Wireless Networks

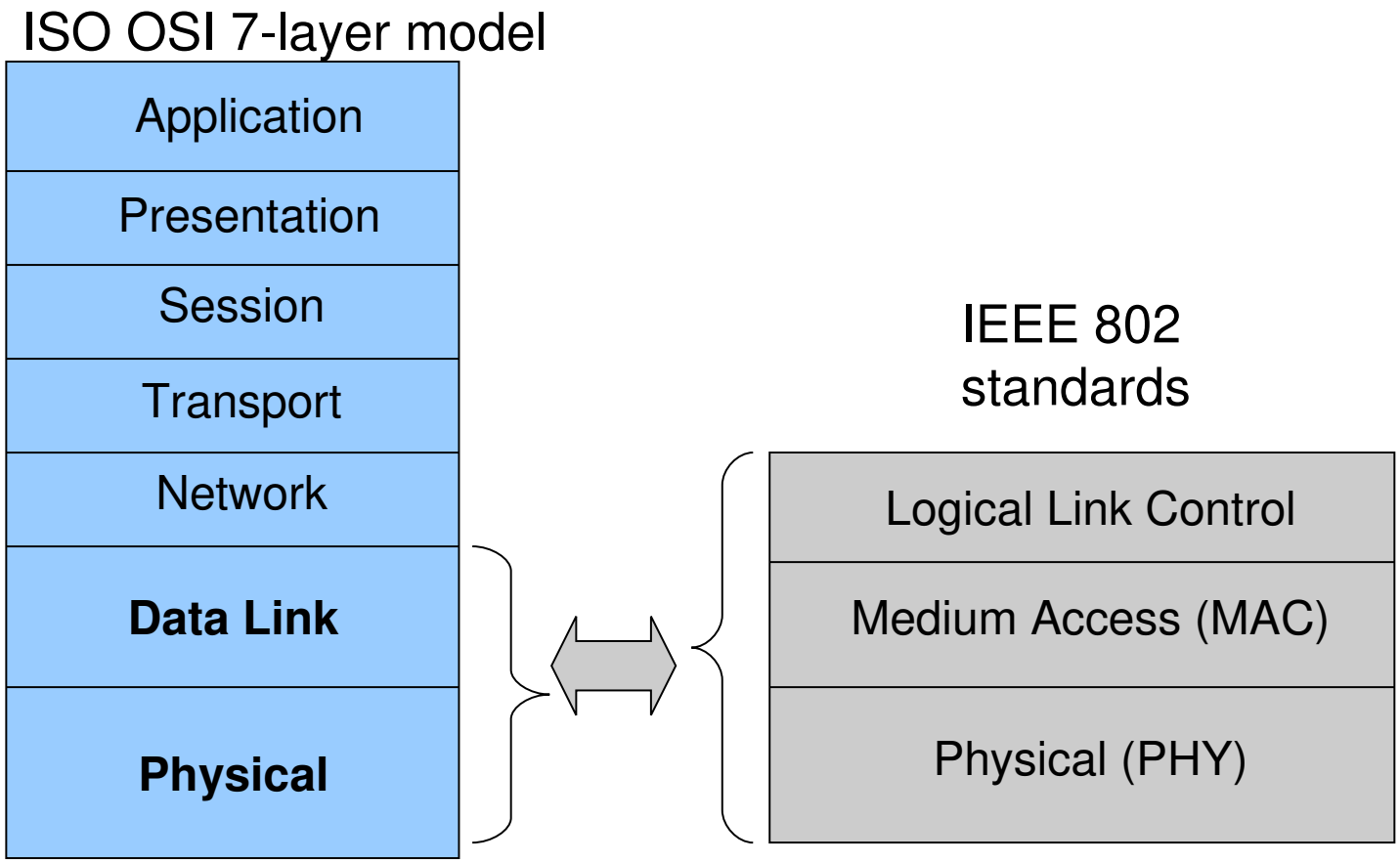
Arquitetura de Redes

Mestrado Integrado
Engenharia de Computadores e Telemática
DETI-UA

universidade de aveiro
deti.ua.pt

Standardization of Wireless Networks

- Wireless networks are standardized by the IEEE under the 802 LAN MAN standards committee.



Wireless networks

- Networks are designed according to the number of users and coverage area
- There are several scales on the number of users and coverage area
  - Personal: PANs → e.g. Bluetooth, ZigBee
  - Local: LANs → IEEE 802.11
  - Regional: WANs → GSM, UMTS, LTE
  - Worldwide : Satellite → Iridium

Wireless LANs: Oveview

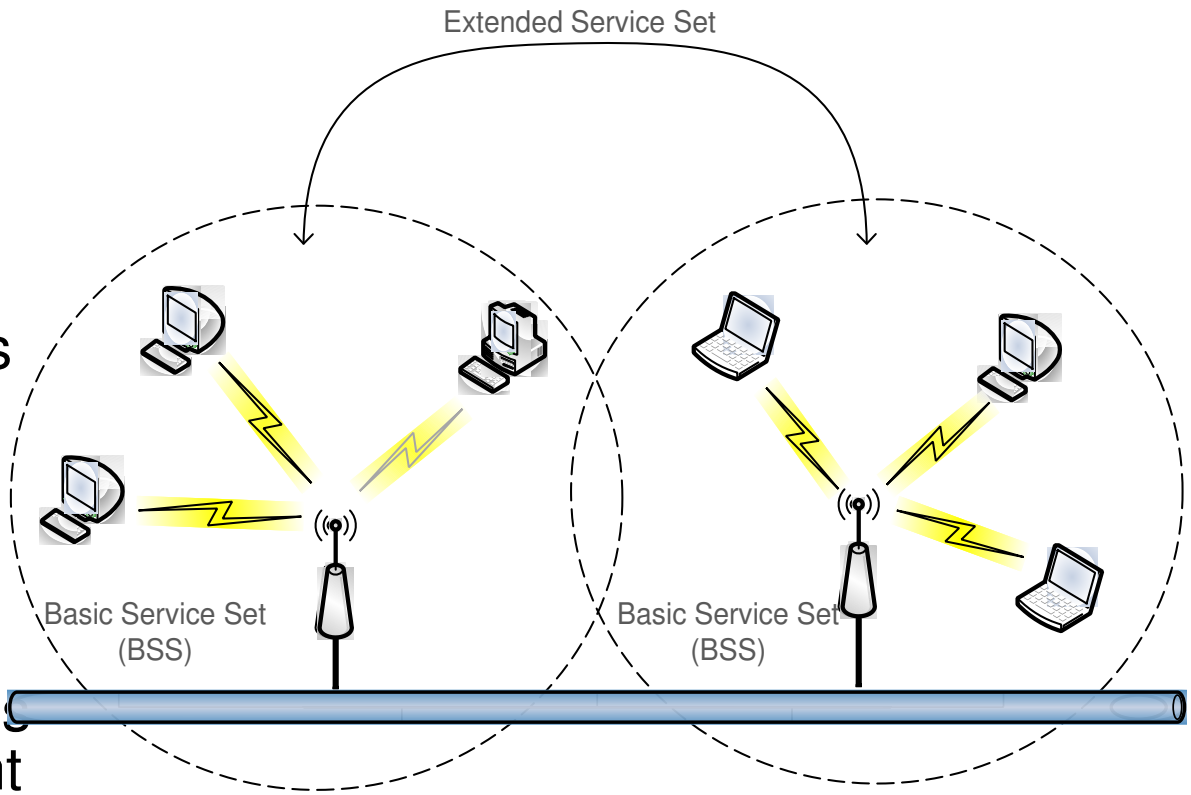
- Two Types
  - Infra-structured
  - Ad-hoc
- Advantages
  - Flexible installation (minimum cables)
  - More robust (no cable problems)
  - One-time installation (conferences, historic buildings)
- Problems
  - Many proprietary solutions
  - Restrictions on the electromagnetic spectrum
  - Lower bandwidths than cabled 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

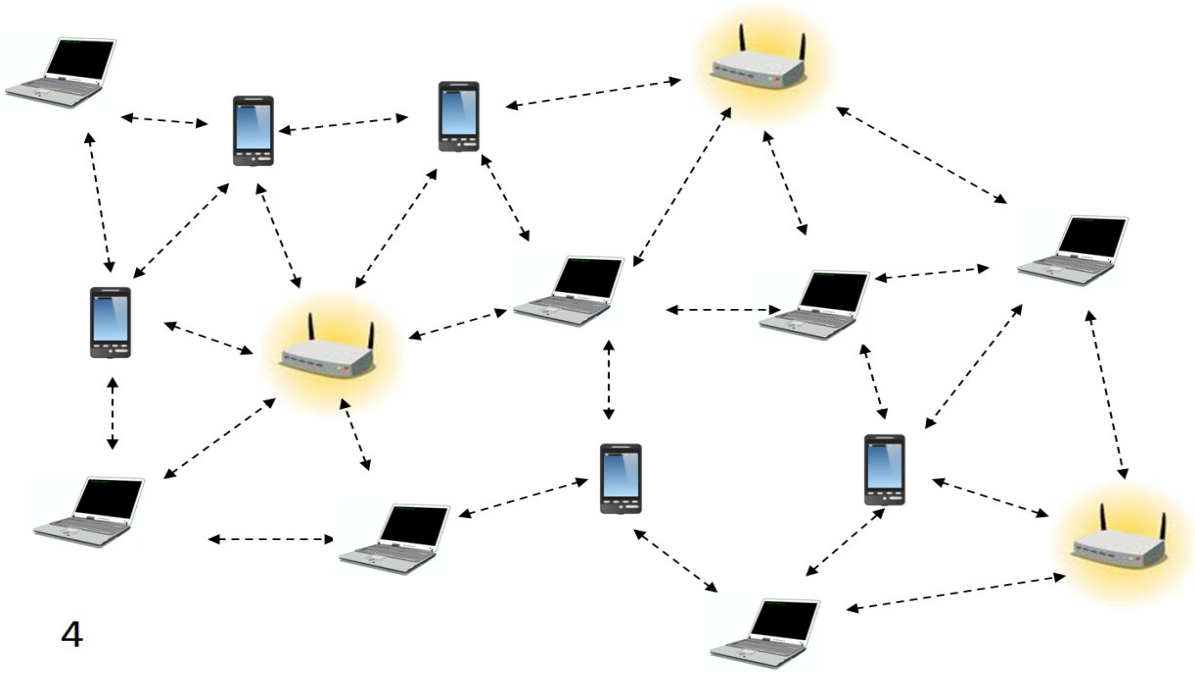
Components

- 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



Ad-hoc Networks (IBSS)

- Temporary set of stations
- Forming an ad-hoc network – an independent BSS (IBSS), means that there is no connection to a wired network
- No AP
- No relay function (direct connection)
- Simple setup

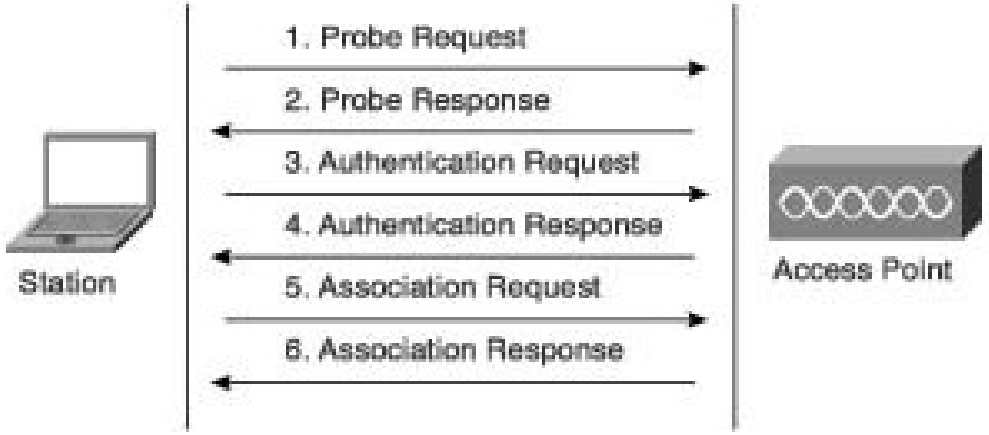


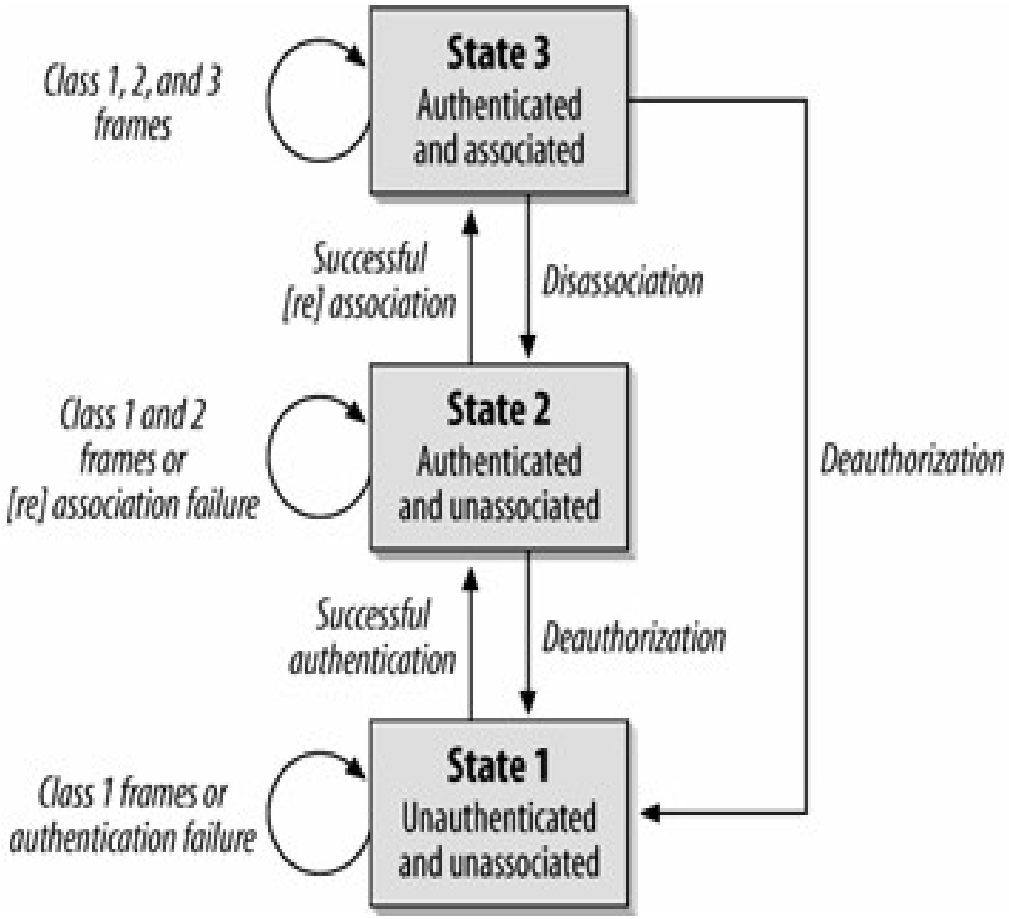
IEEE 802.11 services

- Station services (similar to wired network)
  - Authentication (login)
  - De-authentication (logout)
  - Privacy
  - Data delivery
- Distribution services
  - Association
    - Make logical connection between the AP and the station – the AP will not receive any data from a station before association
  - Re-association (similar to association)
    - Send repeatedly to the AP.
    - Help the AP to know if the station has moved from/to another BSS.
    - After Power Save
  - Disassociation
    - Manually disconnect (PC is shutdown or adapter is ejected)

Joining a BSS

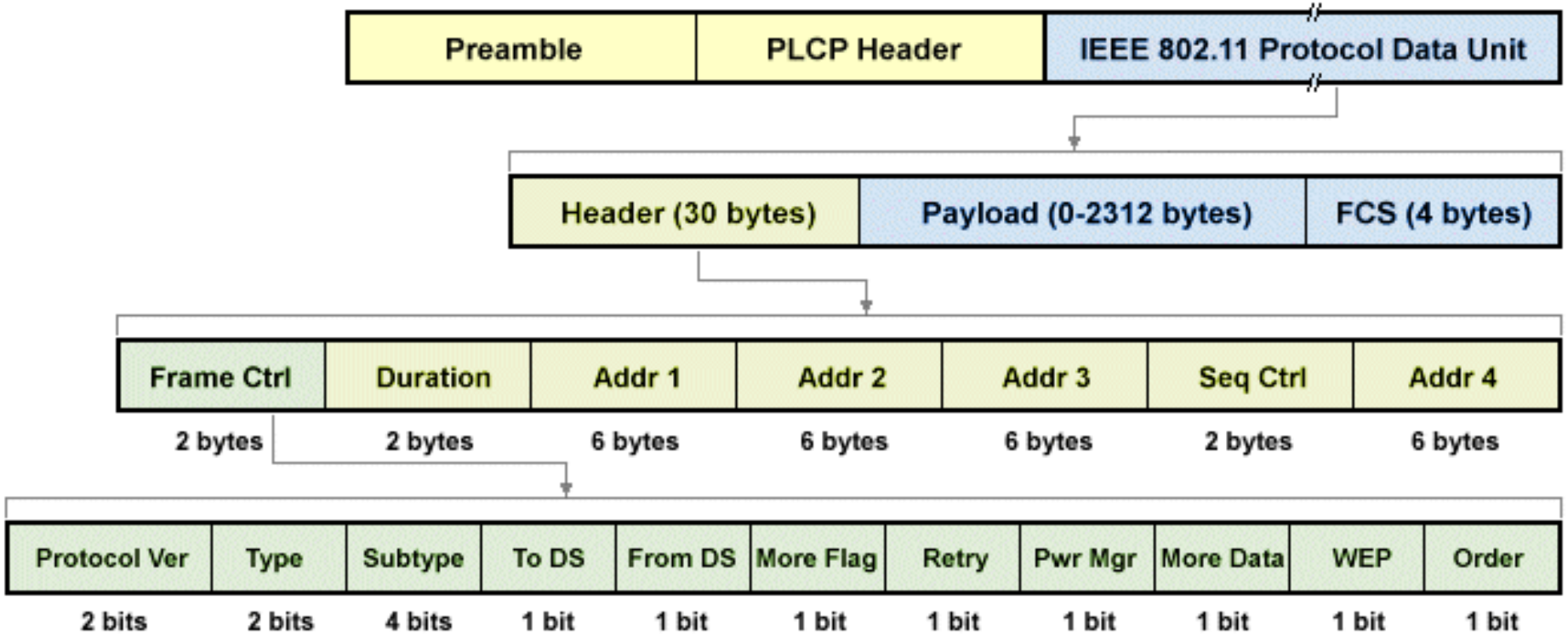
- Station finds BSS/AP by **Scanning/Probing**.
- BSS with AP: both **Authentication** and **Association** are necessary for joining a BSS.





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* sedcure 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

← From Station

```
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 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

```
▾ 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)
    Transmitter address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    Source address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    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]
```

← Node that will receive frame (AP)
← Node that send frame
← Station to receive data
← Station who sent data

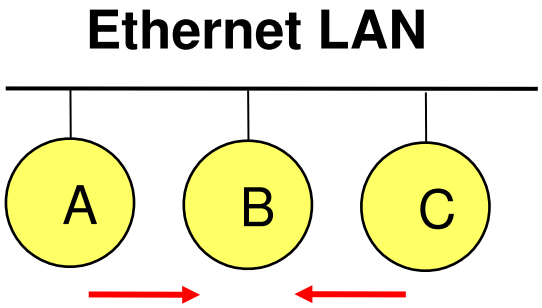
- Station “IntelCor*” sending data to station “D-LinkIn*” (via AP).
- Frame captured between station “IntelCor*” and AP (“Cisco*”).

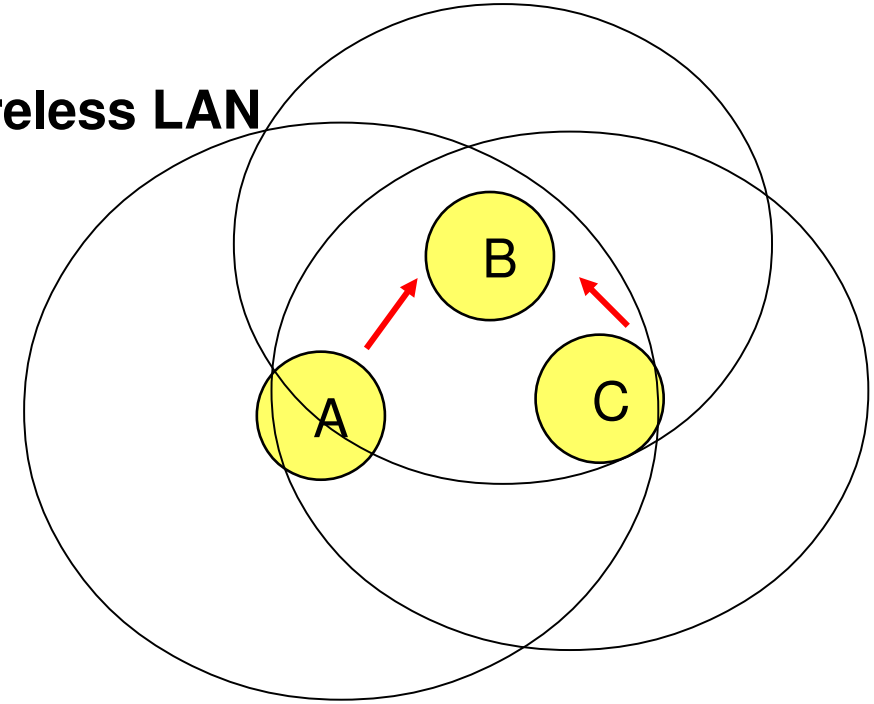
MAC Requirements

- Support different physical layers.
- Allow overlapping of different networks in the same area.
- Support of real-time services.
- Support of roaming.
- Overcome the problem of hidden and exposed nodes.

Wired vs Wireless

- 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)





Wireless MAC

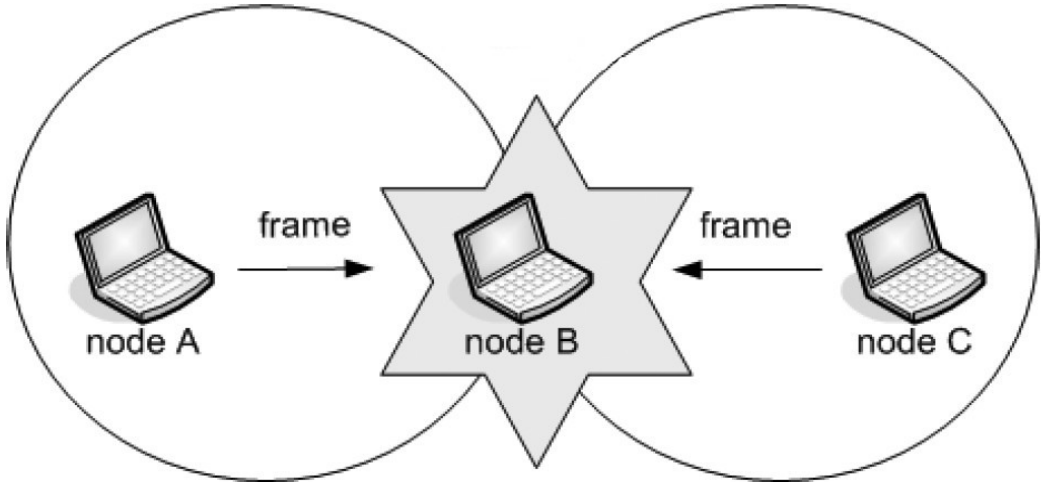
- Wired MACs
  - Typical: CSMA/CD
  - Medium is free → send
  - Listen to sense collision
- What about wireless?
  - Signal power reduces with the square distance
  - Sender can apply CS and CD, but collisions occur in the receiver!
  - Sender may not listen the collision (CD does not work)
  - CS may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

Hidden Nodes

- Hidden terminals
  - A and C do not ear each other.
  - Collision in B, if A and C send at the same time.
  - Neither A or C understand that a collision occurred.

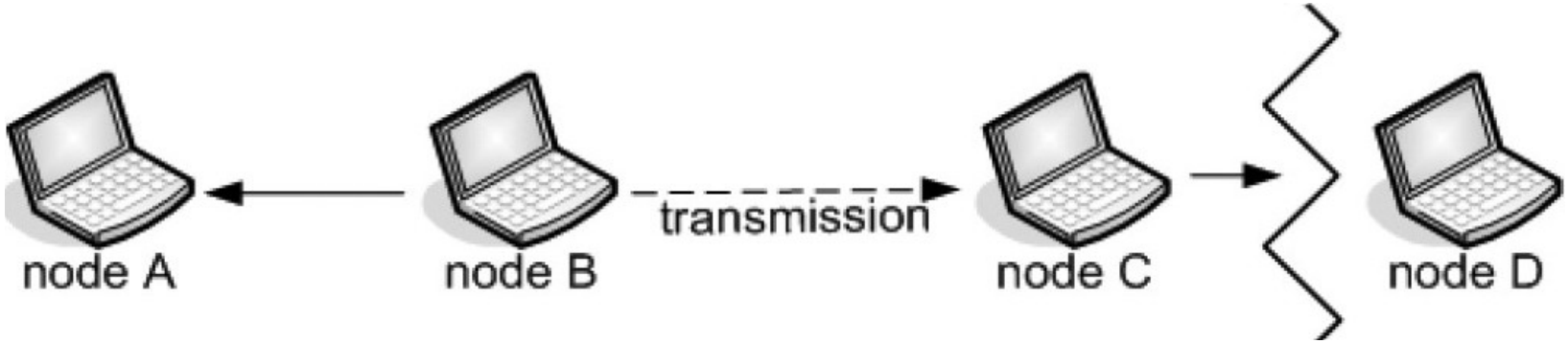
Solution

  - Detect collisions in the receiver.
  - “Virtual carrier sensing”: sender asks the receiver if he is receiving traffic; in the case of absence of answer, he assumes that the channel is busy.



Exposed Nodes/Terminals

- Exposed terminals
  - B transmits to A;
  - Node C wants to transmit to node D but mistakenly thinks that this will interfere with B's transmission to A, so C refrains from transmitting.
    - D is not in the range of B and A is not in the range of C, so traffic could have been transmitted.
  - B and C are exposed terminals.
  - The "exposed node" problem leads to loss of efficiency.

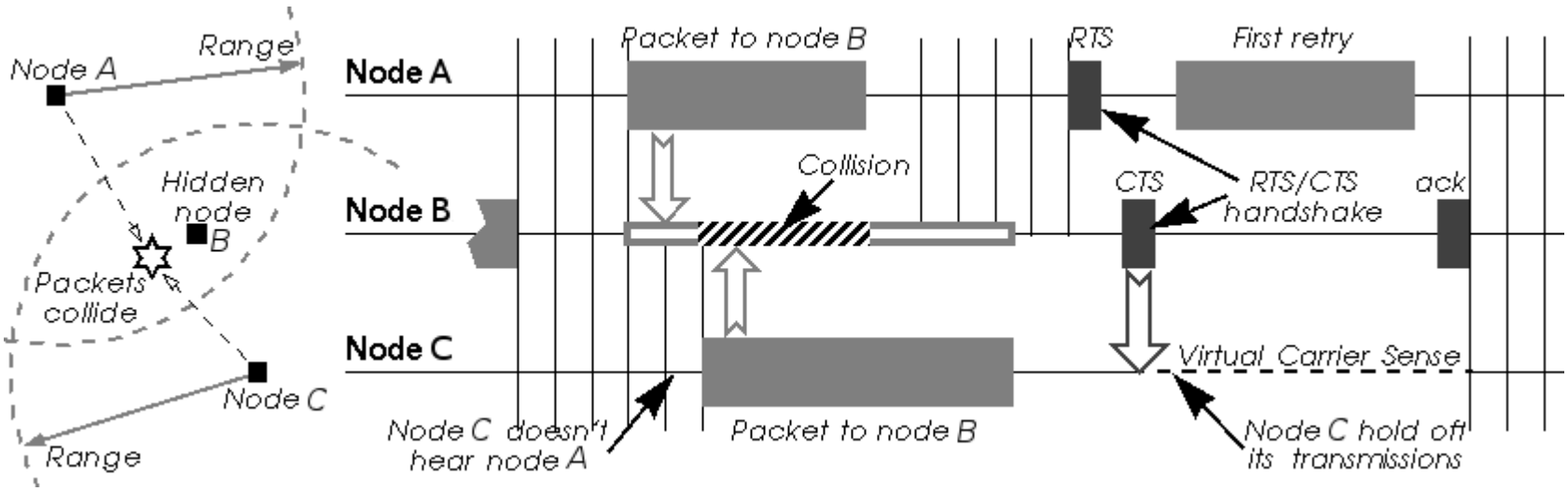


MACA: Multiple Access with Collision Avoidance

- 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 scenarios with a large amount of traffic/collisions.

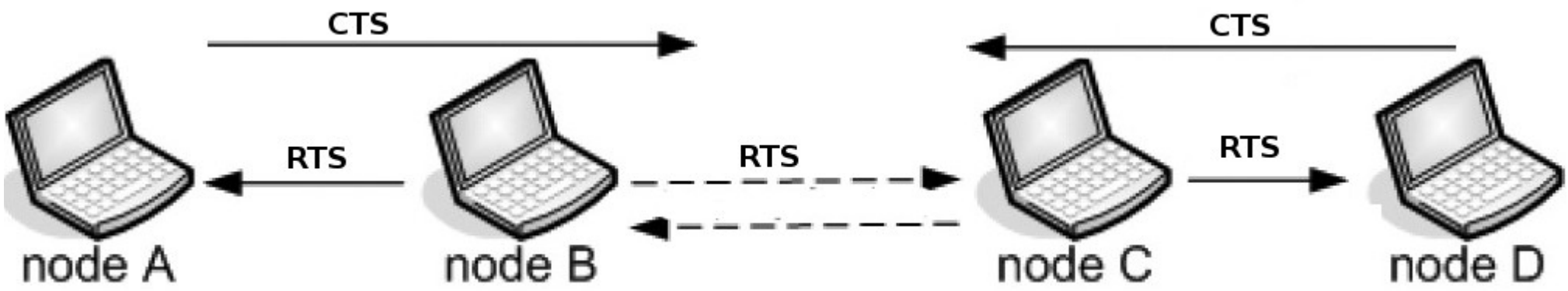
MACA Advantages (1)

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



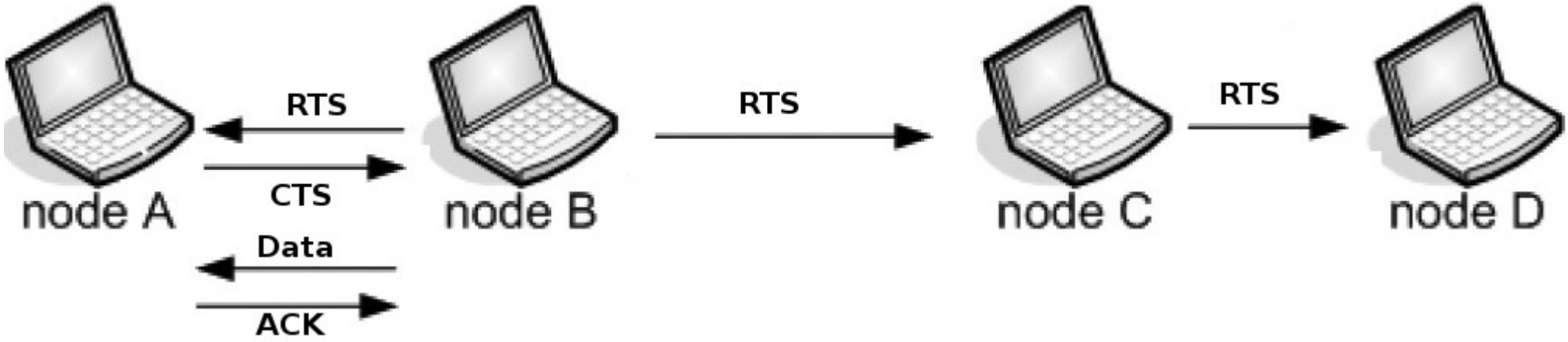
MACA Advantages (2)

- 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.



RST/CTS Frames

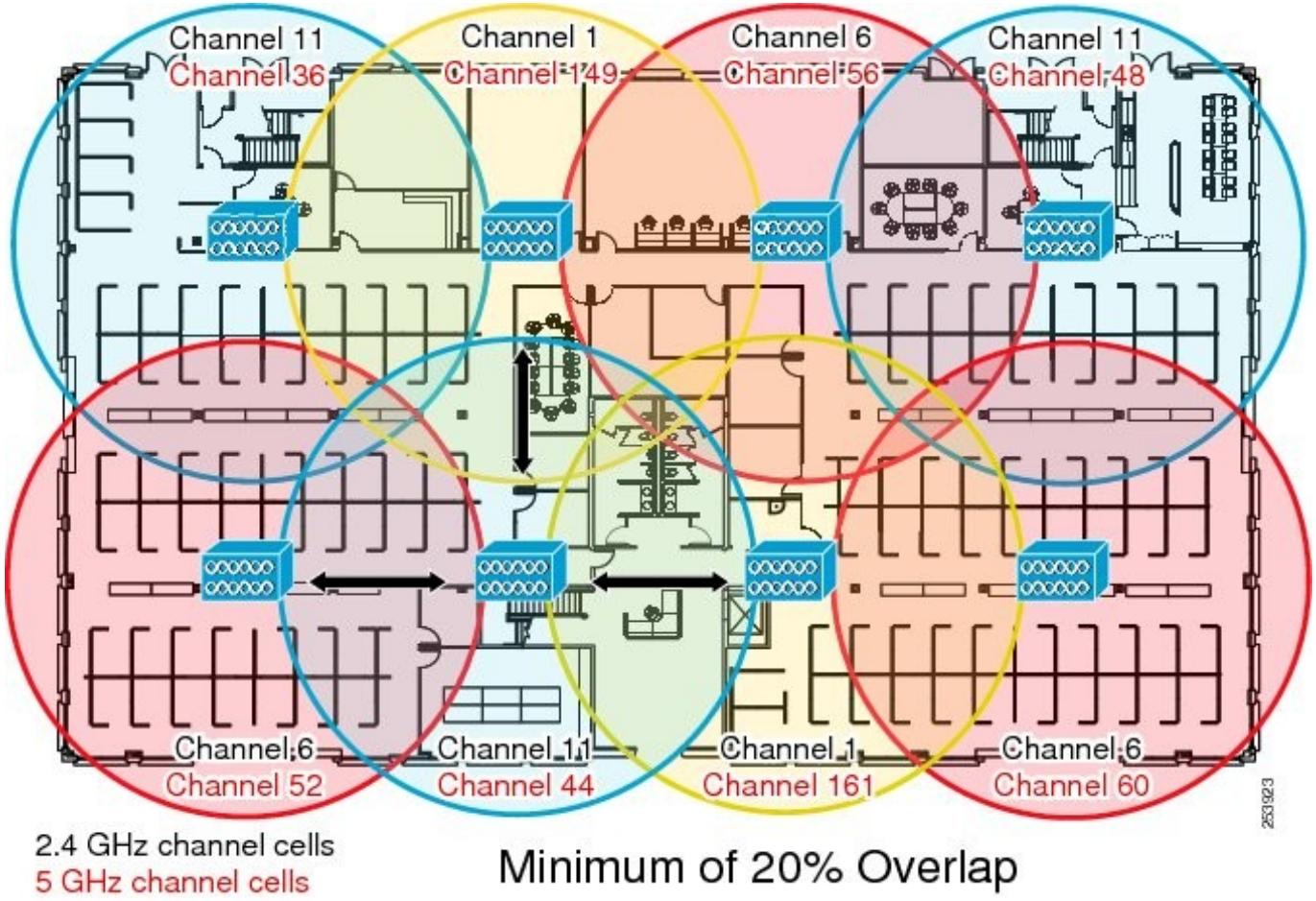
```
IEEE 802.11 Request-to-send, Flags: ........C
  Type/Subtype: Request-to-send (0x001b)
▸ Frame Control Field: 0xb400
  .000 0111 0000 0100 = Duration: 1796 microseconds
  Receiver address: Cisco_2b:d3:70 (f4:cf:e2:2b:d3:70)
  Transmitter address: Microsof_0a:43:e3 (c0:33:5e:0a:43:e3)
  Frame check sequence: 0xe058c51c [unverified]
  [FCS Status: Unverified]
```

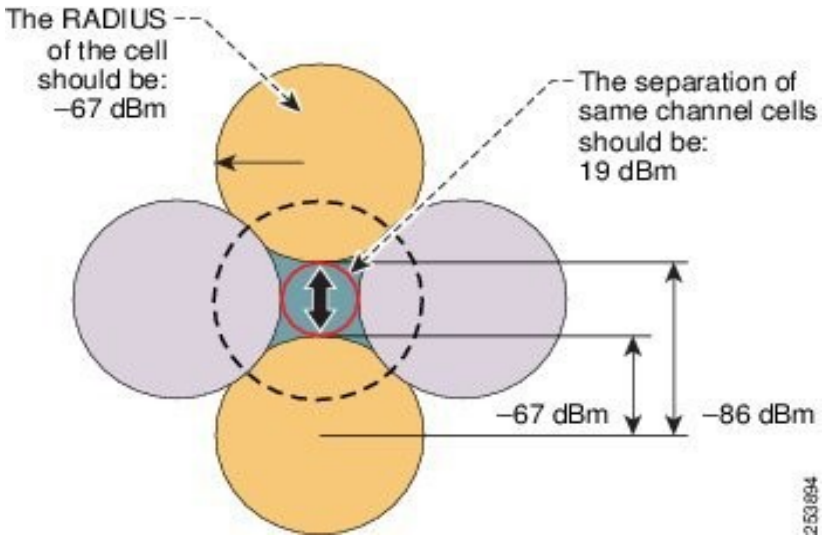
← From Data Transmitter

From Data Receiver →

```
IEEE 802.11 Clear-to-send, Flags: ........C
  Type/Subtype: Clear-to-send (0x001c)
▸ Frame Control Field: 0xc400
  .000 0110 0010 1010 = Duration: 1578 microseconds
  Receiver address: Microsof_0a:43:e3 (c0:33:5e:0a:43:e3)
  Frame check sequence: 0xaac303a8 [unverified]
  [FCS Status: Unverified]
```

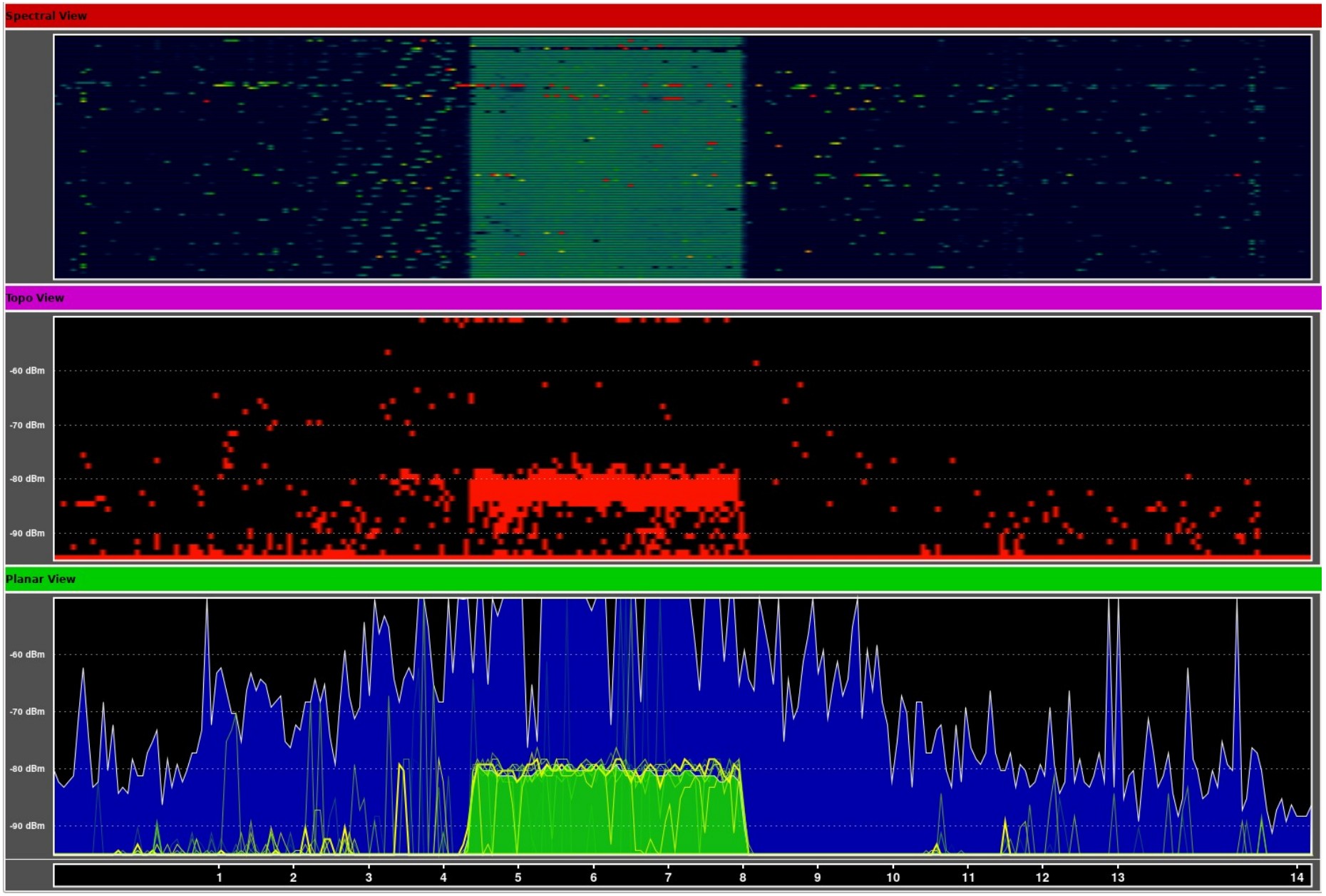
AP Placement and Channel Allocation



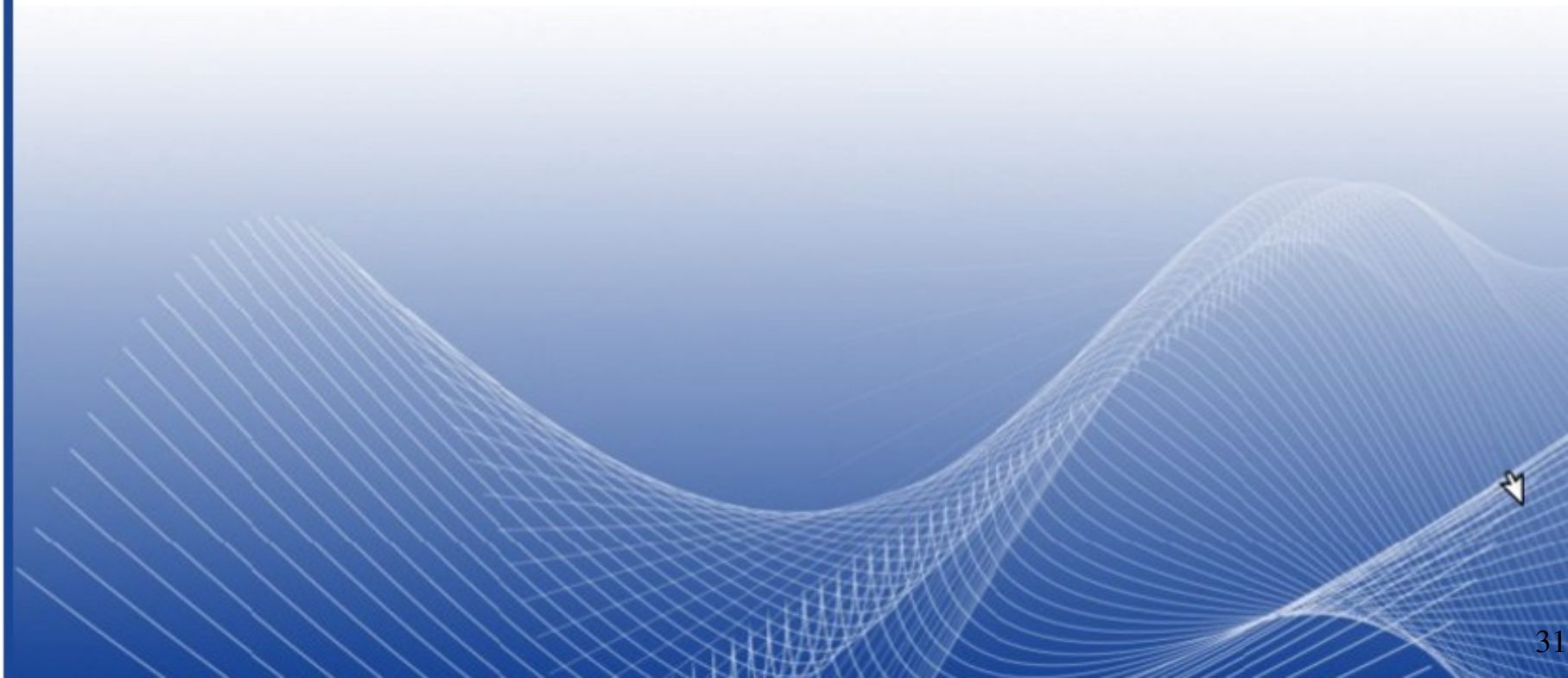


- 802.11n or 802.11ac 5GHz deployment does not have the overlap or collision domain issues of 2.4GHz.

Usage of Spectrum Analysis



Security in WLAN



Cyphering

- **Transforming the data in a non-eligible form to the entities that do not have the appropriate key, through an appropriate function.**

- Objective:
  - Provide confidentiality
  - Generally consists on an algorithm associated to a set of parameters
  - Algorithm should not depend on the parameters (and on the key)

Cyphering Techniques

- Symmetric (private/secret)
  - Only one key for sender and receiver.
  - Same key to code and decode.
- Asymmetric (public)
  - Sender and receiver share a secret key.
  - Use 2 distinct keys, a private and a public.

  Message is cyphered with the public key at the sender; it is decyphered with the private key at the receiver.

  OR

  The 2 keys are used to derive a common secret one.

- There is a correspondence between both keys: only the private key is able to process the message coded by the public key.
- It is not possible to detect the private key based on the public one.

Requirements on the Access to the Network (General)

- Identification of the users in their access to the network.
- Identity ‘substitution’ cannot be possible.
- Easy security support and use.
- Low maintenance effort.
- Allow access to guests.
- Support several authentication mechanisms.
- Additionally
  - Cyphered wireless access.
  - Allocation of VLANs per user or group.

Security in 802.11

- Intends to provide security standards similar to the ones of cabled networks.
  - Wireless is subject to larger security fails.
    - E.g. “sniffing”, “war driving” (km!!), “rogue networks”.
- Simulate the control of the physical medium.
  - Implementing authentication mechanisms for stations.
- Security traditionally included two systems.
  - Wired Equivalent Privacy (WEP), a data encapsulation system.
  - Shared Key Authentication, authentication mechanism.

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)

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

Open Network + Gateways

- Open Network + VPN gateway.
  - Open network, with the client being authenticated in an IP VPN (L3) in order to be able to access its network from outside.
    - Requires VPN client software.
    - Difficult to use by guests.
    - Scalability is being enhanced.
    - VPN controllers can be expensive.
- Open network + web gateway.
  - Open network, with the client being authenticated in web server (L3), providing “credentials”.
    - Easy to use by guests.
    - Standardization is being enhanced.
    - Scalability is being enhanced.
    - A browser needs to be working during the session.

Service Set ID (SSID)

- **SSID – name of the network.**
- Identifies the BSS, emitted in the beacon.
- Networks can block beacon and force the AP to be directly specified by its name.
- This is not very efficient.
  - Operating systems are smarter.
  - The change of SSID requires a new advertisement to all stations.
  - With the increasing number of stations, security will decrease.
  - SSID is only useful to the self-organization of the stations, not to security.

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.**
  - Compatible with work developed in 802.11i.
  - Only supports BSS.
  - 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.
- WPA has two distinct components.
  - Authentication, based on 802.1X.
  - Ciphering based on TKIP (Temporal Key Integrity Protocol).

WPA

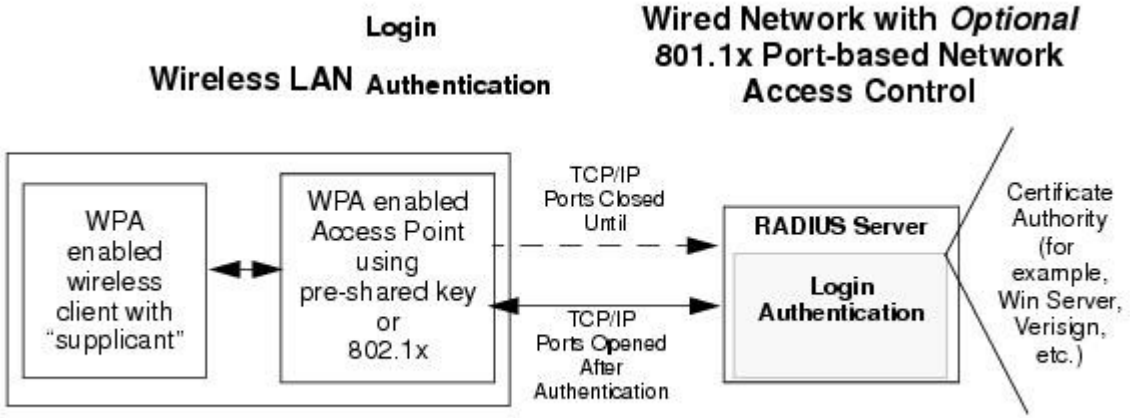
- Authentication
  - 802.1X (≠ 802.11x) – defined for wired and wireless sessions, as a transport protocol
    - EAP (Extensible Authentication Protocol) – like a wrapper for the specific authentication traffic
    - Impact of EAP
      - Authentication does not traverse the AP (STA - server)
      - It is possible to use different authentication methods without changing APs
  - Defines also a Pre-Shared Key (PSK)
    - For local networks
- Temporal Key Integrity Protocol (TKIP) – internal solution with better protection, for actual equipments
  - Greater privacy
    - Uses the same cipher, but now associated to the MAC and a larger IV
    - “Key rollover” with temporal validity
  - Greater integrity
    - Integrity separated key

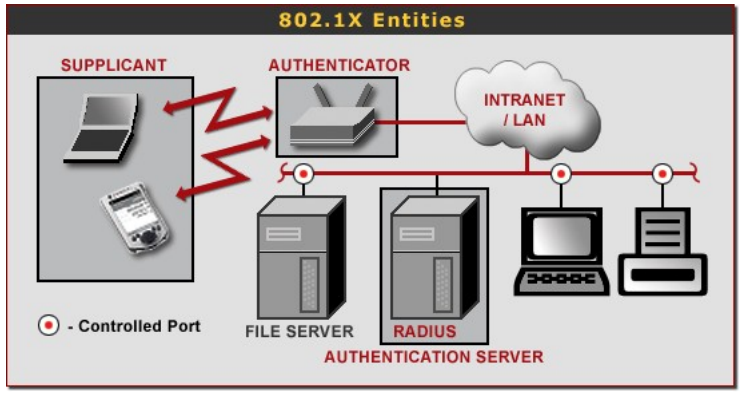
802.11i (WPA2)

- Better than WPA
  - Also includes TKIP
  - Authentication IBSS (ad-hoc mode)?
  - RSN (Robust Security Network) protocol
    - Authentication and ciphering between APs and stations
    - Supports new ciphering protocols, resorting to 802.1x and EAP
    - Supports AES (Advanced Encryption Standard) ciphering
- Problems
  - It does not cipher control and management frames
    - (Disassociate, output power, etc).
  - Requires new hardware

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.
- Resorts to RADIUS servers.
  - Roaming is seamless.





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
```

Wireless (Personal) Area Networks
WPANs

WLANs vs WPANs

- WLAN is oriented to external interconnection.
  - Interacts with cable structure (LAN).
  - Time of connections: hours-days.
  - Portable equipments.
  - Wireless motivation: reconfiguration cost, unexpected mobility.
- WPAN is oriented to internal vision.
  - Interacts with personal objects.
  - Time of connections: seconds-hours.
  - Equipments inherently mobile.
  - Wireless motivation: wires are not convenient, increase of interactivity.

Applications

- Applications include
  - Short-range (< 10 m) connectivity for multimedia applications
    - PDAs, Cameras, Voice (hands free devices)
    - High QoS, high data rate (IEEE 802.15.3)
  - Industrial sensor applications
    - Low speed, low battery, low cost sensor networks (IEEE 802.15.4)
- Common goals
  - No cable connections
  - Little or no infrastructure
  - Device interoperability

IEEE 802.15 WPAN Standards

	ZigBee	Bluetooth	UWB	Wi-Fi
Standard	IEEE 802.15.4	IEEE 802.15.1	IEEE 802.15.3a	IEE 802.11a, b, g, n
Industry organizations	ZigBee Alliance	Bluetooth SIG	UWB Forum and WiMedia Alliance	Wi-Fi Alliance
Topology	Mesh, star, tree	Star	Star	Star
RF frequency	868/915 MHz, 2.4 GHz	2.4 GHz	3.1 to 10.6 GHz (U.S.)	2.4 GHz, 5.8 GHz
Data rate	250 kbits/s	723 kbits/s	110 Mbits/s to 1.6 Gbits/s	11 to 105 Mbits/s
Range	10 to 300 m	10 m	4 to 20 m	10 to 100 m
Power	Very low	Low	Low	High
Battery operation (life)	Alkaline (months to years)	Rechargeable (days to weeks)	Rechargeable (hours to days)	Rechargeable (hours)
Nodes	65,000	8	128	32

Not Personal WPAN

- In more recent WPAN applications the “Personal” is no longer relevant to the technology.
- Machine-to-machine (M2M) communications are getting more relevant.
  - Ex: facility management system with an automatic metering infrastructure (AMI)