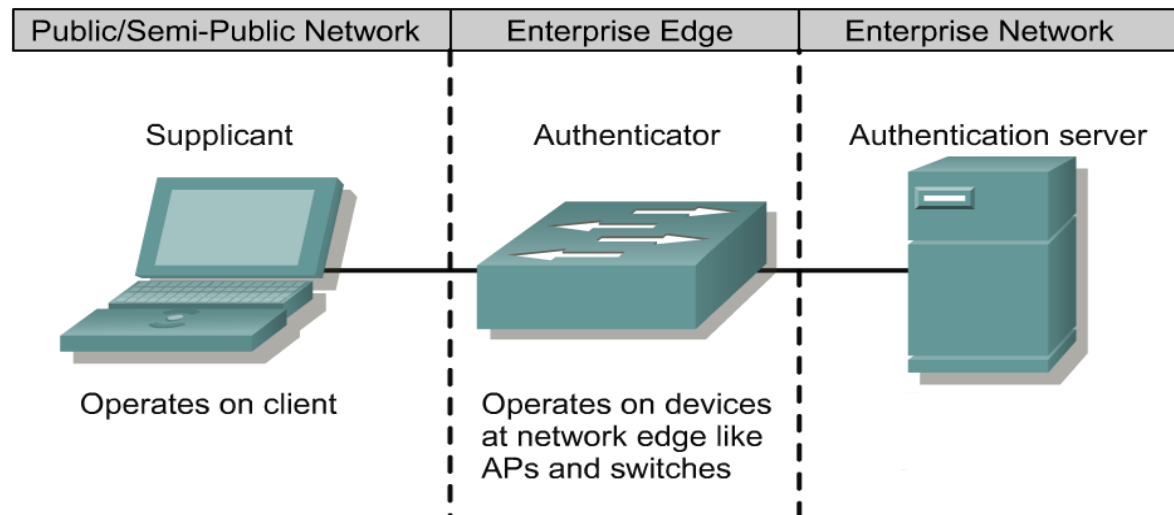# Network Access Control

Segurança em Redes de Comunicações
Mestrado em Cibersegurança
DETI-UA

AAA Architecture

- Enables systematic access security
  - Authentication identifies an user
  - Authorization determines what that user can do
  - Accounting monitors the network usage time for billing purposes
- AAA information is typically stored in an external database or remote authentication server
- Traditional AAA Implementation

Public/Semi-Public Network	Enterprise Edge	Enterprise Network
Supplicant	Authenticator	Authentication server
Operates on client	Operates on devices at network edge like APs and switches	

802.1X

- IEEE 802.1X is an IEEE Standard for Network Access Control (NAC)
  - 802.1X-2001 and 802.1X-2004 only provide authentication.
  - 802.1X-2010 adds optional encryption over the LAN segment.
- It provides an authentication mechanism to devices wishing to attach to a LAN.
- Based on the Extensible Authentication Protocol (EAP).
- AAA protocols/services: TACACS+, RADIUS and DIAMETER.
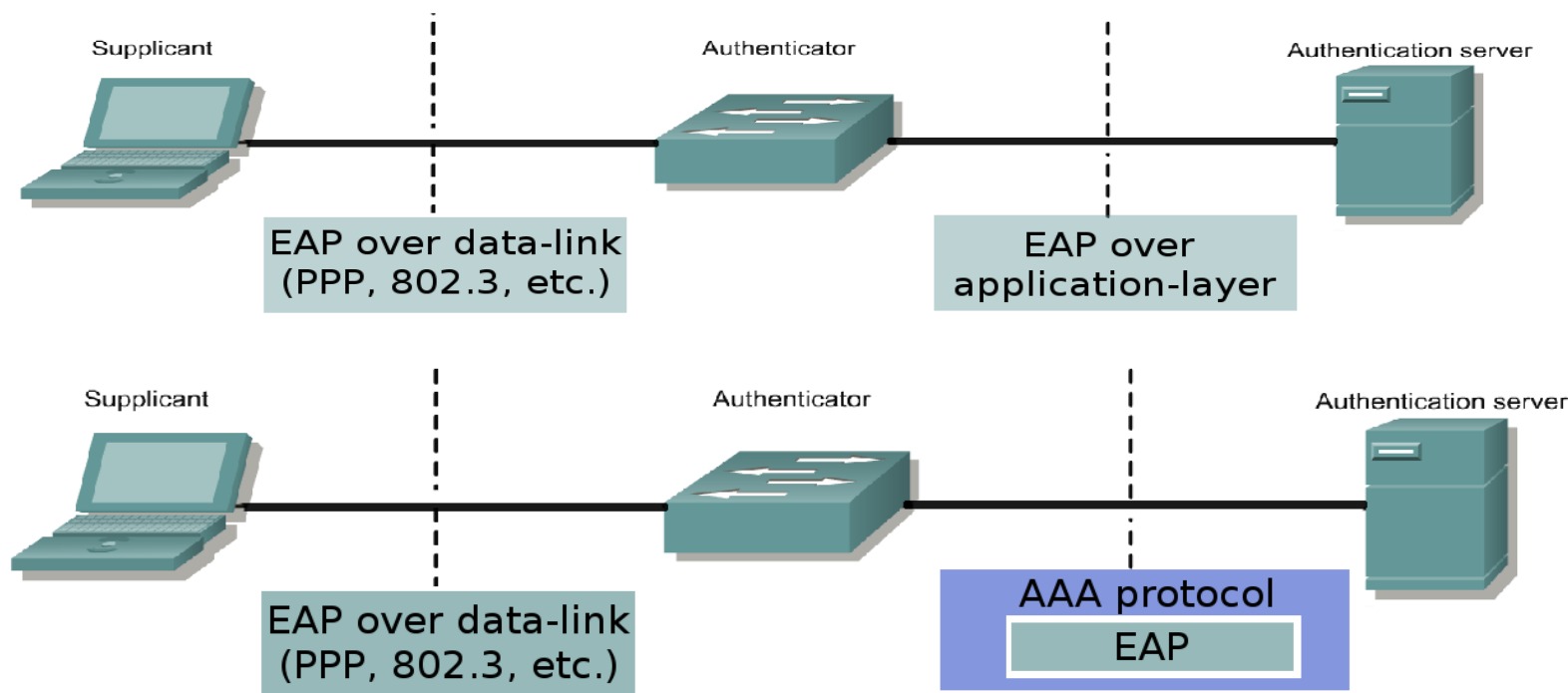
Extensible Authentication Protocol (EAP)

- EAP defined in [RFC3748] was designed to enable extensible authentication for network access in situations in which the Internet Protocol (IP) protocol is not available.
  - Originally developed for use with Point-to-Point Protocol (PPP) [RFC1661]
  - Subsequently also been applied to IEEE 802 wired networks [IEEE-802.1X], Internet Key Exchange Protocol version 2 (IKEv2)[RFC4306], and wireless networks such as [IEEE-802.11] and [IEEE-802.16e].
- EAP is a two-party protocol spoken between the EAP peer and server.
  - Keying material is generated by EAP authentication algorithms, known as "methods".
  - Part of this keying material can be used by EAP methods themselves, and part of this material can be exported.

universidade de aveiro

EAP Overview (1)

- Where EAP key derivation is supported, the conversation typically takes place in three phases:
- Phase 0: Discovery
- Phase 1: Authentication
  - 1a: EAP authentication
  - 1b: AAA Key Transport (optional)
- Phase 2: Secure Association Protocol
  - 2a: Unicast Secure Association
  - 2b: Multicast Secure Association (optional)

universidade de aveiro

EAP Overview (2)

- EAP lower layers implement phase 0, 2a, and 2b in different ways:
  - IEEE 802.1X
    - IEEE 802.1X-2004 does not support discovery (phase 0), nor does it provide for derivation of unicast or multicast secure associations (phase 2).
  - IEEE 802.11
    - Handles discovery via the Beacon and Probe Request/Response mechanisms.
    - Access Points (APs) periodically announce their Service Set Identifiers (SSIDs) as well as capabilities using Beacon frames.
    - Stations can query for APs by sending a Probe Request.
      - Neither Beacon nor Probe Request/Response frames are secured.
    - A 4-way handshake enables the derivation of unicast (phase 2a) and multicast/broadcast (phase 2b) secure associations.

universidade de aveiro

TACACS+

- Terminal Access Controller Access Control System Plus

- Forwards username and password information to a centralized security server

- Centralized server can be either a TACACS database or a database like the UNIX password le with TACACS support

- Features
  - Separates all AAA functionalities
  - Uses TCP
  - Bidirectional authentication
  - All packet is encrypted
  - Limited accounting customization

universidade de aveiro

RADIUS

- Remote Authentication Dial-In User Service
- The network access device operates as a client of RADIUS
- RADIUS servers are responsible for
  - Receiving user connection requests
  - Authenticating the user
  - Return all configuration information necessary for the client to deliver service to the user
- Transactions between the client and RADIUS server are authenticated using a shared secret
- Supports a variety of methods to authenticate a user
  - PAP, CHAP, or MS-CHAP, UNIX login, and other authentication mechanisms
- Combines Authentication and Authorization. Separates Accounting (less flexible than TACACS+)
- Uses UDP (less robust)
- Unidirectional authentication
- Only encrypts the password (less secure)
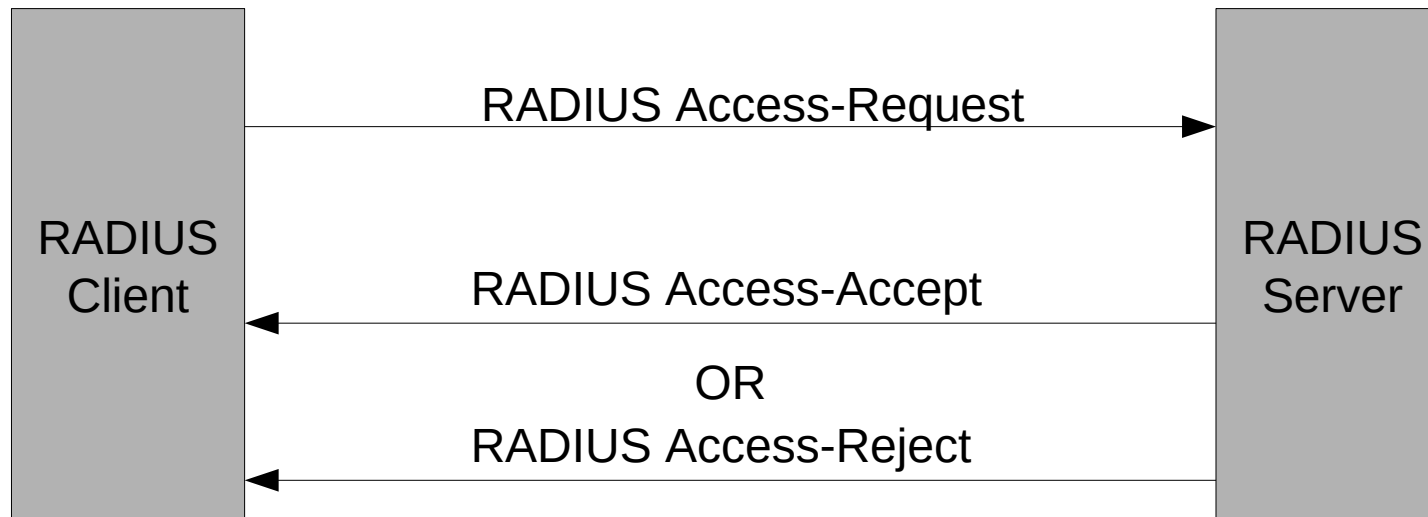- RADIUS accounting can hold more information

universidade de aveiro

RADIUS Packet

Code (1 byte)	Identifier (1 byte)	Length (2 bytes)
Authenticator (16 bytes)		
Attributes		

- Code - Identifies the type of RADIUS packet
  - (1) Access-Request, (2) Access-Accept, (3) Access-Reject, (4) Accounting-Request, (5) Accounting-Response and (11) Access-Challenge
- Identifier - Allows the RADIUS client to match a RADIUS response with the correct pending request (usually is implemented as a counter)
- Authenticator
  - In client Requests – Random value
  - In server Responses - MD5 Hash function of (Code,ID,Length,Request Auth,Attributes,Shared Secret)
- Attributes - Section where an arbitrary number of attribute fields can be sent (e.g. User-Name and User-Password attributes)

universidade de aveiro

RADIUS Protocol (1)

Example - RADIUS exchange involving just a username and user password:

```
┌──────────┐                                              ┌──────────┐
│          │        RADIUS Access-Request       ────────▶ │          │
│          │                                              │          │
│  RADIUS  │                                              │  RADIUS  │
│  Client  │ ◀──────  RADIUS Access-Accept                │  Server  │
│          │                                              │          │
│          │                    OR                        │          │
│          │               RADIUS Access-Reject           │          │
│          │ ◀──────────                                  │          │
└──────────┘                                              └──────────┘
```

- Only password is encrypted
  - The shared secret followed by the Request Authenticator is put through an MD5 hash to create a 16 octet value which is XORed with the password entered by the user
  - If the user password is greater than 16 octets, the password is broken into 16-octet blocks and additional MD5 calculations are performed

RADIUS Protocol (2)

- The RADIUS protocol has a set of vulnerabilities
  - The Access-Request packet is not authenticated at all.
  - Many client implementations do not create Request Authenticators that are sufficiently random.
  - Many administrators choose RADIUS shared secrets with insufficient information entropy and many implementations limit the shared secret key space.

universidade de aveiro

DIAMETER

- DIAMETER is a newest framework in IETF for the next-generation AAA server

- Provides an AAA framework for Mobile-IP

- Does not use the same RADIUS protocol data unit, but is backward compatible with RADIUS to ease migration

- Bidirectional authentication

- It uses UDP but has a scheme that regulates the flow of packets

- Challenge/response attributes can be secured using end-to-end encryption and authentication

- Supports end-to-end security

universidade de aveiro

802.1X - Ethernet vs. WiFi
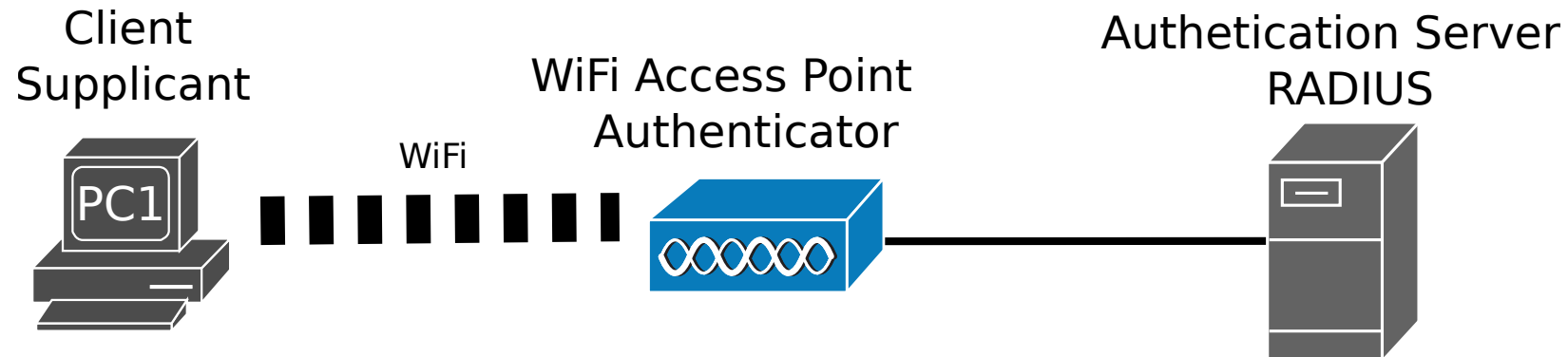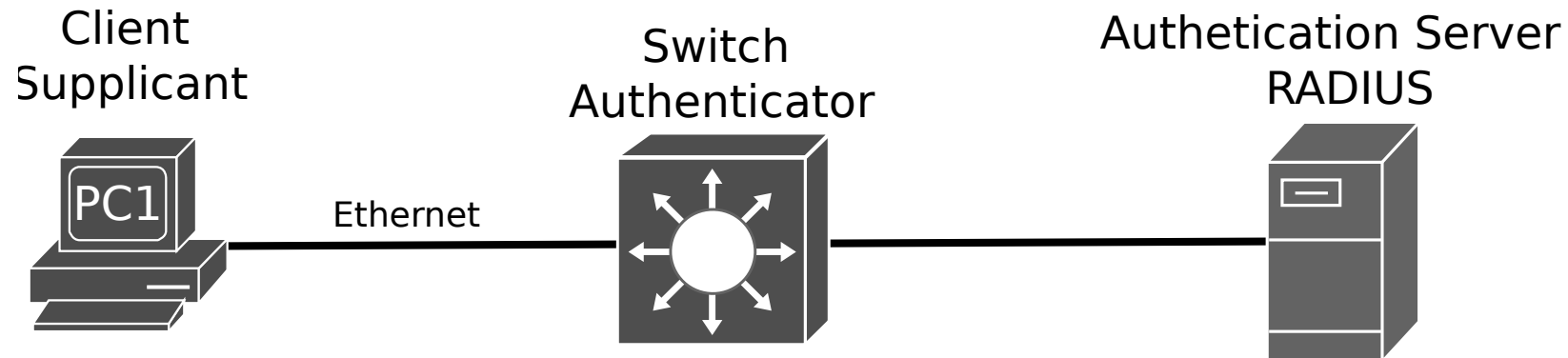
Ethernet - EAP and RADIUS

```
11.564981  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d              EAP      60 Request, Identity
11.565227  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge EAP    60 Response, Identity
11.585255  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d              EAP      60 Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
11.585554  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge EAP    60 Response, Legacy Nak (Response Only)
11.605541  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d              EAP      60 Request, Protected EAP (EAP-PEAP)
11.606107  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge TLSv1  221 Client Hello
11.625805  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d              EAP    1022 Request, Protected EAP (EAP-PEAP)
11.626628  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge EAP    60 Response, Protected EAP (EAP-PEAP)
11.646176  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d              TLSv1  212 Server Hello, Certificate, Server Key Exchange, Server Hello Don
11.649978  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge TLSv1  162 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mes
11.666300  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d              TLSv1   83 Change Cipher Spec, Encrypted Handshake Message
11.666636  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge EAP    60 Response, Protected EAP (EAP-PEAP)
11.686625  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d              TLSv1   61 Application Data
11.686915  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge TLSv1   98 Application Data, Application Data
11.706925  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d              TLSv1   93 Application Data
11.708108  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge TLSv1  162 Application Data, Application Data
11.727323  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d              TLSv1  109 Application Data
11.728248  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge TLSv1   98 Application Data, Application Data
11.747691  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d              TLSv1   61 Application Data
11.748540  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge TLSv1   98 Application Data, Application Data
11.768072  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d              EAP      60 Success
```

```
0.000000    10.0.0.1      10.0.0.100    RADIUS     154 Access-Request id=1
0.000594    10.0.0.100    10.0.0.1      RADIUS     122 Access-Challenge id=1
0.020271    10.0.0.1      10.0.0.100    RADIUS     165 Access-Request id=2
0.020944    10.0.0.100    10.0.0.1      RADIUS     106 Access-Challenge id=2
0.040451    10.0.0.1      10.0.0.100    RADIUS     362 Access-Request id=3
0.049097    10.0.0.100    10.0.0.1      RADIUS    1110 Access-Challenge id=3
0.060742    10.0.0.1      10.0.0.100    RADIUS     165 Access-Request id=4
0.062137    10.0.0.100    10.0.0.1      RADIUS     294 Access-Challenge id=4
0.081103    10.0.0.1      10.0.0.100    RADIUS     303 Access-Request id=5
0.081845    10.0.0.100    10.0.0.1      RADIUS     165 Access-Challenge id=5
0.101366    10.0.0.1      10.0.0.100    RADIUS     165 Access-Request id=6
0.101883    10.0.0.100    10.0.0.1      RADIUS     143 Access-Challenge id=6
0.121651    10.0.0.1      10.0.0.100    RADIUS     239 Access-Request id=7
0.122255    10.0.0.100    10.0.0.1      RADIUS     175 Access-Challenge id=7
0.141930    10.0.0.1      10.0.0.100    RADIUS     303 Access-Request id=8
0.143019    10.0.0.100    10.0.0.1      RADIUS     191 Access-Challenge id=8
0.162277    10.0.0.1      10.0.0.100    RADIUS     239 Access-Request id=9
0.163695    10.0.0.100    10.0.0.1      RADIUS     143 Access-Challenge id=9
0.182642    10.0.0.1      10.0.0.100    RADIUS     239 Access-Request id=10
0.184255    10.0.0.100    10.0.0.1      RADIUS     212 Access-Accept id=10
```

universidade de aveiro

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)
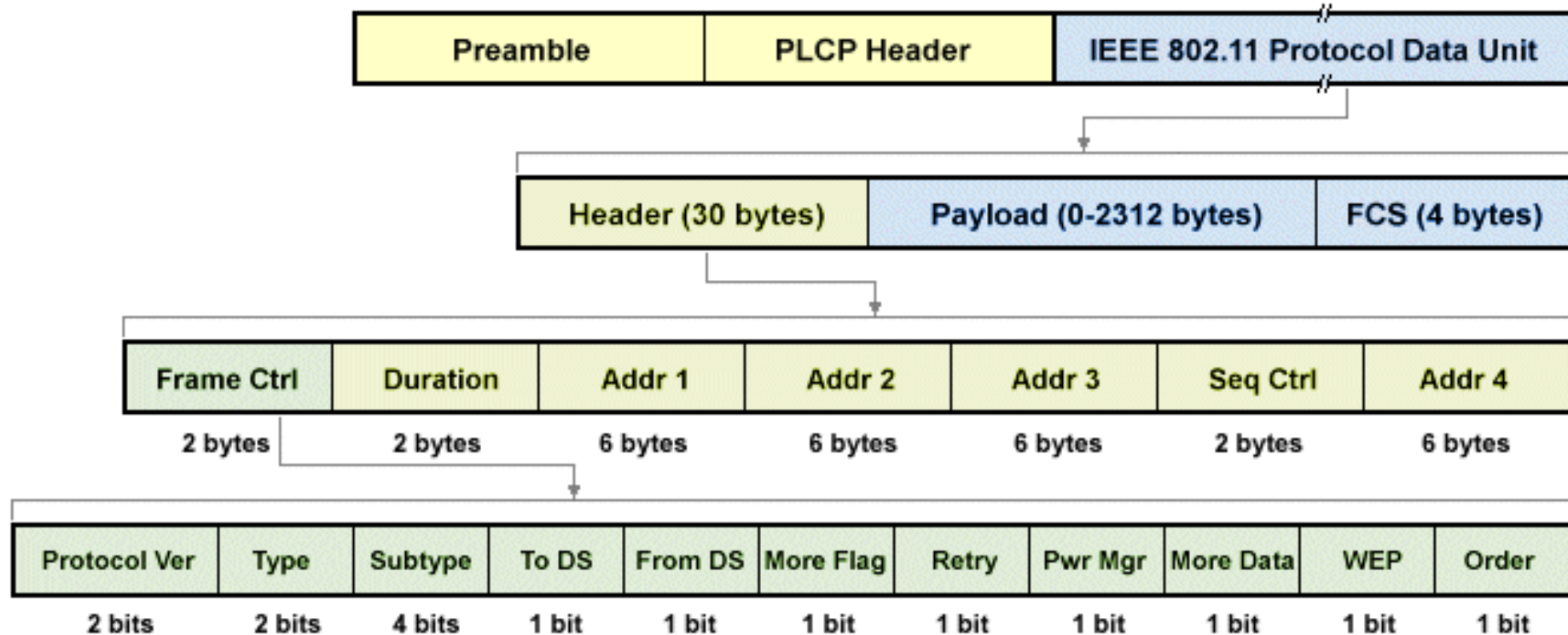
Joining a BSS

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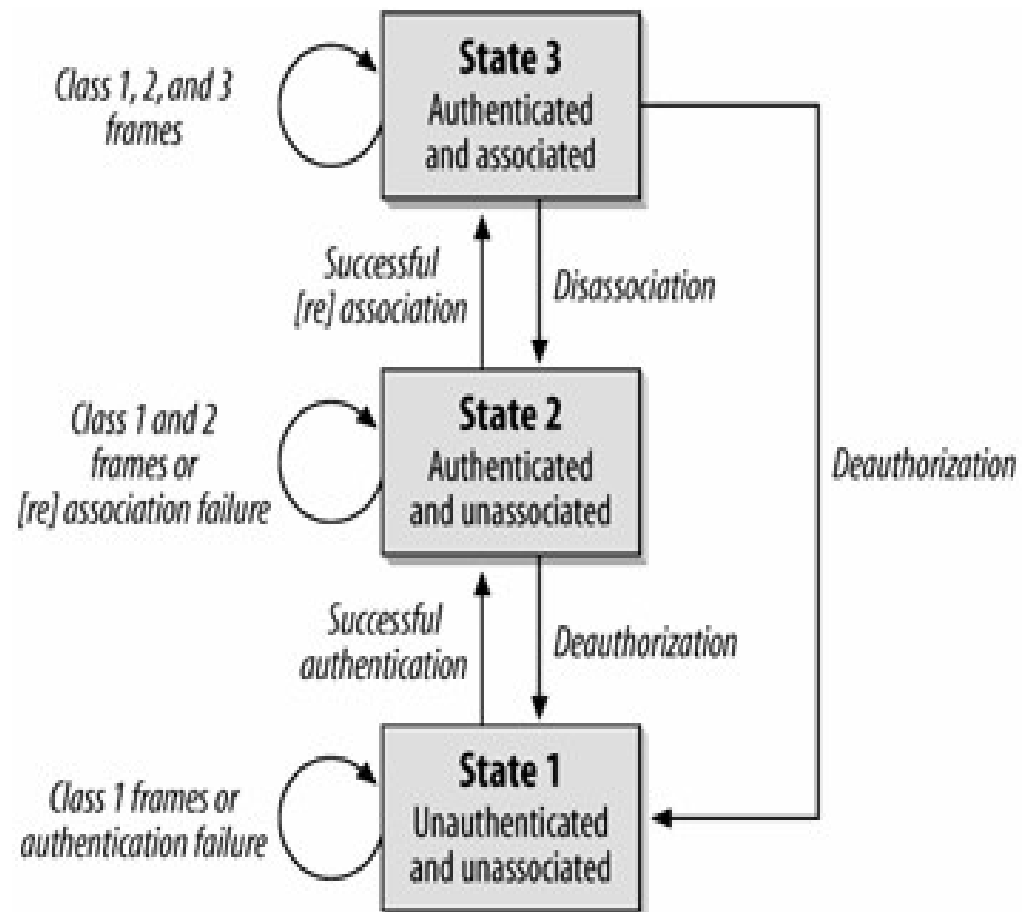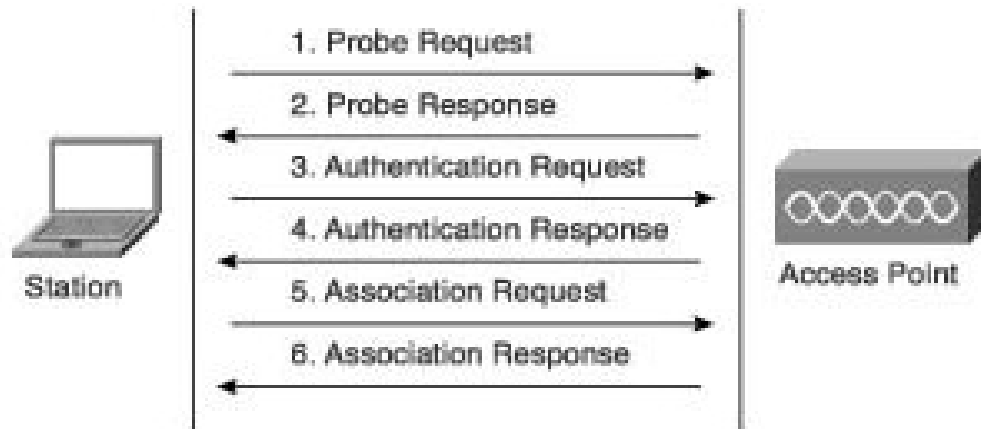
WLAN Frames

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

Preamble	PLCP Header	IEEE 802.11 Protocol Data Unit

Header (30 bytes)	Payload (0-2312 bytes)	FCS (4 bytes)

Frame Ctrl	Duration	Addr 1	Addr 2	Addr 3	Seq Ctrl	Addr 4
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes

Protocol Ver	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgr	More Data	WEP	Order
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

universidade de aveiro

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
```

universidade de aveiro

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
```

universidade de aveiro

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.

universidade de aveiro

Association Request/Response Frames

```
▾ IEEE 802.11 Association Request, Flags: ........                    ← From Station
    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
```

```
                                       ▾ 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
                       From AP →        ▾ 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)           ← Node that will receive frame (AP)
    Transmitter address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)     ← Node that send 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*").

universidade de aveiro

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

WPA* Key Exchange (EAP phase 2)

- Done during the Association process.
  - After Association Request/response frames.
  - Uses (QoS) Data 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
```