# WLAN / 802.11

Canais 2.4 GHz → conseguem ser visíveis até três canais abaixo e acima.

(Rede no canal 3 e rede no canal 7 são ambas visíveis no canal 5 → dá para captuar os beacons de ambas as redes).

- A frequência é dividida em canais

EU: (13 canais, 5MHz entre eles, 2412 - 2472)

Industrial: 14 canais, 5MHz, 2401 - 2495.

5GHz : 5.150 - 5.850

Beacon frame → Tipo 0 (management), subtipo 8.

Contém info sobre a rede Wi Fi, e envia-a periodicamente

anunciam a rede e sincronizam membros de um serviço.

*Podem observar-se beacons de várias redes pois existe um overlap no scan de canais (ex: quando se analisa o canal 5, vê-se os beacons do 4 e 6).

Probe Request → Tipo 0, subtipo 4.
Enviado para que os APs enviem informação sobre as redes WiFi disponíveis para conexão.

Probe response → Tipo 0, subtipo 5
Resposta do AP com info sobre a rede.

RTS (request to send) → Tipo 1 (control), subtipo 11
Enhance sense process. Collision avoidance.

CTS (Clear to send) → Tipo 1, subtipo 12.

ACK → Tipo 1, subtipo 13.
Acknowledgment da AP sobre

a informação recebida.

Tipo 2 (Data) → Data (0), Null (no data - 4), QoS data (8), QoS null (12), Reserved (13).

Periodicidade dos Beacon Frames depende da informação nos 'Fixed Parametens':

- beacon interval : 0,10 s.

'Tagged Parametens':

- SSID
- Supported Rates (velocidade)
- Canal atual

...

Authentication → Tipo 0, subtipo 11

Association request → Tipo 0, subtipo 0

Association response → Tipo 0, subtipo 1

1° passo é a autenticação. O dispositivo mostra a sua identidade com a AP (não há encriptação).

Depois da autenticação vem a associação, onde os dispositivos podem associar para ganhar acesso total à rede.

0

Dispositivo manda association request.
AP verifica e manda association reply com o código 0 de sucesso ou outro de insucesso

Depois, se sucesso, a AP faz fonwarding dos pacotes de/para o dispositivo.

DHCP → Funciona encapsulado por um pacote 802.11 dento do tipo 2 e subtipo 8 (Data, QoS Data).

ARP → São encapsulados nos pacotes 802.11 (semelhante a DHCP em Data (tipo 2) e QoS Data (tipo 8).

ICMP → " " (tipo 2, subtipo 8).

ICMP Echo request:

Flag DS status (0x01)

ICMP Echo reply:

Flag DS status (0x10)

---

Caminho de pacotes entre duas ST dentro da rede:

STA → AP → STB

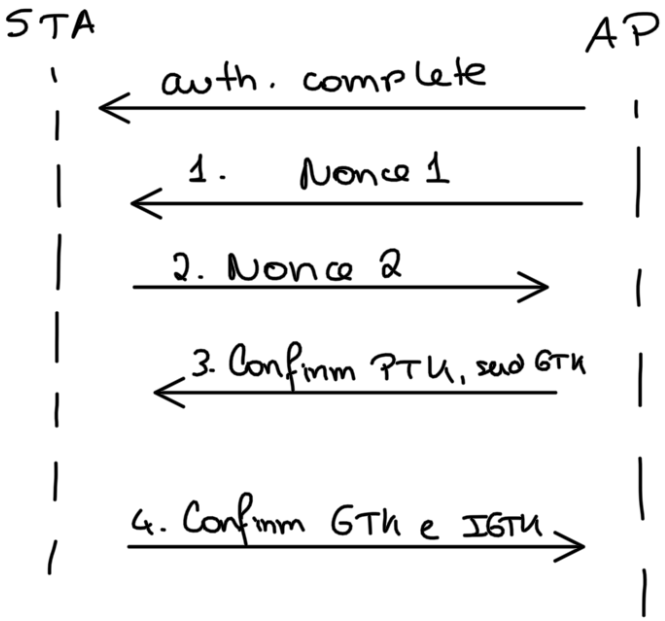
STB → AP → STA

Quando vai de STA → AP, a flag DS Status vai a 0x01. Quando vai da AP para uma STA, a flag vai a 0x10.

Podemos captar o mesmo pacote 2 vezes pois uma das vezes é quando vai da estação para a AP e outra da AP para o destino.

---

4 way handshake EAPOL




Disassociation → Tipo 0, subtipo 10
Fim de uma transmissão, ligação. Vai sair da cell atual.

---

WLAN 2.

Pacotes RTS/CTS → Só são enviados quando o pacote tem tamanho inferior a 200 bytes.

Em pacotes maiores, há fragmentação, onde esta acontece antes dos pacotes irem enviados para a rede.