TÉCNICO LISBOA

Wi-Fi security

Segurança Informática em Redes e Sistemas
2024/25

Ricardo Chaves, David R. Matos

Ack: Carlos Ribeiro, André Zúquete,
Miguel Pardal, Miguel P. Correia

Secure communication: Data Link layer and below

Layers		Responsibility	Approach	Solutions
	Transaction	Local data manipulation applications	End-to-end security	PGP, PEM, S/MIME
OSI Layers	Application	Applications for remote data exchange		HTTPS, IMAPS SSH
	Presentation			
	Session			
	Transport	Operating Systems		TLS
	Network			IPsec
	Link	Devices	Link security	IEEE 802.11*
	Physical			

Roadmap

- Wireless networks
- Wi-Fi / WLANs
  - WEP
  - WPA
  - 802.1X and EAP

Roadmap

- **Wireless networks**
- Wi-Fi / WLANs
  - WEP
  - WPA
  - 802.1X and EAP

Wireless network challenges

- Inexistence of a controlled physical connection
- Worsens the problems of:
  - **Eavesdropping** of data exchanged
    - Breaking *confidentiality*
  - **Impersonation** of machines
    - Breaking *authenticity*

Wireless communication protocols

- Mobile phones
  - GSM
  - GPRS
  - UMTS
- Wireless home phones
  - DECT
- **Data networks**
  - Bluetooth (IEEE 802.15)
  - **Wi-Fi (IEEE 802.11*)**
    - **where * = a, b, g, n, …**
    - **standard for WLAN (Wireless Local Area Networks)**

Roadmap

- Wireless networks
- **Wi-Fi / WLANs**
  - WEP
  - WPA
  - 802.1X and EAP

IEEE 802.11* Architecture

- **Station (STA)**  
  - Device capable of connecting itself to a wireless network
  - Each station has an identifier
    - Media Access Control (MAC) address
- **Access Point (AP)** 
  - Device that allows the interconnection between a wireless network and other equipment or networks
- **Wireless network**
  - Network composed of stations (STA) and access points (APs) that communicate through **radio signals**

New Wi-Fi version names

- New versioning scheme, with sequential numbers
  - To replace the old, confusing standard names with letters, like “802.11ac”
- Wi-Fi versions
  - Wi-Fi 1 would have been 802.11b, released in 1999
  - Wi-Fi 2 would have been 802.11a, also released in 1999
  - Wi-Fi 3 would have been 802.11g, released in 2003
  - Wi-Fi 4 is 802.11n, released in 2009
  - Wi-Fi 5 is 802.11ac, released in 2014
  - Wi-Fi 6 is the new version, also known as 802.11ax. It was released in 2019
  - Wi-Fi 7 expected in 2025…

Wi-Fi security

- 1999
  - WEP – Wired-Equivalent Privacy
- 2003
  - WPA – Wi-Fi Protected Access
- 2004
  - **WPA2 (802.11i)**
- 2018
  - WPA3

IEEE 802.11* Security

- Initial very basic mechanisms and protocols
  - *Service Set Identifier* (SSID)
  - *MAC Address Filtering*
  - *Wired Equivalent Privacy* (WEP)
- Enterprise/campus authentication: 802.1X
  - *Enhanced Authentication Protocol* (EAP)
  - *Protected* EAP (PEAP)

IEEE 802.11*
SSID (Service Set IDentifier)

- **SSID** = identifier/name of a wireless LAN
  - Used by the AP to restrict access of stations
  - Stations have to know and use the SSID of the AP that they are connected to
- Works like a *weak* password
  - Everyone knows it
  - It is exchanged in plaintext in each message
  - The AP announces it

CARLOS_5G_EXT
CARLOS_EXT
DIRECT-90-HP ENVY 5640
DIRECT-tFE0443180msDY
MEO
MEO-10F49A
MEO-39E593 5GHz
MEO-A10B05
MEO-B8A8F0
MEO-B8A8F1-5G
MEO-WiFi
NOS-3610
NOS-5B53
NOS_Wi-Fi_Hotspots
SMC
Thomson724D8F
Vodafone-D36C04
ZON Repeater
ZON-5010
ZON-E490

IEEE 802.11*
MAC Address Filtering

- Each Station has a distinct **MAC**
  - The idea was to be fixed but today can be changed
- Each AP is able to restrict the access of a Station according to their MAC, but:
  - MAC is transmitted in clear text and can be eavesdropped
  - MAC can be spoofed by an attacker

Roadmap

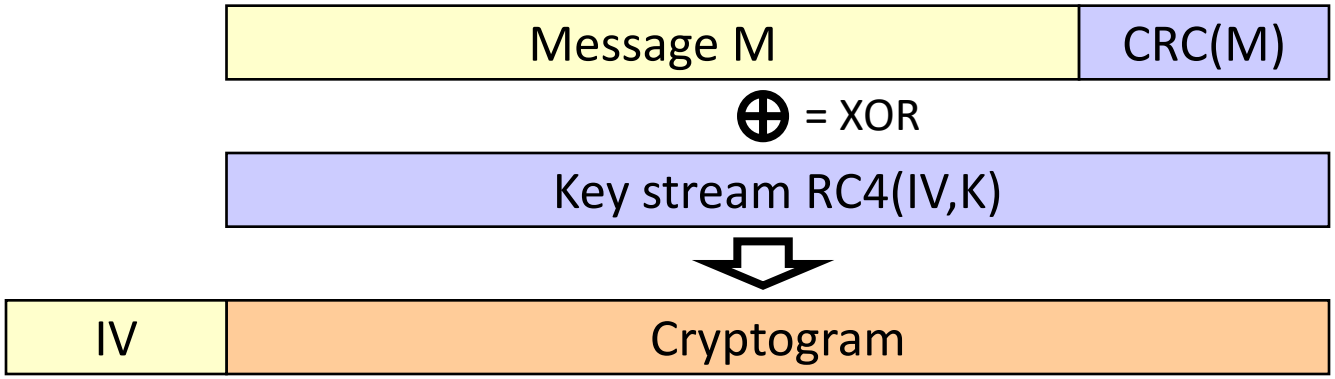
- Secure channels *versus* communication layers
- Wireless networks
- Wi-Fi / WLANs
  - **WEP**
  - WPA
  - 802.1X and EAP

IEEE 802.11*: WEP (*Wired Equivalent Privacy*)

- Goal
  - Protection of radio communications between stations and APs
  - Confidentiality and integrity control
- Usage
  - Uses **shared symmetric keys** of 40 or 104 bits
    - Defined by administrator and shared between stations
  - Manual distribution of keys
  - Uses a **stream cipher**: the RC4 algorithm

WEP message security

- **Integrity and Confidentiality**
  - Every message takes a CRC (Cyclic Redundant Check) value
  - and is encrypted using RC4 (stream cipher)



WEP problems (1/3)

- The **AP** is not authenticated
- Excessive use of the **shared key**
  - No key redistribution
- No control over the variation of the **IV**
  - Which allows ad-hoc repetition of ciphered messages previously sent, modified, or new messages
- It is possible to repeat the same **keystream**

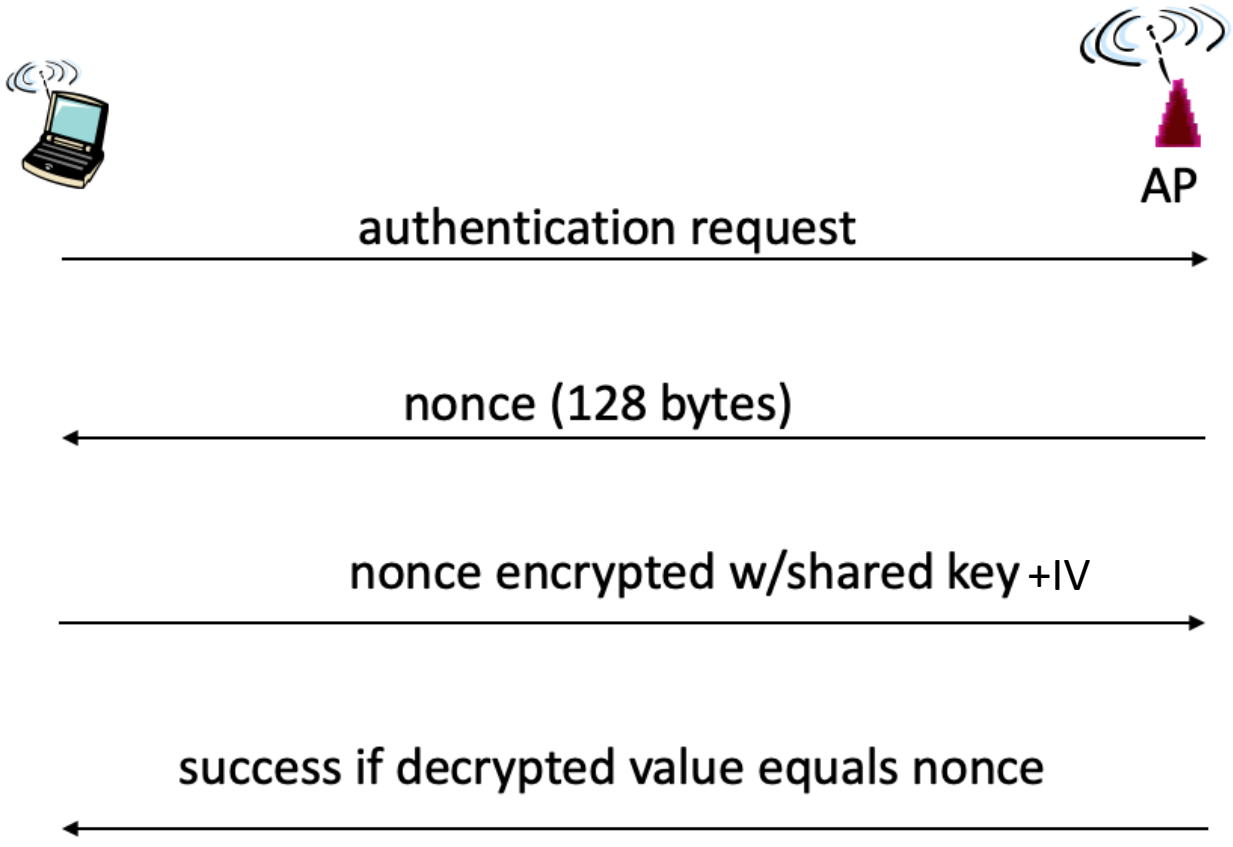
WEP problems (2/3)

- Repetition of **IVs** for the same SSID and the same Key
  - Same IV and Key $\Rightarrow$ same keystream
  - XORing 2 cryptograms obtained with the same keystream, one obtains the XOR of the two messages and their CRC
    - C1 = M1 xor keystream(IV,K)
    - C2 = M2 xor keystream(IV,K)
    - C1 xor C2 = (M1 xor keystream(IV,K)) xor (M2 xor keystream(IV,K)) = M1 xor M2
  - IV has only 24 bits and sometimes is poorly managed
    - Constant (IEEE 802.11 standard states that IV update is optional)
    - 0 on reset (in some equipments)

WEP problems (3/3)

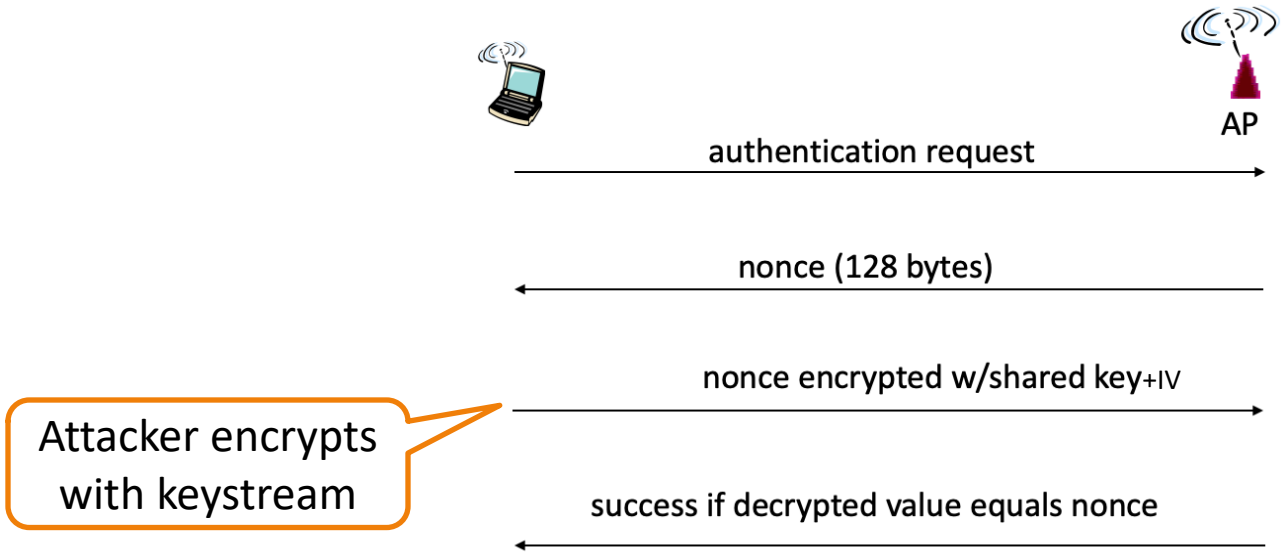
- **Integrity control** is weak
  - CRC-32 (Cyclic Redundancy Check) is a linear function
  - Changing n^{th} bit of cryptogram,
    changes same n^{th} bit in message,
    does a deterministic change of some bits of the CRC
    - Thus, the deciphered CRC can be tampered with by inverting the corresponding CRC bits in the cryptogram

WEP authentication



WEP authentication attacks

- **Authenticating** with the same keystream
  - AP sends message with **nonce** (M) in plaintext to good station
  - Good station ciphers **nonce** and sends it back in cryptogram C
  - Attacker observes C and M, so it can obtain 128 bytes of the keystream for a given **IV**: C = M xor keystream(IV,K)
  - Attacker sends authentication request and uses the keystream 128 bytes (without knowing K) to encrypt the **nonce**



Roadmap

- Secure channels vs communication layers
- Wireless networks
- Wi-Fi / WLANs
  - WEP
  - **WPA**
  - 802.1X and EAP

WPA (*Wi-Fi Protected Access*)

Improvements over WEP:

- **Master key** has 128 bits and is never used to cipher data; **temporary keys** are derived from this master key (TKIP protocol)
- The size of the **IV** is increased to 48 bits
- Each packet is protected with a different key
- **IV** is used as a packet counter: **TSC** (TKIP Sequence Counter)
  - For each new (temporary) integrity key, TSC is reset
  - Out of order TSCs are discarded to prevent replay attacks
- CRC-32 (linear) is 'replaced' by **MIC**hael, a **Message Integrity Code**
  - Computed over the entire unencrypted data in the frame and the source and destination MAC addresses
  - If two wrong MICs are sent within 60s, the key is renewed, to prevent trial-and-error attacks

TKIP (*Temporal Key Integrity Protocol*)

- RC4 stream cipher algorithm
  - Master key is subject to an initial key mixing with the IV of 48 bits
- MIC (Message Integrity Control) in every message
  - 64-bit message integrity check value
- Improved management of dynamic keys
  - **PMK** – Pairwise Master Key (generated by 802.1X)
  - **PTK** – Pairwise Transient Key
    - **PTK** = PRF-512(PMK, “Pairwise key expansion”, ST_MAC, AP_MAC, SNonce, ANonce)
    - ST_MAC, AP_MAC – station and AP MAC addresses
    - Nonce = PRF-256(random, “Init Counter”, MAC, Time)
    - Ensures that every data packet is sent with a unique encryption key

WPA problems

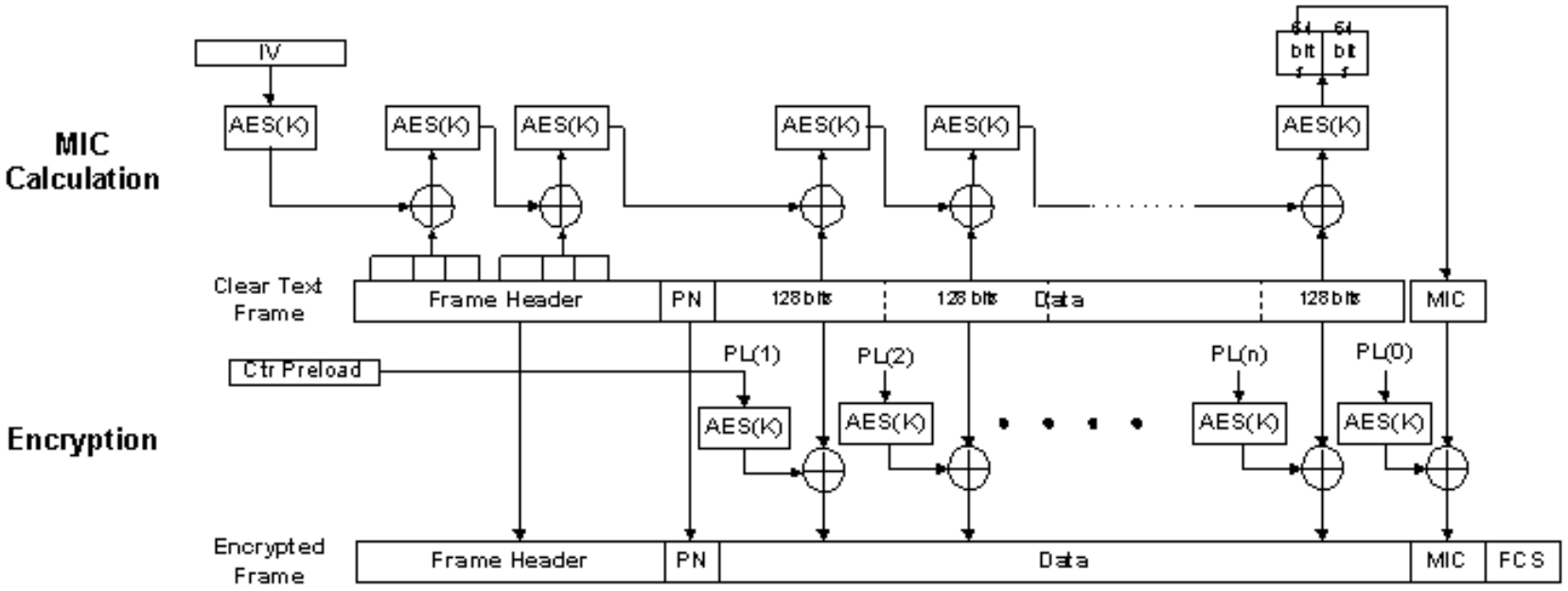
- MIC does not protect the full packet
- In some cases, the same keystream is reused

- WPA was just a *draft* of the IEEE 802.11i standard, known as WPA2
  - Compatible with the same hardware devices as WEP

IEEE 802.11i *a.k.a.* WPA2

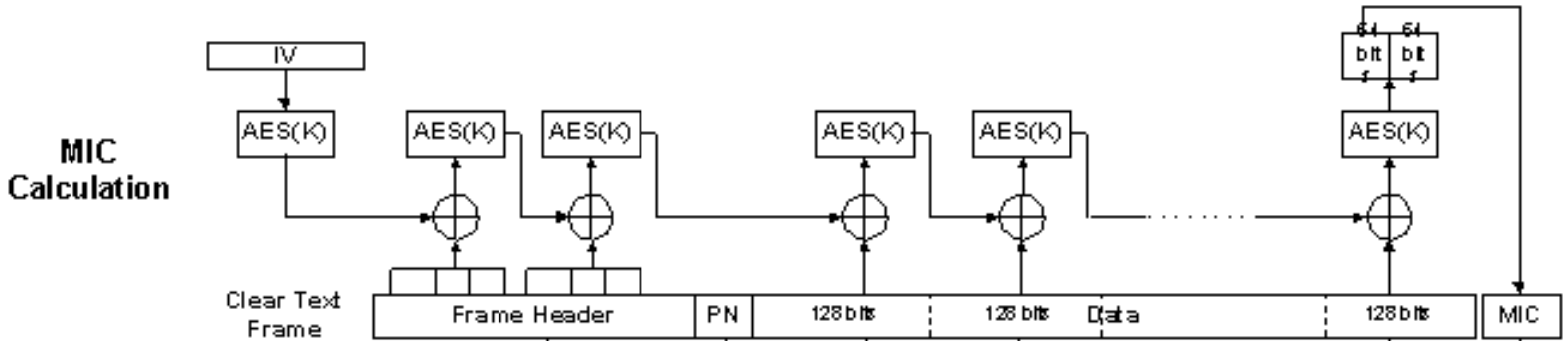
- 802.11i = WPA2 = WPA + AES-CCMP
- WPA – Wi-Fi Protected Access
  - TKIP – Temporal Key Integrity Protocol
  - WPA-Personal / WPA-PSK – uses a pre-shared key
  - WPA-Enterprise / WPA-802.1X - uses **802.1X** with all authentication methods seen above
- AES-CCMP – AES, CTR, CBC-MAC
  - Advanced Encryption Standard (AES) in Counter mode (CTR)
  - CBC-MAC – MAC function based on block cipher (AES) in Cipher Block Chaining (CBC) mode
  - **CCM** = **C**TR + **C**BC-**M**AC
  - **CCMP** = **CCM** + **P**adding

AES CCMP
(Counter Mode with CBC-MAC)

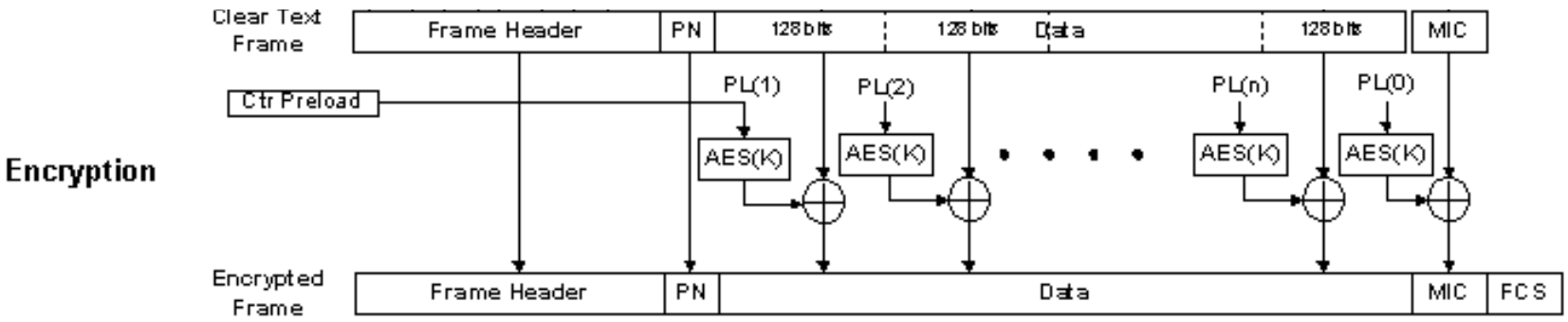


PN – packet number, similar to the TSC (TKIP Sequence Counter)

Integrity protection: AES CBC-MAC



Confidentiality protection: AES Counter Mode



Comparison WEP *vs* WPA *vs* WPA2

	WEP	WPA (TKIP)	WPA2 (AES-CCMP)
Cipher	RC4	RC4	AES CTR
Key size	40 or 104 bits	128 bits encryption, 64 bits authentication	128 bits
Key lifetime	24-bit IV, wrap	48-bit IV	48-bit IV
Frame data integrity	CRC-32	MIChael	CBC-MAC
Frame header integrity	None	MIChael	CBC-MAC
Replay detection	None	IV sequencing	IV sequencing
Key management	None	EAP / 802.1X	EAP / 802.1X

WPA3

- Defined 2018
  - Required since July 2020
- Uses an equivalent 192-bit cryptographic strength in WPA3-Enterprise mode (AES-256 in GCM mode with SHA-384 as HMAC)
  - Still mandates the use of CCMP-128 (AES-128 in CCM mode) as the minimum encryption algorithm in WPA3-Personal mode
- The WPA3 standard also replaces the Pre-Shared Key exchange with Simultaneous Authentication of Equals as defined in IEEE 802.11-2016
  - More secure initial key exchange in personal mode
  - Forward secrecy
  - Mitigate security issues posed by weak passwords
  - Simplify the process of setting up devices with no display interface
- Protection of management frames as specified in the IEEE 802.11w amendment

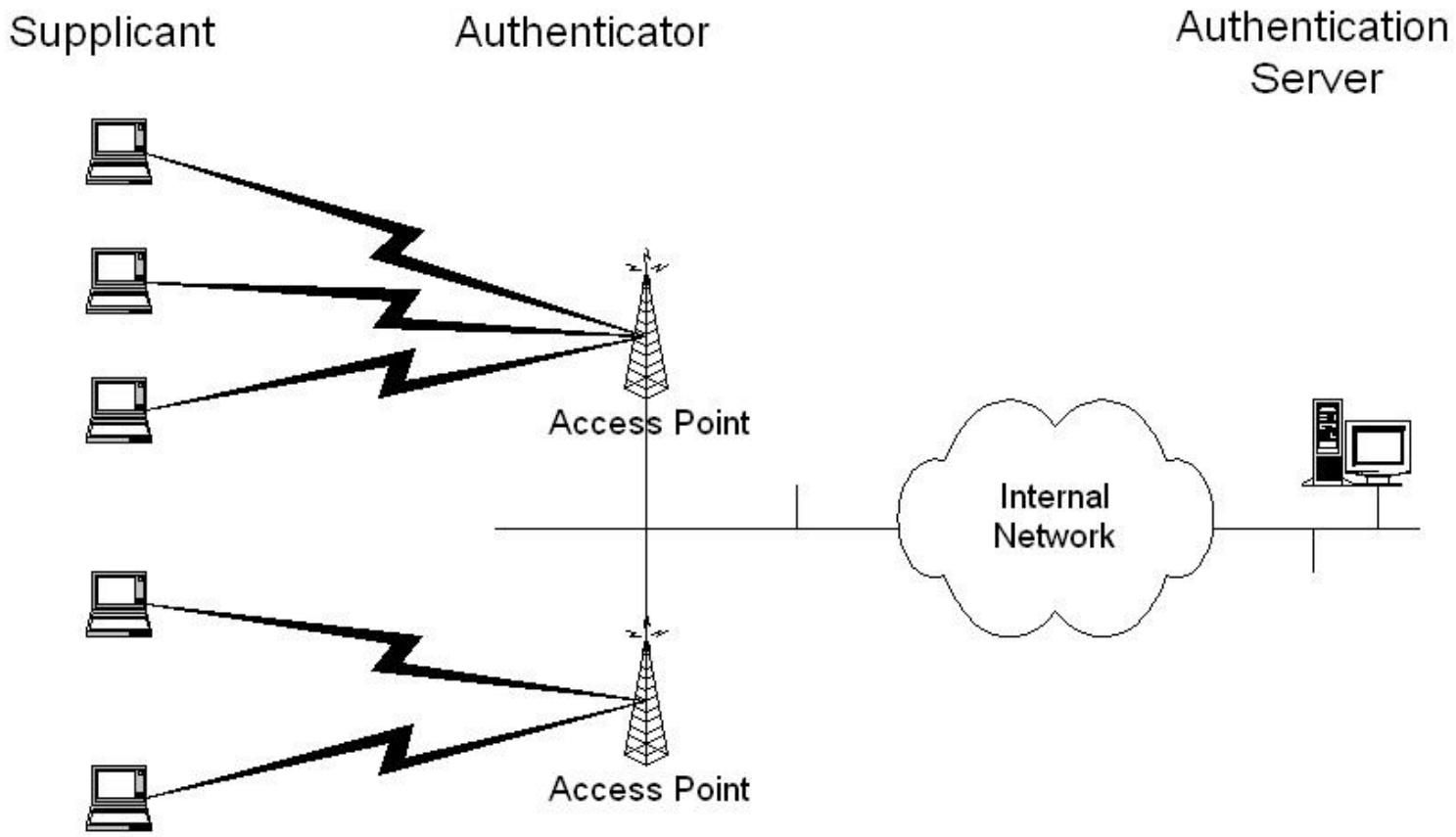
Roadmap

- Secure channels *versus* communication layers
- Wireless networks
- Wi-Fi / WLANs
  - WEP
  - WPA
  - **802.1X and EAP**

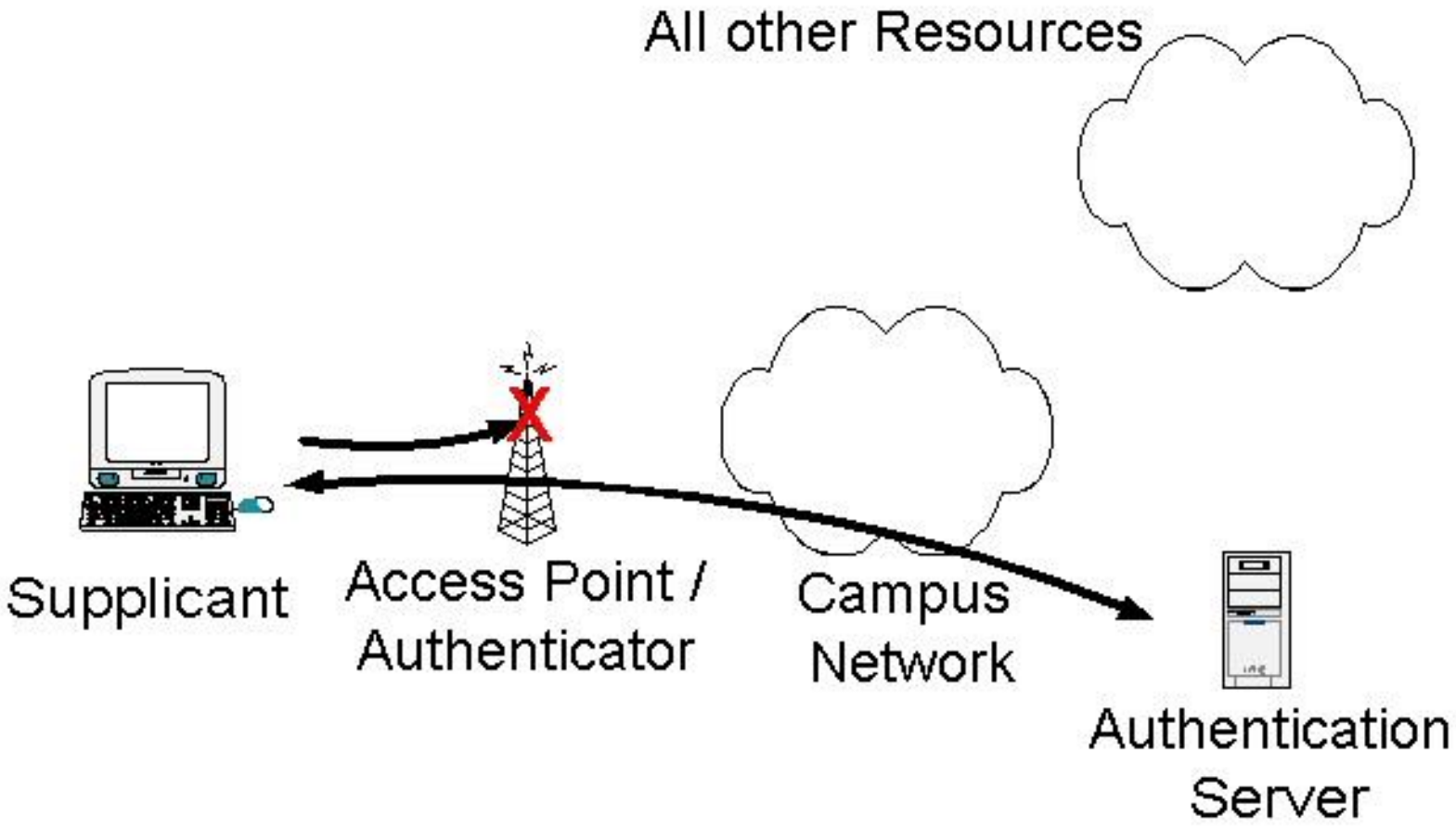
IEEE 802.1X

- Authentication model for IEEE 802 networks
  - Wired and wireless
  - Data link layer mutual authentication
- Standard for **port-based network access control (NAC)**
  - Permits or not an entity to **logically** connect to a port/LAN
  - Logically because physically it already connected somehow
- Originally designed for larger scale networks
  - College campus, etc.
  - Extended model for wireless networks
- Does **authentication** + **key distribution**

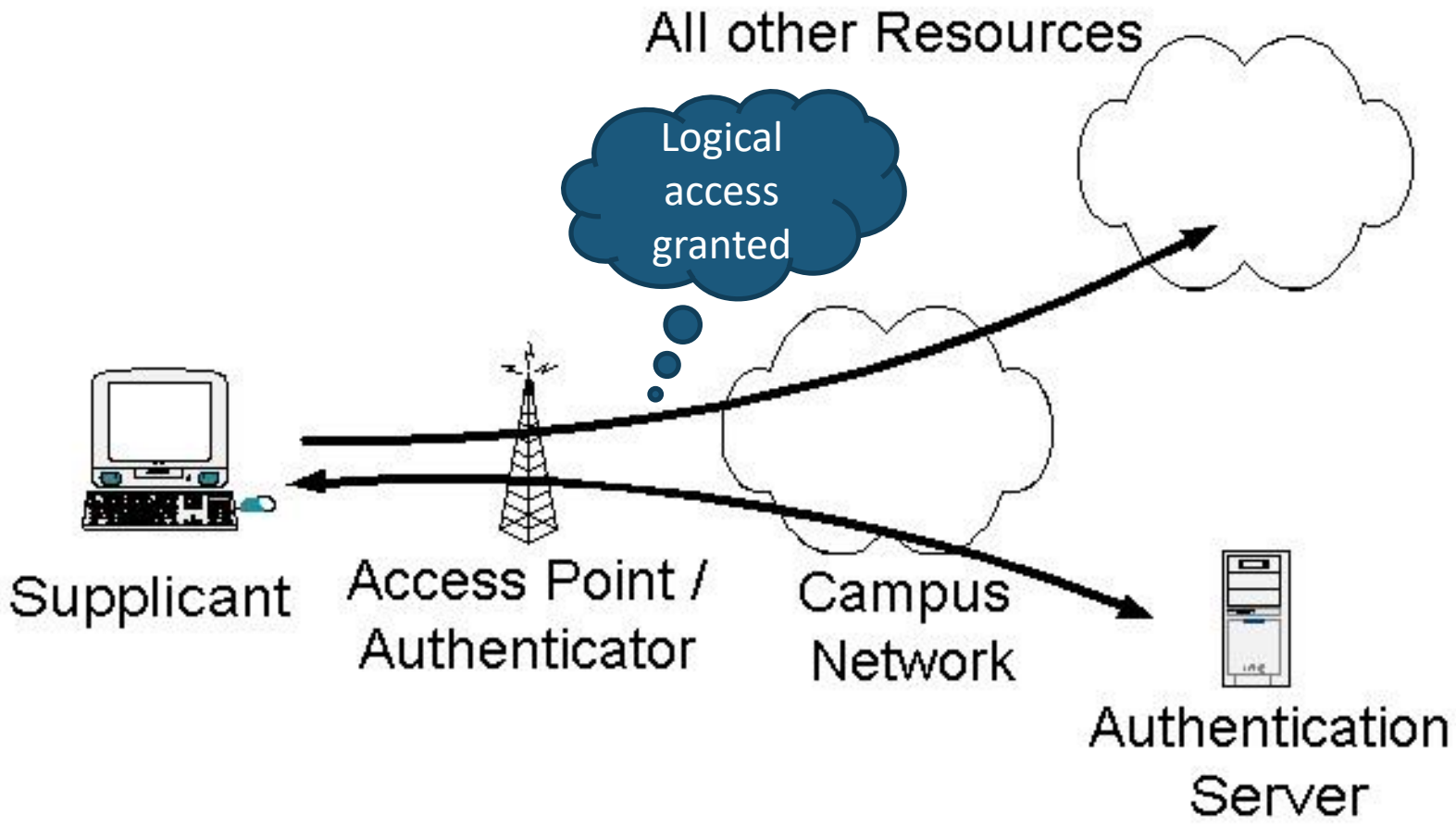
802.1X: Participants



802.1X: Pre-authentication state



802.1X: Post-authentication state

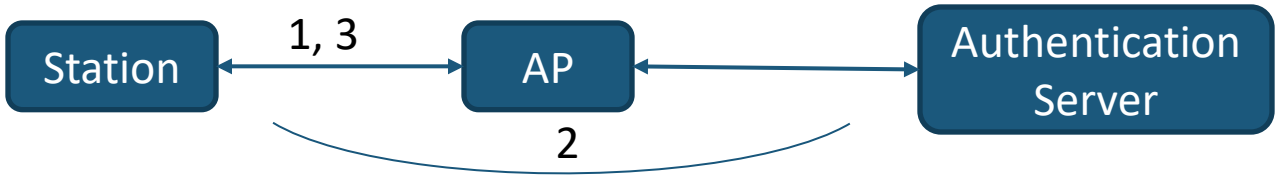


802.1X stages for wireless networks

1. WEP association between Station and AP
   - The protocol we have seen before: authentication request, etc.
2. **EAP** (Extensible Authentication Protocol)
   - **Authentication and key establishment** between Station and Authentication Server; produces **MSK (Master Session Key)**
   - It is a meta-protocol: there are several variations

802.1X encapsulates and extends **EAP** for IEEE 802 networks

3. Four-way handshake
   - Mutual authentication of Station and AP using **nonces** and **MSK**
   - Derive **Temporary Key (TK)** to be used for secure communication
   - Validation of stage 1 requests and responses



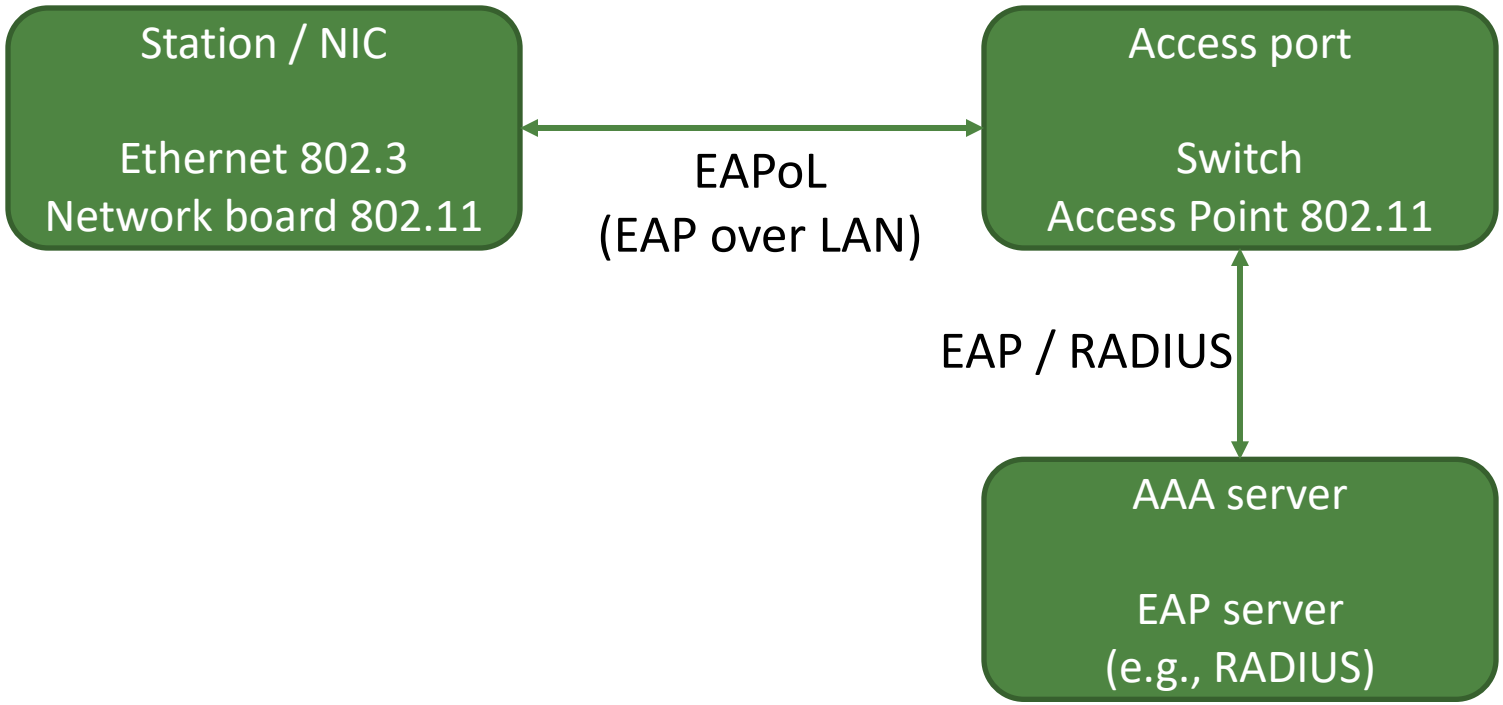
EAP
(Extensible Authentication Protocol)

- Initially designed for PPP (Point-to-Point Protocol)
  - Targeted at 802.1 (for wired networks)
- AP is not involved
  - Only allows the passage of EAP messages
  - The use of different authentication protocols does not imply modification to APs
- EAP was not designed for wireless networks
  - The communication between Stations and APs must be protected during EAP with WEP
  - Mutual authentication may not exist
    - A Station can be tricked by a more powerful AP

EAP – Types of requests

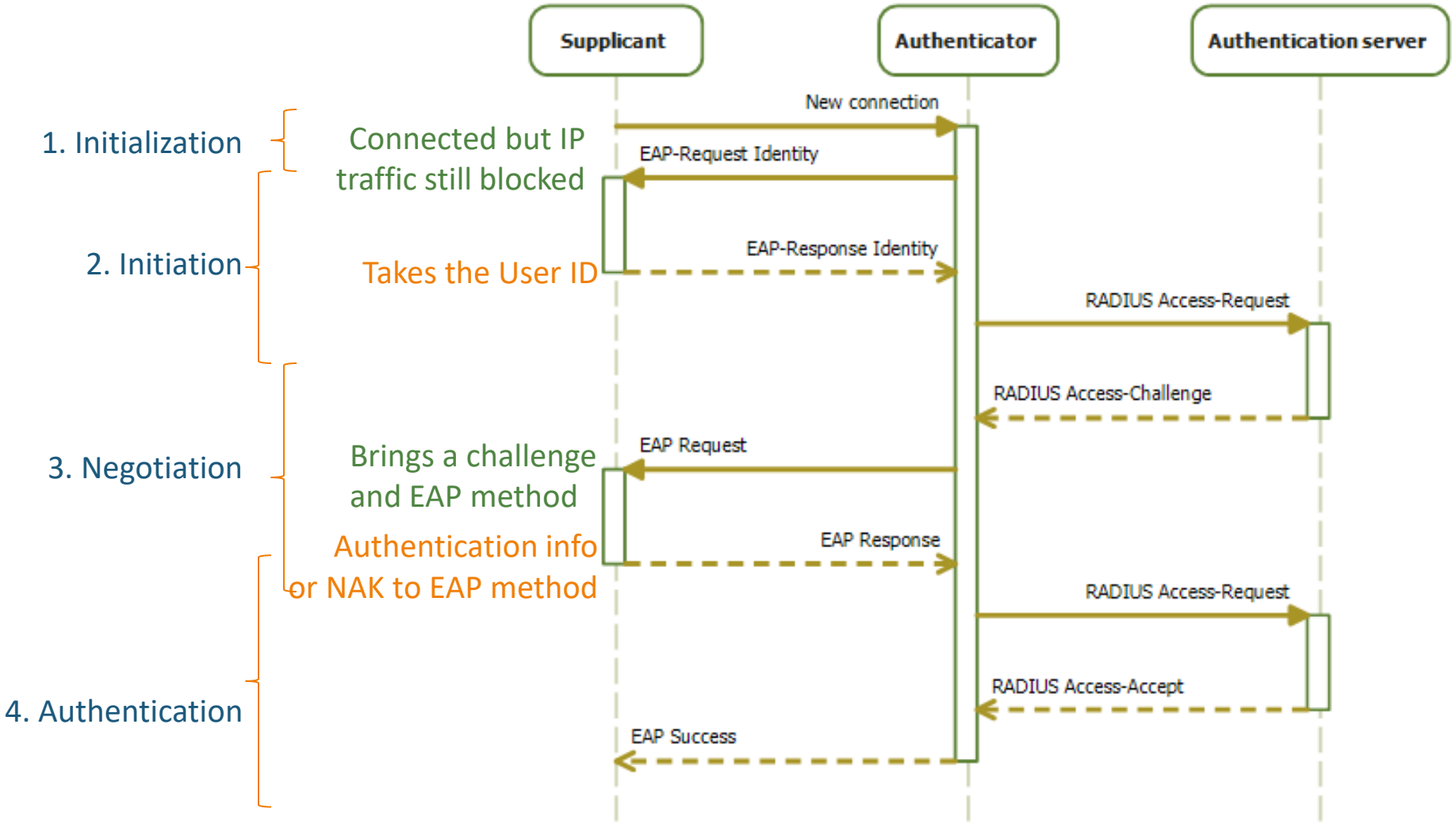
- Type 1: User identity
- Type 2: Message for the user
  - ACK
  - E.g. password about to expire
- Type 3: NAK
- Type 4: MD5 Challenge
- Type 5: One-time password
- Type 6: Cards
  - SecurID, etc.
- Type 13: TLS

802.1X architecture



RADIUS: Remote Authentication Dial-In User Service

Distribution of keys with 802.1X



EAP Protocols

- PAP, CHAP
  - Used by PPP; no mutual authentication, only user authentication
  - We have seen them when we talked about Authentication
- EAP-TLS
  - Requires certificates for both parties
- PEAP, EAP-TTLS
  - Both use TLS tunnels
- LEAP
  - Proprietary (CISCO)

Summary

- Wireless networks
- Wi-Fi / WLANs
  - WEP
  - WPA
  - 802.1X and EAP