Wireless LAN 2/3

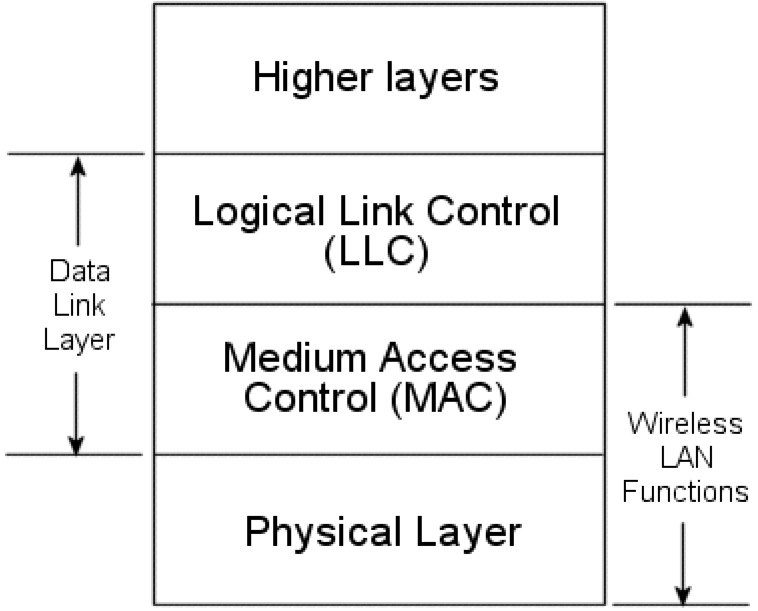
KIS FRI UNIZA

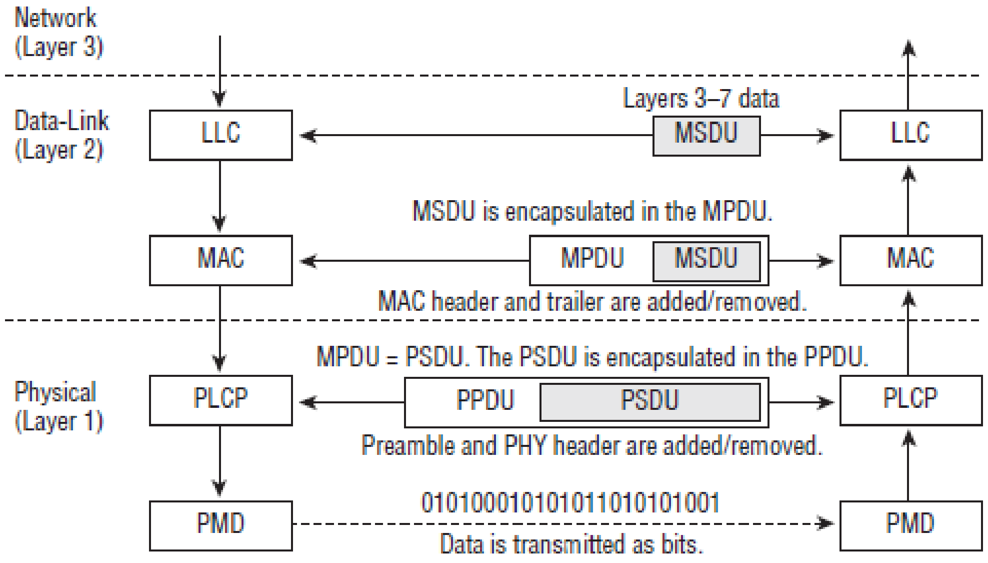
Vytvorené v rámci projektu KEGA 026TUKE-4/2021

IEEE 802.11 Protocol Architecture

- **PHY (Physical Layer)**
  - The physical later transmits the bits of data through the channel by defining electrical, mechanical, and procedural specifications
- **MAC (Media Access Control)**
  - Allows many wireless computers, or any wireless appliances, to share the same frequency. The data needs to be transmitted at different times
- **LLC (Logical Link Control)**
  - Responsible for multiplexing of several network protocols (IPv4/IPv6, IPX, other)
  - Exchanges data between users on either end of a LAN, this is used by IEEE 802.2

PLCP - Physical Layer Convergence Procedure sublayer
PMD - Physical Medium Dependent sublayer
PPDU - PLCP Protocol Data Unit
PSDU - PLCP Service Data Unit
MPDU - MAC Protocol Data Unit
MSDU - MAC Service Data Unit





Network (Layer 3)
Data-Link (Layer 2)
Physical (Layer 1)
LLC
Layers 3–7 data
MSDU
LLC
MSDU is encapsulated in the MPDU.
MAC
MPDU
MSDU
MAC
MAC header and trailer are added/removed.
MPDU = PSDU. The PSDU is encapsulated in the PPDU.
PLCP
PPDU
PSDU
PLCP
Preamble and PHY header are added/removed.
PMD
0101000101010110101010001
PMD
Data is transmitted as bits.

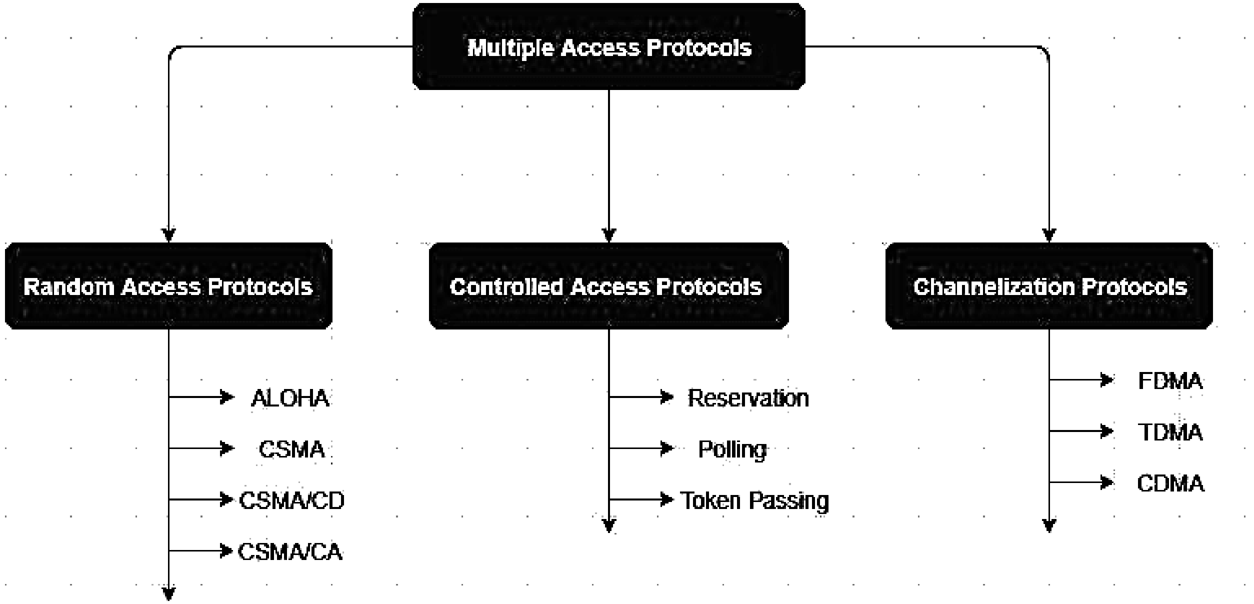
IEEE 802.11 MAC Layer

Multiple Access Protocols - Overview

- A set of methods of controlling access to a single transmission medium in order to provide efficient use of its capacity

- **ALOHA**
  - Whenever a station has a data, it transmits. Sender finds out whether transmission was successful or experienced a collision by listening to the broadcast from the destination station. Sender retransmits after some random time if there is a collision, developed in 1970 by Hawaii university

- **CSMA**
  - Carrier Sense Multiple Access
  - Improvement: starts transmission only if no transmission is ongoing



IEEE 802.3 and 802.11 MAC Layer Overview

- **IEEE 802.3 Ethernet, CSMA/CD**
  - Carrier Sense Multiple Access with Collision Detection
  - Starts transmission only if no transmission is ongoing. Imediately stops ongoing transmission if a collision is detected.
- **IEEE 802.4 Token Bus** – A Token Ring like protocol over a virtual ring on a coaxial cable
- **IEEE 802.5 Token Ring** – A special three-byte frame called a token that is passed around a logical ring of workstations or servers. Only the node possessing the token may transmit.
- **IEEE 802.11 Wireless, CSMA/CA**
  - Carrier Sense Multiple Access with Collision Avoidance
  - Half duplex communication - both transmission and reception cannot happen at the same time, therefore collision detection is not possible when transmitting
  - If another node was heard before the transmission, waits for a period of time (random) for the remote node to stop transmitting before listening again for a free communications channel

IEEE 802.11 MAC Layer

MAC - Media Access Control

- Shared wireless media, provides reliable delivery mechanism for user data over unreliable and noisy wireless media
- Requires participation of all nodes
- Fair distribution wireless bandwidth among all clients
- DCF (Distributed Coordination Function) or PCF (Point Coordination Function) 802.11 media access types are mandatory. The PCF is not widely implemented. DCF is a widely used technique used to prevent collisions in IEEE 802.11-based WLAN standard

Reliable wireless communication needs at least 2 types of frame

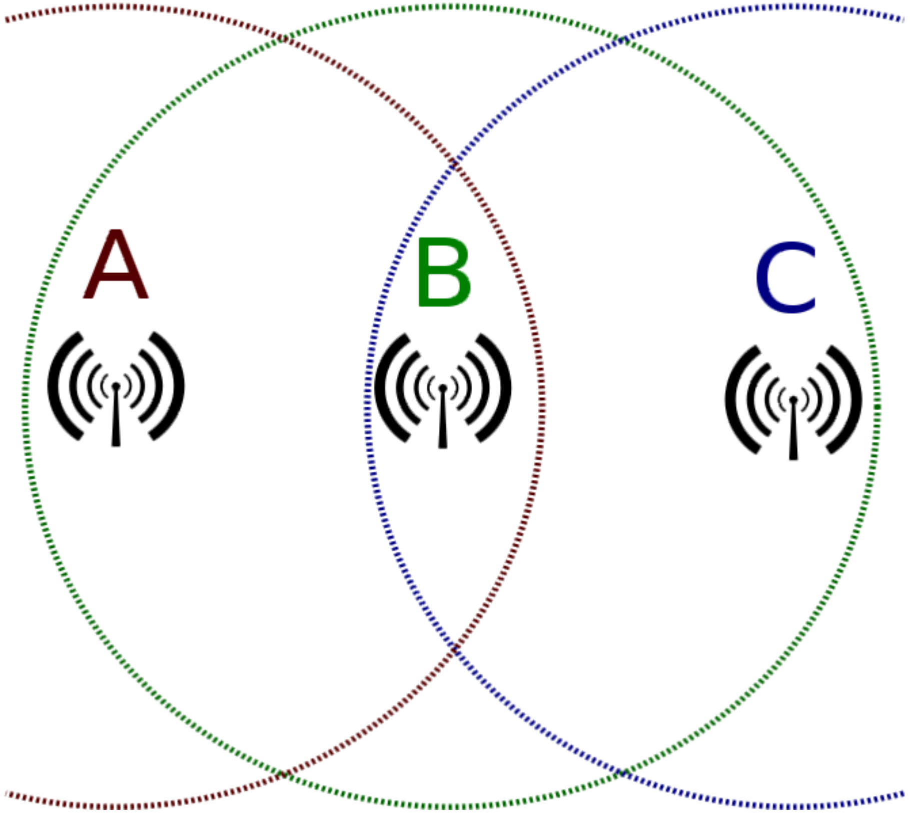
CSMA/CA with ACK

- Requires participation of all nodes – a data frame from source to destination and acknowledgment (ACK) from destination
- If the source does not get ACK, it tries to retransmit based on the algorithm of MAC protocol
- Wireless media is dealing with hidden node problem

IEEE 802.11 MAC Layer

Hidden Node problem

- Even in case the end device is able to operate in full duplex mode there is another issue in wireless environment
- Sending end device checks whether the channel is idle but it can only checks within its broadcast range
- Other end device can be out of the range of the first end device but still on the network connected to AP (node B)
- Therefore, they could both be sending data to the AP at the same time and not aware of the presence of each other
- AP would not be able to receive any data due to collisions



IEEE 802.11 MAC Layer

Hidden Node problem solution - CSMA/CA with RTS/CTS

- 802.11 MAC protocol solves this problem by adding 2 additional frames called RTS (request to send) and CTS (clear to send frames)
- Those 2 frames are quite short comparing to a normal data frame
- If A wants to send data to B, it sends RTS frame and waits for CTS from AP (node B)

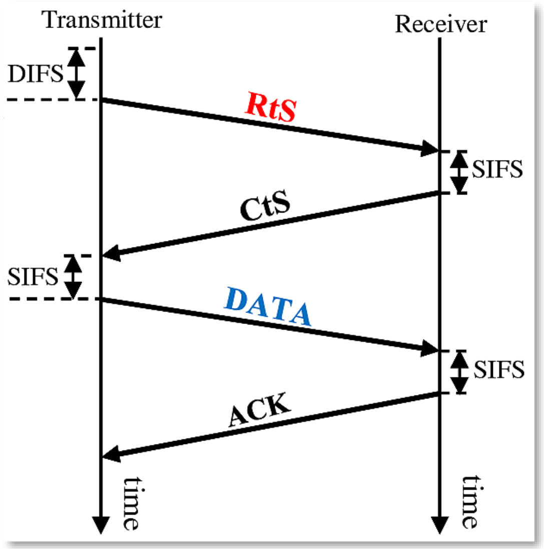
- If both clients A and C send RTS frames to AP at the same time, the collision will happen. However, since RTS is short frame, the collision possibility will be for a short period of time
- If AP (node B) will send CTS to A, node C will also detect CTS frame
- When node A sends RTS, all nodes within the communication range of A hold their transmission until the communication between A and AP (node B) is completed by ACK
- When AP sends CTS, all nodes in the range of AP will hold the transmission until ACK

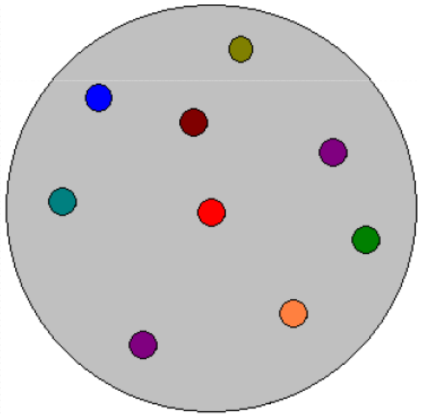
IEEE 802.11 MAC Layer

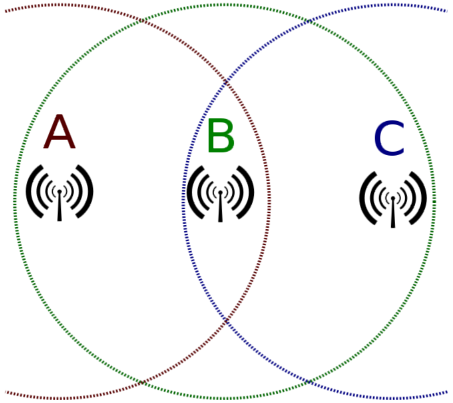
Hidden Node problem – RTS/CTS are not always necessary

- If all nodes are within the communication range, the hidden node problem doesn’t exist, therefore RTS/CTS not necessary
- Alternatively, if the demand for the bandwidth from nodes is low, wireless media is not frequently accessed, there is a little chance for a collision

- Node C can detect data frames and will wait until the end of ACK frame from AP







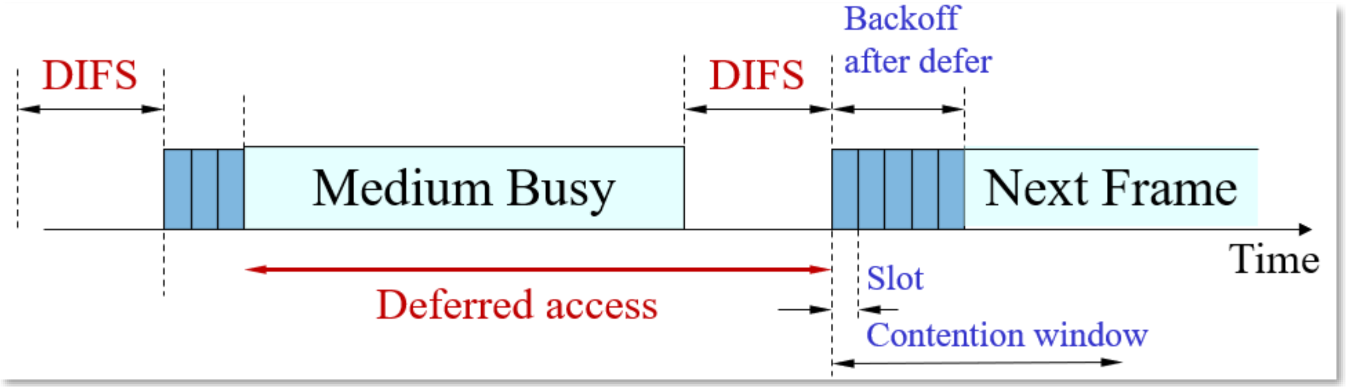
IEEE 802.11 MAC Layer

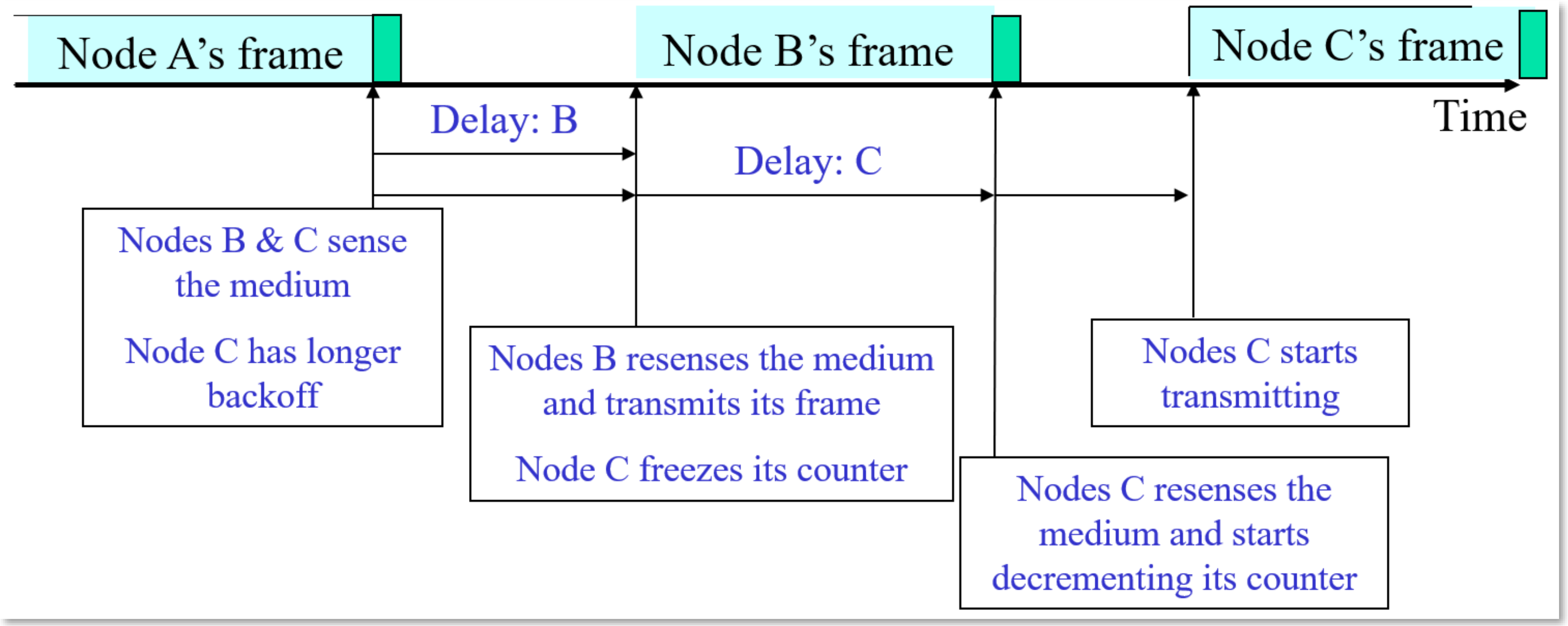
CSMA/CA in details

- All terminals listen to the same medium as CSMA/CD
- Terminal ready to transmit senses the medium
- If medium is busy, it waits until the end of current transmission
- It again waits for an additional predetermined time period **DIFS** (Distributed Inter Frame Space) or **SIFS** (Short Inter Frame Space – after RTS/CTF or Data frame)
- Then picks up a random number of slots (the initial value of **Backoff counter**) within a contention window (random number must be greater than 0 and smaller than a maximum value referred to as the **Contention window**) to wait before transmitting its frame
- If there are transmissions by other terminals during this time period (Backoff time), the terminal *freezes* its counter
- It *resumes* count down after other terminals finish transmission + DIFS. The terminal can start its transmission when the counter reaches to zero

IEEE 802.11 MAC Layer

CSMA/CA in details





Nodes B & C sense the medium

Node C has longer backoff

Nodes B resenses the medium and transmits its frame

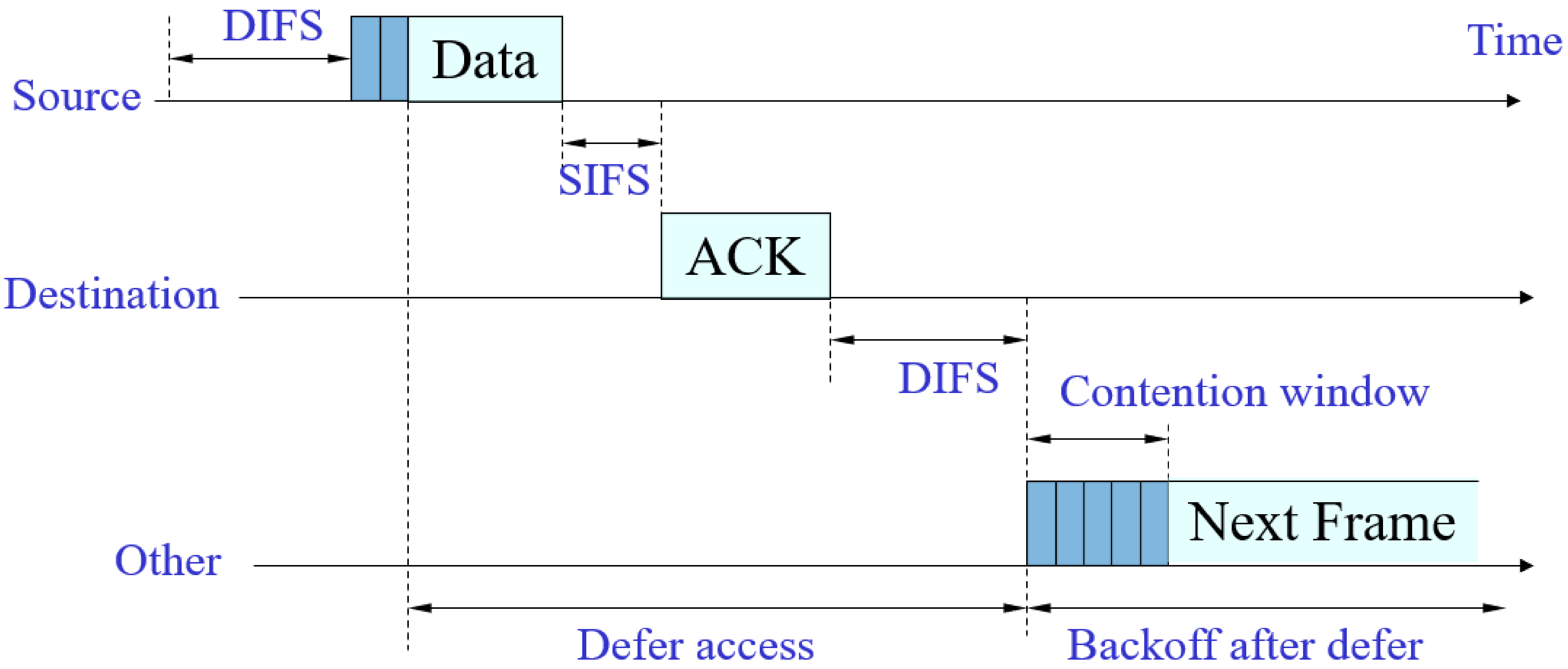
Node C freezes its counter

Nodes C resenses the medium and starts decrementing its counter

Nodes C starts transmitting

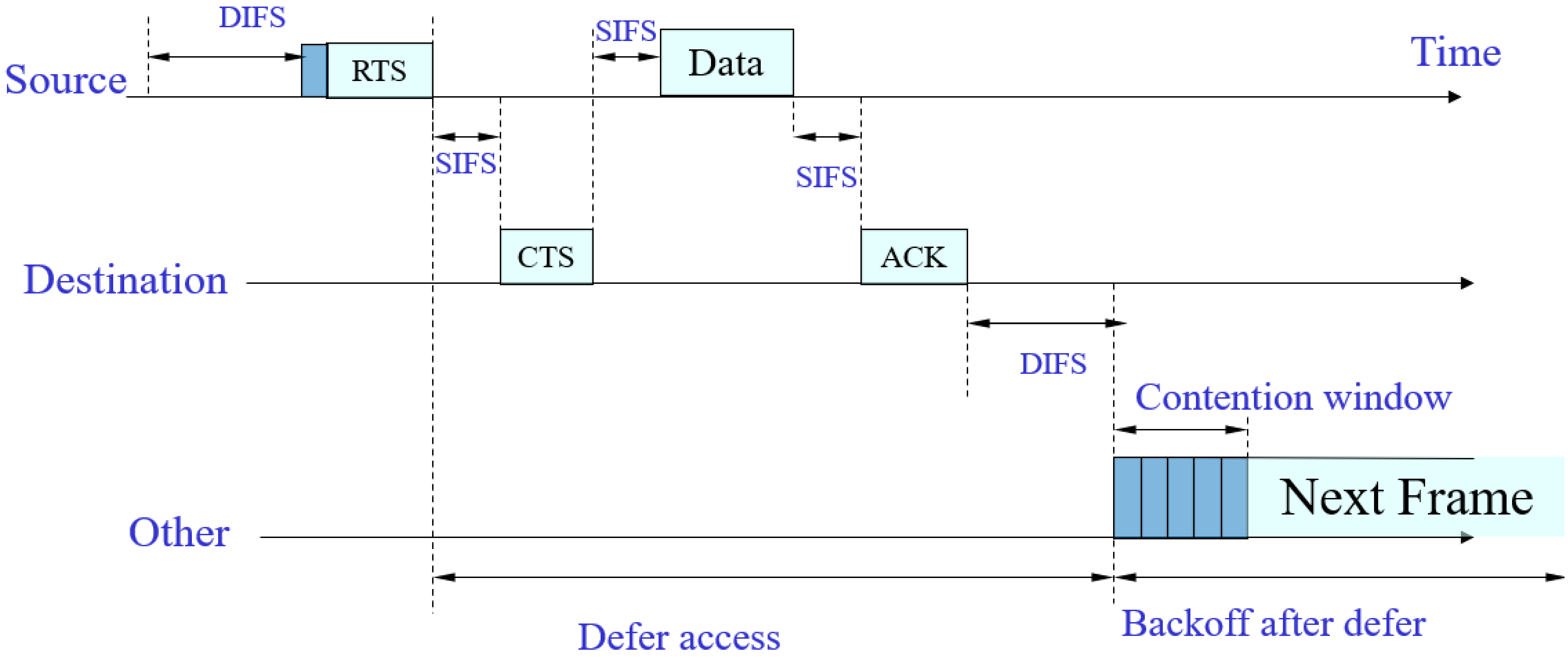
IEEE 802.11 MAC Layer

CSMA/CA with ACK



IEEE 802.11 MAC Layer

CSMA/CD with RTS/CTS



IEEE 802.11 MAC Layer

Retry counters

- A node transmits a frame several time before ir receives ACK
- 2 retry counters: **short retry counter** (short frames) and **long retry counter** (long frames)
- Every time the transmission of a frame fails, the corresponding retry counter is incremented by 1; up to defined limits. In case the limit is reached, the frame is discarded

- Discarded frame needs to be solved by higher layer

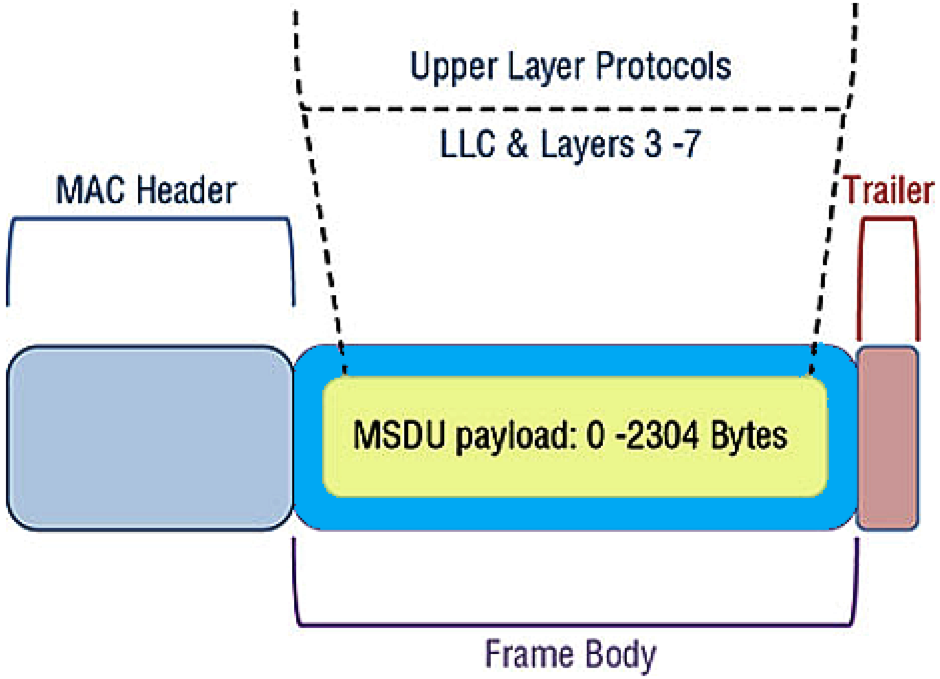
IEEE 802.11 MAC Layer

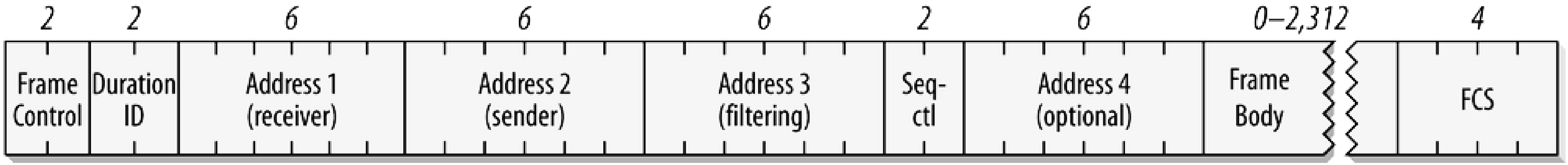
MAC Frame format

MPDU - MAC Protocol Data Unit (also PSDU)

There are three types of 802.11 MAC frames:

- **Management** - used to mange the BSS
- **Control** - control access to the medium
- **Data** - contain payloads that are the layer 3-7 information

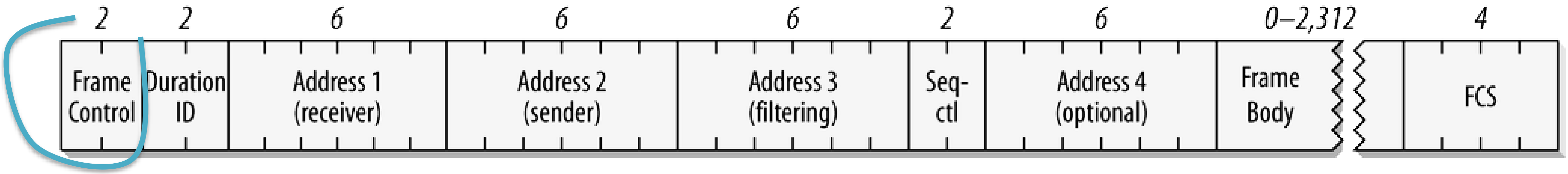




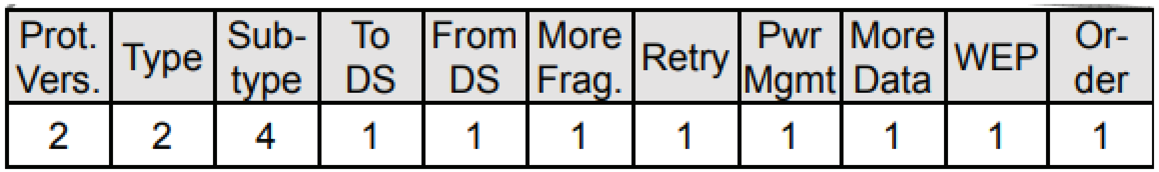
2	2	6	6	6	2	6	0–2,312	4
Frame Control	Duration ID	Address 1 (receiver)	Address 2 (sender)	Address 3 (filtering)	Seq-ctl	Address 4 (optional)	Frame Body	FCS

IEEE 802.11 MAC Layer

Frame Control



2	2	6	6	6	2	6	0–2,312	4
Frame Control	Duration ID	Address 1 (receiver)	Address 2 (sender)	Address 3 (filtering)	Seq-ctl	Address 4 (optional)	Frame Body	FCS



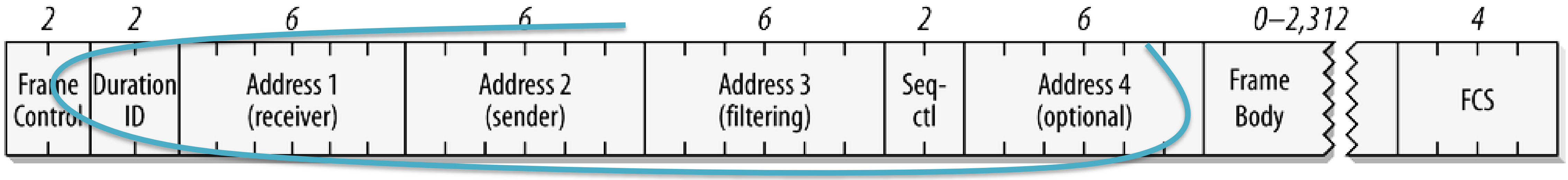
Prot. Vers.	Type	Sub-type	To DS	From DS	More Frag.	Retry	Pwr Mgmt	More Data	WEP	Or-der
2	2	4	1	1	1	1	1	1	1	1

Frame Control - two bits *Protocol Version* subfield, two bits *Type subfield*, and four bits *Subtype subfield*. The remaining subfields can be present or absent depending on the setting of the Type and Subtype subfields

- DS Status – indicates the directionality of the frame
- Power Management - indicates whether the sending device is in active mode or power-save mode
- More Data - Indicates to a device in power-save mode that the AP has more frames to send
- Security - indicates whether encryption and authentication are used

IEEE 802.11 MAC Layer

Other frame fields



2	2	6	6	6	2	6	0–2,312	4
Frame Control	Duration ID	Address 1 (receiver)	Address 2 (sender)	Address 3 (filtering)	Seq-ctl	Address 4 (optional)	Frame Body	FCS

Duration - Typically used to indicate the remaining time needed to receive the next frame transmission. Carries **NAV** (Network Allocation Vector) value

Address 1 - Usually contains the MAC address of the receiving wireless device or AP (DMAC)

Address 2 - Usually contains the MAC address of the transmitting wireless device or AP (SMAC)

Address 3 - Sometimes contains the MAC address of the destination, such as the router interface (default gateway) to which the AP is attached (BSSID)

Sequence Control - Contains the Sequence Number and the Fragment Number subfields. The Sequence Number indicates the sequence number of each frame

Address 4 - Usually missing because it is used only in ad hoc mode

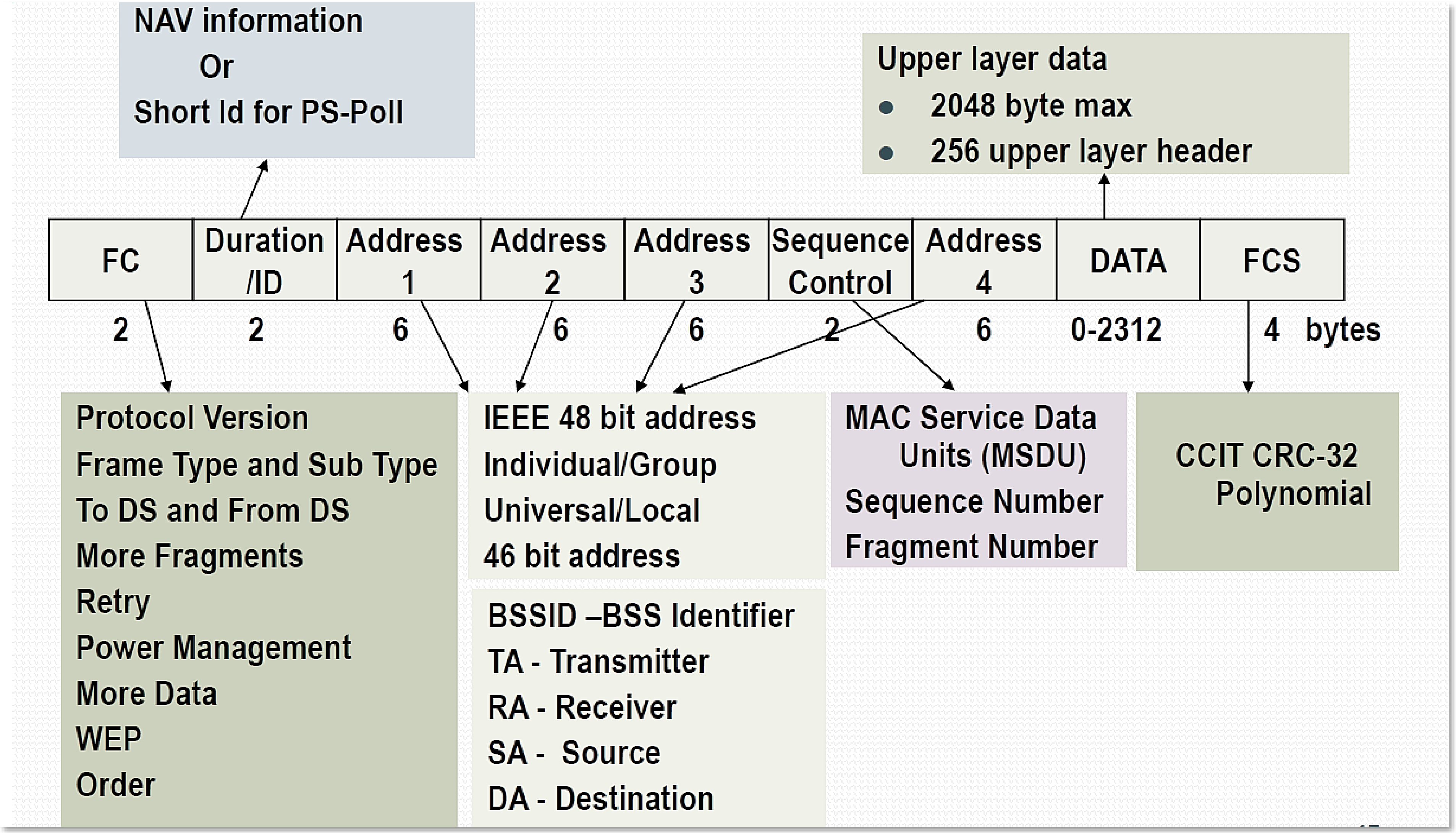
IEEE 802.11 MAC Layer

NAV – Network Allocation Vector

- The mechanism limits the need for physical carrier sensing in order to save power
- The station listening on the wireless media reads the Duration field and sets its NAV.
- Indicator for a station how long it must defer from accessing the medium
- Wireless stations (notebooks, smartphones) are often battery powered, so the station may enter a power saving mode
- A station decrements its NAV counter until zero, wakes up to sense the medium again

IEEE 802.11 MAC Layer

MAC Frame format overview



NAV information
Or
Short Id for PS-Poll

Upper layer data
- 2048 byte max
- 256 upper layer header

FC	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	DATA	FCS	
2	2	6	6	6	2	6	0-2312	4	bytes

Protocol Version
Frame Type and Sub Type
To DS and From DS
More Fragments
Retry
Power Management
More Data
WEP
Order

IEEE 48 bit address
Individual/Group
Universal/Local
46 bit address

BSSID –BSS Identifier
TA - Transmitter
RA - Receiver
SA - Source
DA - Destination

MAC Service Data Units (MSDU)
Sequence Number
Fragment Number

CCIT CRC-32 Polynomial

IEEE 802.11 MAC Layer

Frame subtypes

CONTROL

- RTS
- CTS
- ACK
- PS-Poll
- CF-End & CF-End ACK

DATA

- Data
- Data+CF-ACK
- Data+CF-Poll
- Data+CF-ACK+CF-Poll
- Null Function
- CF-ACK (nodata)
- CF-Poll (nodata)
- CF-ACK+CF+Poll

MANAGEMENT

- Beacon
- Probe Request & Response
- Authentication
- Deauthentication
- Association Request & Response
- Reassociation Request & Response
- Disassociation
- Announcement Traffic Indication Message (ATIM)

Note: CF (Contention Free) control frames are to indicate contention-free functions in PCF medium access method

IEEE 802.11 MAC Layer

Management functionality

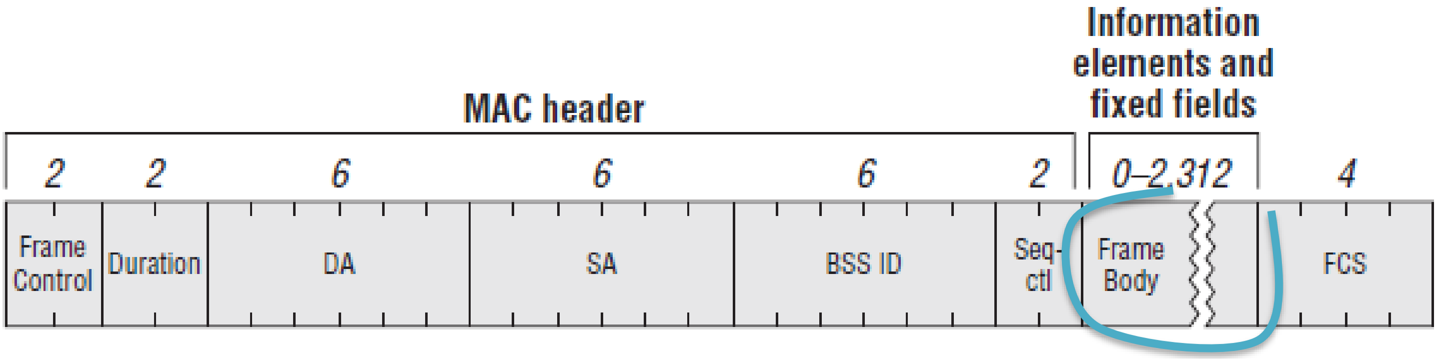
- Establishing the identity of a network station in a wired network is easy as directly connected to the network infrastructure or network L2/L3 node/s.
- Wireless network had to introduce management feature to provide similar functionality

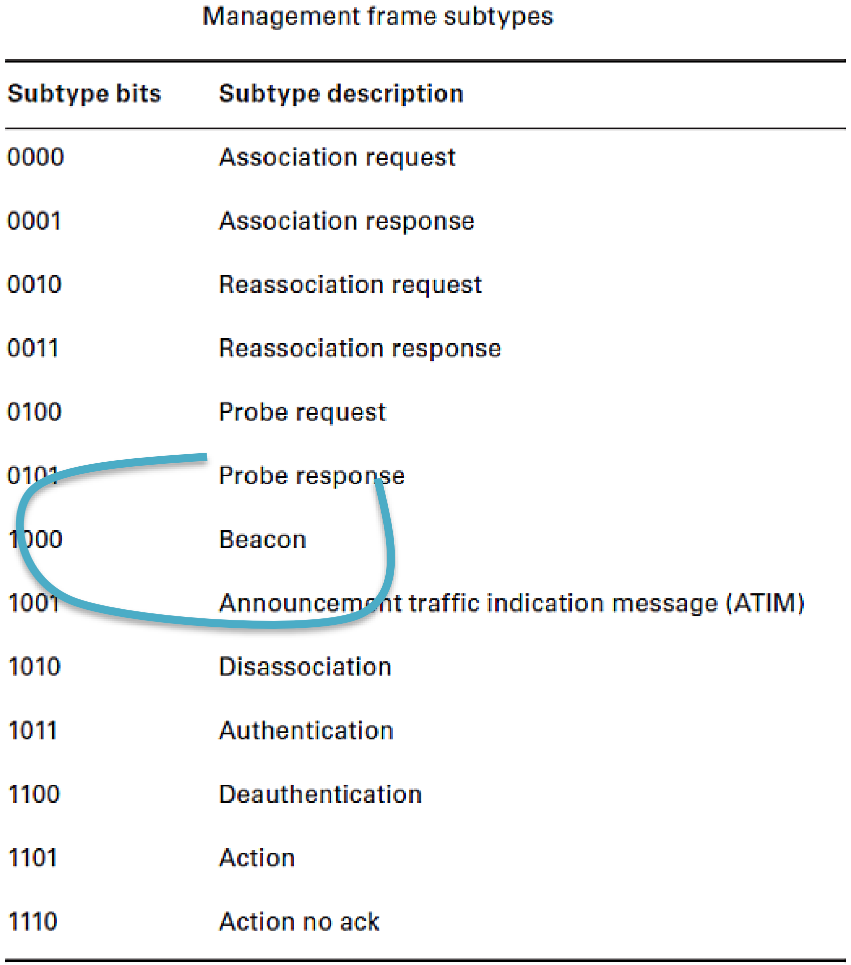
- New client must associate with an AP

  - Scans all channels, listening for beacon frames containing AP's name (SSID) and MAC address
  - Selects AP to associate with
  - Then performs authentication
  - Finally, typically runs DHCP to get IP address in AP's wireless subnet

IEEE 802.11 MAC Layer

Management frames & Beacon frame





Management frame subtypes

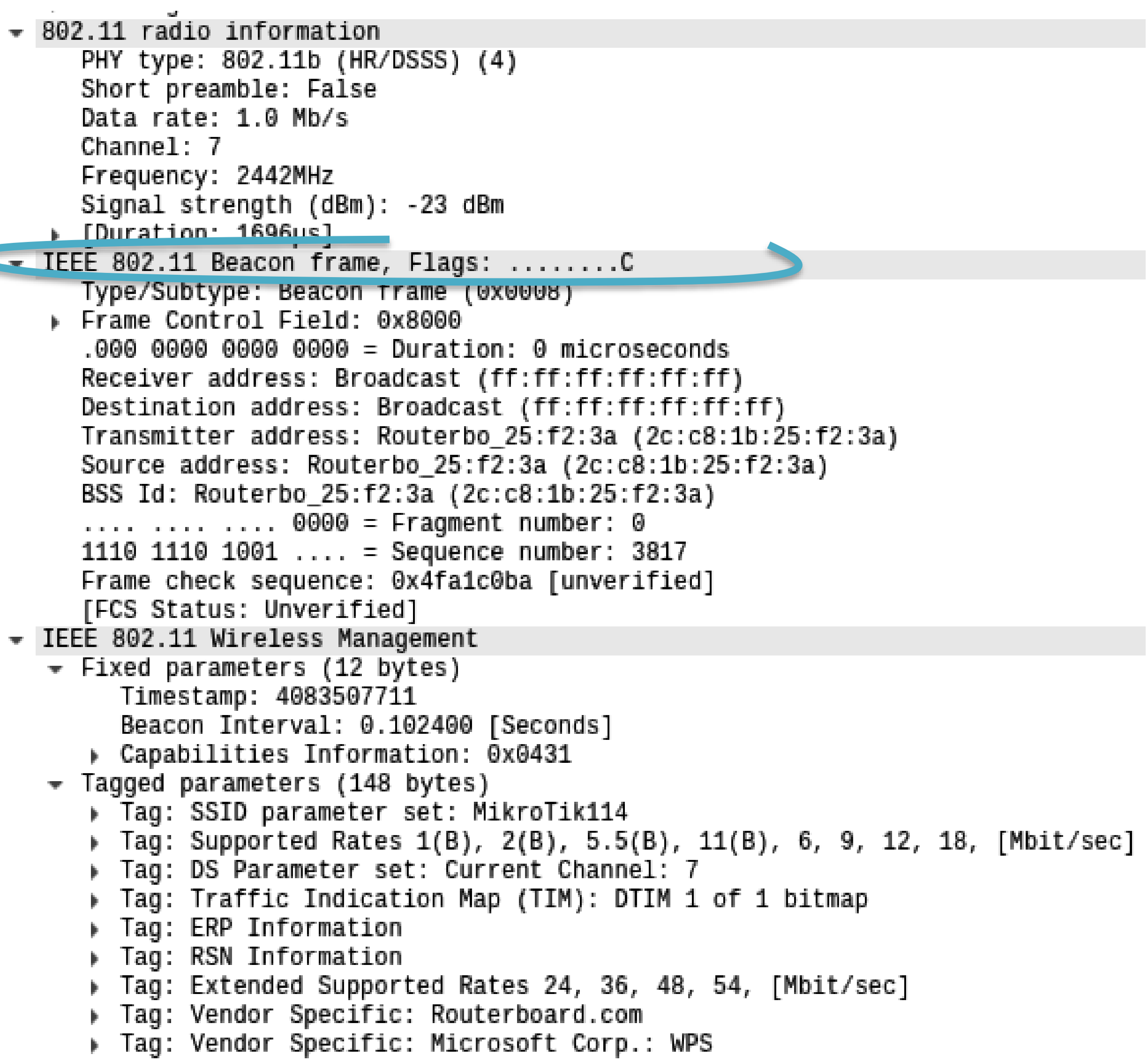
Subtype bits	Subtype description
0000	Association request
0001	Association response
0010	Reassociation request
0011	Reassociation response
0100	Probe request
0101	Probe response
1000	Beacon
1001	Announcement traffic indication message (ATIM)
1010	Disassociation
1011	Authentication
1100	Deauthentication
1101	Action
1110	Action no ack

Beacon broadcast frames - contains all the information about the network. Beacon frames are transmitted periodically by AP, they serve to announce the presence of a wireless LAN with its capabilities – Basic Service Set support

- SSID and BSSID (the MAC address of AP interface)
- Timestamp for sync
- Beacon interval provides info about beacon intervals (around 102.4ms)
- Capability information like supported rates 802.11 standard supported, FHSS, DSSS and other

IEEE 802.11 MAC Layer

Beacon frame



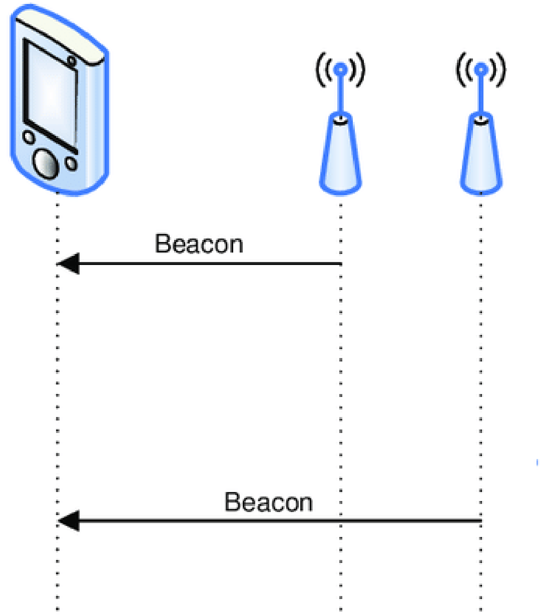
```
▾ 802.11 radio information
    PHY type: 802.11b (HR/DSSS) (4)
    Short preamble: False
    Data rate: 1.0 Mb/s
    Channel: 7
    Frequency: 2442MHz
    Signal strength (dBm): -23 dBm
  ▸ [Duration: 1696us]
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▸ 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: Routerbo_25:f2:3a (2c:c8:1b:25:f2:3a)
    Source address: Routerbo_25:f2:3a (2c:c8:1b:25:f2:3a)
    BSS Id: Routerbo_25:f2:3a (2c:c8:1b:25:f2:3a)
    .... .... .... 0000 = Fragment number: 0
    1110 1110 1001 .... = Sequence number: 3817
    Frame check sequence: 0x4fa1c0ba [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (12 bytes)
      Timestamp: 4083507711
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0431
  ▾ Tagged parameters (148 bytes)
    ▸ Tag: SSID parameter set: MikroTik114
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 7
    ▸ Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
    ▸ Tag: ERP Information
    ▸ Tag: RSN Information
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Vendor Specific: Routerboard.com
    ▸ Tag: Vendor Specific: Microsoft Corp.: WPS
```

- IEEE 802.11b frame
  - 1Mbps data rate
  - Channel 7
  - Subtype is Beacon
  - Receive and Destination address is the same
  - Transmitter and Source address is the same
- TIM / DTIM – Traffic Indicator Map / Delivery TIM
  - TIM information element advertises if any associated stations have buffered unicast frames
  - DTIM is to broadcast / multicast traffic
- ERP – Extended Rate PHY (802.11g)
  - 802.11g radios use a new technology ERP
  - ERP field contains info about non-ERP (802.11b) STAs
  - In this case RTS/CTS exchange uses a PHY rate of 1 Mbps using DBPSK modulation as specified by DSSS
  - Backward compatibility
- RSN – Robust Security Network
  - Negotiates the authentication and encryption algorithms
- DS - Distribution System – indicates infrastructure type and parameters

IEEE 802.11 MAC Layer

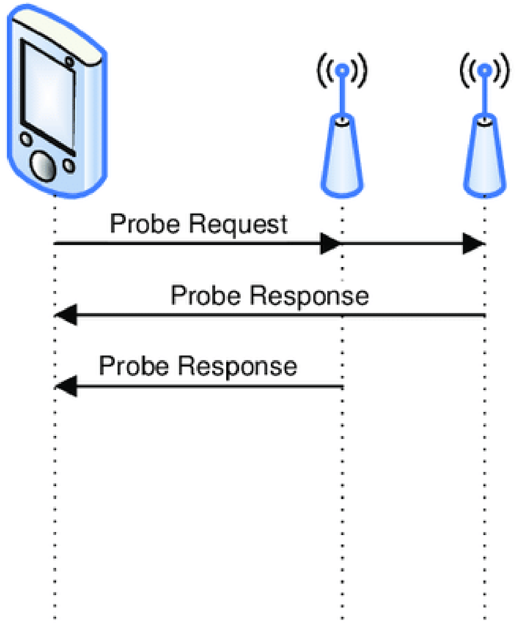
802.11: Passive and Active scanning

- Typically performed by clients, a mechanism to find out APs within range



Passive scanning

- Beacon frames sent from APs periodically
- When captured by client
- Authentication & Association Requests follows
- Saves battery, once per second, this mode cannot be disabled

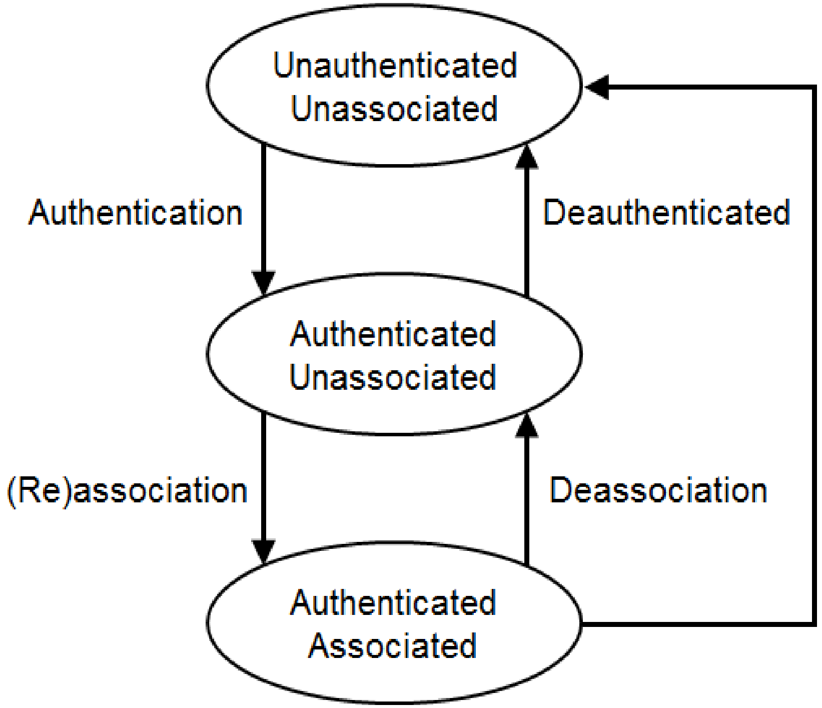


Active scanning

- Probe Request frame broadcast from Client
- Probe Response frames sent from APs
- Authentication & Association Requests follows

IEEE 802.11 MAC Layer

802.11 Authentication and Association



3 connection states

- Unauthenticated & Unassociated
- Authenticated & Unassociated
- Authenticated & Associated

Authentication

- To prove client's identity to AP
- Open System or Shared Key (WEP) authentication, typically Open System used

Association

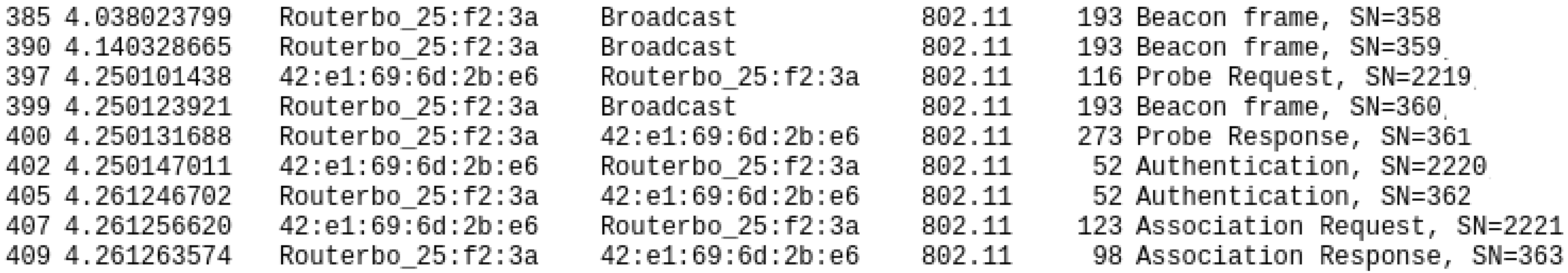
- Registration to AP, resource allocation on AP
- Negotiated after authentication
- After established, data forwarding

- Keep in mind that 802.11 authentication is not the same as WPA/WPA2 or 802.1x authentication which occurs during and/or after Association phase
- 802.11 authentication was originally designed for WEP however this security scheme has been proved insecure therefore already deprecated

IEEE 802.11 MAC Layer

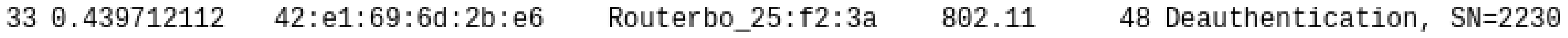
802.11 Authentication and Association (ACKs not visible, skipped)

- SSID MikroTik114, BSSID 2c:c8:1b:25:f2:3a
- Active scanning by client 42:e1:69:6d:2b:e6

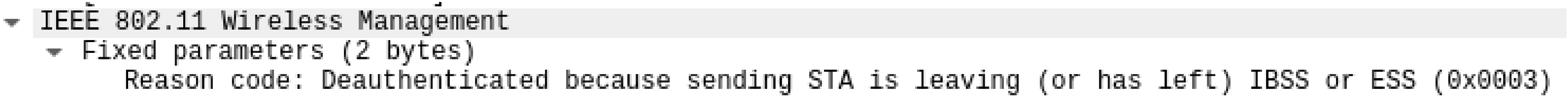


```
385 4.038023799   Routerbo_25:f2:3a   Broadcast           802.11    193 Beacon frame, SN=358
390 4.140328665   Routerbo_25:f2:3a   Broadcast           802.11    193 Beacon frame, SN=359
397 4.250101438   42:e1:69:6d:2b:e6   Routerbo_25:f2:3a   802.11    116 Probe Request, SN=2219
399 4.250123921   Routerbo_25:f2:3a   Broadcast           802.11    193 Beacon frame, SN=360
400 4.250131688   Routerbo_25:f2:3a   42:e1:69:6d:2b:e6   802.11    273 Probe Response, SN=361
402 4.250147011   42:e1:69:6d:2b:e6   Routerbo_25:f2:3a   802.11     52 Authentication, SN=2220
405 4.261246702   Routerbo_25:f2:3a   42:e1:69:6d:2b:e6   802.11     52 Authentication, SN=362
407 4.261256620   42:e1:69:6d:2b:e6   Routerbo_25:f2:3a   802.11    123 Association Request, SN=2221
409 4.261263574   Routerbo_25:f2:3a   42:e1:69:6d:2b:e6   802.11     98 Association Response, SN=363
```

802.11 Deauthentication and Deassociation



```
 33 0.439712112   42:e1:69:6d:2b:e6   Routerbo_25:f2:3a   802.11     48 Deauthentication, SN=2230
```

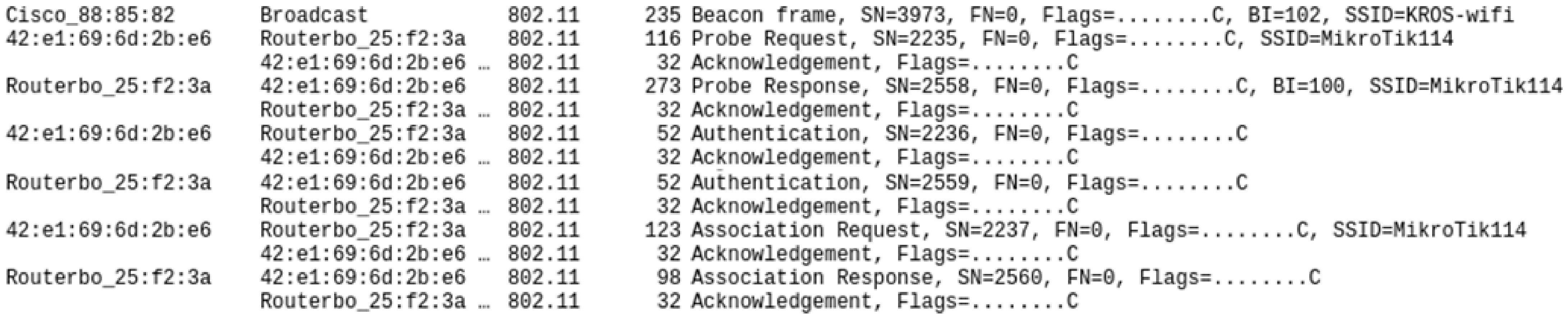


```
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (2 bytes)
      Reason code: Deauthenticated because sending STA is leaving (or has left) IBSS or ESS (0x0003)
```

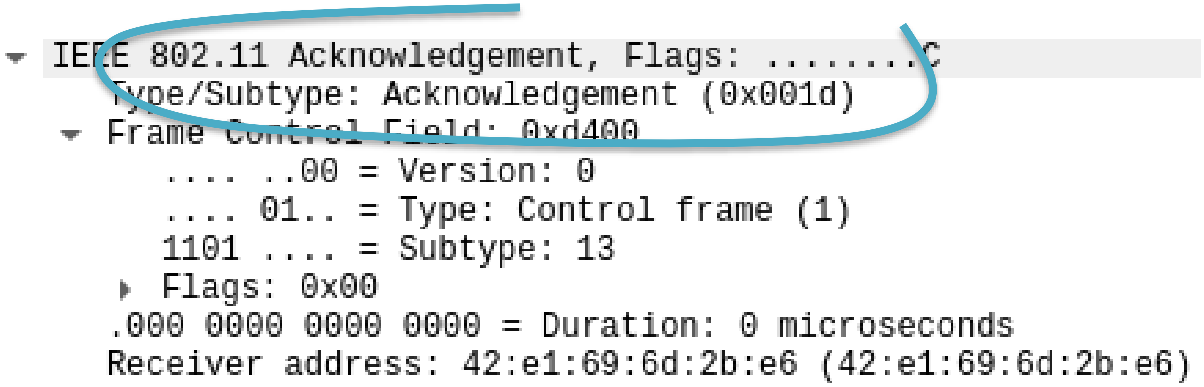
IEEE 802.11 MAC Layer

802.11 Authentication and Association (including ACKs)

- SSID MikroTik114, BSSID 2c:c8:1b:25:f2:3a
- Active scanning by client 42:e1:69:6d:2b:e6



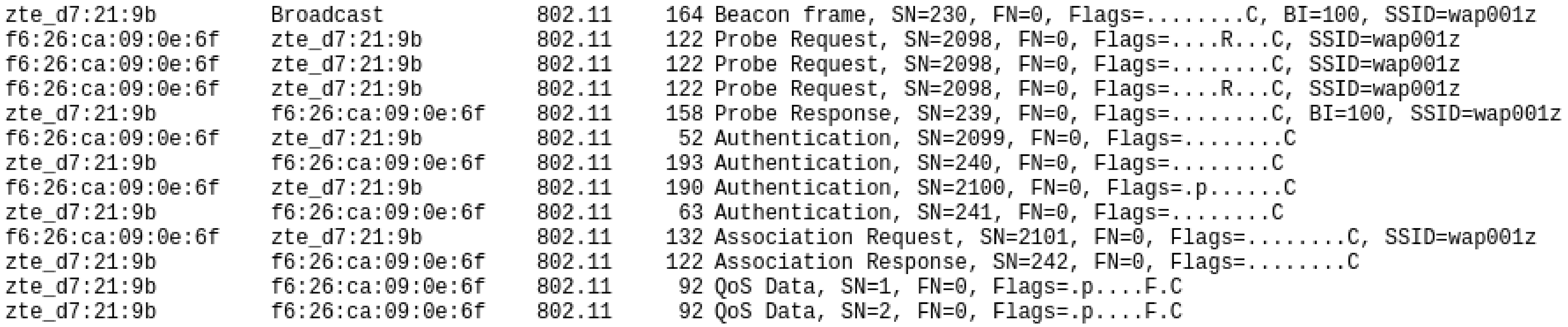
```
Cisco_88:85:82       Broadcast            802.11     235 Beacon frame, SN=3973, FN=0, Flags=........C, BI=102, SSID=KROS-wifi
42:e1:69:6d:2b:e6    Routerbo_25:f2:3a    802.11     116 Probe Request, SN=2235, FN=0, Flags=........C, SSID=MikroTik114
                     42:e1:69:6d:2b:e6 …  802.11      32 Acknowledgement, Flags=........C
Routerbo_25:f2:3a    42:e1:69:6d:2b:e6    802.11     273 Probe Response, SN=2558, FN=0, Flags=........C, BI=100, SSID=MikroTik114
                     Routerbo_25:f2:3a …  802.11      32 Acknowledgement, Flags=........C
42:e1:69:6d:2b:e6    Routerbo_25:f2:3a    802.11      52 Authentication, SN=2236, FN=0, Flags=........C
                     42:e1:69:6d:2b:e6 …  802.11      32 Acknowledgement, Flags=........C
Routerbo_25:f2:3a    42:e1:69:6d:2b:e6    802.11      52 Authentication, SN=2559, FN=0, Flags=........C
                     Routerbo_25:f2:3a …  802.11      32 Acknowledgement, Flags=........C
42:e1:69:6d:2b:e6    Routerbo_25:f2:3a    802.11     123 Association Request, SN=2237, FN=0, Flags=........C, SSID=MikroTik114
                     42:e1:69:6d:2b:e6 …  802.11      32 Acknowledgement, Flags=........C
Routerbo_25:f2:3a    42:e1:69:6d:2b:e6    802.11      98 Association Response, SN=2560, FN=0, Flags=........C
                     Routerbo_25:f2:3a …  802.11      32 Acknowledgement, Flags=........C
```



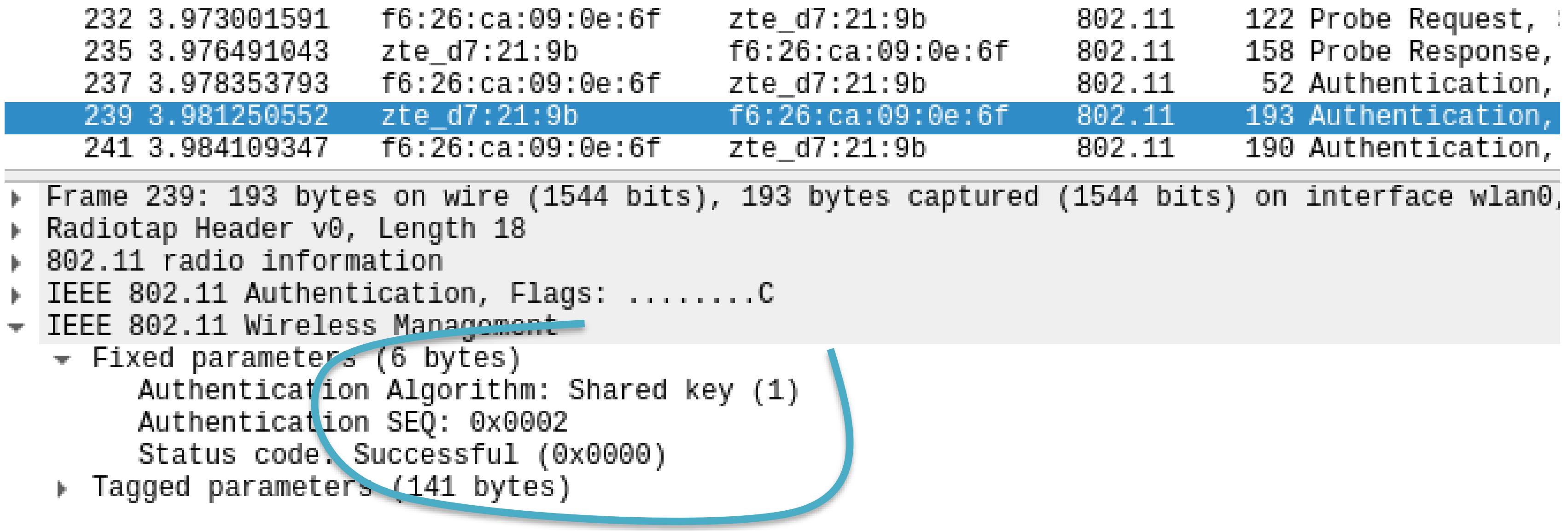
```
▾ IEEE 802.11 Acknowledgement, Flags: ........C
    Type/Subtype: Acknowledgement (0x001d)
  ▾ Frame Control Field: 0xd400
       .... ..00 = Version: 0
       .... 01.. = Type: Control frame (1)
       1101 .... = Subtype: 13
     ▸ Flags: 0x00
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: 42:e1:69:6d:2b:e6 (42:e1:69:6d:2b:e6)
```

IEEE 802.11 MAC Layer

802.11 Authentication - WEP



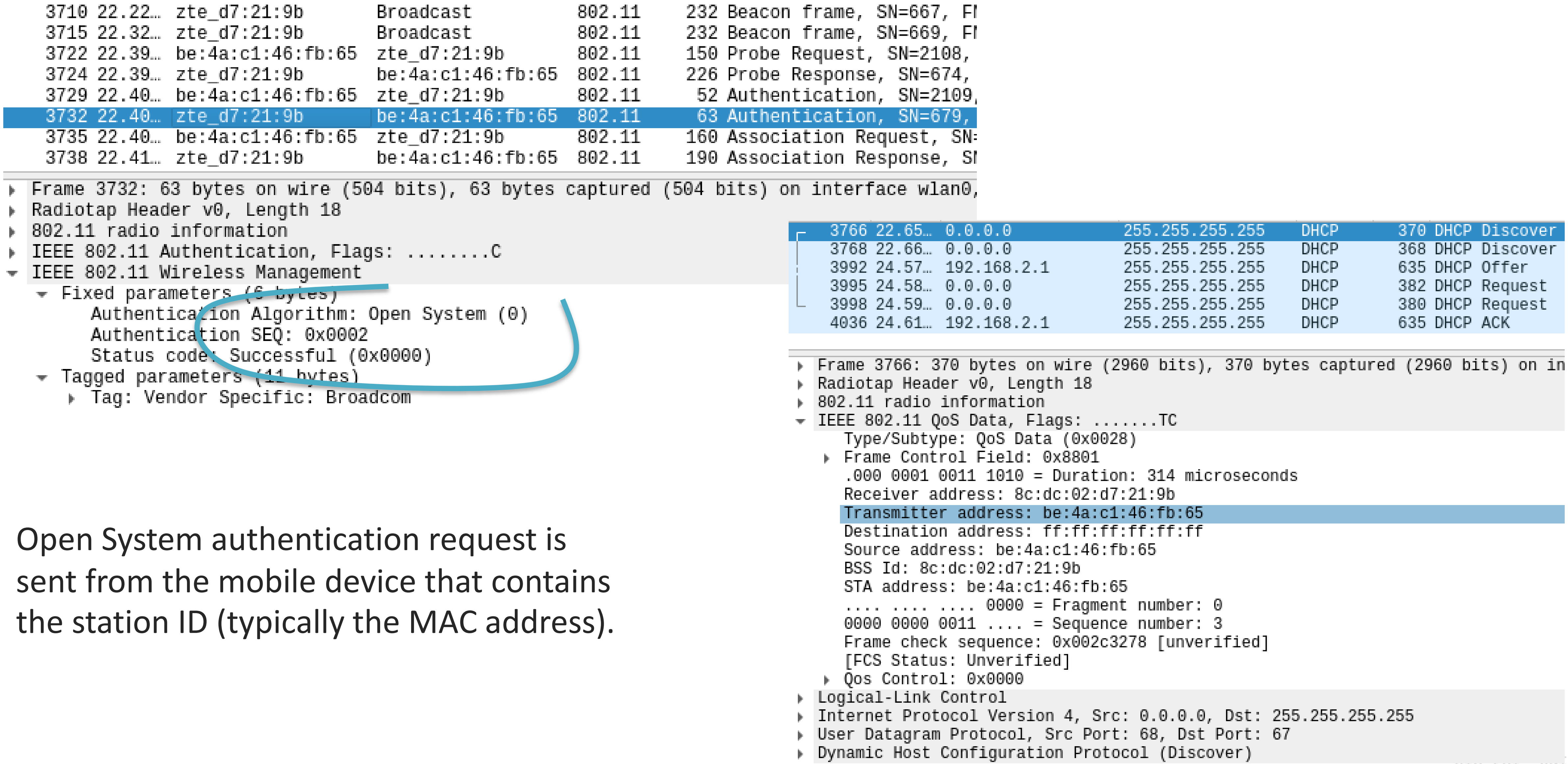
```
zte_d7:21:9b          Broadcast             802.11     164 Beacon frame, SN=230, FN=0, Flags=........C, BI=100, SSID=wap001z
f6:26:ca:09:0e:6f     zte_d7:21:9b          802.11     122 Probe Request, SN=2098, FN=0, Flags=....R...C, SSID=wap001z
f6:26:ca:09:0e:6f     zte_d7:21:9b          802.11     122 Probe Request, SN=2098, FN=0, Flags=........C, SSID=wap001z
f6:26:ca:09:0e:6f     zte_d7:21:9b          802.11     122 Probe Request, SN=2098, FN=0, Flags=....R...C, SSID=wap001z
zte_d7:21:9b          f6:26:ca:09:0e:6f     802.11     158 Probe Response, SN=239, FN=0, Flags=........C, BI=100, SSID=wap001z
f6:26:ca:09:0e:6f     zte_d7:21:9b          802.11      52 Authentication, SN=2099, FN=0, Flags=........C
zte_d7:21:9b          f6:26:ca:09:0e:6f     802.11     193 Authentication, SN=240, FN=0, Flags=........C
f6:26:ca:09:0e:6f     zte_d7:21:9b          802.11     190 Authentication, SN=2100, FN=0, Flags=.p......C
zte_d7:21:9b          f6:26:ca:09:0e:6f     802.11      63 Authentication, SN=241, FN=0, Flags=........C
f6:26:ca:09:0e:6f     zte_d7:21:9b          802.11     132 Association Request, SN=2101, FN=0, Flags=........C, SSID=wap001z
zte_d7:21:9b          f6:26:ca:09:0e:6f     802.11     122 Association Response, SN=242, FN=0, Flags=........C
zte_d7:21:9b          f6:26:ca:09:0e:6f     802.11      92 QoS Data, SN=1, FN=0, Flags=.p....F.C
zte_d7:21:9b          f6:26:ca:09:0e:6f     802.11      92 QoS Data, SN=2, FN=0, Flags=.p....F.C
```



```
    232 3.973001591    f6:26:ca:09:0e:6f     zte_d7:21:9b          802.11     122 Probe Request,
    235 3.976491043    zte_d7:21:9b          f6:26:ca:09:0e:6f     802.11     158 Probe Response,
    237 3.978353793    f6:26:ca:09:0e:6f     zte_d7:21:9b          802.11      52 Authentication,
    239 3.981250552    zte_d7:21:9b          f6:26:ca:09:0e:6f     802.11     193 Authentication,
    241 3.984109347    f6:26:ca:09:0e:6f     zte_d7:21:9b          802.11     190 Authentication,

▸ Frame 239: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) on interface wlan0,
▸ Radiotap Header v0, Length 18
▸ 802.11 radio information
▸ IEEE 802.11 Authentication, Flags: ........C
▾ IEEE 802.11 Wireless Management
   ▾ Fixed parameters (6 bytes)
        Authentication Algorithm: Shared key (1)
        Authentication SEQ: 0x0002
        Status code: Successful (0x0000)
   ▸ Tagged parameters (141 bytes)
```

IEEE 802.11 MAC Layer

802.11 Authentication – Open System only, no other security



```
3710 22.22… zte_d7:21:9b       Broadcast          802.11    232 Beacon frame, SN=667, FN
3715 22.32… zte_d7:21:9b       Broadcast          802.11    232 Beacon frame, SN=669, FN
3722 22.39… be:4a:c1:46:fb:65  zte_d7:21:9b       802.11    150 Probe Request, SN=2108,
3724 22.39… zte_d7:21:9b       be:4a:c1:46:fb:65  802.11    226 Probe Response, SN=674,
3729 22.40… be:4a:c1:46:fb:65  zte_d7:21:9b       802.11     52 Authentication, SN=2109,
3732 22.40… zte_d7:21:9b       be:4a:c1:46:fb:65  802.11     63 Authentication, SN=679,
3735 22.40… be:4a:c1:46:fb:65  zte_d7:21:9b       802.11    160 Association Request, SN=
3738 22.41… zte_d7:21:9b       be:4a:c1:46:fb:65  802.11    190 Association Response, SN
```

```
▸ Frame 3732: 63 bytes on wire (504 bits), 63 bytes captured (504 bits) on interface wlan0,
▸ Radiotap Header v0, Length 18
▸ 802.11 radio information
▸ IEEE 802.11 Authentication, Flags: ........C
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0002
      Status code: Successful (0x0000)
  ▾ Tagged parameters (11 bytes)
    ▸ Tag: Vendor Specific: Broadcom
```

```
3766 22.65… 0.0.0.0        255.255.255.255  DHCP   370 DHCP Discover
3768 22.66… 0.0.0.0        255.255.255.255  DHCP   368 DHCP Discover
3992 24.57… 192.168.2.1    255.255.255.255  DHCP   635 DHCP Offer
3995 24.58… 0.0.0.0        255.255.255.255  DHCP   382 DHCP Request
3998 24.59… 0.0.0.0        255.255.255.255  DHCP   380 DHCP Request
4036 24.61… 192.168.2.1    255.255.255.255  DHCP   635 DHCP ACK
```

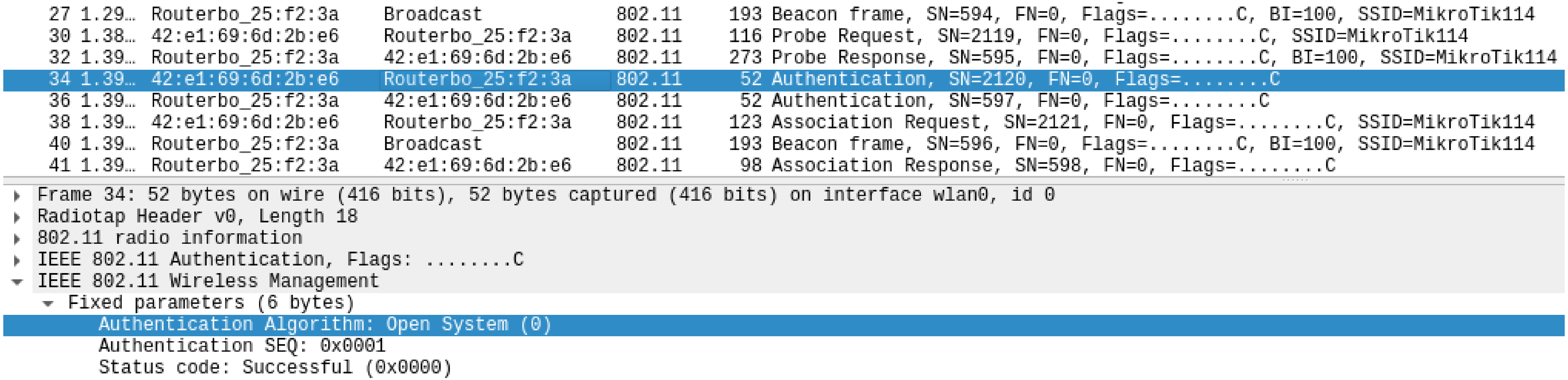
```
▸ Frame 3766: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on in
▸ Radiotap Header v0, Length 18
▸ 802.11 radio information
▾ IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  ▸ Frame Control Field: 0x8801
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: 8c:dc:02:d7:21:9b
    Transmitter address: be:4a:c1:46:fb:65
    Destination address: ff:ff:ff:ff:ff:ff
    Source address: be:4a:c1:46:fb:65
    BSS Id: 8c:dc:02:d7:21:9b
    STA address: be:4a:c1:46:fb:65
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0011 .... = Sequence number: 3
    Frame check sequence: 0x002c3278 [unverified]
    [FCS Status: Unverified]
  ▸ Qos Control: 0x0000
▸ Logical-Link Control
▸ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▸ Dynamic Host Configuration Protocol (Discover)
```

Open System authentication request is sent from the mobile device that contains the station ID (typically the MAC address).

IEEE 802.11 MAC Layer

802.11i-2004 Authentication

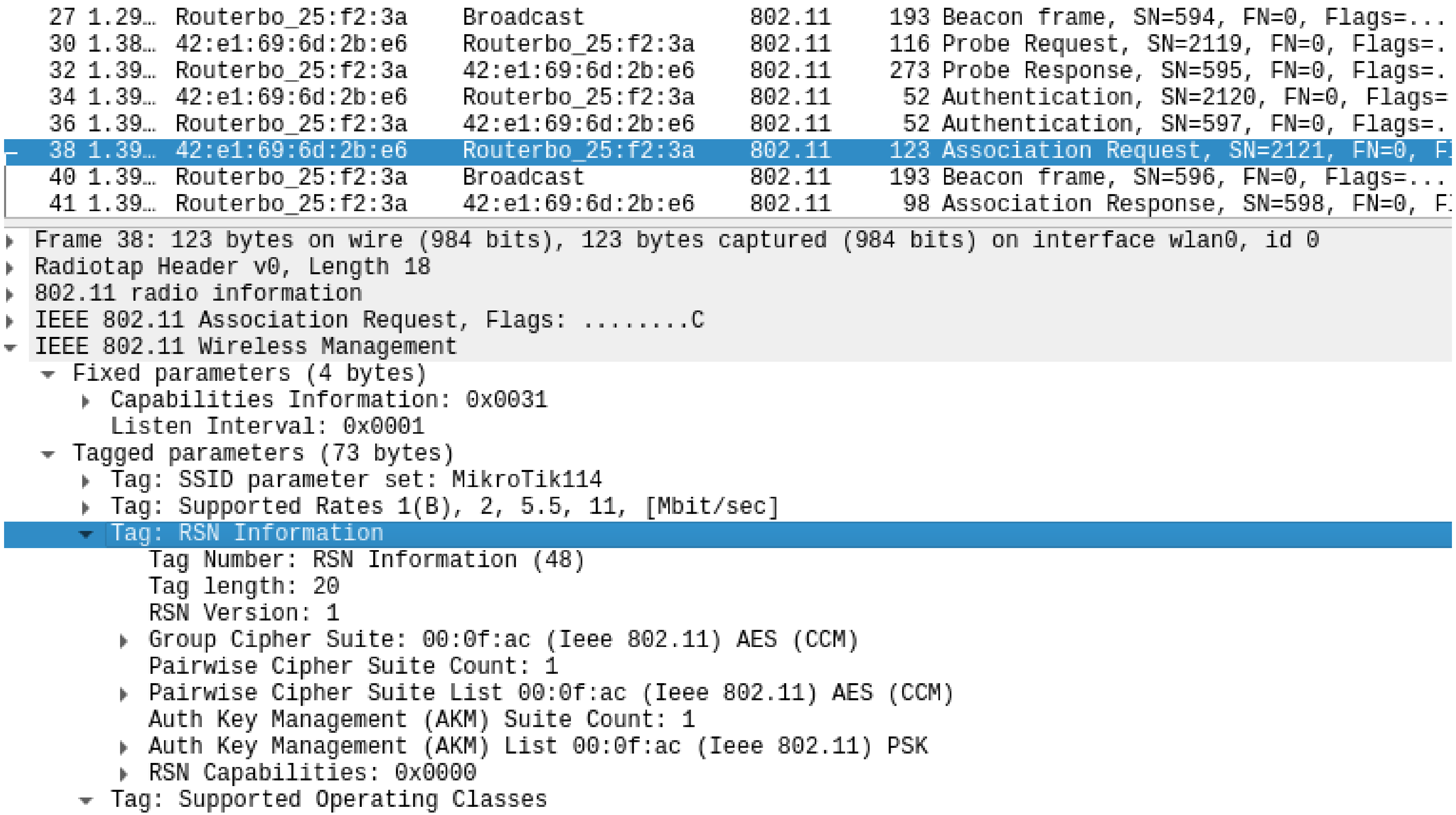
- WPA/WPA2 is just a commercial name for a complete implementation of the 802.11i specification, the amendment to the original 802.11
- 802.11i introduces the concept of Robust Security Network Association (RSNA)



```
27 1.29… Routerbo_25:f2:3a    Broadcast            802.11     193 Beacon frame, SN=594, FN=0, Flags=........C, BI=100, SSID=MikroTik114
30 1.38… 42:e1:69:6d:2b:e6    Routerbo_25:f2:3a    802.11     116 Probe Request, SN=2119, FN=0, Flags=........C, SSID=MikroTik114
32 1.39… Routerbo_25:f2:3a    42:e1:69:6d:2b:e6    802.11     273 Probe Response, SN=595, FN=0, Flags=........C, BI=100, SSID=MikroTik114
34 1.39… 42:e1:69:6d:2b:e6    Routerbo_25:f2:3a    802.11      52 Authentication, SN=2120, FN=0, Flags=........C
36 1.39… Routerbo_25:f2:3a    42:e1:69:6d:2b:e6    802.11      52 Authentication, SN=597, FN=0, Flags=........C
38 1.39… 42:e1:69:6d:2b:e6    Routerbo_25:f2:3a    802.11     123 Association Request, SN=2121, FN=0, Flags=........C, SSID=MikroTik114
40 1.39… Routerbo_25:f2:3a    Broadcast            802.11     193 Beacon frame, SN=596, FN=0, Flags=........C, BI=100, SSID=MikroTik114
41 1.39… Routerbo_25:f2:3a    42:e1:69:6d:2b:e6    802.11      98 Association Response, SN=598, FN=0, Flags=........C

▸ Frame 34: 52 bytes on wire (416 bits), 52 bytes captured (416 bits) on interface wlan0, id 0
▸ Radiotap Header v0, Length 18
▸ 802.11 radio information
▸ IEEE 802.11 Authentication, Flags: ........C
▾ IEEE 802.11 Wireless Management
    ▾ Fixed parameters (6 bytes)
        Authentication Algorithm: Open System (0)
        Authentication SEQ: 0x0001
        Status code: Successful (0x0000)
```

IEEE 802.11 MAC Layer

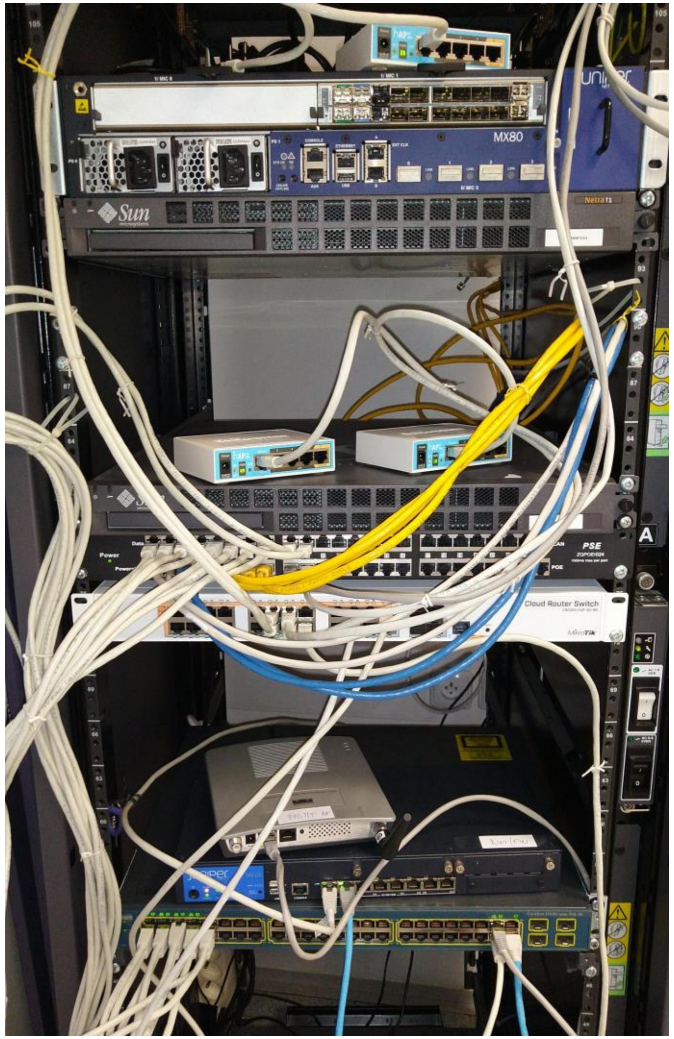
802.11i-2004 Authentication



```
 27 1.29… Routerbo_25:f2:3a    Broadcast            802.11     193 Beacon frame, SN=594, FN=0, Flags=...
 30 1.38… 42:e1:69:6d:2b:e6    Routerbo_25:f2:3a    802.11     116 Probe Request, SN=2119, FN=0, Flags=.
 32 1.39… Routerbo_25:f2:3a    42:e1:69:6d:2b:e6    802.11     273 Probe Response, SN=595, FN=0, Flags=.
 34 1.39… 42:e1:69:6d:2b:e6    Routerbo_25:f2:3a    802.11      52 Authentication, SN=2120, FN=0, Flags=
 36 1.39… Routerbo_25:f2:3a    42:e1:69:6d:2b:e6    802.11      52 Authentication, SN=597, FN=0, Flags=.
 38 1.39… 42:e1:69:6d:2b:e6    Routerbo_25:f2:3a    802.11     123 Association Request, SN=2121, FN=0, F
 40 1.39… Routerbo_25:f2:3a    Broadcast            802.11     193 Beacon frame, SN=596, FN=0, Flags=...
 41 1.39… Routerbo_25:f2:3a    42:e1:69:6d:2b:e6    802.11      98 Association Response, SN=598, FN=0, F

Frame 38: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface wlan0, id 0
Radiotap Header v0, Length 18
802.11 radio information
IEEE 802.11 Association Request, Flags: ........C
IEEE 802.11 Wireless Management
   Fixed parameters (4 bytes)
      Capabilities Information: 0x0031
      Listen Interval: 0x0001
   Tagged parameters (73 bytes)
      Tag: SSID parameter set: MikroTik114
      Tag: Supported Rates 1(B), 2, 5.5, 11, [Mbit/sec]
      Tag: RSN Information
         Tag Number: RSN Information (48)
         Tag length: 20
         RSN Version: 1
         Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
         Pairwise Cipher Suite Count: 1
         Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
         Auth Key Management (AKM) Suite Count: 1
         Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
         RSN Capabilities: 0x0000
      Tag: Supported Operating Classes
```

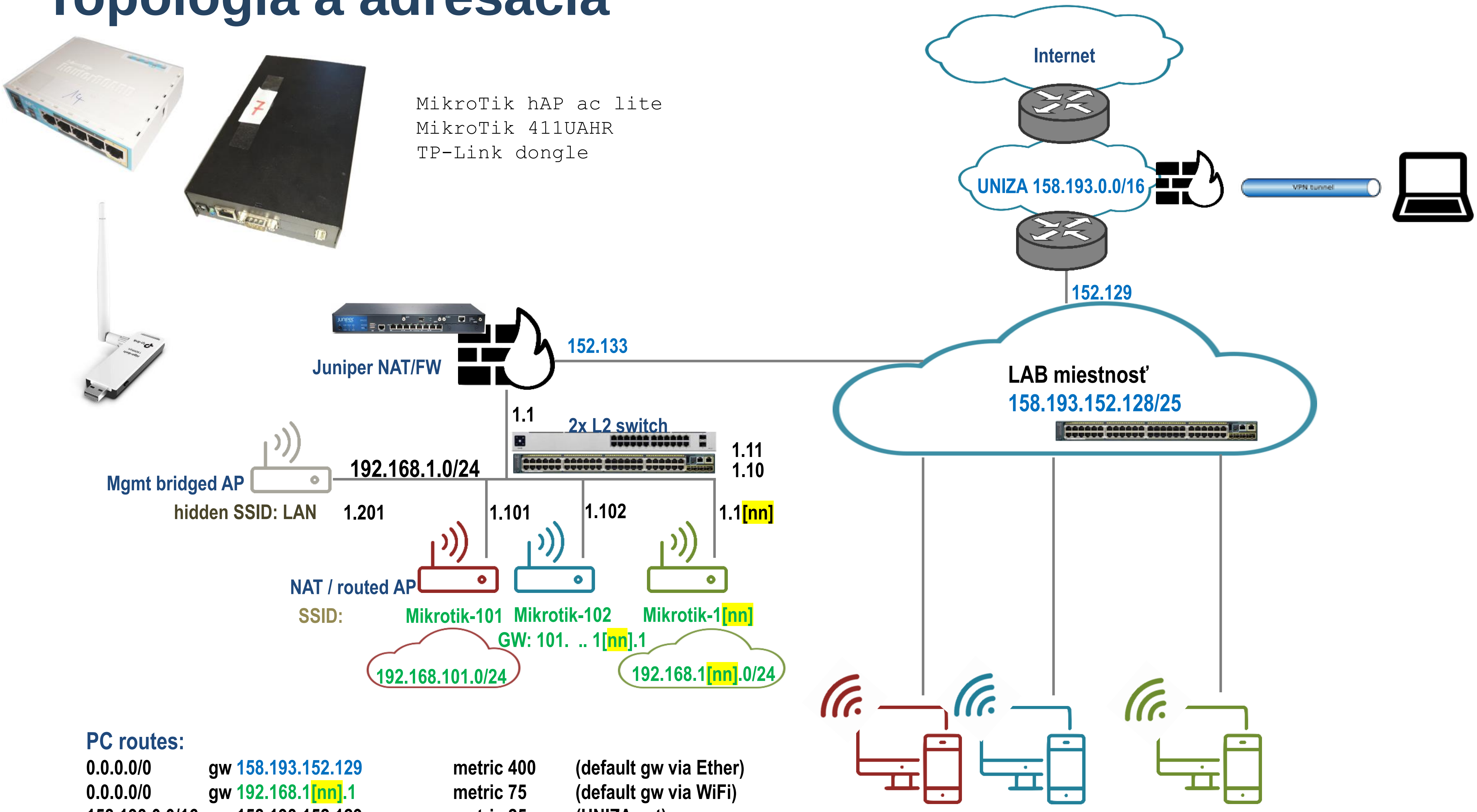
LAB Basic Setup

LAB



Topológia a adresácia

```
MikroTik hAP ac lite
MikroTik 411UAHR
TP-Link dongle
```



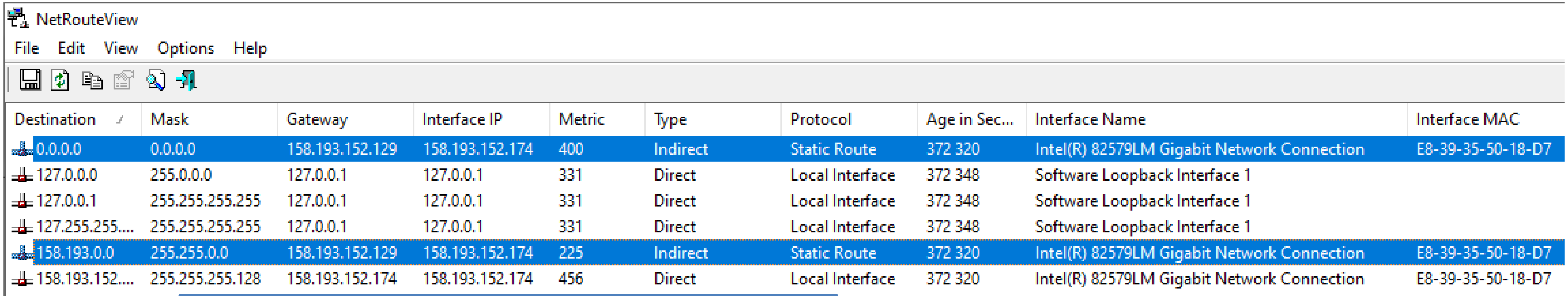
PC routes:

0.0.0.0/0	gw 158.193.152.129	metric 400	(default gw via Ether)
0.0.0.0/0	gw 192.168.1[nn].1	metric 75	(default gw via WiFi)
158.193.0.0/16	gw 158.193.152.129	metric 25	(UNIZA net)

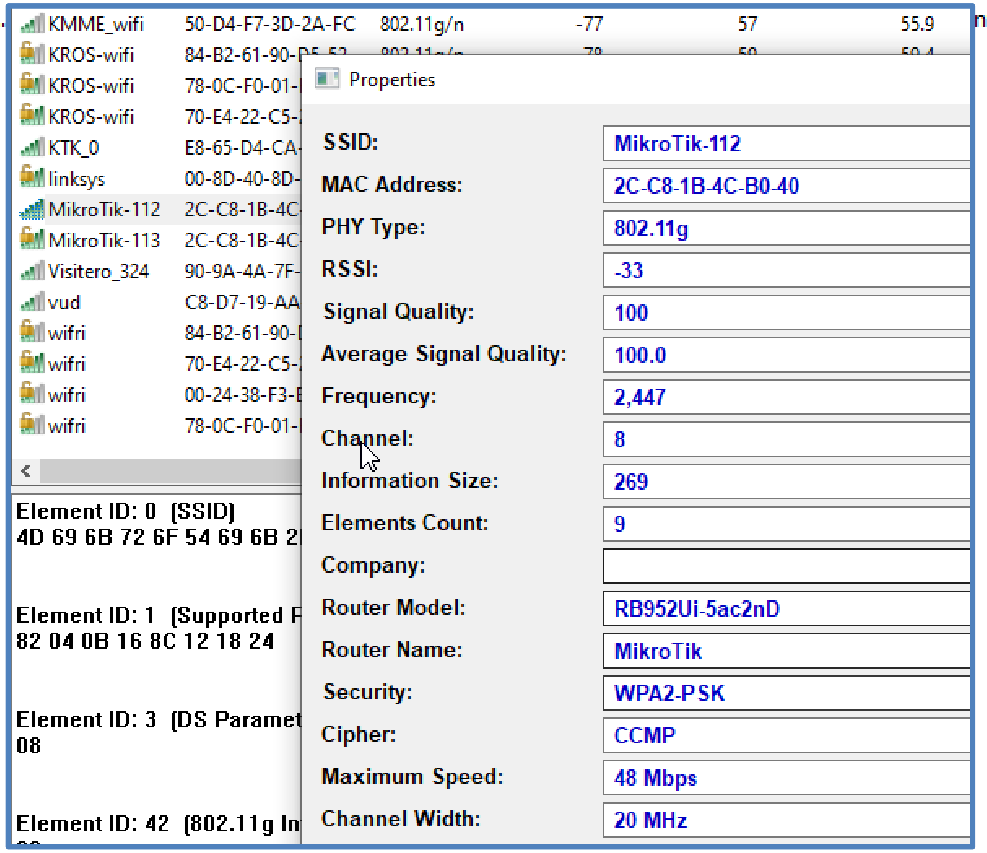
Adresácia a skupiny

Skupina	Model	Meno	S/N	Wlan MAC	Ether MAC	SSID	WPA2 Pre-shared Key	NET	uplink	login	pass
1	411UAHR	Mikrotik 1	24D10199373A	00:0C:42:44:6F:8E	00:0C:42:44:6F:8D	Mikrotik-101	!234567*	192.168.101.1/24	192.168.1.101	admin	k!s143
2	411UAHR	Mikrotik 2	24D1019445AE	00:0C:42:49:1D:1A	00:0C:42:49:1D:19	Mikrotik-102	!234567*	192.168.102.1/24	192.168.1.102	admin	k!s143
3	411UAHR	Mikrotik 3	24D101944462	00:0C:42:49:1C:D6	00:0C:42:49:1C:D5	Mikrotik-103	!234567*	192.168.103.1/24	192.168.1.103	admin	k!s143
4	411UAHR	Mikrotik 4	24D1019445BE	00:0C:42:49:1D:0A	00:0C:42:49:1D:09	Mikrotik-104	!234567*	192.168.104.1/24	192.168.1.104	admin	k!s143
5	411UAHR	Mikrotik 5	24D10199371A	00:0C:42:44:6F:AE	00:0C:42:44:6F:AD	Mikrotik-105	!234567*	192.168.105.1/24	192.168.1.105	admin	k!s143
6	411UAHR	Mikrotik 6	24D1019445B4	00:0C:42:49:1D:04	00:0C:42:49:1D:03	Mikrotik-106	!234567*	192.168.106.1/24	192.168.1.106	admin	k!s143
7	411UAHR	Mikrotik 7	24D10194447C	00:0C:42:49:1C:CC	00:0C:42:49:1C:CB	Mikrotik-107	!234567*	192.168.107.1/24	192.168.1.107	admin	k!s143
8	411UAHR	Mikrotik 8	24D10199372A	00:0C:42:44:6F:9E	00:0C:42:44:6F:9D	Mikrotik-108	!234567*	192.168.108.1/24	192.168.1.108	admin	k!s143
9	411UAHR	Mikrotik 9	24D10194442A	00:0C:42:49:1C:9E	00:0C:42:49:1C:9D	Mikrotik-109	!234567*	192.168.109.1/24	192.168.1.109	admin	k!s143
10	411UAHR	Mikrotik 10	24D101993724	00:0C:42:44:6F:94	00:0C:42:44:6F:93	Mikrotik-110	!234567*	192.168.110.1/24	192.168.1.110	admin	k!s143
11	RB952Ui-5ac2nD	Mikrotik 11	CC3E0EDD4C25	2C:C8:1B:4C:F9:B6	2C:C8:1B:4C:F9:B0	Mikrotik-111	!234567*	192.168.111.1/24	192.168.1.111	admin	k!s143
12	RB952Ui-5ac2nD	Mikrotik 12	CC3E0E60402C	2C:C8:1B:4C:B0:40	2C:C8:1B:4C:B0:3A	Mikrotik-112	!234567*	192.168.112.1/24	192.168.1.112	admin	k!s143
13	RB952Ui-5ac2nD	Mikrotik 13	CC3E0E52B863	2C:C8:1B:4C:D3:E7	2C:C8:1B:4C:D3:E1	Mikrotik-113	!234567*	192.168.113.1/24	192.168.1.113	admin	k!s143
14	RB952Ui-5ac2nD	Mikrotik 14	CC3E0E83DB79	2C:C8:1B:25:F2:3A	2C:C8:1B:25:F2:34	Mikrotik-114	!234567*	192.168.114.1/24	192.168.1.114	admin	k!s143
15	RB952Ui-5ac2nD	Mikrotik 15	CC3E0EC59727	2C:C8:1B:26:04:26	2C:C8:1B:26:04:20	Mikrotik-115	!234567*	192.168.114.1/24	192.168.1.114	admin	k!s143

PC routing table & Wireless Info



Destination	Mask	Gateway	Interface IP	Metric	Type	Protocol	Age in Sec...	Interface Name	Interface MAC
0.0.0.0	0.0.0.0	158.193.152.129	158.193.152.174	400	Indirect	Static Route	372 320	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	331	Direct	Local Interface	372 348	Software Loopback Interface 1	
127.0.0.1	255.255.255.255	127.0.0.1	127.0.0.1	331	Direct	Local Interface	372 348	Software Loopback Interface 1	
127.255.255....	255.255.255.255	127.0.0.1	127.0.0.1	331	Direct	Local Interface	372 348	Software Loopback Interface 1	
158.193.0.0	255.255.0.0	158.193.152.129	158.193.152.174	225	Indirect	Static Route	372 320	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7
158.193.152....	255.255.255.128	158.193.152.174	158.193.152.174	456	Direct	Local Interface	372 320	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7
158.193.152....	255.					nterface	372 320	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7

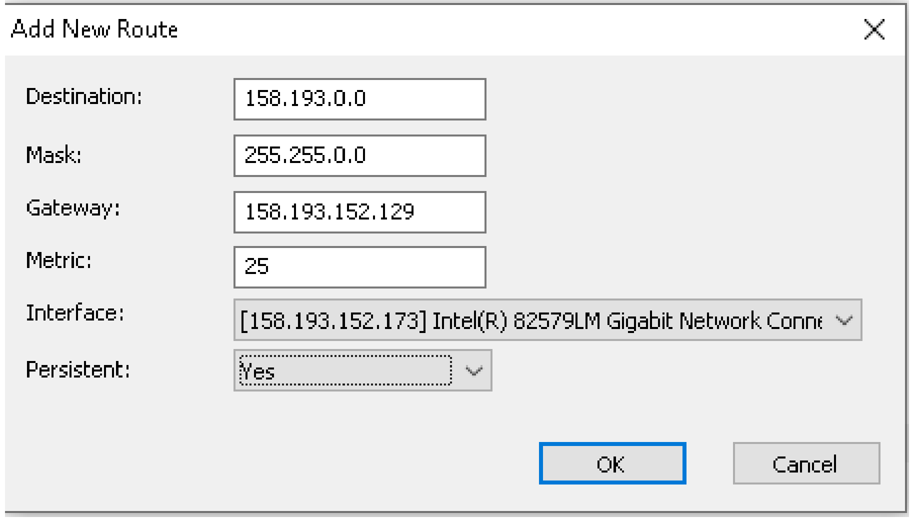


KMME_wifi	50-D4-F7-3D-2A-FC	802.11g/n	-77	57	55.9
KROS-wifi	84-B2-61-90-D5-52	802.11g/n	-78	50	50.4
KROS-wifi	78-0C-F0-01-				
KROS-wifi	70-E4-22-C5-				
KTK_0	E8-65-D4-CA-				
linksys	00-8D-40-8D-				
MikroTik-112	2C-C8-1B-4C				
MikroTik-113	2C-C8-1B-4C				
Visitero_324	90-9A-4A-7F-				
vud	C8-D7-19-AA				
wifri	84-B2-61-90-[				
wifri	70-E4-22-C5-				
wifri	00-24-38-F3-E				
wifri	78-0C-F0-01-				

```
Element ID: 0  (SSID)
4D 69 6B 72 6F 54 69 6B 2

Element ID: 1  (Supported F
82 04 0B 16 8C 12 18 24

Element ID: 3  (DS Paramet
08

Element ID: 42  (802.11g In
```

Properties

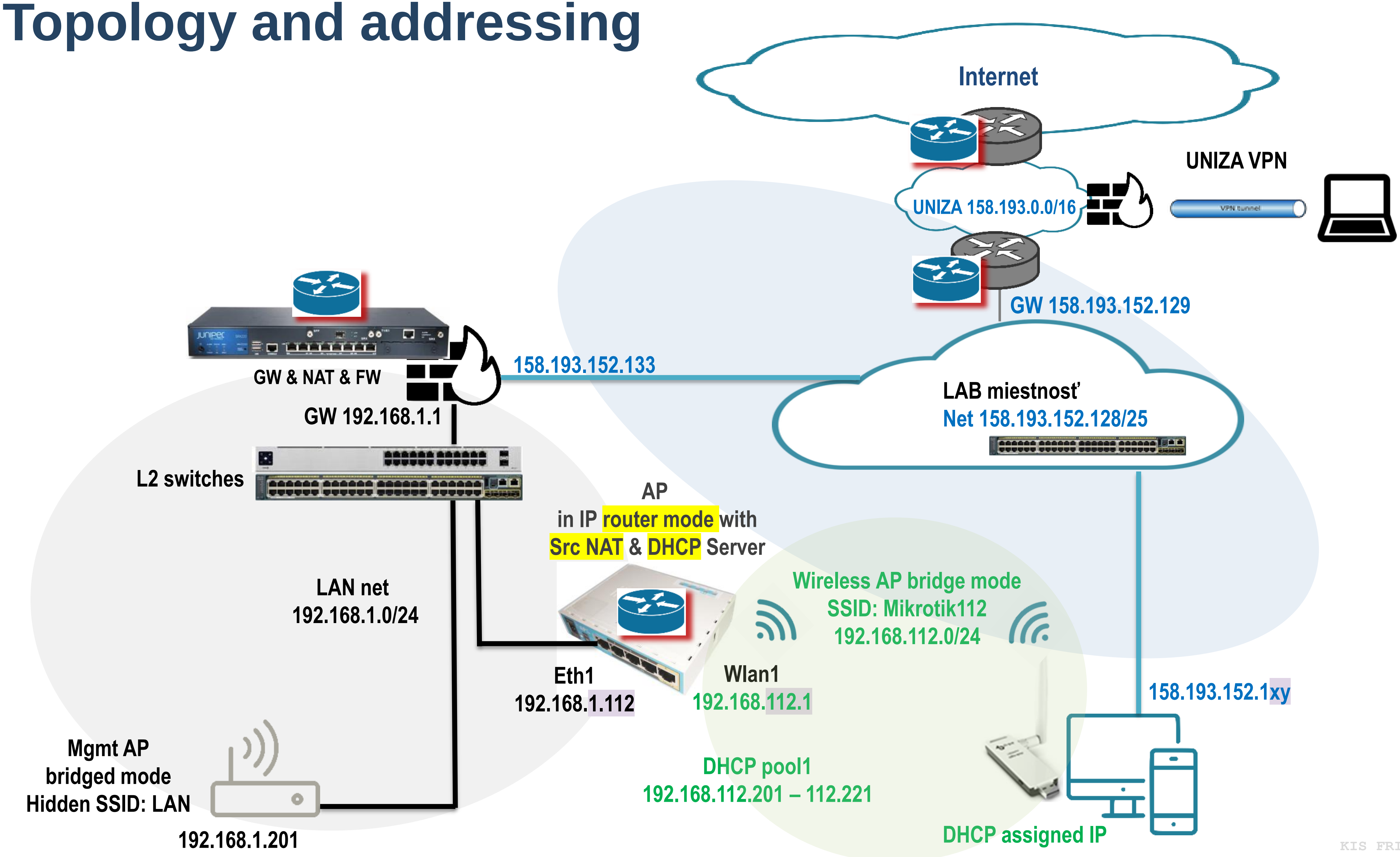
SSID:	MikroTik-112
MAC Address:	2C-C8-1B-4C-B0-40
PHY Type:	802.11g
RSSI:	-33
Signal Quality:	100
Average Signal Quality:	100.0
Frequency:	2,447
Channel:	8
Information Size:	269
Elements Count:	9
Company:	
Router Model:	RB952Ui-5ac2nD
Router Name:	MikroTik
Security:	WPA2-PSK
Cipher:	CCMP
Maximum Speed:	48 Mbps
Channel Width:	20 MHz



Add New Route

Destination:	158.193.0.0
Mask:	255.255.0.0
Gateway:	158.193.152.129
Metric:	25
Interface:	[158.193.152.173] Intel(R) 82579LM Gigabit Network Conne
Persistent:	Yes

Topology and addressing



Internet

UNIZA VPN

UNIZA 158.193.0.0/16

GW 158.193.152.129

158.193.152.133

GW & NAT & FW

GW 192.168.1.1

LAB miestnosť
Net 158.193.152.128/25

L2 switches

AP
in IP router mode with
Src NAT & DHCP Server

LAN net
192.168.1.0/24

Wireless AP bridge mode
SSID: Mikrotik112
192.168.112.0/24

Eth1
192.168.1.112

Wlan1
192.168.112.1

158.193.152.1xy

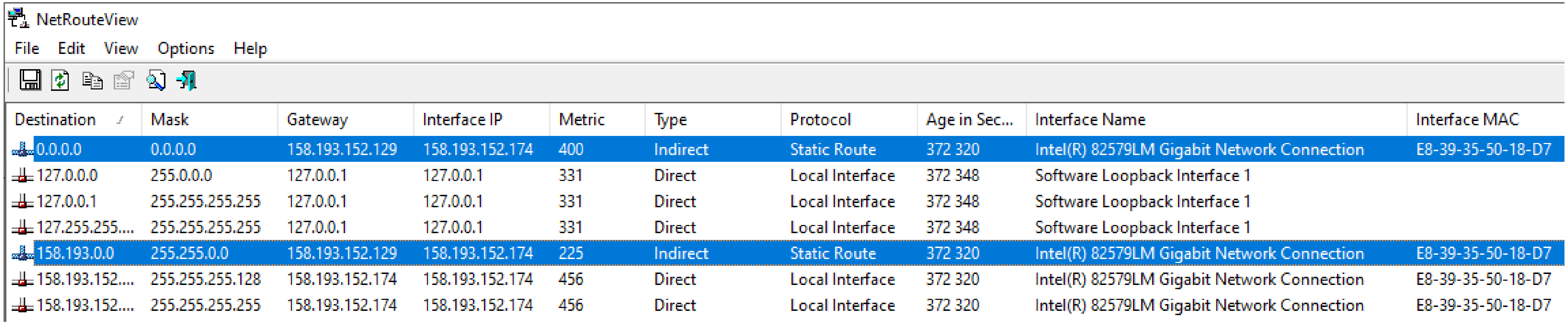
Mgmt AP
bridged mode
Hidden SSID: LAN

192.168.1.201

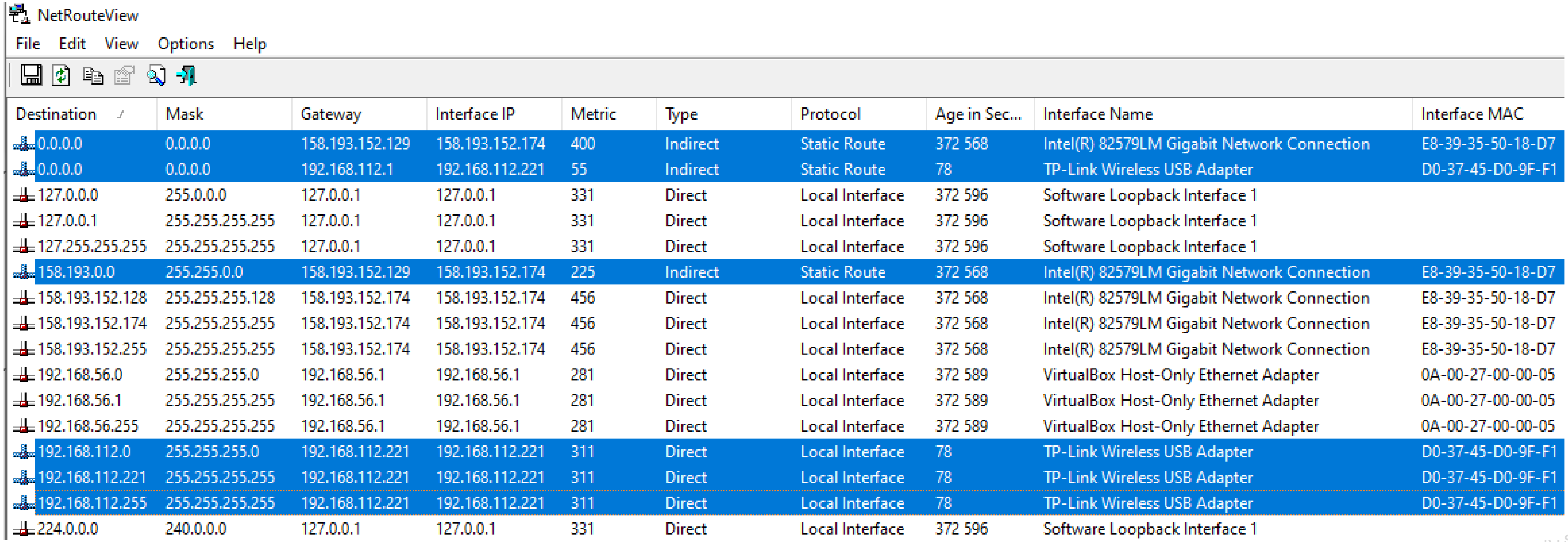
DHCP pool1
192.168.112.201 – 112.221

DHCP assigned IP

PC routing table & Wireless Info



Destination	Mask	Gateway	Interface IP	Metric	Type	Protocol	Age in Sec...	Interface Name	Interface MAC
0.0.0.0	0.0.0.0	158.193.152.129	158.193.152.174	400	Indirect	Static Route	372 320	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	331	Direct	Local Interface	372 348	Software Loopback Interface 1	
127.0.0.1	255.255.255.255	127.0.0.1	127.0.0.1	331	Direct	Local Interface	372 348	Software Loopback Interface 1	
127.255.255....	255.255.255.255	127.0.0.1	127.0.0.1	331	Direct	Local Interface	372 348	Software Loopback Interface 1	
158.193.0.0	255.255.0.0	158.193.152.129	158.193.152.174	225	Indirect	Static Route	372 320	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7
158.193.152....	255.255.255.128	158.193.152.174	158.193.152.174	456	Direct	Local Interface	372 320	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7
158.193.152....	255.255.255.255	158.193.152.174	158.193.152.174	456	Direct	Local Interface	372 320	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7



Destination	Mask	Gateway	Interface IP	Metric	Type	Protocol	Age in Sec...	Interface Name	Interface MAC
0.0.0.0	0.0.0.0	158.193.152.129	158.193.152.174	400	Indirect	Static Route	372 568	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7
0.0.0.0	0.0.0.0	192.168.112.1	192.168.112.221	55	Indirect	Static Route	78	TP-Link Wireless USB Adapter	D0-37-45-D0-9F-F1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	331	Direct	Local Interface	372 596	Software Loopback Interface 1	
127.0.0.1	255.255.255.255	127.0.0.1	127.0.0.1	331	Direct	Local Interface	372 596	Software Loopback Interface 1	
127.255.255.255	255.255.255.255	127.0.0.1	127.0.0.1	331	Direct	Local Interface	372 596	Software Loopback Interface 1	
158.193.0.0	255.255.0.0	158.193.152.129	158.193.152.174	225	Indirect	Static Route	372 568	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7
158.193.152.128	255.255.255.128	158.193.152.174	158.193.152.174	456	Direct	Local Interface	372 568	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7
158.193.152.174	255.255.255.255	158.193.152.174	158.193.152.174	456	Direct	Local Interface	372 568	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7
158.193.152.255	255.255.255.255	158.193.152.174	158.193.152.174	456	Direct	Local Interface	372 568	Intel(R) 82579LM Gigabit Network Connection	E8-39-35-50-18-D7
192.168.56.0	255.255.255.0	192.168.56.1	192.168.56.1	281	Direct	Local Interface	372 589	VirtualBox Host-Only Ethernet Adapter	0A-00-27-00-00-05
192.168.56.1	255.255.255.255	192.168.56.1	192.168.56.1	281	Direct	Local Interface	372 589	VirtualBox Host-Only Ethernet Adapter	0A-00-27-00-00-05
192.168.56.255	255.255.255.255	192.168.56.1	192.168.56.1	281	Direct	Local Interface	372 589	VirtualBox Host-Only Ethernet Adapter	0A-00-27-00-00-05
192.168.112.0	255.255.255.0	192.168.112.221	192.168.112.221	311	Direct	Local Interface	78	TP-Link Wireless USB Adapter	D0-37-45-D0-9F-F1
192.168.112.221	255.255.255.255	192.168.112.221	192.168.112.221	311	Direct	Local Interface	78	TP-Link Wireless USB Adapter	D0-37-45-D0-9F-F1
192.168.112.255	255.255.255.255	192.168.112.221	192.168.112.221	311	Direct	Local Interface	78	TP-Link Wireless USB Adapter	D0-37-45-D0-9F-F1
224.0.0.0	240.0.0.0	127.0.0.1	127.0.0.1	331	Direct	Local Interface	372 596	Software Loopback Interface 1	

Ďakujem za pozornosť.

roman dot kaloc at uniza dot sk

Vytvorené v rámci projektu KEGA 026TUKE-4/2021