Network Technology 2 –

Lennart Franked
email:lennart.franked@miun.se
Tel:060-148683

Informations- och Kommunikationssystem (IKS)
Mittuniversitetet

18/03-2014

Wireless Network Types

- WPAN Wireless Personal-Area Network
  - Cover area up to 100 meters.
  - I.e. Bluetooth
- WLAN - Wireless Local Area Network
  - Cover area up to 300 meters.
  - I.e. WiFi 802.11a/b/g/n/ac/ad
- WWAN - Wireless Wide-Area Network
  - Cover areas up to a couple of kilometres.
  - I.e. 3G, 4G, WIMAX
- Focus of todays lecture is on IEEE 802.11 standards.

Wireless Network Types

- WPAN Wireless Personal-Area Network
  - Cover area up to 100 meters.
  - I.e. Bluetooth
- WLAN - Wireless Local Area Network
  - Cover area up to 300 meters.
  - I.e. WiFi 802.11a/b/g/n/ac/ad
- WWAN - Wireless Wide-Area Network
  - Cover areas up to a couple of kilometres.
  - I.e. 3G, 4G, WIMAX
- Focus of todays lecture is on IEEE 802.11 standards.

802.11 Standards

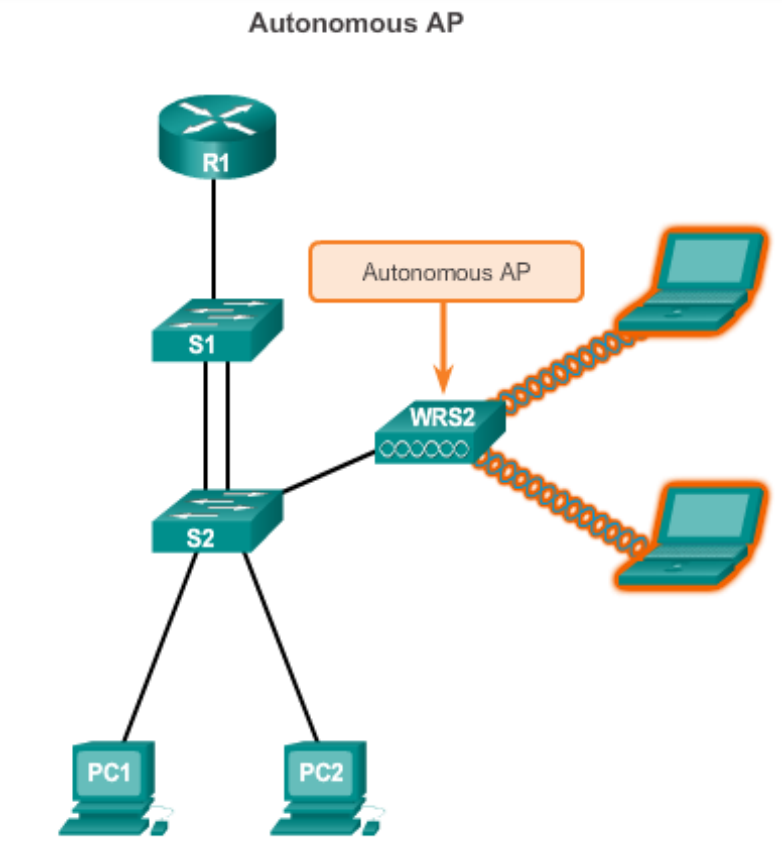
Table 1 : 802.11 Standards

IEEE Standard	Maximum Speed	Frequency	Backwards Compatible
802.11	2Mb/s	2.4GHz	–
802.11a	54Mb/s	5GHz	–
802.11b	11Mb/s	2.4GHz	–
802.11g	54Mb/s	2.4GHz	802.11b
802.11n	600Mb/s	2.4GHz and 5GHz	802.11a/b/g
802.11ac	1.3Gb/s	5GHz	802.11a/n
802.11ad	7Gb/s	2.4GHz, 5GHz and 60 GHz	802.11a/b/g/n/ac

Wi-Fi Certifications

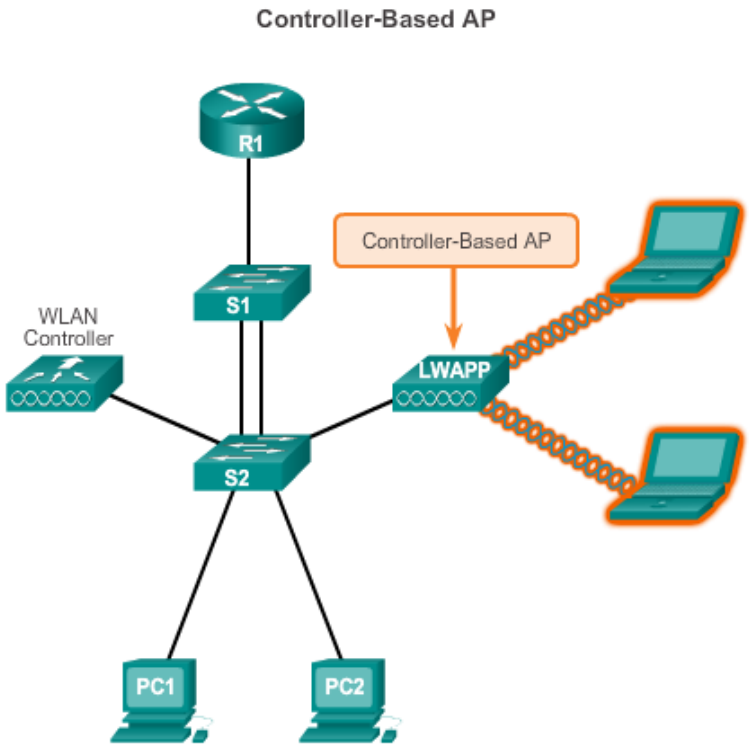
- Wi-Fi Alliance ensures compatibility between manufacturers.
- Compatibility insurance includes:
  - IEEE 802.11a/b/g/n/ac/ad
  - IEEE 802.11i - WPA2, EAP
  - Wi-Fi Protected Setup (WPS)
  - Wi-Fi Direct
  - Wi-Fi Passpoint
  - Wi-Fi Miracast

Access Point Types



- Managed Individually

Access Point Types Cont.



- Managed using a separate WLAN-controller

WiFi Antenna types

- Numerous types of antennas:
  - Omnidirectional - 360 degree coverage.
  - Directional - Focuses the signal in one direction.
  - Yagi - Type of directional antenna, high yield, narrow band, long range.

WiFi Topologies – Ad Hoc

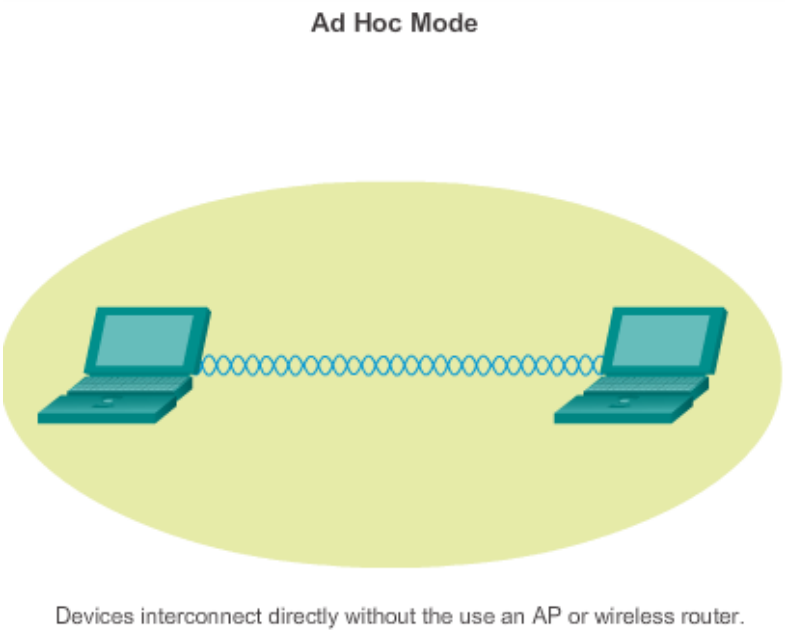
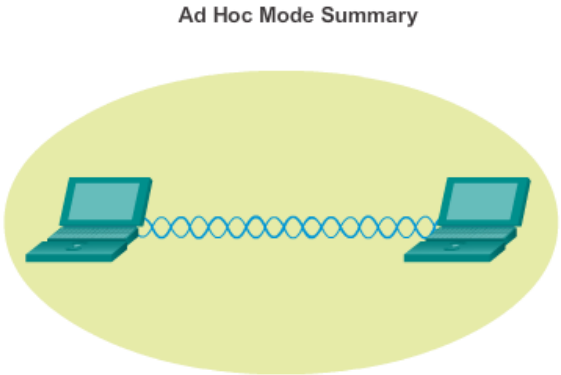


Figure 1 : WiFi ad-hoc topology

WiFi Topologies – Tethering



IBSS Summary	
WLAN Topology Mode	Ad Hoc
802.11 Wireless Topology	Independent BSS
Number of APs	None
802.11 Coverage Area	Basic Service Area (BSA)

Figure 2 : Tethering - Personal WiFi hot spot

WiFi Topologies – Infrastructure

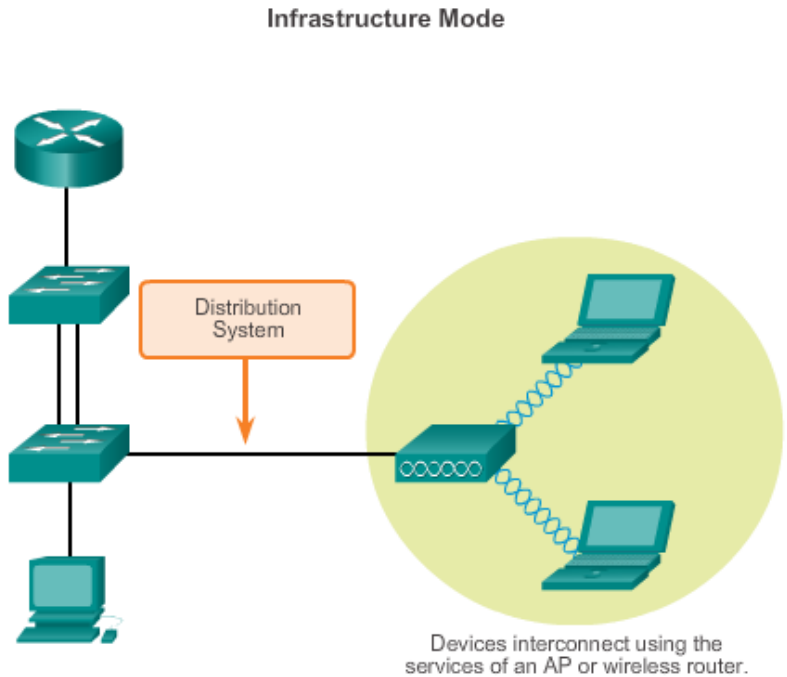
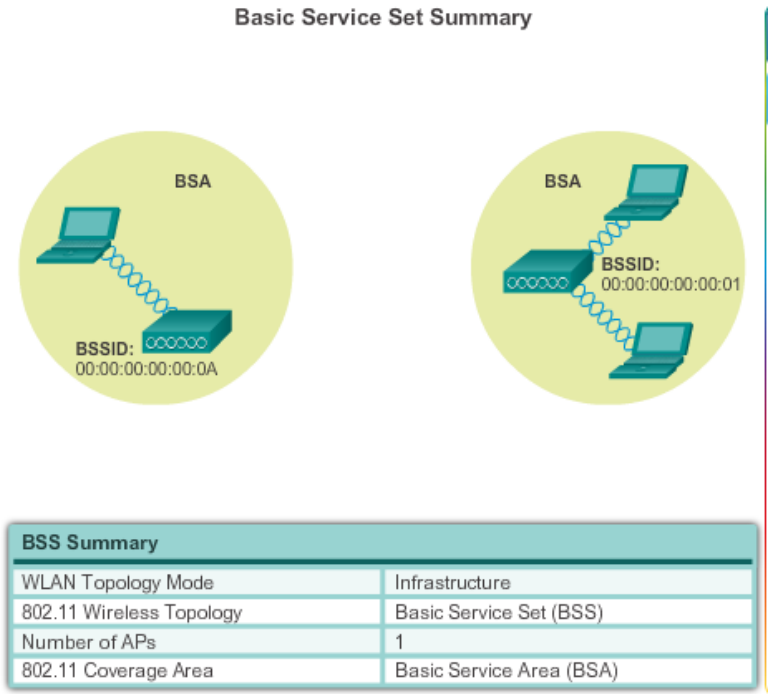


Figure 3 : Infrastructure mode

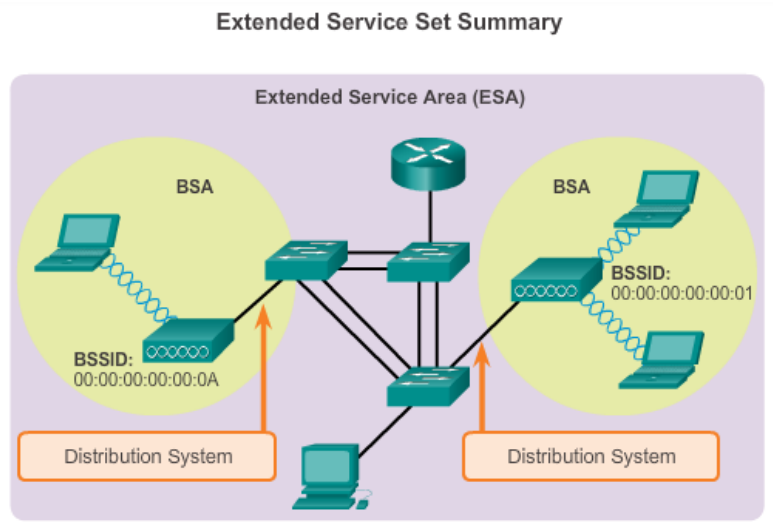
WiFi Topologies – Infrastructure - BSS



BSS Summary	
WLAN Topology Mode	Infrastructure
802.11 Wireless Topology	Basic Service Set (BSS)
Number of APs	1
802.11 Coverage Area	Basic Service Area (BSA)

Figure 4 : Basic Service Set

WiFi Topologies – Infrastructure - ESS



ESS Summary	
WLAN Topology Mode	Infrastructure
802.11 Wireless Topology	Extended Service Set (ESS)
Number of APs	2 or more
802.11 Coverage Area	Extended Service Area (ESA)

Figure 5 : Extended Serice Set

Wireless 802.11 Frame

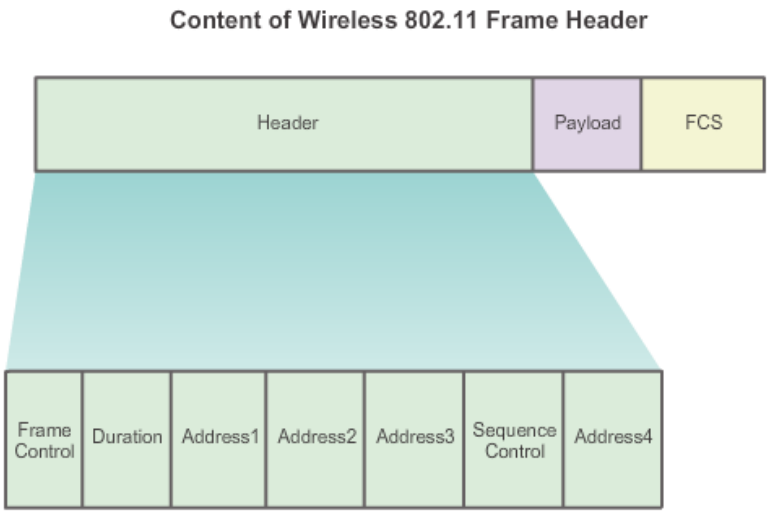


Figure 6 : 802.11 Frame Header overview

- Frame Control – Identify type of frame
- Duration – Indication of how how long the medium is busy before other stations can contend for medium.
- Address 1-4 – MAC addresses of devices involved in the transfer.
- Sequence Control – Contains Sequence and Fragment numbers.
- Payload – Data
- FCS – Frame Check Sequence.

Wireless 802.11 Frame Control

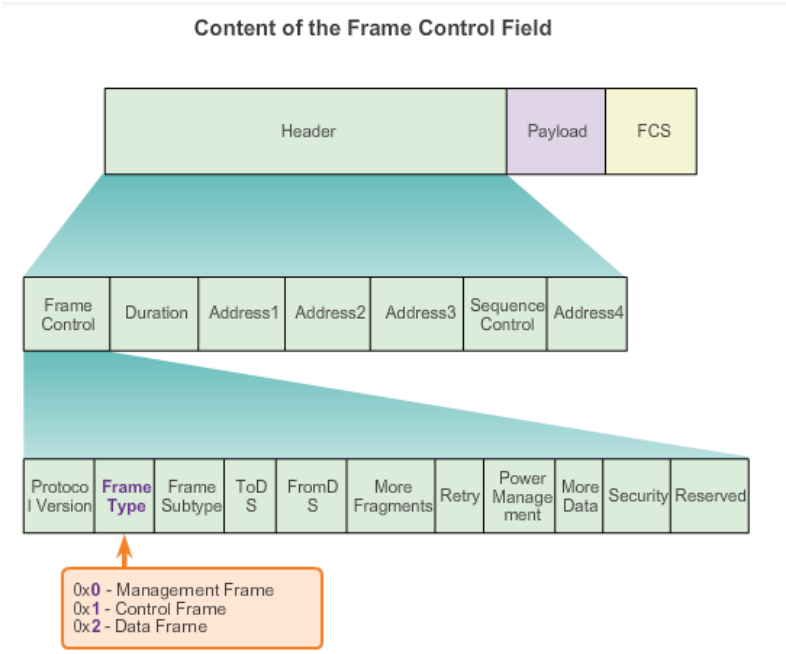


Figure 7 : 802.11 Frame Control Header Field Overview

- Protocol Version –
- Frame Type/Frame Subtype – Type of frame i.e. management frame, data frame, control frame, followed by specific function of that frame.
- ToDS/FromDS – Direction of frame in respect to Distribution systems.
- More Fragments – Last fragment or more to come.
- Retry – Indicates if the frame is resent or not.
- Power Management – Active or power save.
- More Data – Indicates that more data is to be sent. Used for devices in power-save mode.
- Security – Whether or not Security is used.

Wireless 802.11 Frame Types

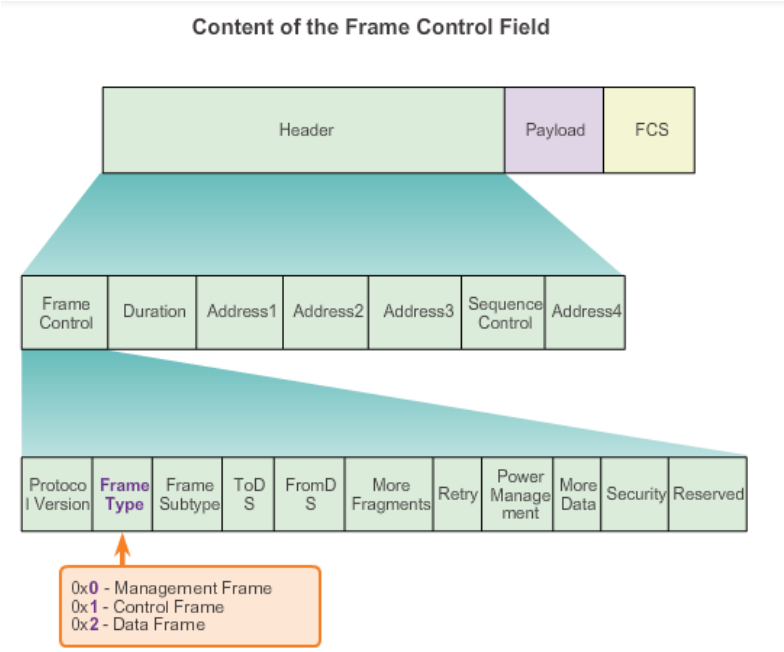


Figure 8 : 802.11 Frame Type Header Field Overview

- Management Frame – Communication maintenance, finding, authenticating, associating.
- Control Frame – RTS, CTS, ACK.
- Data Frame – Carrying the payload.

Wireless 802.11 Frame Types

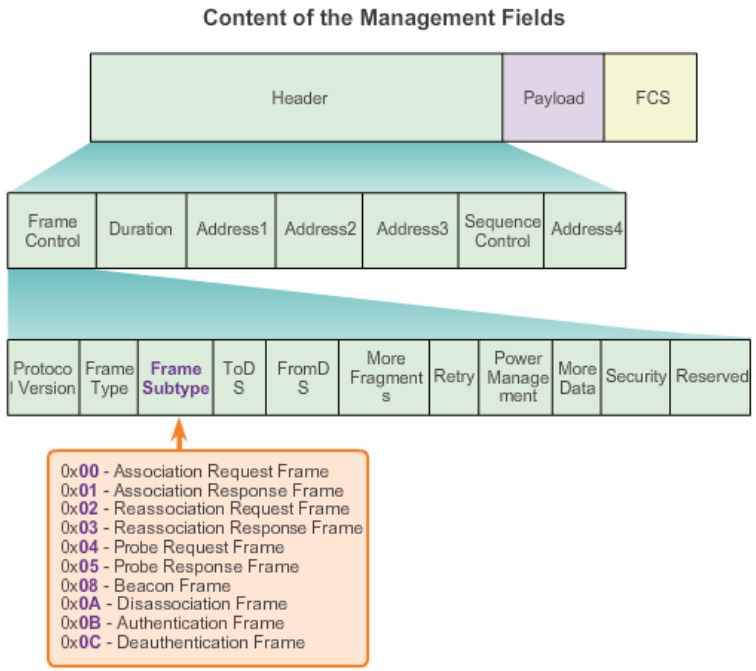


Figure 9 : 802.11 Management Frames Overview

- Association request – Sent from station to associate itself with an AP.
- Association response – Sent from AP to accept or reject association request.
- Reassociation request – Sent if station lost connection to AP.
- Reassociation response – Sent as a response to reassociation request.
- Probe request – Sent from a station when requestion information.
- Probe response – Sent from an AP as a response to Probe request.

Wireless 802.11 Frame Types cont.

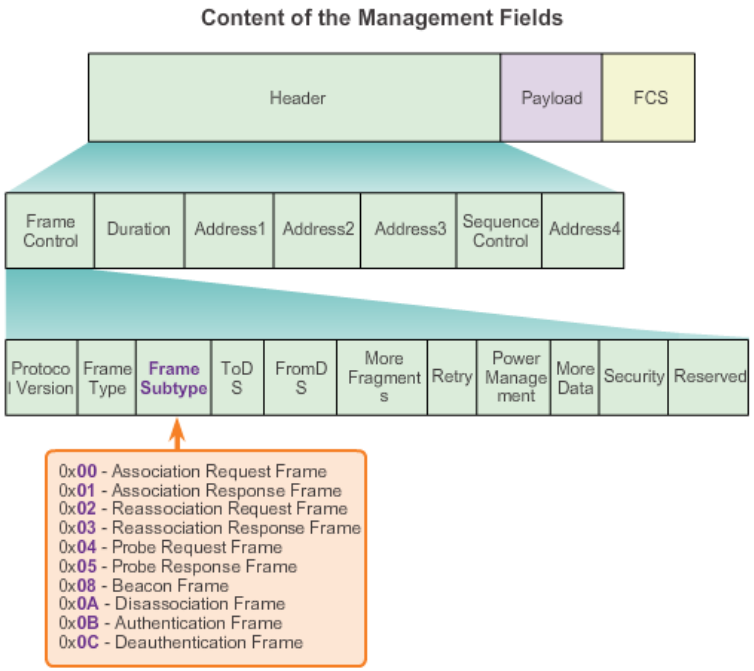


Figure 10 : 802.11 Management Frames Overview

- Beacon – Sent periodically from AP announcing its presence.
- Disassociation frame – Sent from station wanting to terminate connection.
- Authentication frame – Used for authentication. Contains ID information.
- Deauthentication – Sent from one station to another for terminating connection.

Wireless 802.11 Frame Types

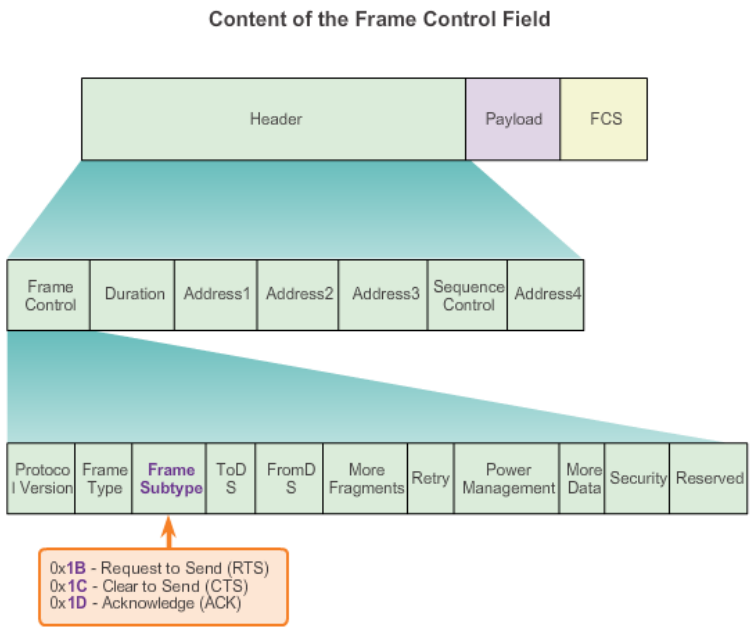


Figure 11 : 802.11 Frame Control Type Field Overview

- Request to Send – Sent from station that wants to use transmission media.
- Clear to Send – Sent from AP as a response to CTS.
- Acknowledgement – Acknowledge receiving frame.

These frames are used for the CSMA/CA contention method used by 802.11.

802.11 Control Frames

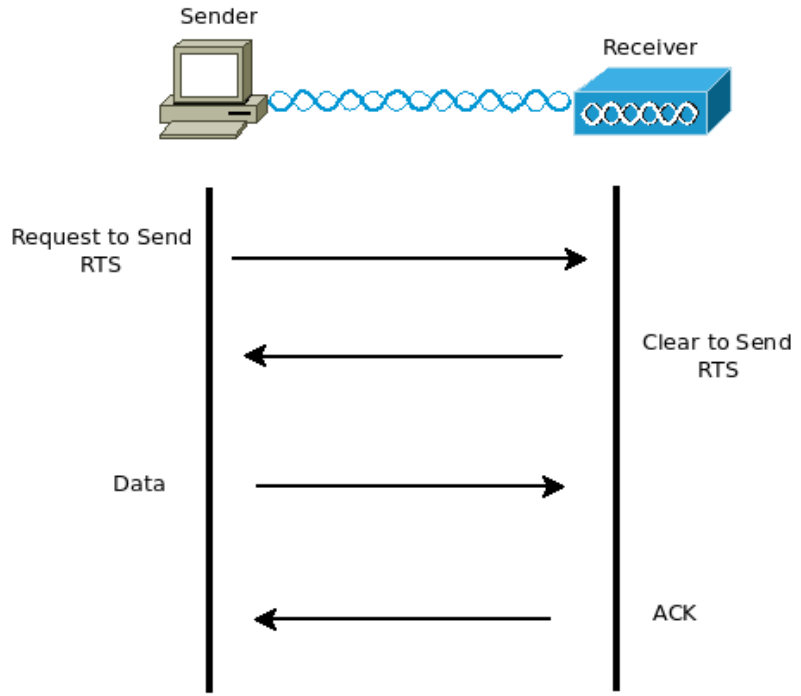


Figure 12 : Exchange of 802.11 Control Frames

CSMA/CA

Carrier Sense Multiple Access / Collision Avoidance

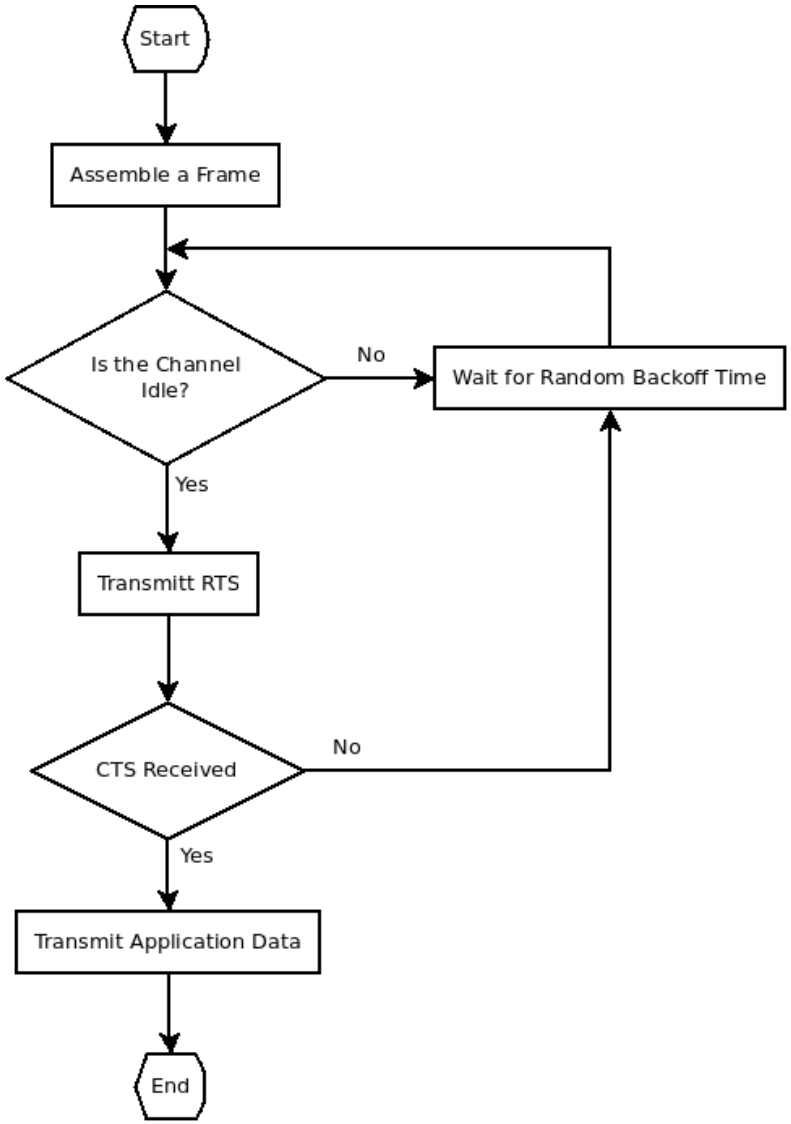


Figure 13 : CSMA/CA Flowchart

Wireless 802.11 Associations

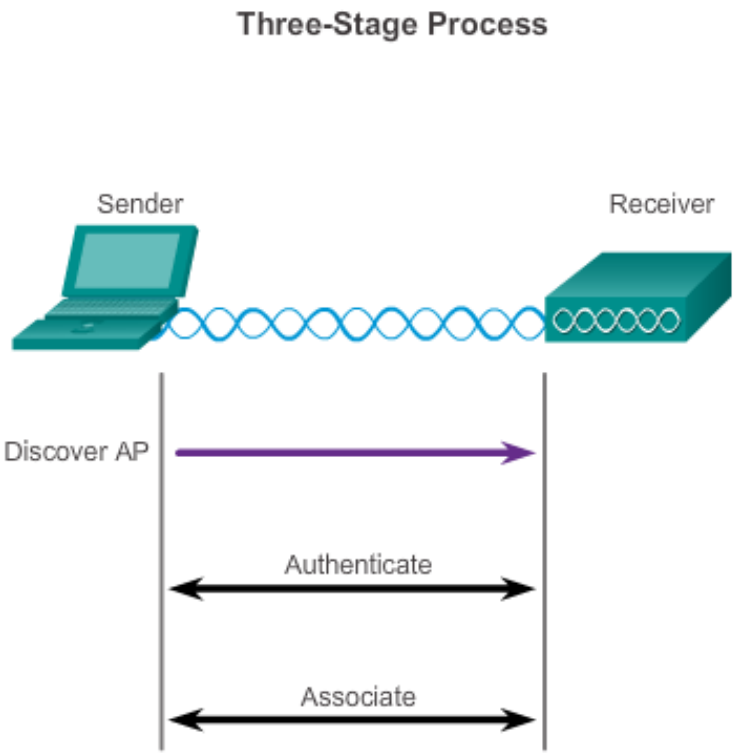


Figure 14 : 802.11 AP Association

- For an AP and a station to associate they must agree on association parameters.
  - SSID
  - Password
  - Network mode - 802.11 a/b/g/n/ac/ad
  - Security - Open, WEP, WPA, WPA2
  - Channel

Discovering Access Points

- Passive mode
  - Stations can passively find available networks.
  - AP advertises its presence using beacons
- Active mode
  - Stations must actively search for available AP
  - Stations must know network parameters, such as SSID
  - Probe requests are sent on multiple channels.

Frequency Channel Usage

- Direct Sequence Spread Spectrum (DSSS)
  - Spreads the signal over a larger frequence band making it more resistant to interference.
  - Used by 802.11b
- Frequency-hopping Spread Spectrum (FHSS)
  - Hopping between frequency channels
  - Allows for more efficient use of channels.
  - Used by legacy 802.11.
- Orthogonal Frequency-Division Multiplexing (OFDM)
  - Divides a channel into multiple subchannels
  - Efficient channel usage
  - Makes it possible to use MIMO.
  - Used in 802.11a/g/n/ac

Channels - 802.11b

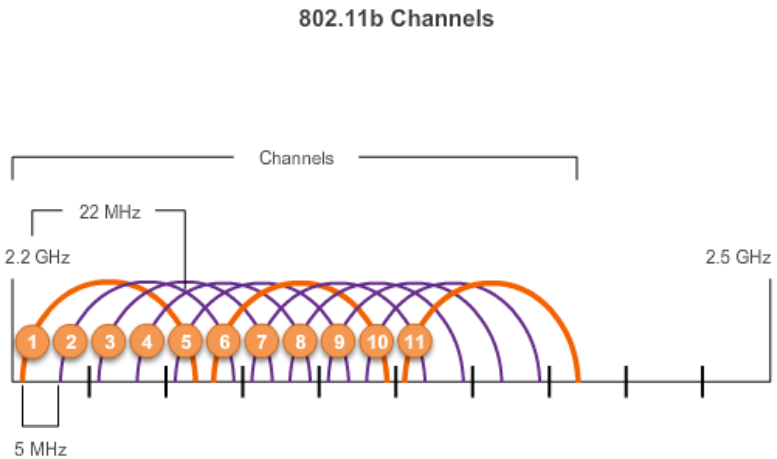


Figure 15 : 2.4GHz channels in 802.11b

802.11b supports three non-overlapping channels

Channels - 802.11g/n

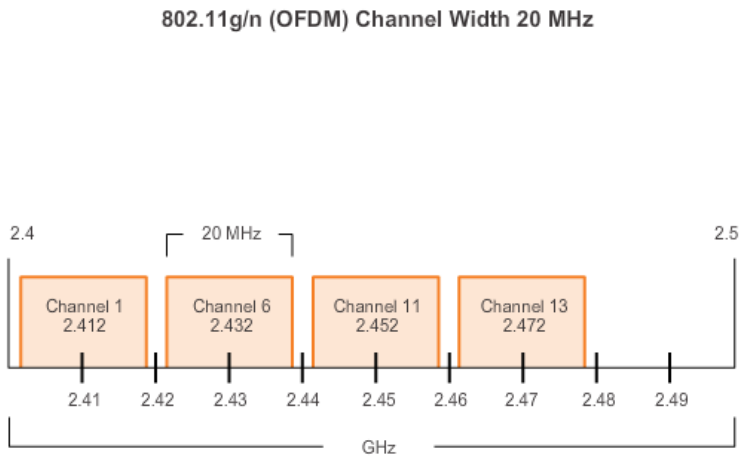


Figure 16 : 2.4GHz channels in 802.11g/n

802.11g/n supports four non-overlapping channels

Channel bonding - 802.11n

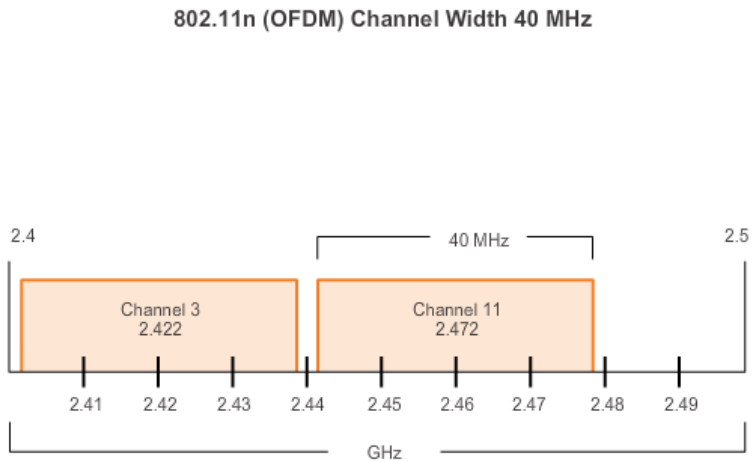


Figure 17 : 2.4GHz channels in 802.11n using channel bonding

802.11n supports two non-overlapping channels when using channel bonding

Planning AP Deployment

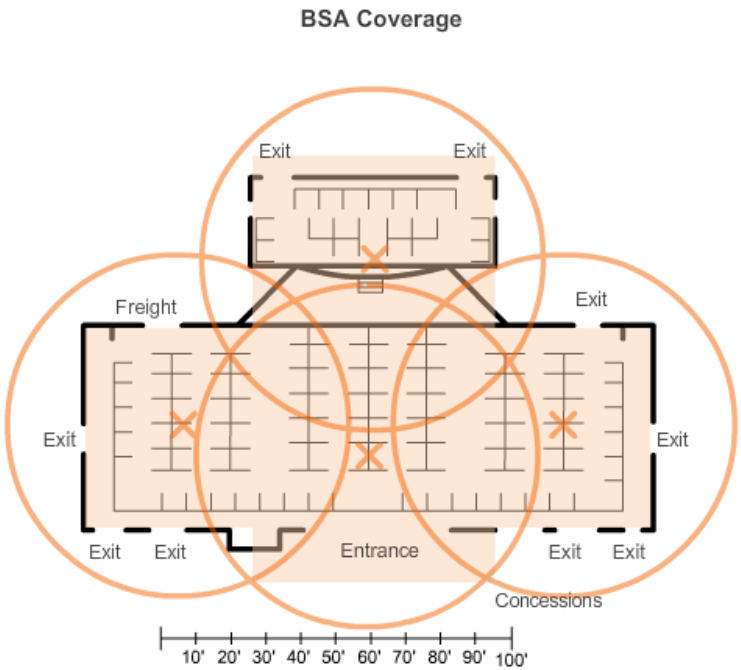


Figure 18 : Planning a WLAN Deployment

Aim for 15% overlap of the BSAs.

Overview - Wireless threats

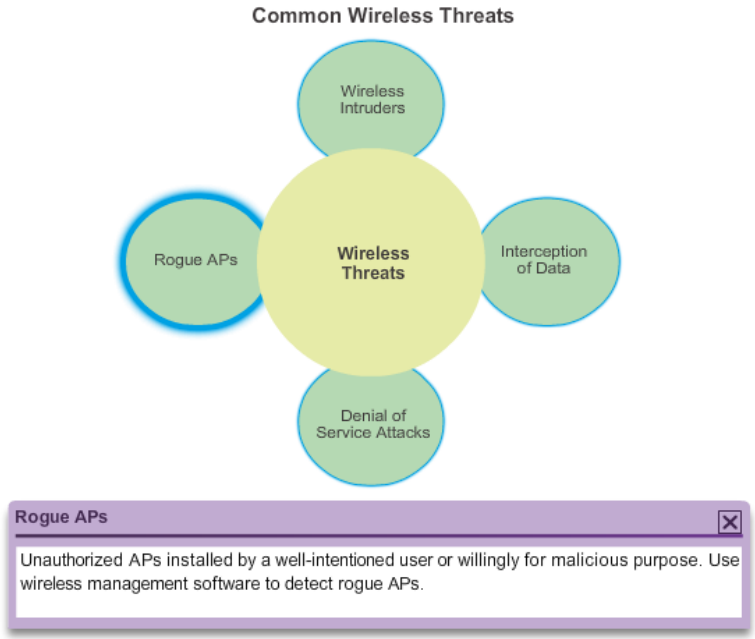


Figure 19 : Planning a WLAN Deployment

802.11b supports three non-overlapping channels

DoS Attacks

- Improper configuration
- Disconnect Attack
- CTS Flood
- Medium interference
  - Intentional interference from an attacker
  - Unintentional interference from devices (Phones, Microwaves etc.)

DoS Attacks cont.

- Spoofed Disconnect Attack
  - An attacker sends a series of Disassociate frames to all stations.
  - Will cause the stations to disconnect.
  - All stations will send a reassociation frames at the same time, creating a large traffic burst.
- CTS-flood
  - Misuse of CSMA/CA contention method.
  - Attacker floods the network with CTS-frames
  - Causes all stations connected to the network to withhold sending their data.

Rogue Access Point

- Connecting an access point to a network without authorization.
- Allows unsecured access to a network.
- Allows for man-in-the-middle attack.
- Monitor the radio spectrum for rogue access points.

Questions?