Cisco Systems
Networking Academy
Cisco.com

Wireless

CCNA Exploration Semester 3

Chapter 7

CCNA CISCO CERTIFIED™

Topics

- Components and basic operation of wireless LANs
- Basic WLAN security
- Configure and verify basic wireless LAN access
- Troubleshoot wireless client access

Wireless problems

- Interference
- Signal strength, blind spots
- Security – anyone with receiver within range can pick up signals
- Regulations differ in different countries

Standards

	PAN	LAN	MAN	WAN
Standards	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM CDMA Satellite
Speed	< 1 Mbps	11-54 Mbps	10 – 100+ Mbps	10 Kbps – 2 Mbps
Range	Short	medium	Medium-long	Long

Wireless and Ethernet

- Wireless workstations connect to cabled Ethernet network via an access point (AP).
- Collisions can occur both with Ethernet and with wireless.
- Ethernet detects and recovers (CSMA/CD)
- Wireless uses collision avoidance (CSMA/CA).
- Frame format is different.

802.11a

- Introduced 1999, not compatible with 802.11b
- OFDM modulation (faster, up to 54Mbps)
  - Orthogonal Frequency-Division Multiplexing
- More costly than 802.11b
- 5 GHz band not free, licence is needed.
- Smaller antennas, less interference
- Poorer range, absorbed more by walls etc.
- Not allowed in some countries.

802.11b

- Introduced 1999, not compatible with 802.11a
- DSSS modulation, slower, 1, 2, 5.5, 11 Mbps
  - Direct-Sequence Spread Spectrum
- Cheaper than 802.11a
- 2.4 GHz band.
- More interference as many appliances use this band
- Longer range, less easily obstructed.

802.11g

- Introduced 2003
- Compatible with 802.11b
- DSSS modulation, to 11 Mbps or OFDM to 54 Mbps
- 2.4 GHz band.
- More interference as many appliances use this band
- Longer range, less easily obstructed.

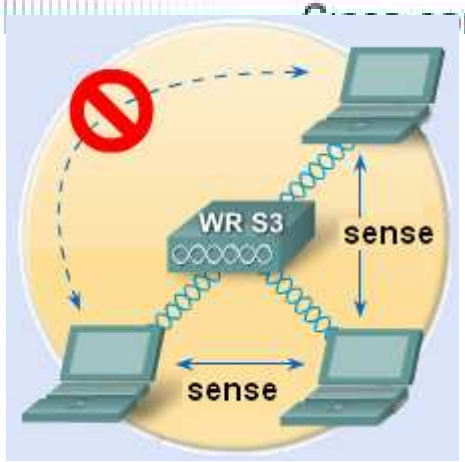
802.11n

- Expected Sept 2008, in draft now.
- May use both 2.4 and 5 GHz band
- MIMO-OFDM (*Multiple Input Multiple Output)*
  - Splits high data rate stream into several low data rate streams, transmits simultaneously using multiple antennae.
- Possibly up to 248 Mbps with 2 streams
- Longer range, 70 metres

Access point, shared medium

- Access point acts like a hub (not switch)
- Wireless is a shared medium
- 802.11 uses CSMA/CA
- Devices detect activity on the medium, send signals if all is clear.
- Signal is acknowledged if it is received
- Attenuation limits distance of client from access point.

Hidden nodes



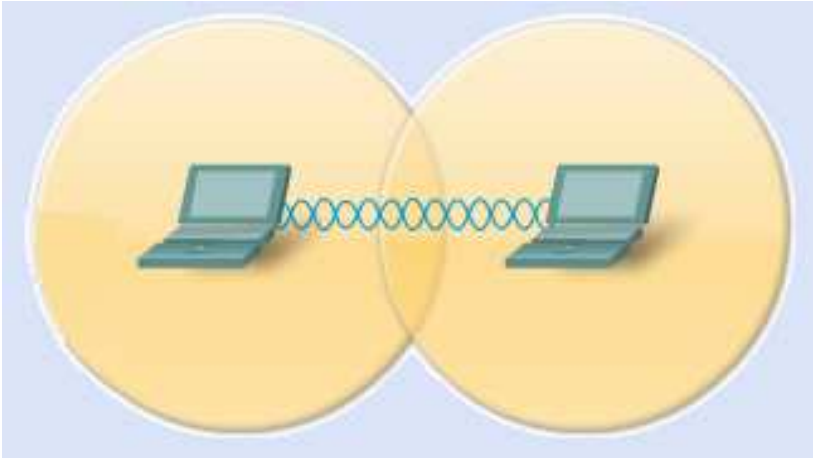
- If two stations cannot sense each others' signals then they may transmit at the same time and have a collision.
- Request to send/clear to send (RTS/CTS) avoids this.
- Station requests the medium, access point allocates it for long enough to complete the transmission.

Wireless router

- Commonly used for Internet access
- Acts as router, Ethernet switch and wireless access point.
- Configure for mode 802.11a, b, g, or n
- Configure shared service set identifier (SSID) to identify network
- Select channel within 2.4GHz band. Adjacent access points need non-overlapping channels.

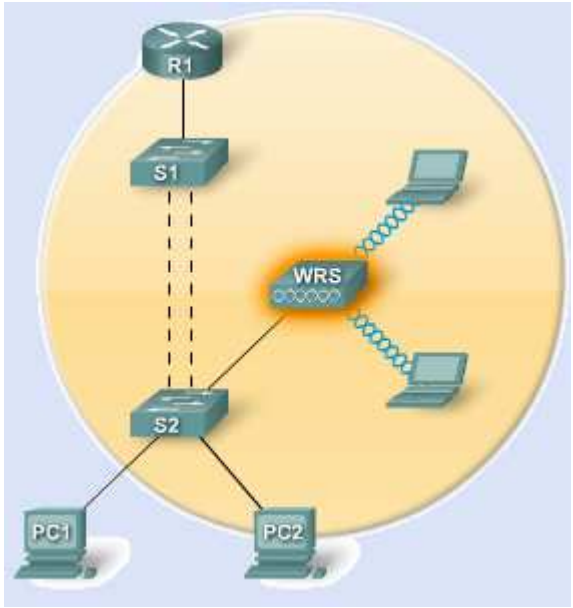
Ad hoc topology

- No access point
- Peer to peer
- Negotiate parameters
- Independent basic service set
- Area covered is basic service area (BSA).



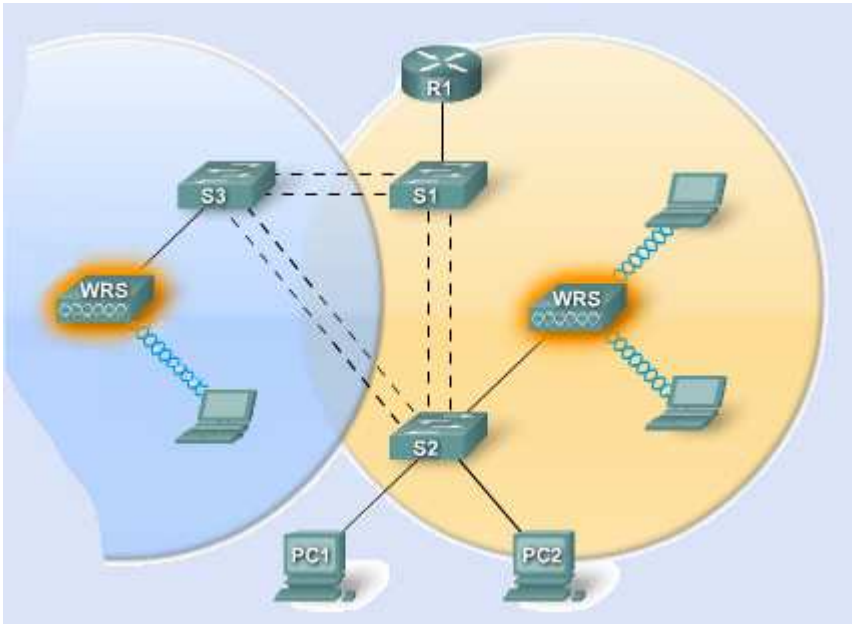
Basic service set topology

- One access point
- Access point manages parameters for clients
- Infrastructure mode
- Area covered is basic service area (BSA).

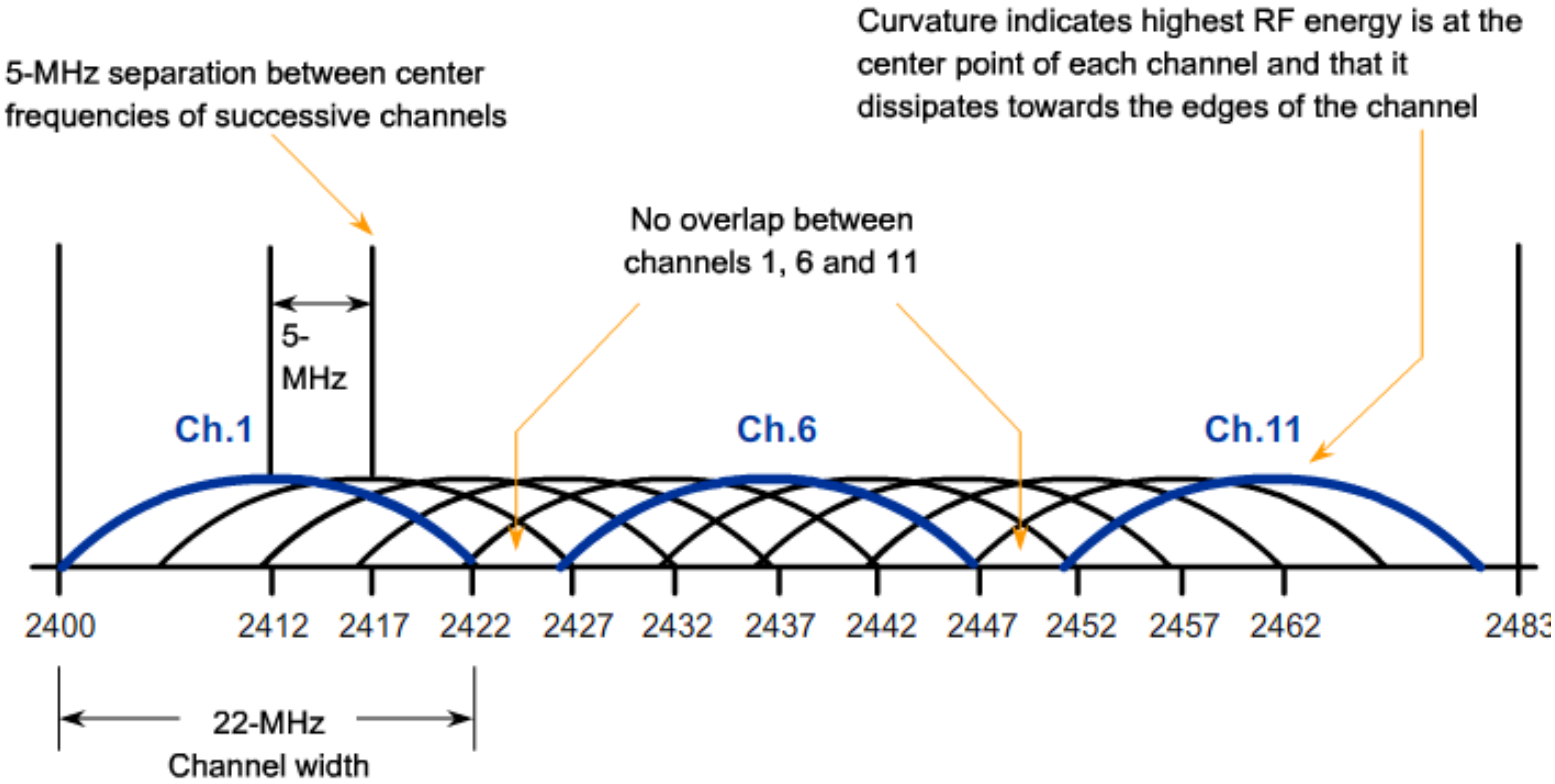


Extended service set topology

- More than one access point
- Access point manages parameters for clients
- Infrastructure mode
- Area covered is extended service area (ESA).



Channels



2.4-GHz RF Band

Beacon and probe

- Access point may send out a beacon at regular intervals for clients to detect.
- Client sends a probe specifying the SSID and bit rates supported. Access point responds.
- Client can send probe with no SSID to look for any network. Access point may be configured to respond, or not.

Authentication

- Client requests authentication.
- Access point responds.
- 802.11 had two authentication mechanisms. NULL (Open Authentication) does not give privacy. Wired Equivalency Protection (WEP) uses a shared key.

Association

- Request from client and response.
- Finalizes security options
- Finalizes bit rate options
- Sets up data link
- Client learns the access point MAC address (BSSID)
- Access point maps a logical port known as the association identifier (AID) to the WLAN client.

Placing access points

- Above obstructions.
- At least 3 feet from metal obstructions.
- Vertically and high up.
- In locations where users will work.
- But not too close to people.
- Work out the coverage for each AP.
- Allow enough overlap.

Security threats

- War drivers look for an unsecured network that will provide Internet access.
- Hackers (Crackers) enter systems to steal data or cause harm. They can often get past weak security.
- Employees may install rogue access points without permission and without implementing the necessary security.

Man in the middle

- Attacker modifies the NIC of a laptop with special software so that it accepts all traffic, not just traffic addressed to it.
- Uses packet sniffing software, such as Wireshark, to observe a client station connecting to an access point. Detects names, IP addresses, ID and the challenge and associate response.
- Can then monitor network.

Denial of service

- Use common devices to create interference. (cordless phone, microwave, baby monitor)
- Flood the network with clear-to-send (CTS) messages. Clients then send simultaneously and cause a constant stream of collisions.
- Send a series of disassociate commands so that clients repeatedly disconnect then try to reassociate.

802.11 original authentication

- Open authentication – no privacy or security "Authenticate me." "All right."
- WEP shared key authentication – weak encryption algorithm could be cracked. 32 bit key had to be entered by hand. Prone to error and not easily scalable.

Authentication developments

- Vendors created their own security systems
- Wi-Fi Alliance developed WiFi Protected Access (WPA) security method.
- 802.11i standard introduced - similar to the Wi-Fi Alliance WPA2 standard.

TKIP and AES encryption

- Temporal Key Integrity Protocol (TKIP) encryption mechanism is certified as WPA by Wi-Fi Alliance.
- TKIP uses the original encryption algorithm used by WEP but addresses its weaknesses.
- TKIP encrypts the Layer 2 payload and carries out a message integrity check to detect tampering.
- Advanced Encryption Standard (AES) encryption mechanism is certified as WPA2. Has additional features.
- AES is the preferred method.

Configuring Access Point

1. Check wired operation: DHCP, Internet access
2. Install access point
3. Configure access point without security
4. Install one wireless client without security
5. Check wireless network operation
6. Configure security
7. Check wireless network operation

Basic Wireless Settings

- Network Mode – Lets you choose the right mode for your devices. B, G, N, mixed or BG mixed. You can disable wireless operation.
- Network Name (SSID) – should be changed from the default. Must be the same for all devices on the network.
- SSID broadcast can be enabled or disabled.

More Basic Wireless Settings

- Radio Band –
  - For Wireless-N devices only, select Wide - 40MHz Channel.
  - For Wireless-G and Wireless-B only, select Standard - 20MHz Channel.
  - For mixed devices, keep the default Auto.
- Wide Channel - If you selected Wide for the Radio Band, Select a channel from the drop-down menu.
- Standard Channel - Select the channel.

Security

- Choose PSK2 (WPA2 or IEEE 802.11i) if all client devices are able to use it.
- If some older devices do not support WPA2 then choose the best security mode that is supported by all devices.
- Encryption – AES is stronger than TKIP. Use AES with WPA2.

Configure the client

- Choose the network to connect to.
- Enter the SSID
- Choose the authentication method
- Choose the encryption method
- Enter the network key.

Troubleshooting

- Generally start with the physical layer and then move up.
- Eliminate the client PC as the source of trouble before checking the rest of the network.

Troubleshooting – no connectivity

Cisco.com

- Check that the PC has an IP address.
- Try connecting the PC to the wired network and ping a known address
- Try a different wireless NIC. Reload drivers as necessary.
- Check the security mode and encryption settings on the client. Do they match the access point?

Troubleshooting – poor connection

Cisco.com

- Check distance to access point
- Check the channel settings on the client.
- Check for devices that might be causing interference (cordless phone, microwave oven etc).

Troubleshooting – looking wider

- Are all devices in place?
- Are they all powered on?
- Are wired links working correctly?
- Is there a neighbouring access point using an overlapping wave band?
- Are access points badly placed?

The End