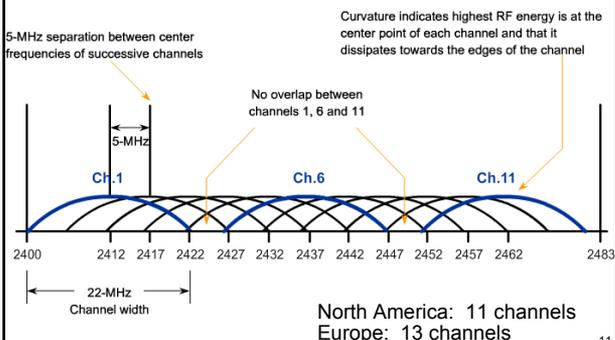
Resolve Issues of Incorrect Channel Settings

802.11 Topologies: Ad Hoc Network

- Also called an Independent Basic Service Set (IBSS)
- Operates without an AP

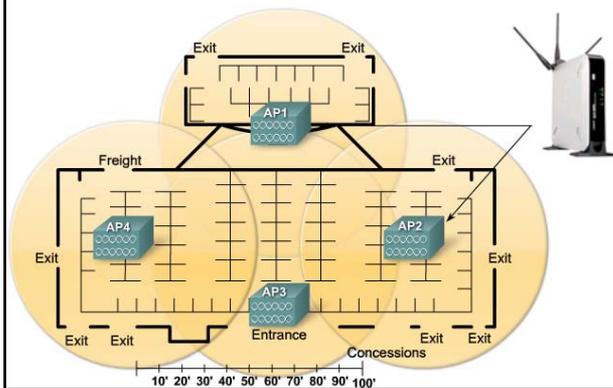| APs	None
Topology	IBSS
Connection	Peer-to-Peer
Mode	Ad hoc
Coverage	Basic Service Area (BSA)

802.11 Topologies

- Basic Service Set (BSS)
    - A group of stations that communicate with each other through a single AP
- Basic Service Area (BSA)
    - The coverage area for the BSS
- BSS identifier (BSSID)
    - The MAC address of the access point serving the BSS.

802.11g clients

AP supports both 802.11b/g

WR S2

802.11b client forces faster clients who are contending for the channel to wait longer.

802.11b client

802.11 Topologies: Infrastructure mode

Exit   Exit

AP1

Freight   Exit

AP4   AP2

Exit   Exit

AP3

Exit   Exit   Entrance   Exit   Exit

Concessions

10' 20' 30' 40' 50' 60' 70' 80' 90' 100'
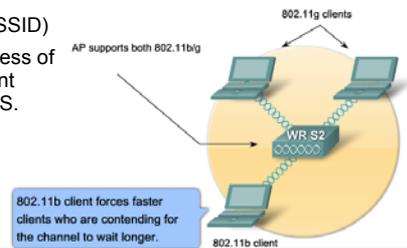
802.11 Topologies: Infrastructure mode

- Extended Service Set (ESS)
    - BSS's joined through a common wired distribution system.
- An ESS should have 10 to 15 percent overlap between cells in an extended service area (ESA).
- A client associates with just one AP in the ESS at any given time
- An ESS generally includes a common SSID to allow a user to roam from AP to AP

Client and Access Point Association

- Beacons - Frames used by the WLAN network to advertise its presence. Broadcast periodically.
- Probes - Frames used by WLAN clients to find their networks.
- Authentication - A process which is an artefact from the original 802.11 standard, but still required by the standard.
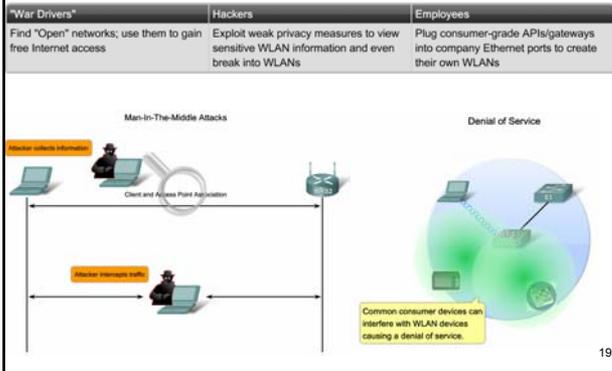- Association - The process for establishing the data link between an access point and a WLAN client.

Client and Access Point Association

- Before a client can send data, it goes through the following three-stage process:
- Stage 1 - 802.11 Probing
- Stage 2 - 802.11 Authentication:
    - Open authentication, is fundamentally a NULL authentication.
    - Wired Equivalency Protection (WEP) key. It is not recommended.
- Stage 3 - 802.11 Association
    - Client learns the BSSID, which is the access point MAC address, and the access point maps a logical port known as the association identifier (AID) to the client.

Threats to Wireless LAN Security

"War Drivers"	Hackers	Employees
Find "Open" networks; use them to gain free Internet access	Exploit weak privacy measures to view sensitive WLAN information and even break into WLANs	Plug consumer-grade APIs/gateways into company Ethernet ports to create their own WLANs

19

Limited Wireless Security Methods

- Open and WEP are artefacts from the original 802.11, but still required by the standard.
- Open authentication is really "no authentication,"
- WEP shared key encryption is crackable and not scalable.
- The 32-bit WEP keys are manually managed, so users enter them by hand.
- SSID 'cloaking' – disable AP SSID broadcasts
  - The SSID can be sniffed because it is sent in clear text
- Filtering MAC addresses
  - Defeated by sniffing MAC addresses and MAC spoofing

20

Current Security Standard: 802.11i/WPA2

- Security should conform to 802.11i standard which incorporates the following features:
- AES Encryption (Advanced Encryption Standard)
- Authentication: 802.11x
- Dynamic key management using a security server such as RADIUS
- WPA is a WLAN security implementation developed by Wi-Fi Alliance. Uses TKIP encryption.
- WPA2 updated to conform to 802.11i. Uses AES encryption. Preferred standard

21

Configuring the WRT300N Access Point

- Access the web-based utility of the AP with a browser, and enter the WRT300N default IP address, 192.168.1.1,
- All devices connecting to the AP must use the same security type as the one configured on the AP
- If an AP is configured for WEP, both the type of encryption (WEP) and the shared key must match between the client and the AP.
- If WPA is being used, the encryption algorithm is TKIP
- If WPA2 or 802.11i is used, AES is required as the encryption algorithm.

22

Configuring Basic Wireless Settings

Select the Wireless Security Protocol

Summary

- Wireless LANs use standards such as
    IEEE 802.11a
    IEEE 802.11b
    IEEE 802.11g
    IEEE 802.11n
- Basic Service Set
    – Mobile clients use a single access point for connectivity
- Extended Service Set
    – Multiple access point that share an SSID

Summary

- WLAN security practices/methods include
    – MAC address filtering
    – SSID cloaking
    – Implementing WPA2
- Configuration of wireless NIC and access point
    – Configure both of them the same way
        • SSID
- Troubleshooting WLANs include doing the following:
    – Check channel setting
    – Check for interference