Ethernet and Wireless

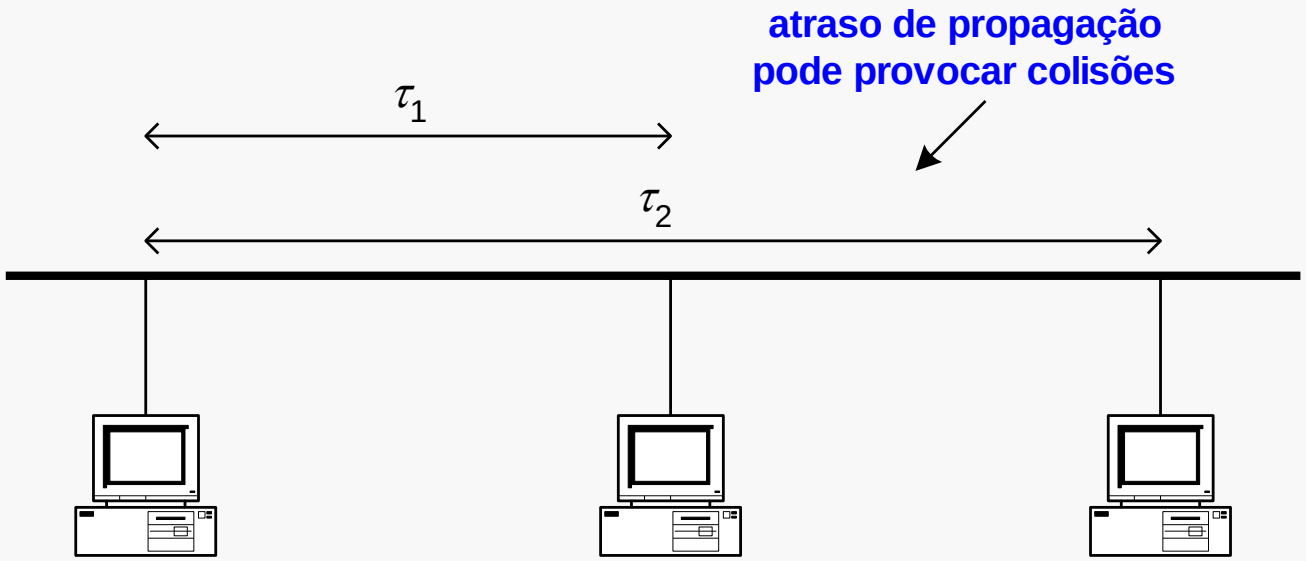
Redes de Comunicações 1

Licenciatura em Engenharia de Computadores e Informática

DETI-UA, 2021/2022

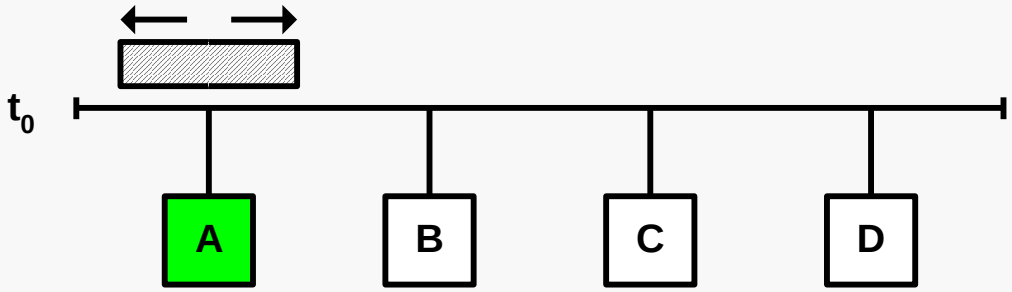
CSMA (Carrier Sense Multiple Access)

- As estações transmitem e recebem no mesmo canal
- As estações **escutam o meio antes de transmitir**; só transmitem se o meio for detectado livre
- O número de colisões é minimizado
- Podem ocorrer colisões porque as estações estão a alguma distância umas das outras

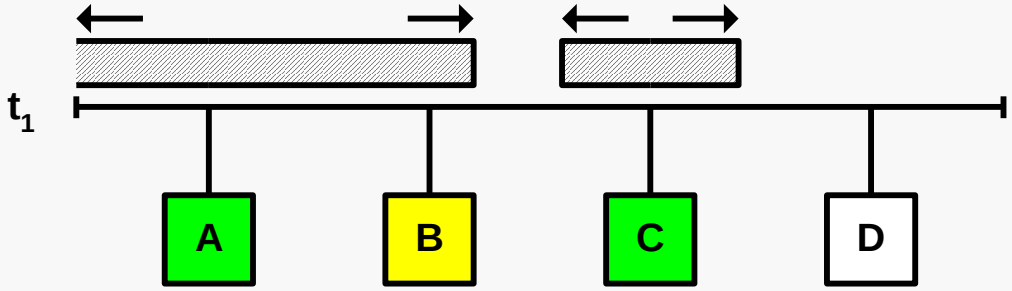


CSMA/CD (CSMA *with Collision Detection*) (I)

- **As estações quando detectam uma colisão param de transmitir**

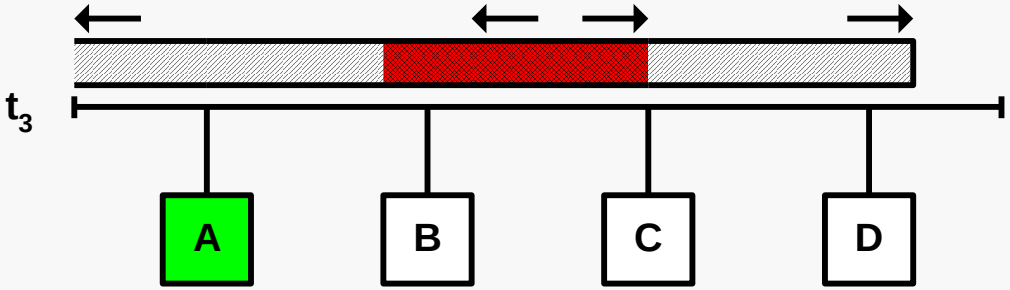


A estação A detecta o meio livre e inicia a sua transmissão

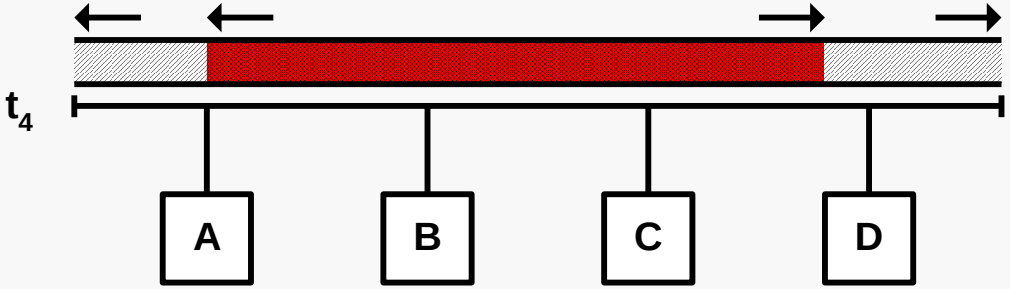


A estação B pretende transmitir mas não o faz porque detecta o meio ocupado; a estação C inicia a transmissão

CSMA/CD (II)

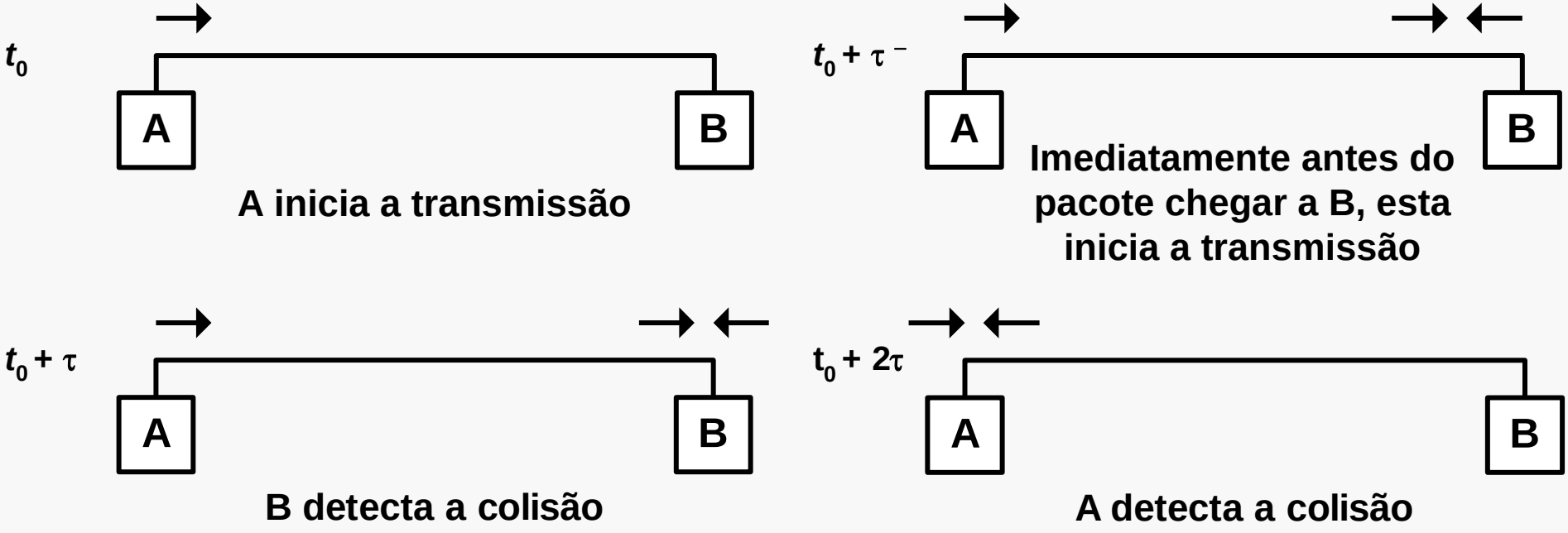


C detecta a colisão e pára de transmitir



A detecta a colisão e pára de transmitir

CSMA/CD (III)



Garantir que todas as estações emissoras detectam colisões

⇒

tempo mínimo de transmissão de um pacote > *round-trip delay*

CSMA/CD (IV)

- é forçado um intervalo mínimo entre o fim de uma transmissão ou receção e o início de nova transmissão (IFS - Inter Frame Spacing = 9.6 μs @ 10 Mb/s)
- se o meio é detetado ocupado as estações continuam a escutar até que o meio seja detetado livre; quanto isso acontecer, transmitem imediatamente (o protocolo diz-se 1-persistente)
- quando uma estação transmissora deteta uma colisão, interrompe a transmissão da sua trama e envia para o canal uma sequência de bits, designada por JAM
- depois do envio de JAM a estação espera um tempo aleatório até retransmitir, definido pelo Algoritmo de Recuo Binário Exponencial Truncado

CSMA/CD (V)

- **O número de ranhuras temporais (time slots) de atraso antes da *n*-ésima tentativa de retransmissão é uma v.a. *r* uniformemente distribuída no intervalo**

$$0 \leq r < 2^k, \text{ com } k = \min(n,10)$$

- **Duração da ranhura = 64 bytes = 512 bits = 51.2 μs (10 Mbps)**
- **Exemplo:**
  - $n = 1 \Rightarrow r = 0$ ou 1 (0 ou 51.2 μs)
  - $n = 2 \Rightarrow r = 0, 1, 2$ ou 3 (0, 51.2, 102.4 ou 153.6 μs)
    ⋮
  - $n > 10$, atraso máximo fixado em $2^{10}-1 = 1023$ ranhuras
- **Número máximo de tentativas de retransmissão = 16**

CSMA-CD - desempenho

A utilização do CSMA/CD é

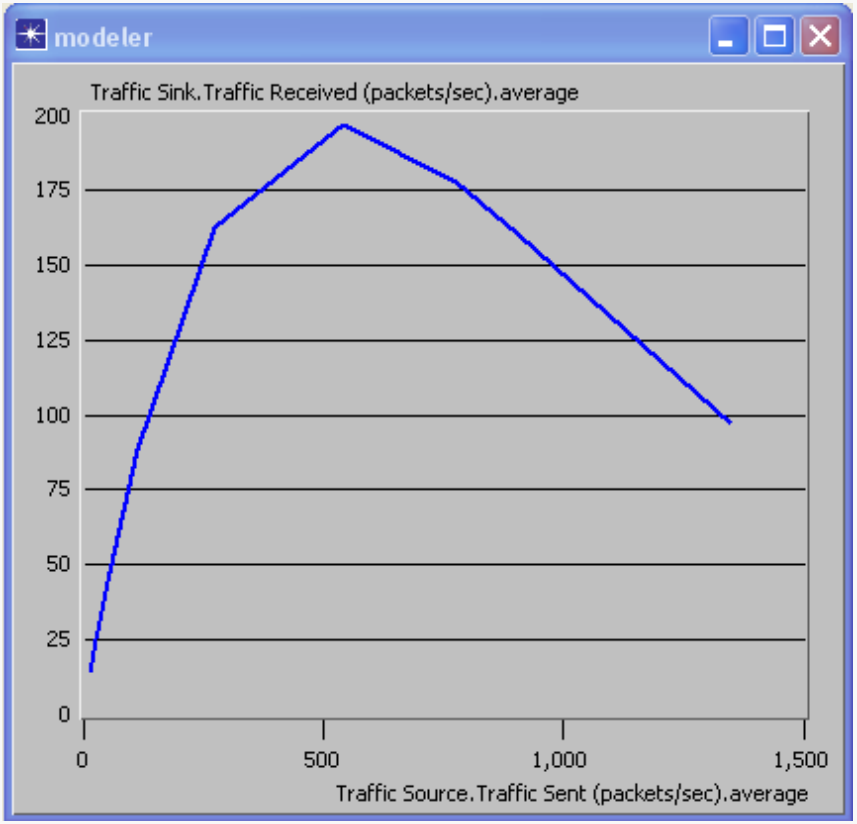
$$S \underset{N \to \infty}{\to} \frac{1}{1 + 3.44a}$$

$a = \tau/T$, T – tempo de transmissão de um pacote (tempo útil)

- a<1

CSMA-CD - desempenho

- Aumento de tráfego de entrada
  - Aumento de tráfego transmitido, mas…
  - Aumento das colisões

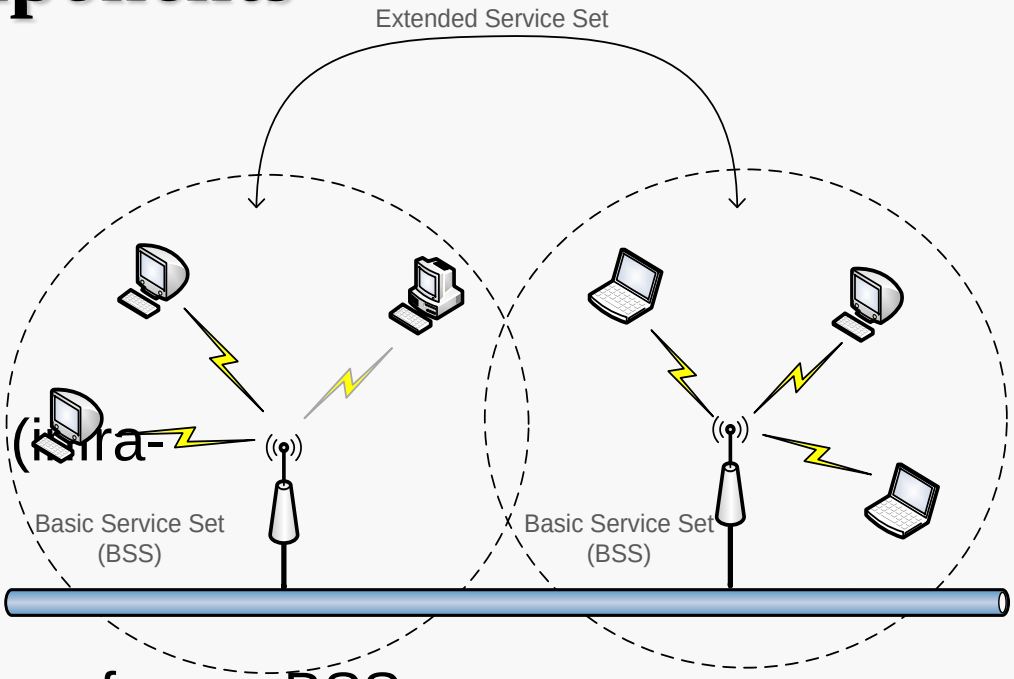


Wireless Networks

Evolution of WLAN standards

- **WiFi 1 - 802.11b, 1999, 2.4 GHz band, 11 Mbps data rate**
- **WiFi 2 - 802.11a, 1999, 5 GHz band, 54 Mbps data rate**
- **WiFi 3 - 802.11g, 2003, 2.4 GHz band, 54 Mbps data rate**
- **WiFi 4 - 802.11n, 2009, 2.4 and 5 GHz bands, ~600 Mbps data rate**
- **WiFi 5 - 802.11ac, 2013, 5 GHz band, ~1.3 Gbps data rate**
- **WiFi 6 - 802.11ax, 2019, 1 to 7GHz bands, >11Gbps data rate**

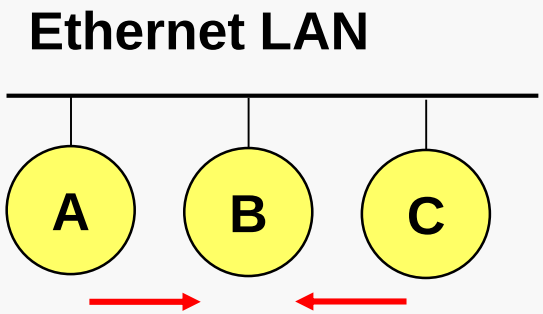
Components

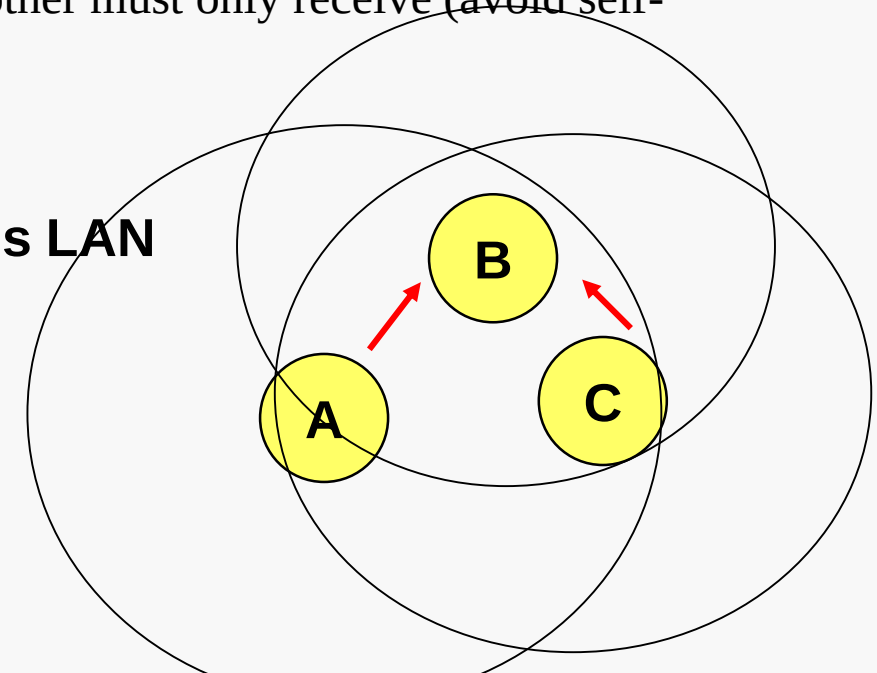


- Station (STA)
  - Mobile terminal
- Access Point (AP)
  - STA connect to access points (infra-structured networks)
- Basic Service Set (BSS)
  - STA and AP with same coverage form a BSS
  - Group of IEEE 802.11 stations associated to an Access Point (AP)
  - Known through the SSID
- Extended Service Set (ESS)
  - Several BSSs interconnected by APs form a ESS

Wired vs Wireless differences

- A and C sense the channel empty simultaneously
  - Send traffic at the same time
- Ethernet: sender can detect collision
- Wireless: radios cannot detect collision (work in half-duplex)
  - Full-duplex: both can transmit and receive information between each other simultaneously
  - Half-duplex: transmission and reception of information must happen alternatively. While one point is transmitting, the other must only receive (avoid self-interference)



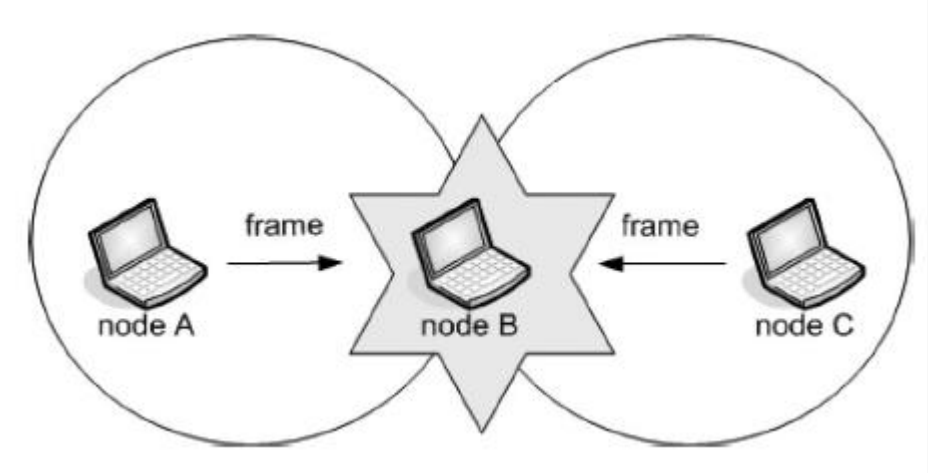


Wireless MAC

- Wired MACs
  - Typical: CSMA/CD
  - Medium is free → send
  - Listen to sense collision
- What about wireless?
  - Signal power reduces with the square distance
  - Sender can apply CS and CD, but collisions occur in the receiver!
    - Sender may not listen the collisoon (CD does not work)
    - CS may not work either with hidden nodes

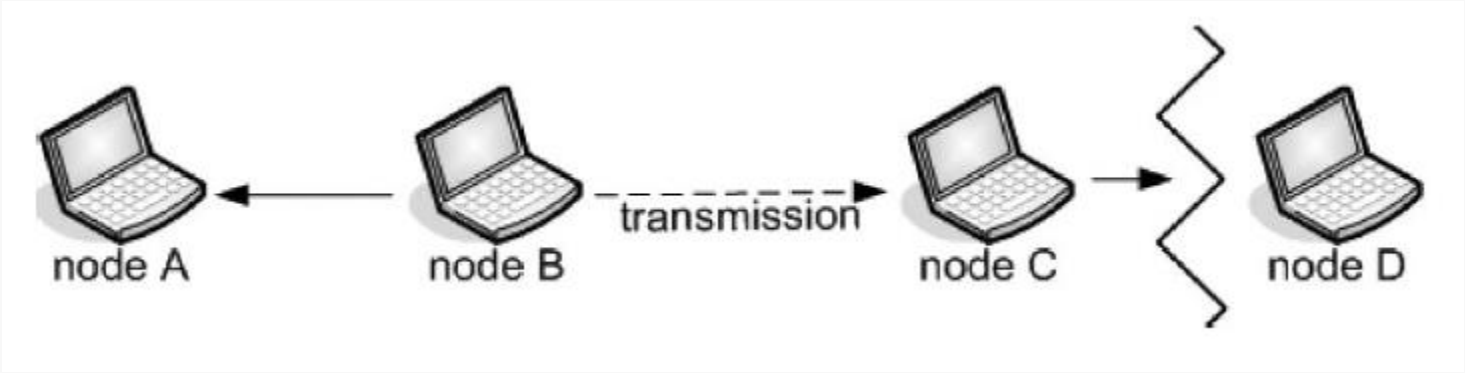
Hidden nodes

- Hidden terminals
  - A and C do not ear each other
  - Collision in B, if A and C send at the same time
  - Nor A nor C understand that collision occured
- Solution
  - Detect collisions in the receiver
  - “virtual carrier sensing”: sender asks the receiver if he is receiving traffic; in the case of absense of answer, he assumes that the channel is busy



Exposed nodes

- Exposed terminals
  - B sends to A; C wants to send to D
  - C senses the network and discovers that the medium is occupied
  - D is not in the range of B and A is not in the range of C, so the traffic could be transmitted
  - A and D are exposed terminals
- The transmissions could be done in parallel with no collision

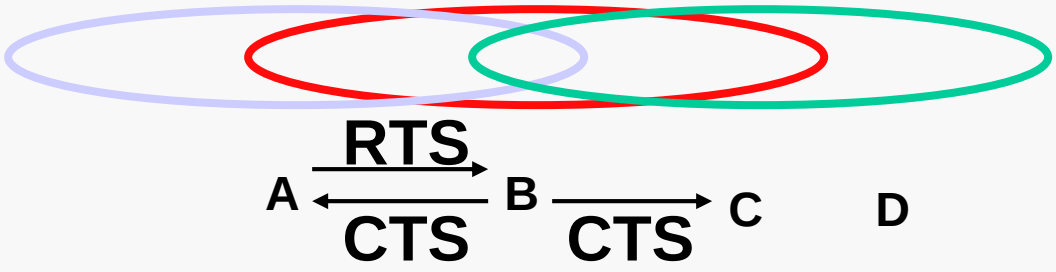


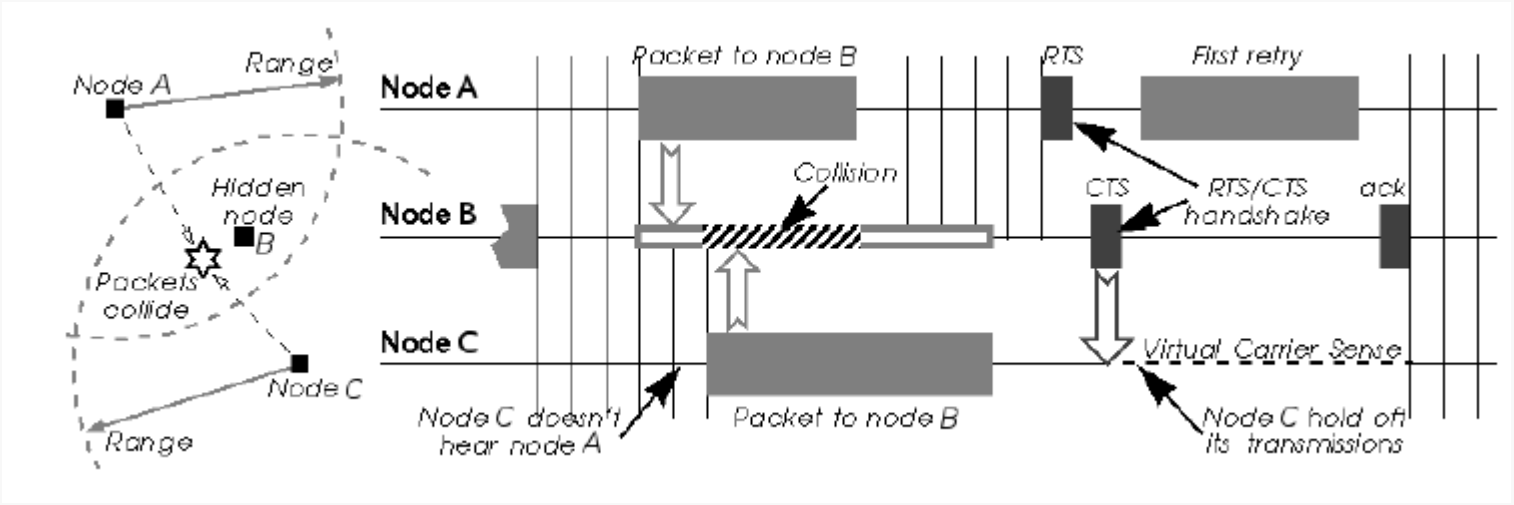
MACA: Multiple Access with Collision Avoidance

- MACA: avoids collisions using signalling packets
  - RTS (request to send)
    - A small packet is sent before transmitting
  - CTS (clear to send)
    - Receiver provides the right to transmit, when it is able to receive
- Signaling packets (RTS/CTS) contain
  - Sender address
  - Receiver address
  - Packet length (to be transmitted)
- Used in networks scenario with a large amount of traffic/collisions

MACA: Hidden Nodes

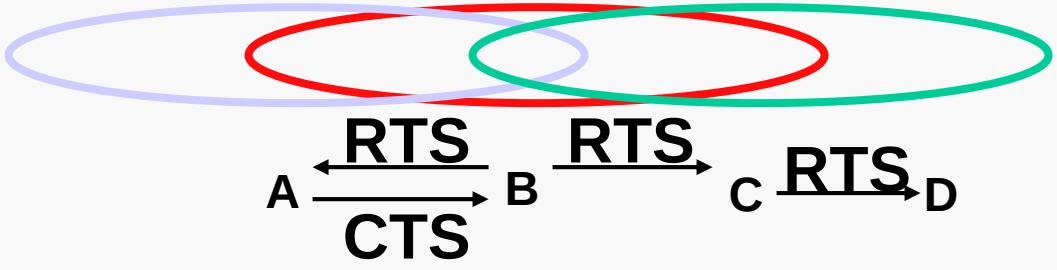
- MACA and hidden nodes
  - A, C → B (?)
  - A –-RTS → B
  - B –- CTS → A
  - C ears CTS of B
  - C waits for the period announced in A transmission

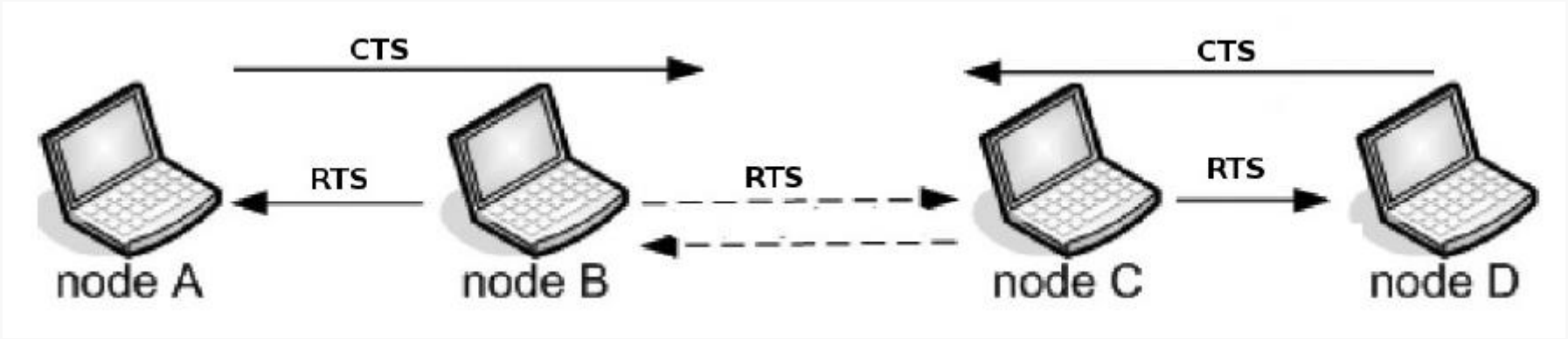




MACA: Exposed Nodes

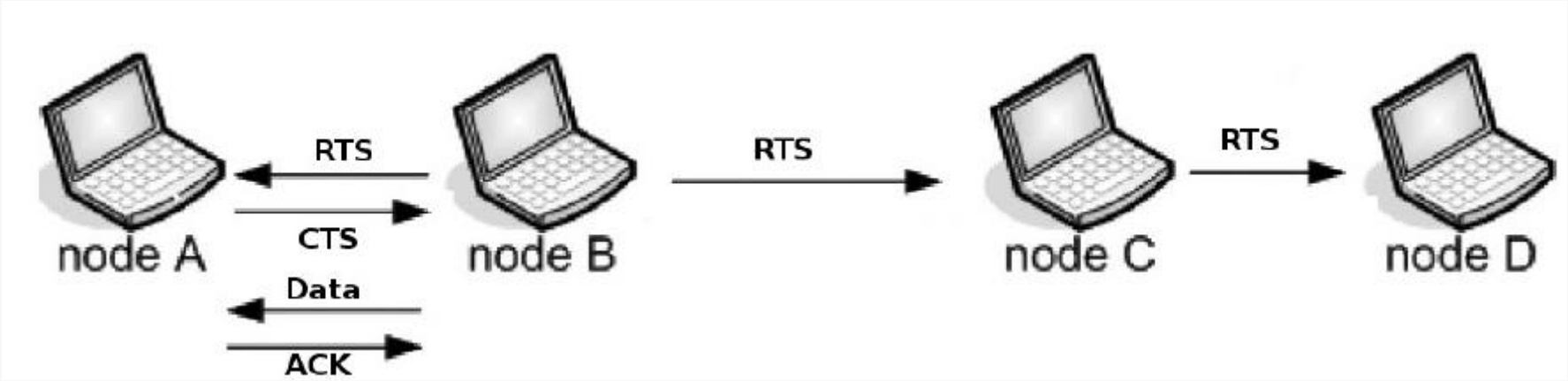
- MACA and exposed nodes
  - B → A, C → D(?)
  - B RTS → A
  - A CTS → B
  - C ears RTS of B
  - C does not ear CTS of A
  - C RTS → D





MAC reliability

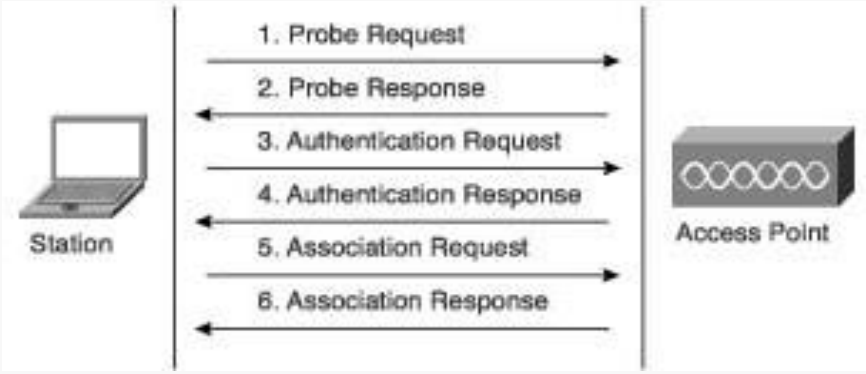
- Wireless connections are very prone to errors
  - Transport is not reliable
- Solution: use acknowledgements
  - When A receives DATA from B, answers with ACK.
  - If B does not receive ACK, B retransmits
  - C and D will not transmit until the ACK (to avoid collisions)
  - Total expected duration (including ACK) is included in the RTS/CTS packets

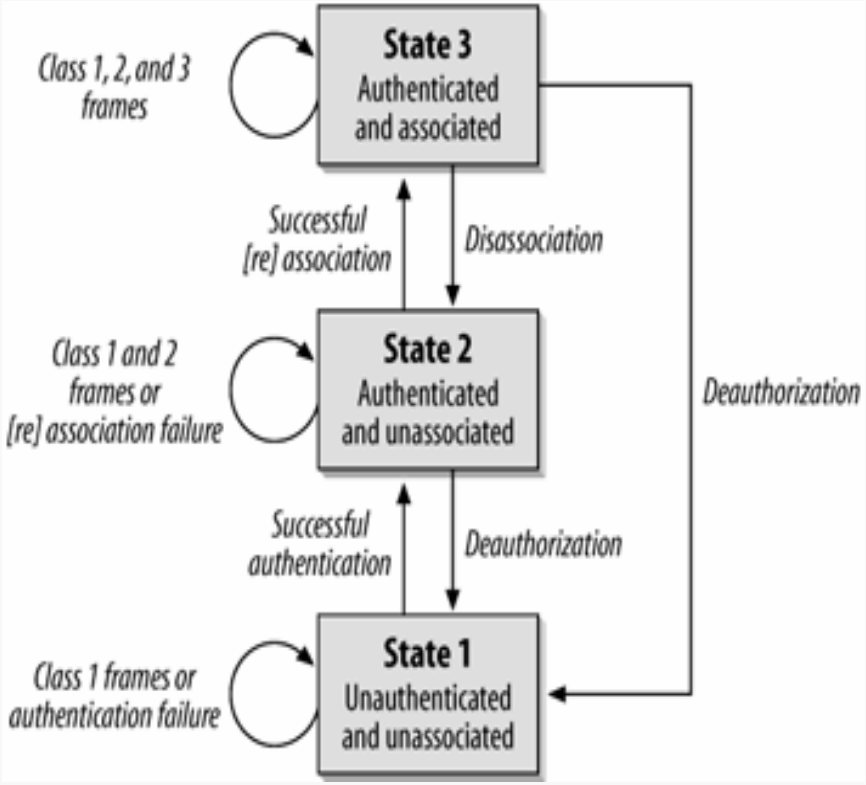


Wireless Networks: how to start a connection?

Joining a BSS

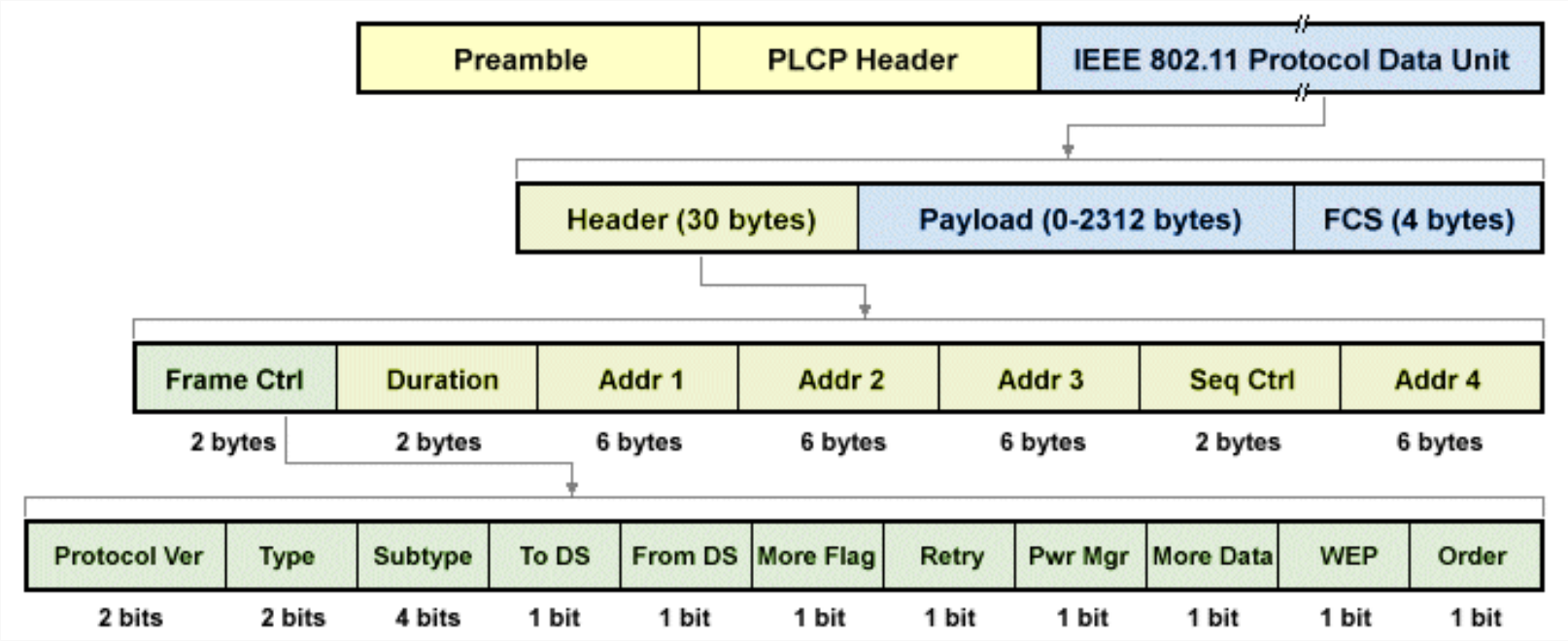
- **Station finds BSS/AP by Scanning/Probing.**
- **BSS with AP: both Authentication and Association are necessary for joining a BSS.**





WLAN Frames

- Three types of frames
  - Control: RTS, CTS, ACK
  - Management
  - Data
- Header is different for the different types of frames.



Joining BSS with AP: Scanning

- A station willing to join a BSS must get in contact with the AP. This can happen through:

- 1. Passive scanning
  - The station scans the channels for a Beacon frame that is sent periodically from an AP to announce its presence and provide the SSID, and other parameters for WNICs within range

- 2. Active scanning (the station tries to find an AP)
  - The station sends a Probe Request frame - Sent from a station when it requires information from another station
  - All AP's within reach reply with a Probe Response frame - Sent from an AP containing capability information, supported data rates, etc., after receiving a probe request frame

Beacon Frame

```
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▸ Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    .... .... .... 0000 = Fragment number: 0
    1001 1000 1010 .... = Sequence number: 2442
    Frame check sequence: 0x6f0b825c [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (12 bytes)
      Timestamp: 660070796
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0421
  ▾ Tagged parameters (123 bytes)
    ▸ Tag: SSID parameter set: LABCOM
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 13
    ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Cisco CCX1 CKIP + Device Name
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (1) (1)
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX version = 5
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled
```

Probe Request/Response Frames

```
IEEE 802.11 Probe Request, Flags: ........C
  Type/Subtype: Probe Request (0x0004)
  Frame Control Field: 0x4000
  .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Transmitter address: Microsof_0a:43:e3 (c0:33:5e:0a:43:e3)
  Source address: Microsof_0a:43:e3 (c0:33:5e:0a:43:e3)
  BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
  .... .... .... 0000 = Fragment number: 0
  1100 1011 0001 .... = Sequence number: 3249
  Frame check sequence: 0xc7056d0a [unverified]
  [FCS Status: Unverified]
IEEE 802.11 wireless LAN
  Tagged parameters (62 bytes)
    Tag: SSID parameter set: TD_WIFI_GUEST
    Tag: Supported Rates 1, 2, 5.5, 6, 9, 11, 12, 18, [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 13
    Tag: HT Capabilities (802.11n D1.10)
    Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
```

```
IEEE 802.11 Probe Response, Flags: ........C
  Type/Subtype: Probe Response (0x0005)
  Frame Control Field: 0x5000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: IntelCor_d2:98:58 (28:b2:bd:d2:98:58)
  Destination address: IntelCor_d2:98:58 (28:b2:bd:d2:98:58)
  Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... .... 0000 = Fragment number: 0
  1010 0010 1001 .... = Sequence number: 2601
  Frame check sequence: 0x80831320 [unverified]
  [FCS Status: Unverified]
IEEE 802.11 wireless LAN
  Fixed parameters (12 bytes)
    Timestamp: 664064263
    Beacon Interval: 0.102400 [Seconds]
    Capabilities Information: 0x0421
  Tagged parameters (117 bytes)
    Tag: SSID parameter set: LABCOM
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 13
    Tag: ERP Information
    Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    Tag: Cisco CCX1 CKIP + Device Name
    Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (1) (1)
    Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX version = 5
    Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
    Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled
```

Joining BSS with AP: Authentication

- Once an AP is found/selected, a station goes through authentication
- Open system authentication (default, 2-step process)
  - Station sends authentication frame with its identity
  - AP sends frame as an Ack / NAck
- Shared key authentication
  - Stations receive shared secret key through secure channel independent of 802.11
  - After the WNIC sends its initial authentication request, it will receive an authentication frame from the AP containing a challenge text
  - The WNIC sends an authentication frame containing the encrypted version of the challenge text to the AP.
  - The AP ensures the text was encrypted with the correct key by decrypting it with its own key.
  - The result of this process determines the WNIC's authentication status.

Authentication Frames

- Nowadays, WPA* secure networks use “Open System”.
- Non-”Open System” authentication was used for WEP protected networks (unsecured and functionally deprecated).

```
IEEE 802.11 Authentication, Flags: ........
  Type/Subtype: Authentication (0x000b)
▸ Frame Control Field: 0xb000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Destination address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Transmitter address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Source address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... .... 0000 = Fragment number: 0
  0001 0100 1011 .... = Sequence number: 331
IEEE 802.11 wireless LAN
▾ Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
```

← From Station

From AP →

```
IEEE 802.11 Authentication, Flags: ........C
  Type/Subtype: Authentication (0x000b)
▸ Frame Control Field: 0xb000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... .... 0000 = Fragment number: 0
  1010 1001 0000 .... = Sequence number: 2704
  Frame check sequence: 0x9f8350e1 [unverified]
  [FCS Status: Unverified]
IEEE 802.11 wireless LAN
▾ Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0002
    Status code: Successful (0x0000)
```

Joining BSS with AP: Association

- Once a station is authenticated, it starts the association process, i.e., information exchange about the AP/station capabilities and roaming
  - STA → AP: Associate Request frame
    - Enables the AP to allocate resources and synchronize. The frame carries information about the WNIC, including supported data rates and the SSID of the network the station wishes to associate with.
  - AP → STA: Association Response frame
    - Acceptance or rejection to an association request. If it is an acceptance, the frame will contain information such as association ID and supported data rates.
  - New AP informs old AP (if it is a handover).
- Only after association is completed, a station can transmit and receive data frames.

Association Request/Response Frames

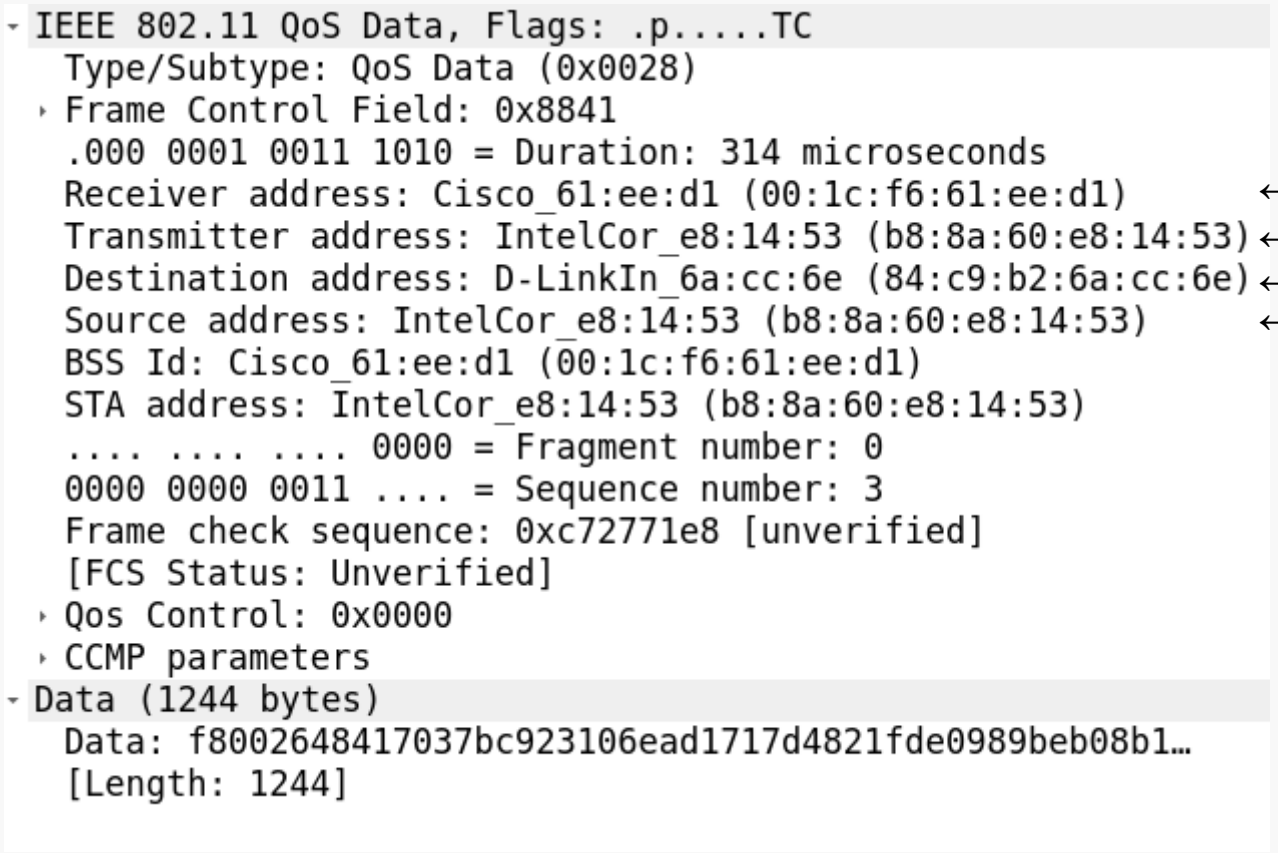
```
IEEE 802.11 Association Request, Flags: ........
  Type/Subtype: Association Request (0x0000)
 Frame Control Field: 0x0000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Destination address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Transmitter address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Source address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... .... 0000 = Fragment number: 0
  0001 0100 1100 .... = Sequence number: 332
IEEE 802.11 wireless LAN
 Fixed parameters (4 bytes)
  Capabilities Information: 0x0421
   Listen Interval: 0x000a
 Tagged parameters (43 bytes)
  Tag: SSID parameter set: LABCOM
  Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
  Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
  Tag: Extended Capabilities (8 octets)
  Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information E
```

← From Station

From AP →

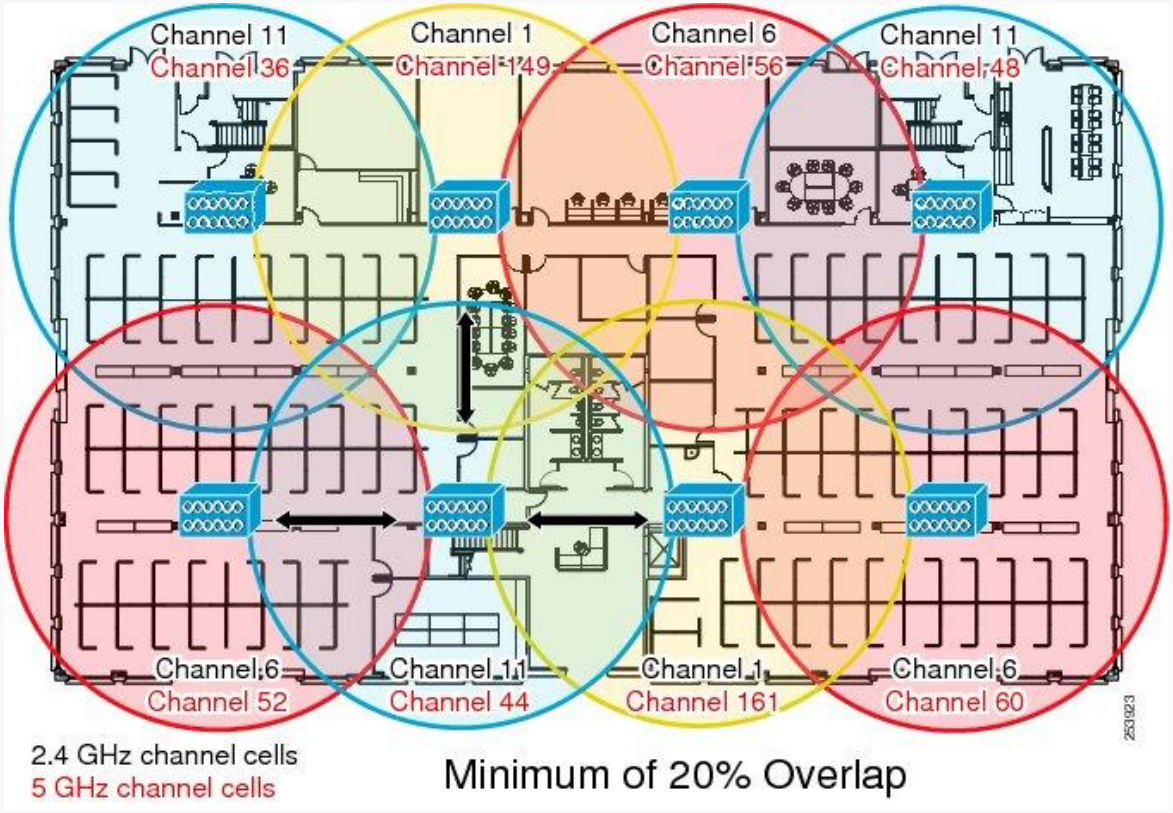
```
IEEE 802.11 Association Response, Flags: ........C
  Type/Subtype: Association Response (0x0001)
 Frame Control Field: 0x1000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... .... 0000 = Fragment number: 0
  1010 1001 0001 .... = Sequence number: 2705
  Frame check sequence: 0xe7103b15 [unverified]
  [FCS Status: Unverified]
IEEE 802.11 wireless LAN
 Fixed parameters (6 bytes)
  Capabilities Information: 0x0421
   Status code: Successful (0x0000)
   ..00 0000 0000 0001 = Association ID: 0x0001
 Tagged parameters (42 bytes)
  Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
  Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
  Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

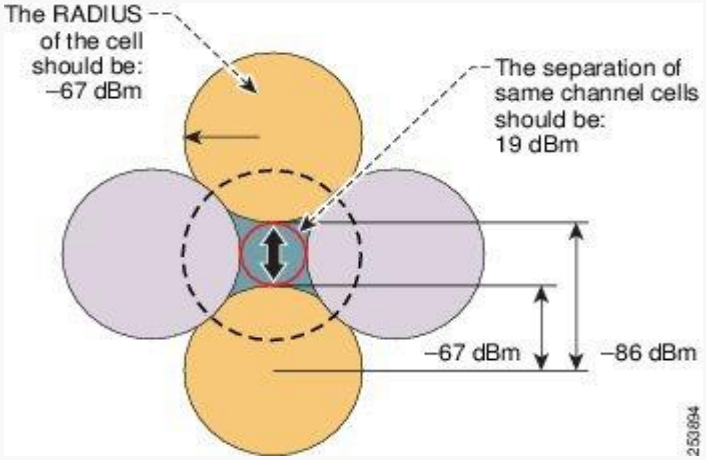
Data Frame



- Station “IntelCor*” sending data to station “D-LinkIn*” (via AP).
- Frame captured between station “IntelCor*” and AP (“Cisco*”).

AP Placement and Channel Allocation





- **802.11n or 802.11ac 5GHz deployment does not have the overlap or collision domain issues of 2.4GHz.**