Nätverksteknik B - Introduktion till Trådlösa nätverk

Lennart Franked

Information och Kommunikationssystem (IKS)
Mittuniversitetet

4 februari 2016

- WPAN Wireless Personal-Area Network
  - Täcker ett område på upp till 100 meter.
  - Exempel: Bluetooth
- WLAN - Wireless Local Area Network
  - Täcker ett område på upp till 300 meter.
  - Exempel: WiFi 802.11a/b/g/n/ac/ad
- WWAN - Wireless Wide-Area Network
  - Täcker ett område på flera kilometer.
  - I.e. 3G, 4G, WIMAX
- Dagens fokus ligger på IEEE 802.11.

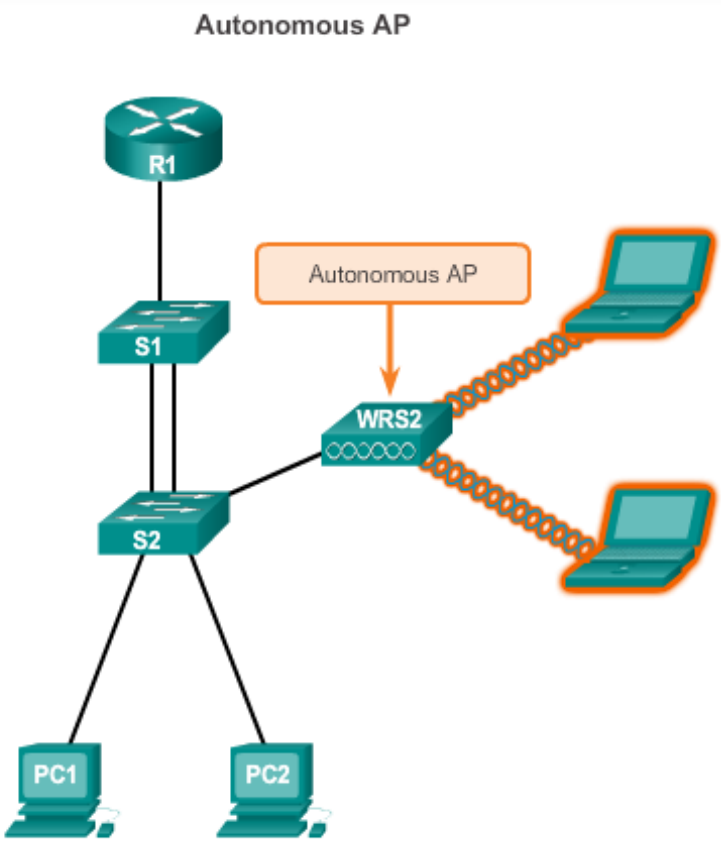
Tabell: 802.11 Standards[1]

IEEE Standard	Max Hastighet	Frekvens	Bakåtkompabilitet
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 Alliance försäkrar kompatibilitet mellan tillverkare.
- Försäkran om kompatibilitet täcker in:
  - 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

Typer av accesspunkter

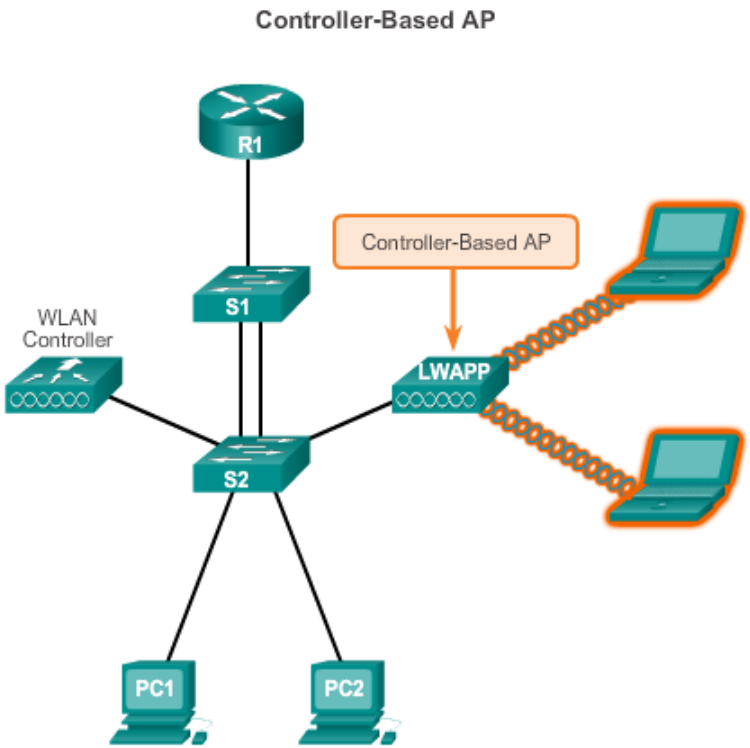
Koncept



Figur: Autonom accesspunkt [1]

- Hanteras individuellt

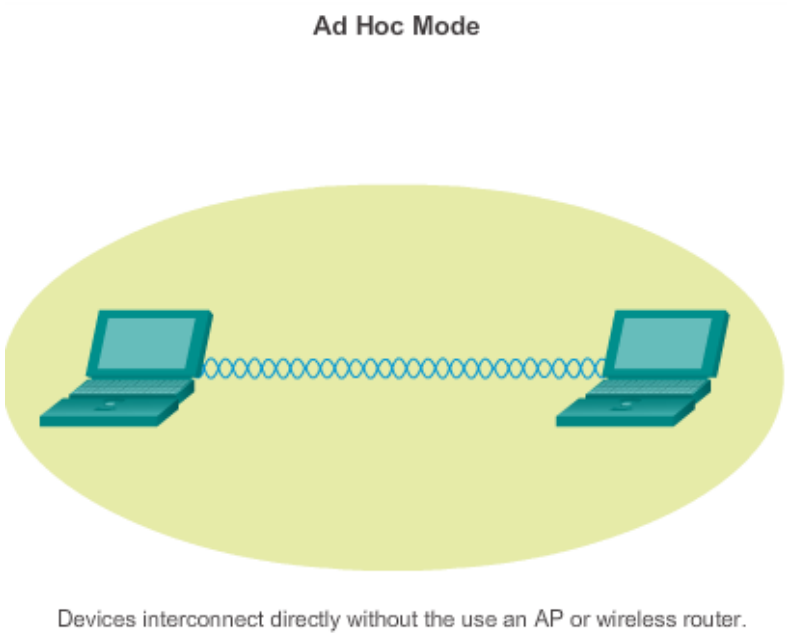
Typer av accesspunkter II



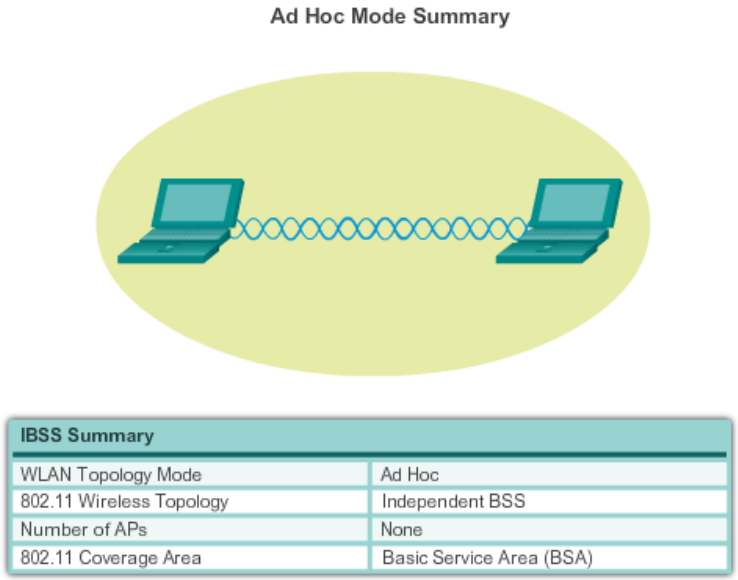
- Hanteras med hjälp utav en separat 'WLAN-controller'

Figur: Kontroller för Accesspunkter[1]

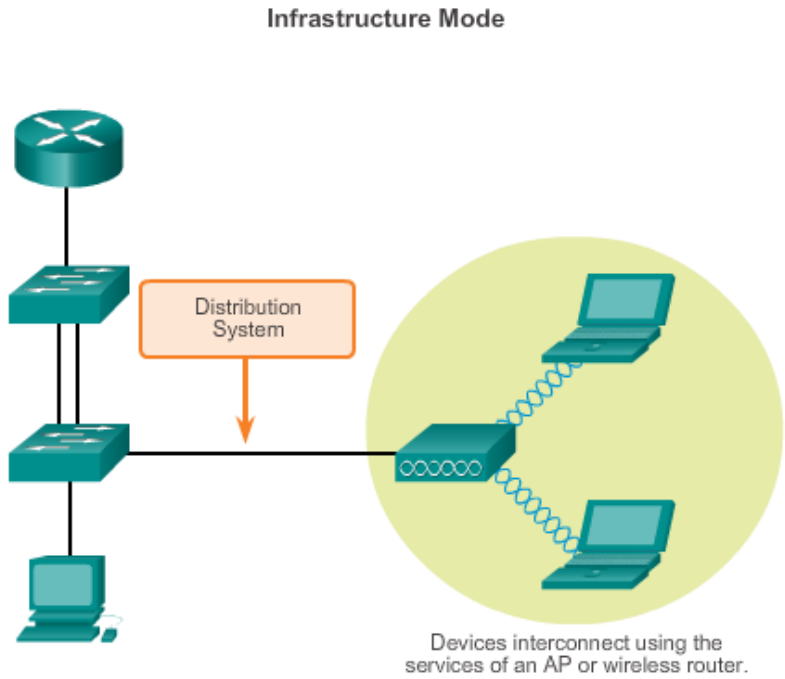
- Antal varianter av antenner:
  - Omni-direktionell - 360 täckning.
  - Direktionell - Fokuserar signalen i en riktning.
  - Yagi - Typ av direktionell antenn. Hög styrka, smalt band, lång räckvidd.



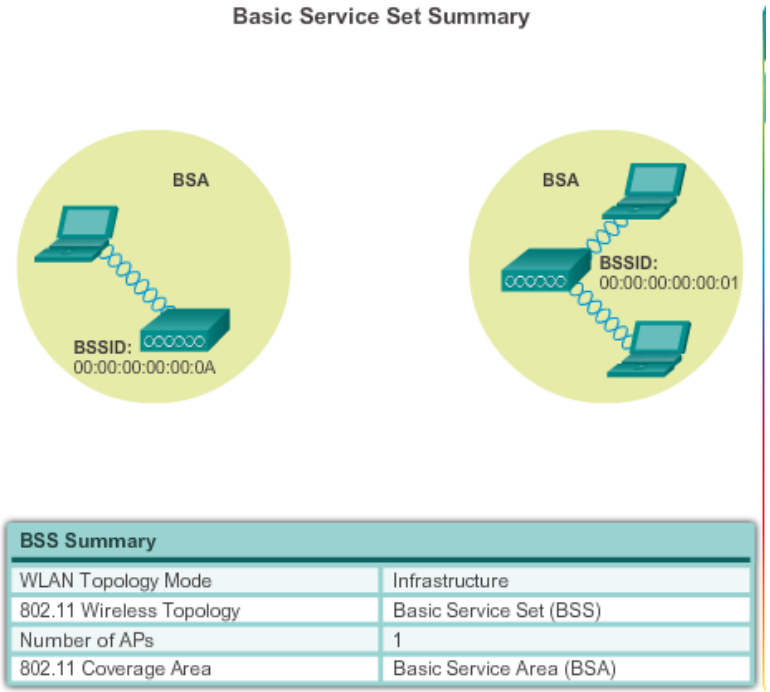
Figur: WiFi ad-hoc topologi[1]



Figur: Tethering - Personlig WiFi hot spot[1]

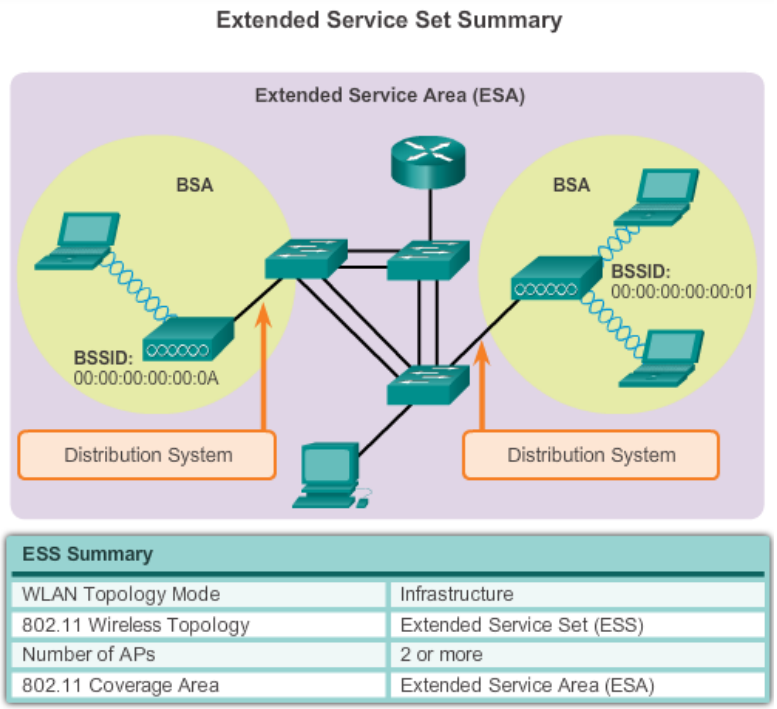


Figur: Infrastruktur[1]



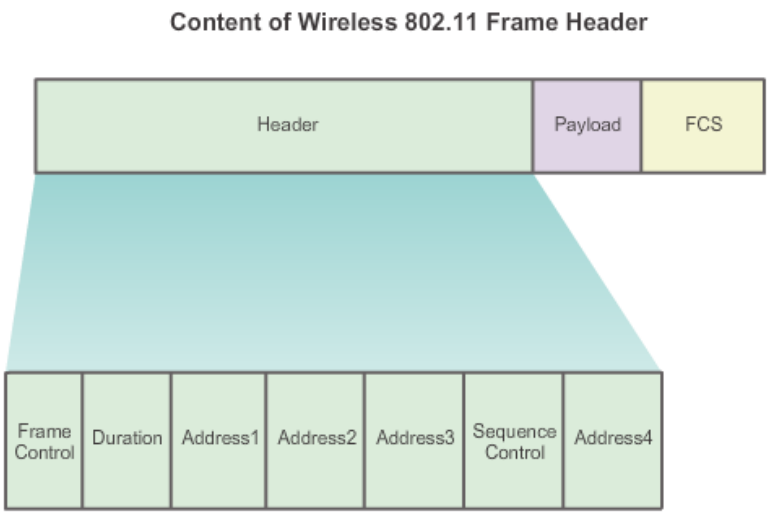
BSS Summary	
WLAN Topology Mode	Infrastructure
802.11 Wireless Topology	Basic Service Set (BSS)
Number of APs	1
802.11 Coverage Area	Basic Service Area (BSA)

Figur: Basic Service Set[1]



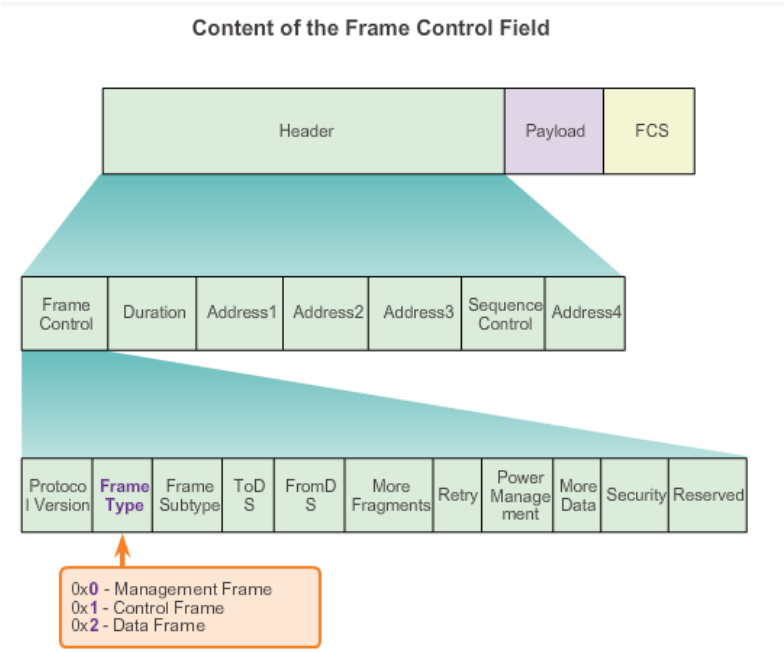
ESS Summary	
WLAN Topology Mode	Infrastructure
802.11 Wireless Topology	Extended Service Set (ESS)
Number of APs	2 or more
802.11 Coverage Area	Extended Service Area (ESA)

Figur: Extended Service Set[1]



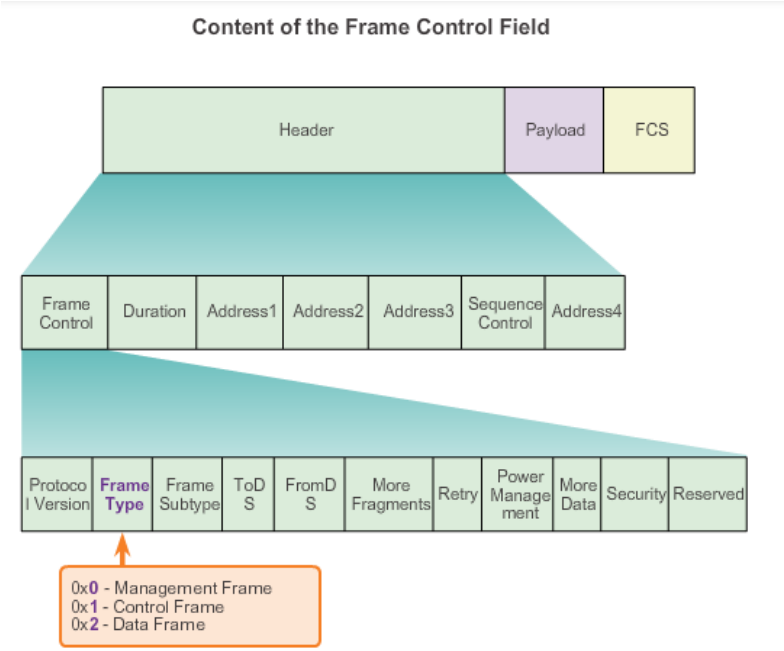
Figur: 802.11 Frame Header overview[1]

- Frame Control – Typ av ram
- Duration – Hur länge mediet är upptaget innan andra stationer kan försöka få tillgång.
- Address 1-4 – MAC-adresser på de enheter som är involverade i dataöverföringen.
- Sequence Control – Sekvens och Fragment nummer.
- Payload – Data
- FCS – Frame Check Sequence.



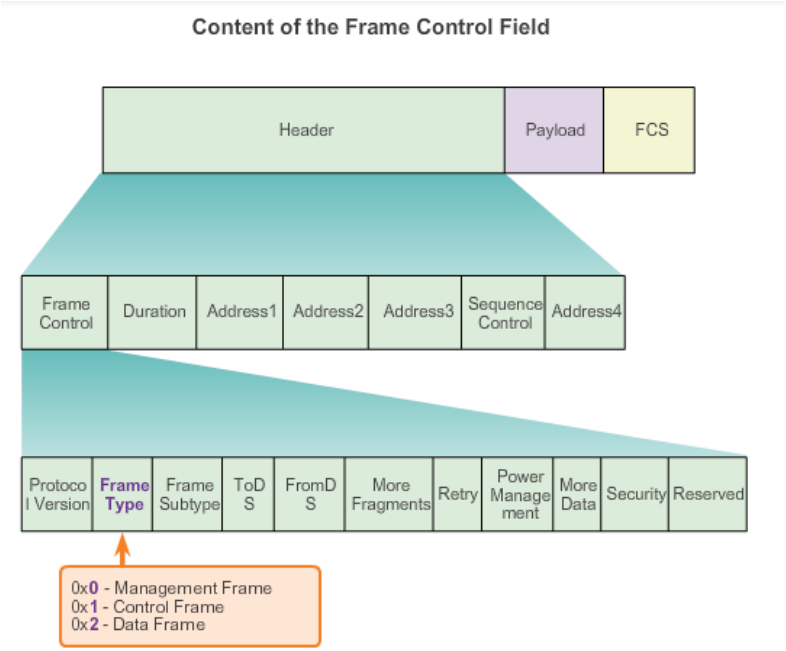
Figur: 802.11 Frame Control Header Field Översikt[1]

- Protocol Version –
- Frame Type/Frame Subtype – Typ av ram exempelvis management frame, data frame, control frame, följt utav specifika funktioner för den ramen.
- ToDS/FromDS – Riktning av ramen i förhållande till distributionssystemet.
- More Fragments – Sista fragmentet?



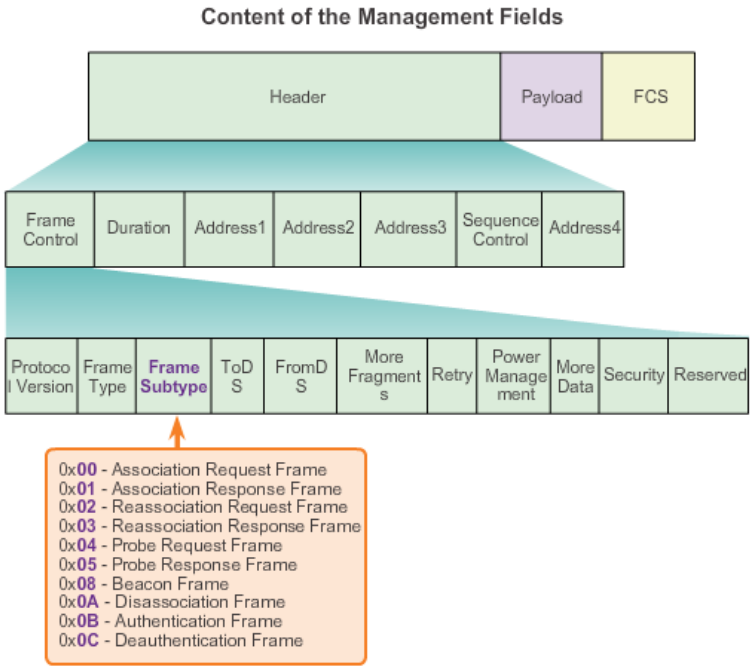
Figur: 802.11 Frame Control Header Field Översikt[1]

- Retry – Är ramen omskickad eller inte.
- Power Management – Active or power save.
- More Data – Kommer mer data att skickas? Används vid Power-save.
- Security – Ifall någon säkerhetsmekanism används.



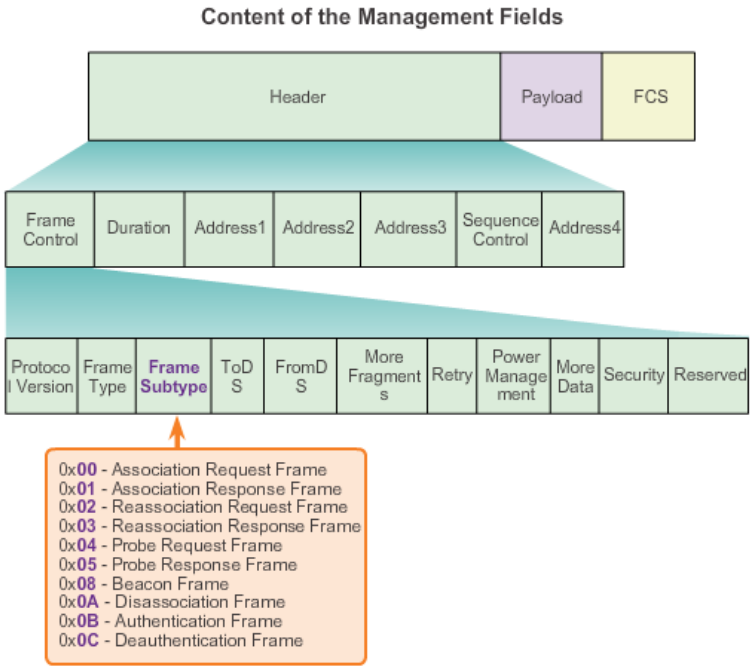
Figur: 802.11 Frame Type Header Field Översikt[1]

- Management Frame – Upprätthålla kommunikation, söka efter stationer och accesspunkter, authentisering, associering.
- Control Frame – RTS, CTS, ACK.
- Data Frame – payload.



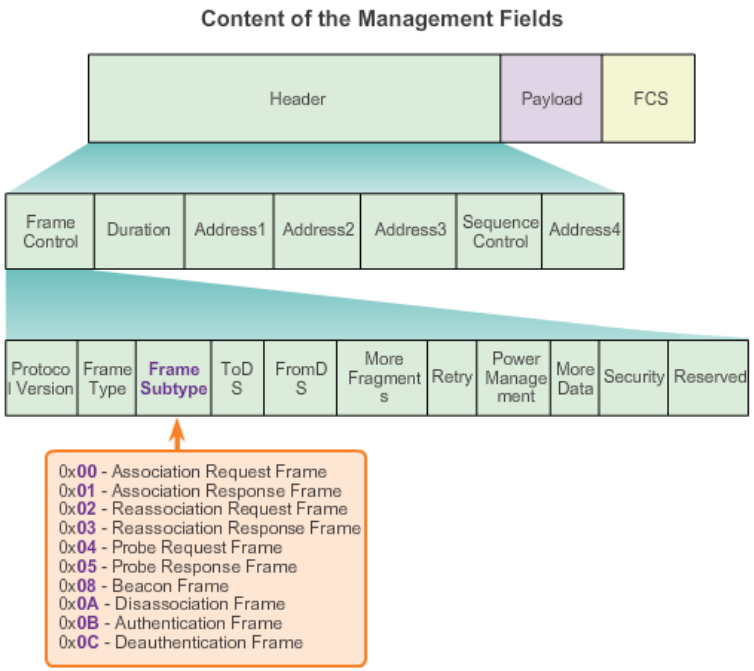
Figur: 802.11 Management Frames Översikt[1]

- 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.



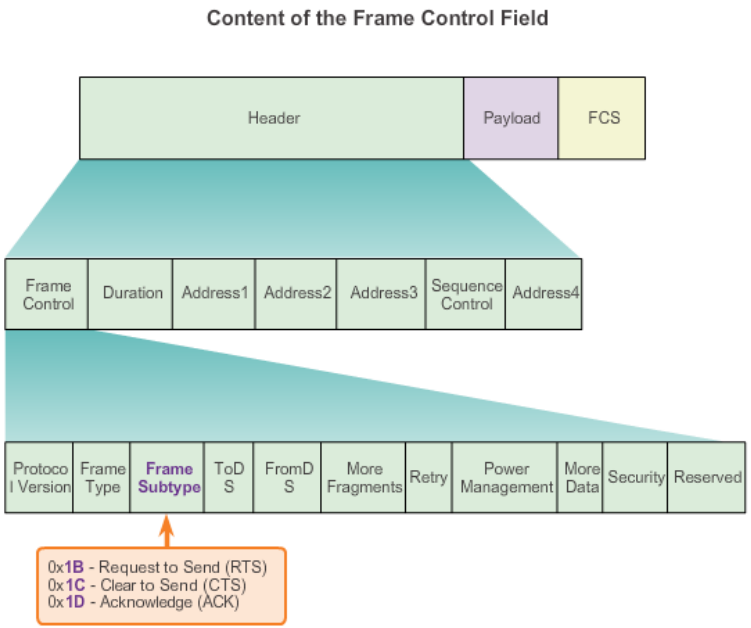
Figur: 802.11 Management Frames Översikt[1]

- 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.



Figur: 802.11 Management Frames Översikt[1]

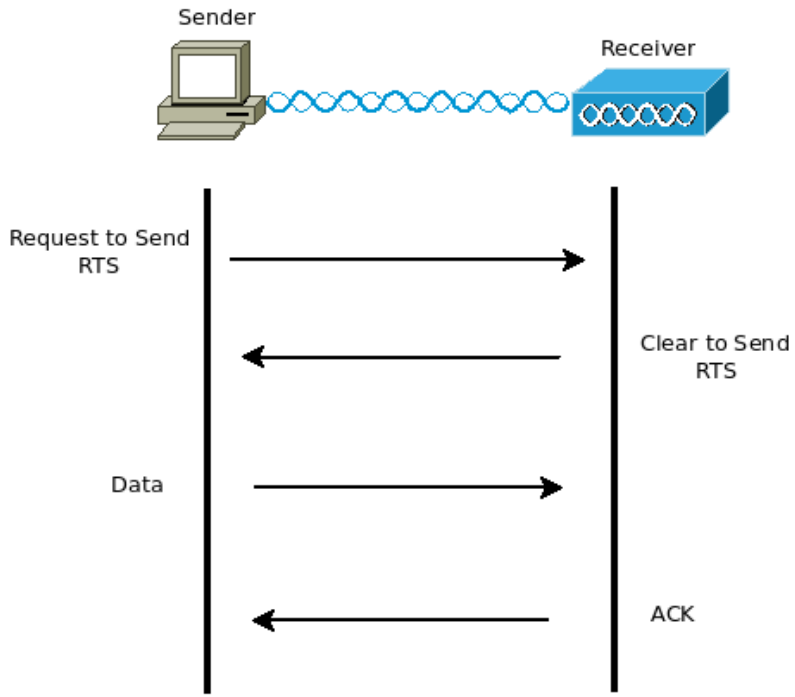
- Beacon – Skickas periodiskt från AP för att uppmärksamma om att den finns.
- Disassociation frame – Skickas från stationen då anslutningen ska stängas.
- Authentication frame – Används för authentisering. Innehåller ID information
- Deauthentication – Skickas från en station till en annan för att avsluta anslutningen.



Figur: 802.11 Frame Control Type Field Översikt[1]

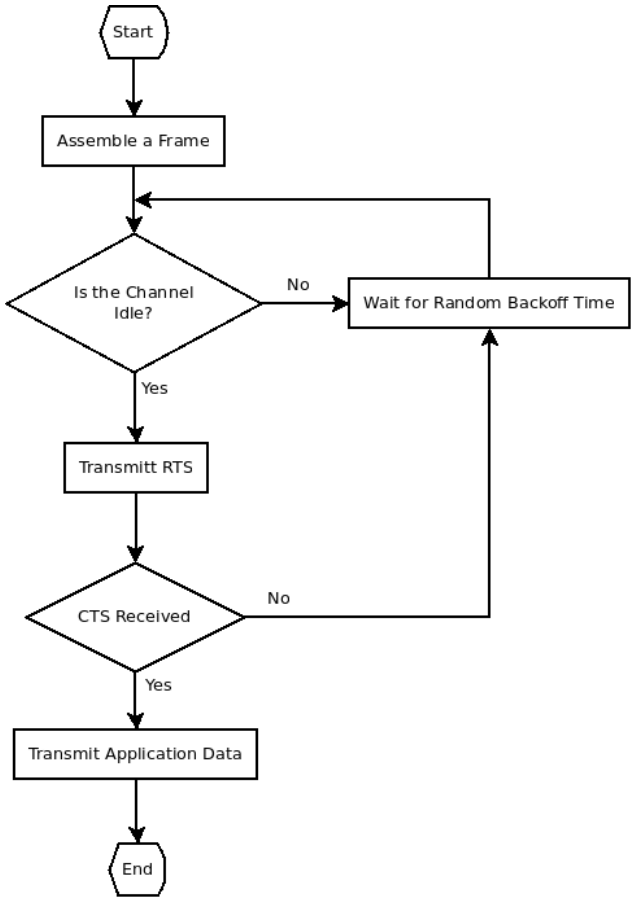
- Request to Send – Skickas från en station som vill använda mediet.
- Clear to Send – Skickas från Access punkten som ett svar på RTS.
- Acknowledgement – Bekräftelse.

[4]Används för CSMA/CA

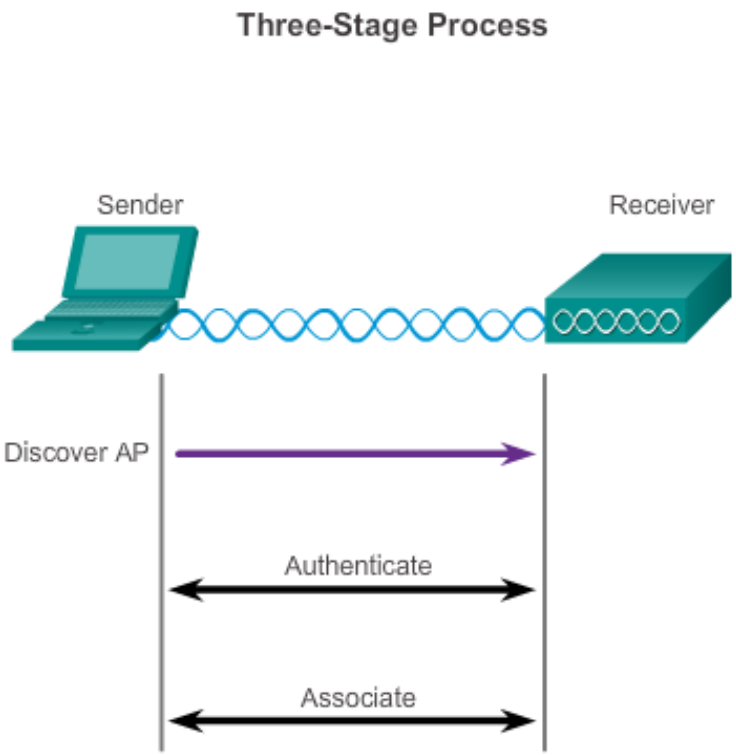


Figur: Utbyte av 802.11 Control Frames

Carrier Sense Multiple Access / Collision Avoidance



Figur: CSMA/CA Flowchart[1]

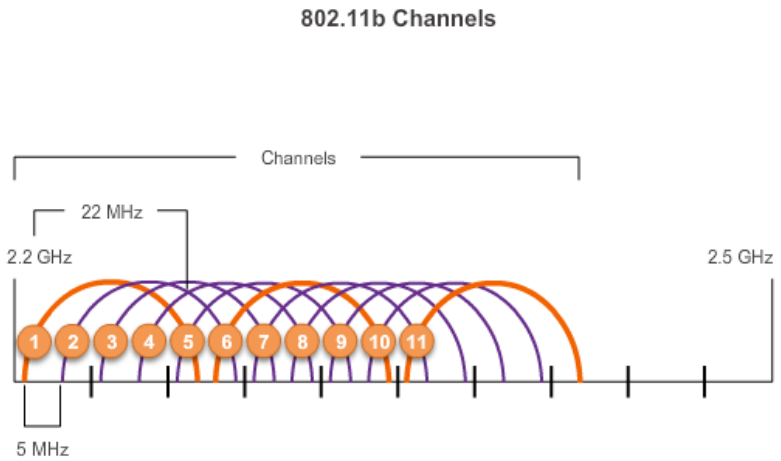


Figur: 802.11 AP Association[1]

- För en AP och en station att bli associerade måste de komma överens om följande parametrar.
  - SSID
  - Password
  - Network mode - 802.11 a/b/g/n/ac/ad
  - Security - Open, WEP, WPA, WPA2
  - Channel

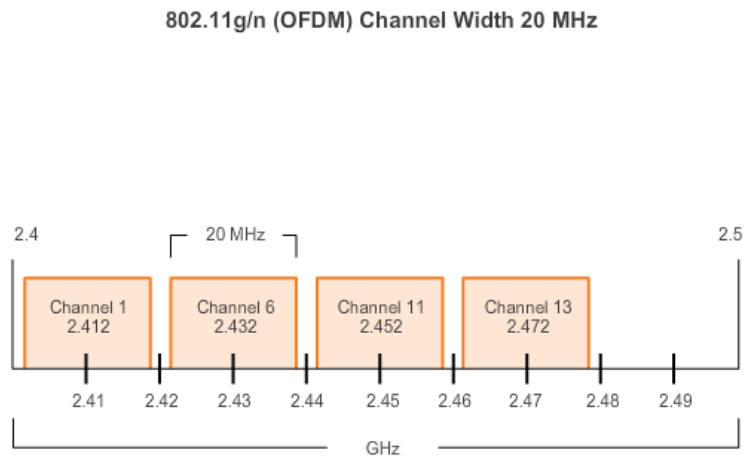
- Passive mode
  - Stationer kan passivt hitta tillgängliga nätverk.
  - Accesspunkter annonserar sig själva med hjälp utav 'beacons'.
- Active mode
  - Stationer måste aktivt söka efter tillgängliga accesspunkter.
  - Stationer måste veta nätverksparametrar, exempelvis SSID.
  - Prober skickas ut på flera kanaler.

- Direct Sequence Spread Spectrum (DSSS)
  - Sprids över ett större frekvensband, gör det mer resistant mot störningar.
  - > Används av 802.11b
- Frequency-hopping Spread Spectrum (FHSS)
  - Hoppar mellan olika frekvenskanaler.
  - Möjliggör en effektivare användning av kanaler.
  - Används av legacy 802.11.
- Orthogonal Frequency-Division Multiplexing (OFDM)
  - Delar upp en kanal i flera subkanaler.
  - Använder kanalerna mer effektivt.
  - Möjliggör användningen av MIMO.
  - Används i 802.11a/g/n/ac



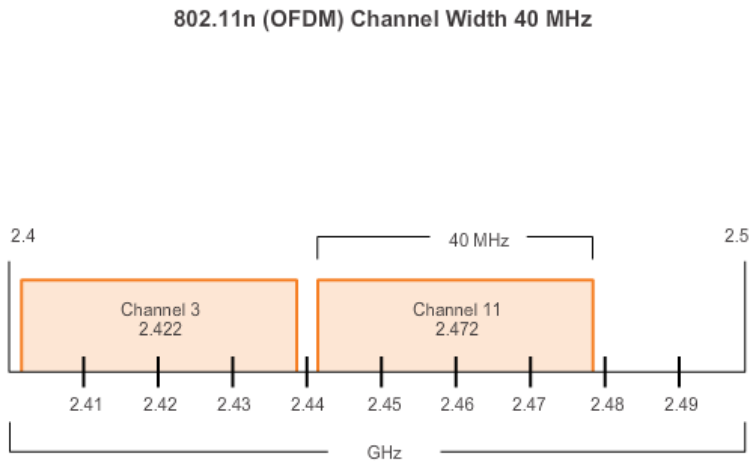
Figur: 2.4GHz channels in 802.11b[1]

802.11b stödjer tre ej-överlappande kanaler



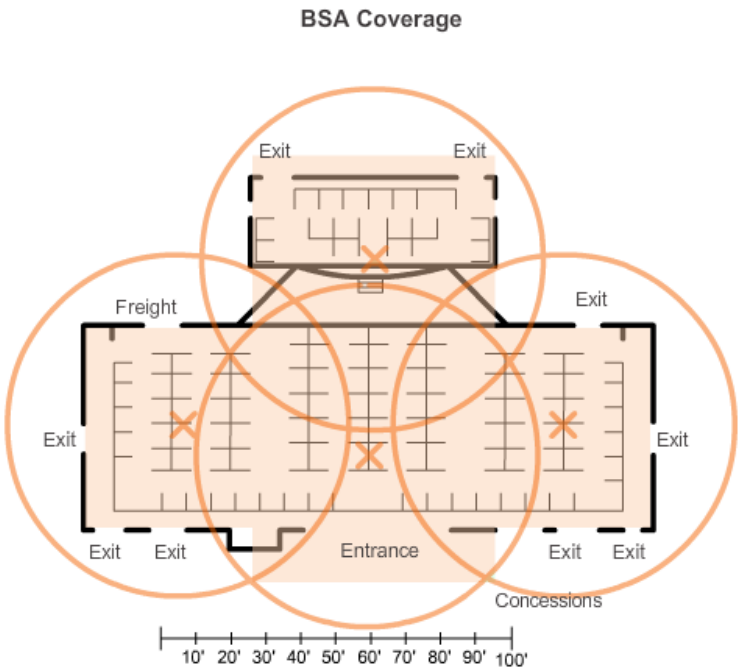
Figur: 2.4GHz channels in 802.11g/n[1]

802.11g/n stödjer fyra ej-överlappande kanaler



Figur: 2.4GHz channels in 802.11n using channel bonding[1]

802.11n stödjer två ej-överlappande kanaler vid 'channel bondning'

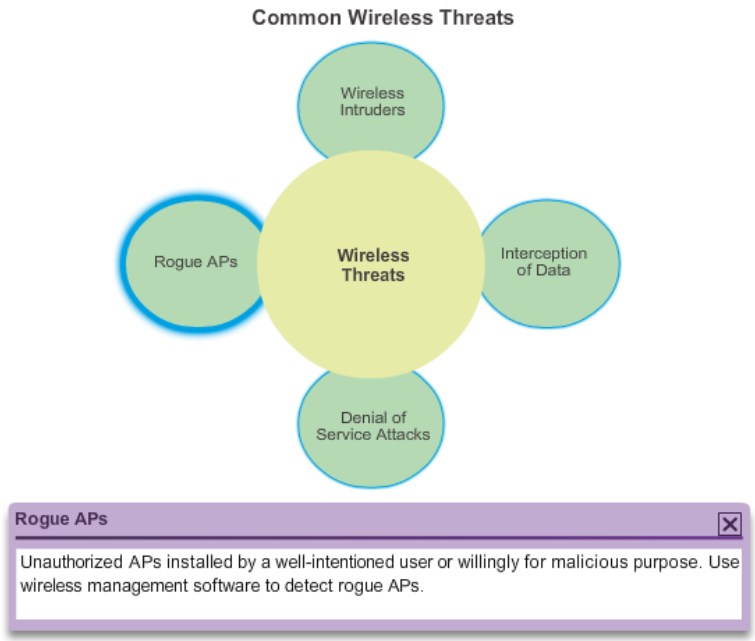


Figur: WLAN Deployment[1]

Försök skapa 15% överlapp av BSA.

Översikt - Wireless threats

Threats connected to Wireless Networks



Figur: Överblick hot[1]

DoS attacker

- Dålig konfiguration
- Disconnect attack
- CTS Flod
- Störning av medium.
  - Avsiktlig
  - Oavsiktlig (telefoner, Microwaves etc.)

Spoofad disconnect Attack

- En angripare skickar en serie 'disassociate frames' till alla stationer.
- Orsakar att stationerna stänger ner anslutningen.
- Alla stationer kommer att begära att bli associerade igen samtidigt.
- Genererar en stor mängd data.

CTS-flood

- Utnyttjar CSMA/CA 'contention method'.
- Angriparen flodar nätverket med CTS-ramar
- Resulterar i att stationerna inte skickar något data.

Rouge Access Point

- Ansluter en accesspunkt utan godkännande.
- Tillåter osäker anslutning till nätverket.
- Möjliggör en Man-in-the-middle attack.
- Övervaka efter nya accesspunkter.

Referenser

Connecting networks : companion guide. Indianapolis, Indiana, 2014.