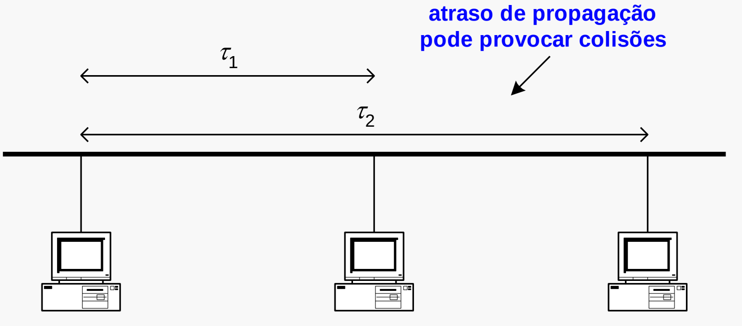
Ethernet and Wireless

Redes de Comunicações 1

Licenciatura em Engenharia de Computadores e Informática

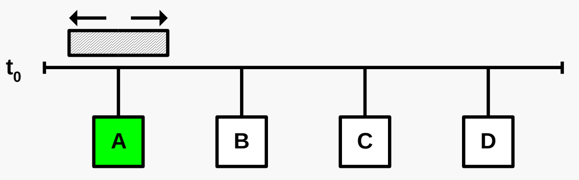
CSMA (Carrier Sense Multiple Access)

- Stations transmit and receive in the same channel
- They sense the medium before transmission; only transmit if medium is free
- Number of collisions is minimized
- Collisions can occur because stations are distanced from each other

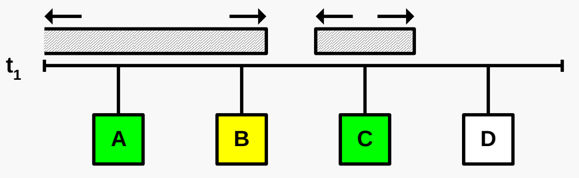


CSMA/CD (CSMA *with Collision Detection*) (I)

- **Stations stop transmitting when they detect collisions**

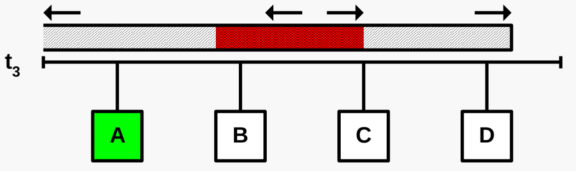


A estação A detecta o meio livre e inicia a sua transmissão

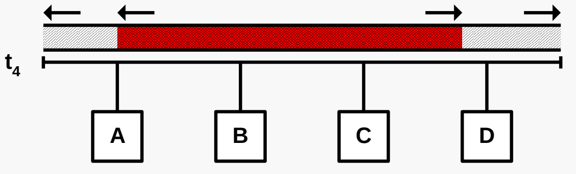


A estação B pretende transmitir mas não o faz porque detecta o meio ocupado; a estação C inicia a transmissão

CSMA/CD (II)

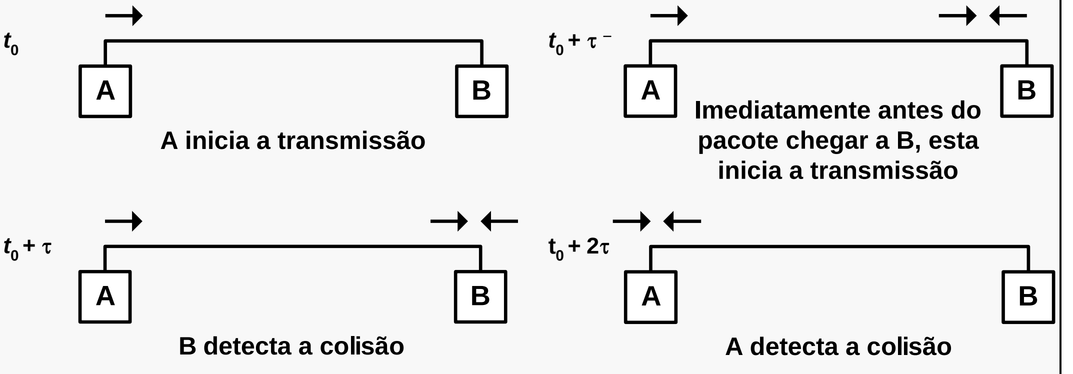


C detecta a colisão e pára de transmitir



A detecta a colisão e pára de transmitir

CSMA/CD (III)



Guarantee that all transmittion stations detect collisions

⇒

Minimum time to transmit a packet > *round-trip delay*

CSMA/CD (IV)

- The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol used on Ethernet works as follows: the medium access is ruled by carrier sense (the sending station first detects if the medium is being used by another station) and collision detection (the sending station checks if the medium has the same data being sent by it).
- When a station has an Ethernet frame to be sent, it first checks if the medium is busy with the transmission of a frame by another station. If the medium is free for an Inter Frame Spacing (IFS) time period, it starts sending its frame. If the medium is busy, it waits that the medium becomes free, waits another IFS time period and starts sending its frame (it is said that the protocol is 1-persistent since all stations waiting to transmit during a busy period will transmit their frames with 100% of probability as soon as the medium becomes free for a IFS time period).
- IFS is the minimum time interval required by all stations to accommodate one frame before being prepared to start receiving another frame. For example, in 10 Mbps Ethernet, the IFS is 9.6 μs.
- Note that it is possible that two (or more) stations start transmitting frames almost at the same time originating a collision. In a collision, multiple frames are being simultaneously transmitted and, therefore, will not be correctly received by any station. When a sending station detects a collision, it stops the frame transmission and sends a JAM signal (aimed to guarantee that all stations detect the collision). Then, it waits for a random period of time to send the frame again. This random period is defined by the Truncated Binary Exponential Backoff Algorithm described in the next slide.

Ethernet

The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol used on Ethernet works as follows: the medium access is ruled by carrier sense (the sending station first detects if the medium is being used by another station) and collision detection (the sending station checks if the medium has the same data being sent by it).

When a station has an Ethernet frame to be sent, it first checks if the medium is busy with the transmission of a frame by another station. If the medium is free for an Inter Frame Spacing (IFS) time period, it starts sending its frame. If the medium is busy, it waits that the medium becomes free, waits another IFS time period and starts sending its frame (it is said that the protocol is 1-persistent since all stations waiting to transmit during a busy period will transmit their frames with 100% of probability as soon as the medium becomes free for a IFS time period).

IFS is the minimum time interval required by all stations to accommodate one frame before being prepared to start receiving another frame. For example, in 10 Mbps Ethernet, the IFS is 9.6 μs.

Note that it is possible that two (or more) stations start transmitting frames almost at the same time originating a collision. In a collision, multiple frames are being simultaneously transmitted and, therefore, will not be correctly received by any station. When a sending station detects a collision, it stops the frame transmission and sends a JAM signal (aimed to guarantee that all stations detect the collision). Then, it waits for a random period of time to send the frame again. This random period is defined by the Truncated Binary Exponential Backoff Algorithm described in the next slide.

CSMA/CD (V)

- **Number of time slots of delay before the n^{th} retry is a random variable uniformly distributed in the interval**

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

- **Duration of the slot = 64 bytes = 512 bits = 51.2 μs (10 Mbps)**
- **Example:**
  - $n = 1 \Rightarrow r = 0$ **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)**

    ⋮
  - $n > 10$**, maximum delay fixed to** $2^{10}-1 = 1023$ **slots**
- **Maximum number of retries = 16**

Truncated Binary Exponential Backoff Algorithm

When a collision is detected by a sending station, the time that the station waits to send again its frame is given by an integer number r of time slots. In 10 Mbps and 100 Mbps Ethernet technologies, the time slot is defined by the time taken to transmit a minimum size frame of 64 bytes (64 Bytes = 64 × 8 = 512 bits), which is 51.2 μs (in 10 Mbps technologies) or 5.12 μs (in 100 Mbps technologies).

A maximum of 16 retransmissions is allowed beyond which the frame is discarded by the sending station.

In the n^{th} retransmission of the same frame (with $n \le 16$), the number of waiting time slots r is a uniform random value between $0 \le r < 2^k$, where k is the minimum value between n and 10.

Note that the average waiting time is short in the first retransmissions, grows exponentially with the number of retransmissions until the 10^{th} one and remains the same above the 10^{th} retransmission.

CSMA-CD - performance

Utilization of CSMA/CD is

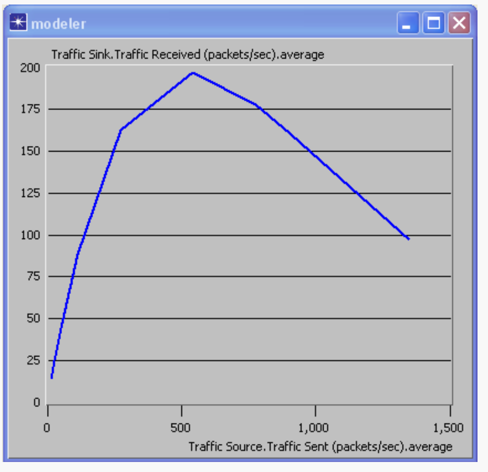
$$S \underset{N \to \infty}{\to} \frac{1}{1+3.44a}$$

$a = \tau/T$, T – transmission time of a packet (useful time)

- a<1

CSMA-CD - performance

- Increase of transmission traffic
  - Increase of collisions



9

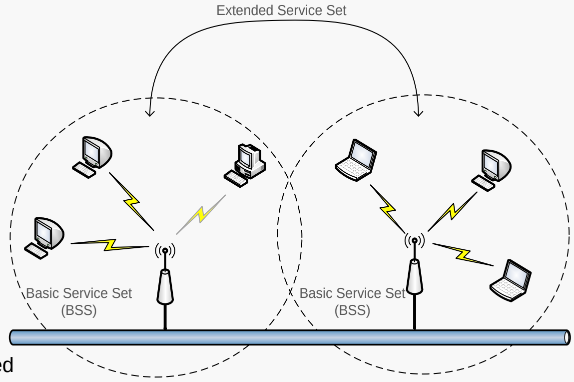
Wireless Networks

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 (2021 6E), 2.4, 5, (6 GHz 6E) bands, ~9.611 Gbps data rate
- WiFi 7 – 802.11be, 2024, 2.4, 5, 6 GHz, ~23 Gbps data rate
- WiFi 8 - 802.11bn, exp. 2028, 2.4, 5, 6 GHz, ~100 GHz data rate

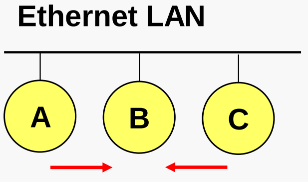
Components

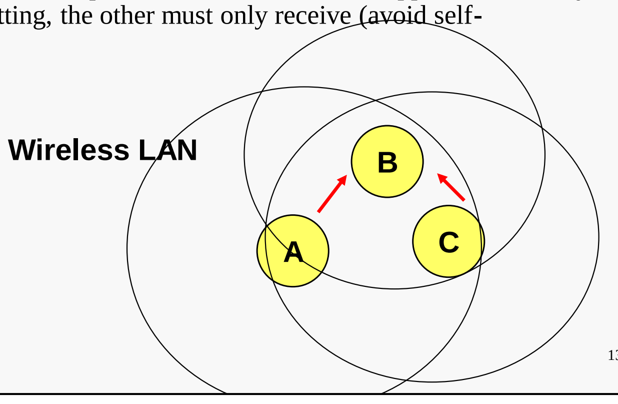
- Station (STA)
  - Mobile terminal
- Access Point (AP)
  - STA connect to access points (infra-structured networks)
- Basic Service Set (BSS)
  - STA and AP with same coverage form a BSS
  - Group of IEEE 802.11 stations associated to an Access Point (AP)
  - Known through the SSID
- Extended Service 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 collision (CD does not work)
  - ➢ CS may not work either with hidden nodes

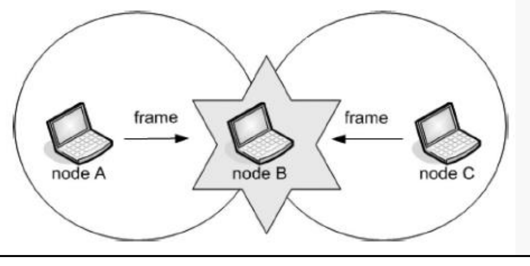
14

CD – colision detection

CS – carrier sense

Hidden nodes

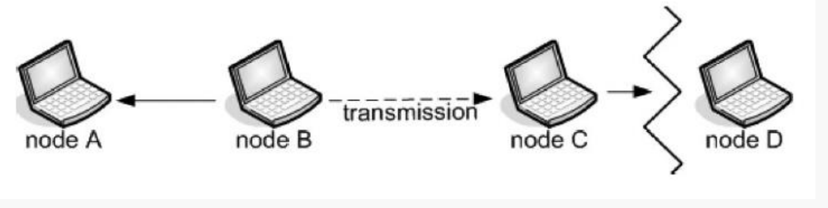
- Hidden terminals
  - A and C do not ear each other
  - Collision in B, if A and C send at the same time
  - Nor A nor C understand that collision occured
- Solution
  - Detect collisions in the receiver
  - "virtual carrier sensing": sender asks the receiver if he is receiving traffic; in the case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



15

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



16

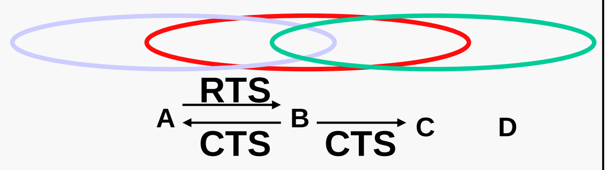
MACA: Multiple Access with Collision Avoidance

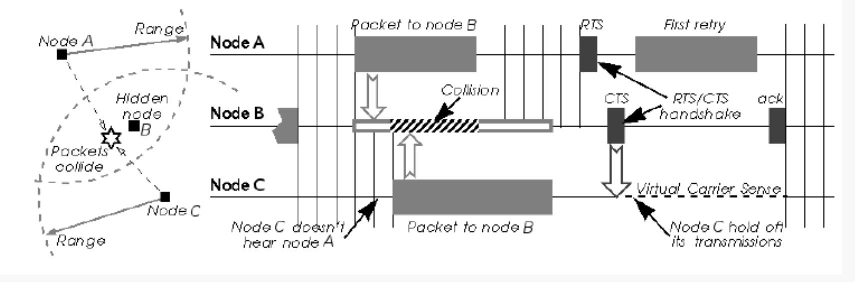
- MACA: avoids collisions using signalling packets
  - RTS (request to send)
    - A small packet is sent before transmitting
  - CTS (clear to send)
    - Receiver provides the right to transmit, when it is able to receive
- Signaling packets (RTS/CTS) contain
  - Sender address
  - Receiver address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

17

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

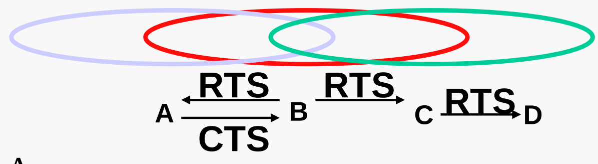


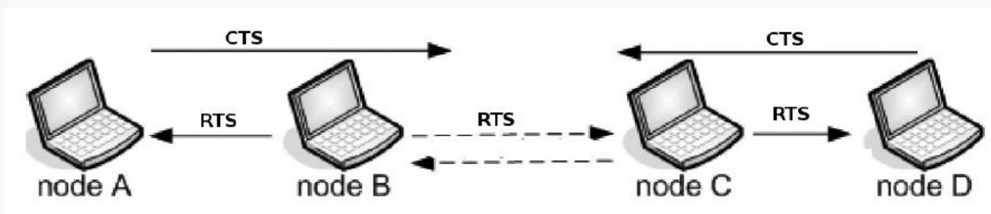


18

MACA: Exposed Nodes

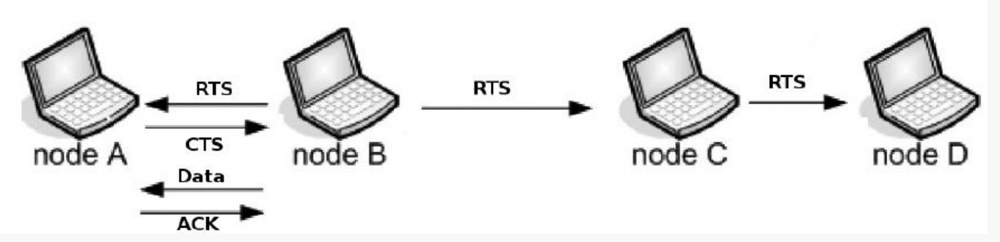
- MACA and exposed nodes
  - B → A, C → D(?)
  - B RTS → A
  - A CTS → B
  - C ears RTS of B
  - C does not ear CTS of A
  - C RTS → D





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

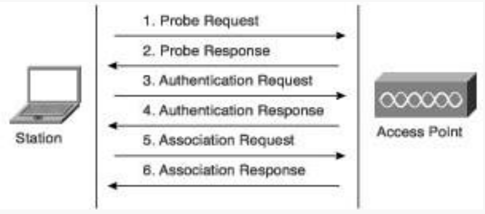


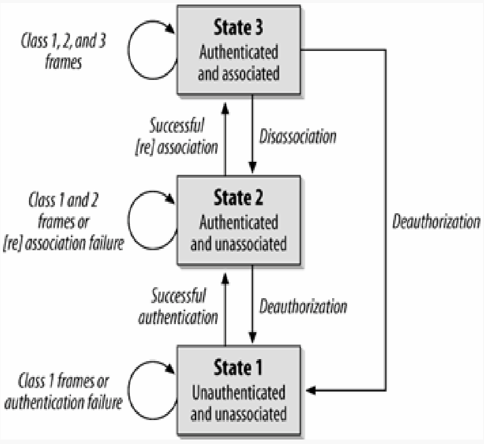
20

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.

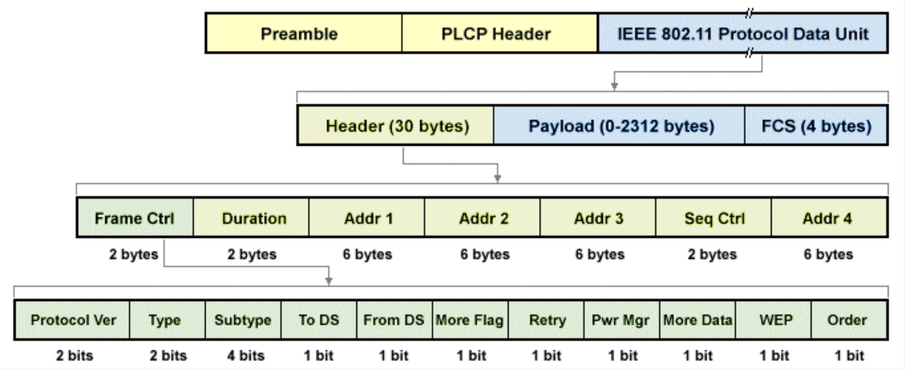




22

WLAN Frames

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



23

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]
```

WiFi 4

```
- 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.**

29

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
```

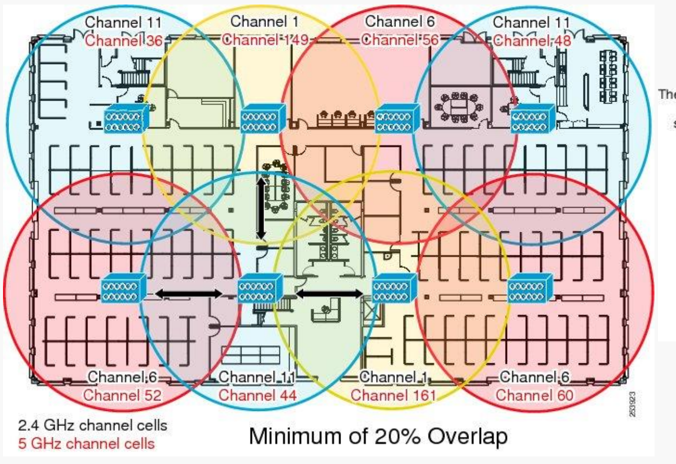
30

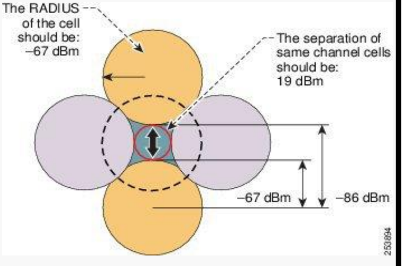
Data Frame

```
IEEE 802.11 QoS Data, Flags: .p.....TC
  Type/Subtype: QoS Data (0x0028)
  Frame Control Field: 0x8841
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)        ← Node that will receive frame (AP)
  Transmitter address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)  ← Node that sends frame
  Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)  ← Station to receive data
  Source address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)       ← Station who sent data
  BSS Id: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
  STA address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
  .... .... .... 0000 = Fragment number: 0
  0000 0000 0011 .... = Sequence number: 3
  Frame check sequence: 0xc72771e8 [unverified]
  [FCS Status: Unverified]
  Qos Control: 0x0000
  CCMP parameters
Data (1244 bytes)
  Data: f8002648417037bc923106ead1717d4821fde0989beb08b1…
  [Length: 1244]
```

- **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.**

Security in WLANs

Authentication and authorization mechanisms

- **Changing according to the organization and the security level**
  - Open network
  - Open network + MAC authentication
  - Open network + VPN-gateway
  - Open network + web-gateway
  - SSID
  - Shared key: WEP
  - Wi-Fi Protected Access (WPA)
  - IEEE 802.11i (WPA2)
  - IEEE 802.1X
  - Virtual Private Networks (VPNs)

34

Open Network(s)

- **Open network**
  - Network is open, providing IP addresses with DHCP
  - There is no authentication and access is free
  - Does not require specific software
  - Access control is complicated
  - It is possible to 'see' all traffic in the network (sniffing)
- **Open network + MAC authentication**
  - The control of the station MAC address is added
  - Larger management load
    - ... But MAC addresses can be falsified
    - ... Difficult to support guests
    - ... Impossible to use in public environments

WEP Protocol

- **Wired Equivalent Privacy → shared key scheme.**
- **Part of basic 802.11 standard.**
- **Security protocol at link layer (L2).**
- **Designed to be computationally efficient and self-synchronized.**
- **The station has to know the key (like a password) to access the AP.**
- **With passive monitoring, it can be broken (in seconds)**
  - Header is not ciphered, all destinations and origins are visible.
  - Control frames are not ciphered, and then they can be changed.
  - AP is not authenticated and can be falsified.

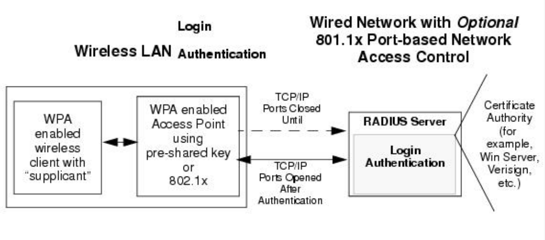
WPA and 802.11i (WPA2)

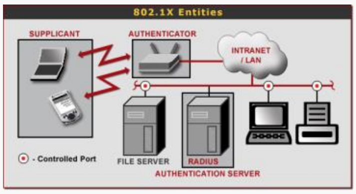
- **IEEE 802.11i - IEEE 802.11 task group “MAC enhancement for wireless security”.**
- **Wi-Fi Protected Access (WiFi Alliance), WPA, is a subset internal in 802.11i.**
  - **Used in Eduroam**
  - **Defined to work in actual equipment.**
    - Firmware update only.
  - **Pass-phrase constant and shared, but keys are generated per session.**
  - **Used in the AP and station.**
  - **Uses “Open System” during authentication phase.**
- **WPA has two distinct components.**
  - **Authentication, based on 802.1X.**
    - Login and password – it is the user that is authenticated anywhere in the world
    - Does not need to know any password of the AP
    - Contact to a local server and a remote server where the user belongs
  - **Ciphering based on TKIP (Temporal Key Integrity Protocol).**

37

IEEE 802.1X

- **Layer 2 solution between station and AP.**
  - Available in many equipments (e.g. IEEE 802.xx).
  - Web systems frequently use 802.1X.
- **Several authentication-mechanisms available (EAP-MD5, EAP-TLS, EAP-TTLS, PEAP)**
- **Multiple standard ciphering algorithms .**
- **Can cipher data with dynamic keys.**

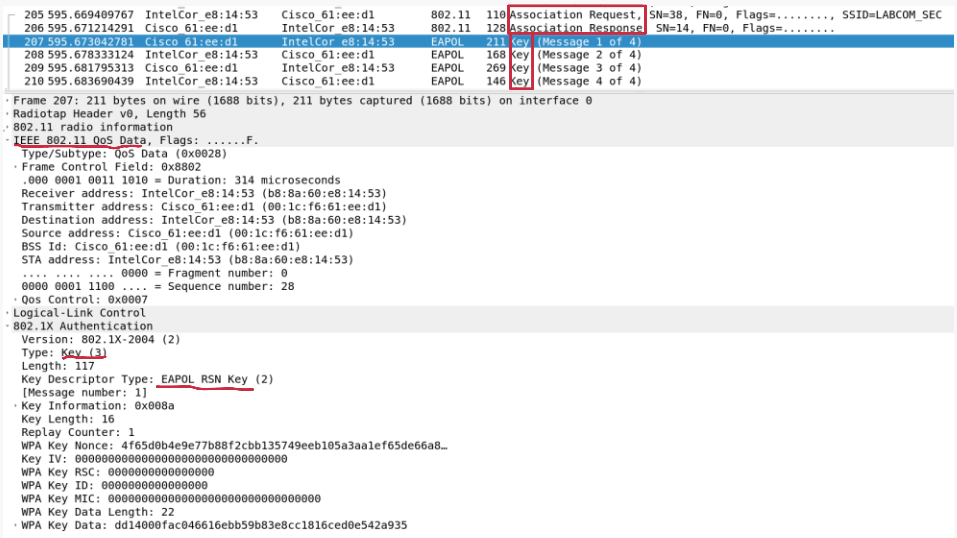




38

WPA* Key Exchange

- **Done during the Association process.**
  - After Association Request/response frames.



```
205 595.669409767  IntelCor_e8:14:53   Cisco_61:ee:d1      802.11  110 Association Request, SN=38, FN=0, Flags=........, SSID=LABCOM_SEC
206 595.671214291  Cisco_61:ee:d1      IntelCor_e8:14:53   802.11  128 Association Response  SN=14, FN=0, Flags=........
207 595.673042781  Cisco_61:ee:d1      IntelCor_e8:14:53   EAPOL   211 Key (Message 1 of 4)
208 595.678333124  IntelCor_e8:14:53   Cisco_61:ee:d1      EAPOL   168 Key (Message 2 of 4)
209 595.681795313  Cisco_61:ee:d1      IntelCor_e8:14:53   EAPOL   269 Key (Message 3 of 4)
210 595.683690439  IntelCor_e8:14:53   Cisco_61:ee:d1      EAPOL   146 Key (Message 4 of 4)
Frame 207: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits) on interface 0
Radiotap Header v0, Length 56
802.11 radio information
IEEE 802.11 QoS Data, Flags: ......F.
  Type/Subtype: QoS Data (0x0028)
  Frame Control Field: 0x8802
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
  Transmitter address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
  Destination address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
  Source address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
  BSS Id: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
  STA address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
  .... .... .... 0000 = Fragment number: 0
  0000 0001 1100 .... = Sequence number: 28
  Qos Control: 0x0007
Logical-Link Control
802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 1]
  Key Information: 0x008a
  Key Length: 16
  Replay Counter: 1
  WPA Key Nonce: 4f65d0b4e9e77b88f2cbb135749eeb105a3aa1ef65de66a8…
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 00000000000000000000000000000000
  WPA Key Data Length: 22
  WPA Key Data: dd14000fac046616ebb59b83e8cc1816ced0e542a935
```