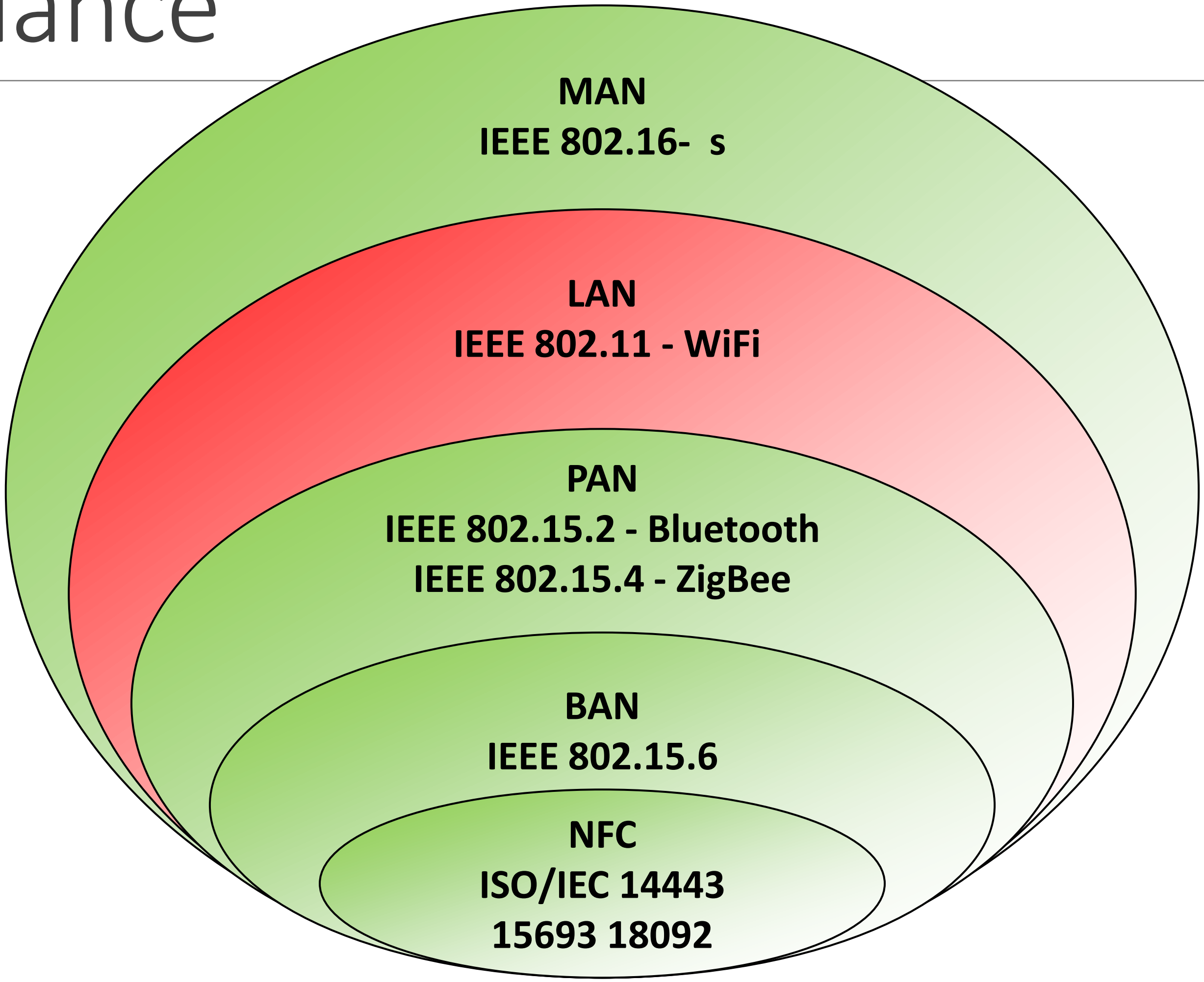
Security in 802.11 wireless networks

Wireless (data) communications: A glance



Wireless vs. cabled communications: Security issues

Broadcast communication

- Hard to enforce physical propagation boundaries
- Typical physical boundaries are useless to avoid:
  - Interference with communications
  - Eavesdropping of communications

Mitigation

- Reduce interference and eavesdropping capabilities
  - At the physical layer
  - At the data link layer

Reduce interference and eavesdropping capabilities: Physical layer

Prevent eavesdroppers from decoding the channel

- Channel coding needs to use some shared secret

Example: Bluetooth FHSS (Frequency Hoping Spread Spectrum)

- Carrier changes frequency in a pattern known to both transmitter and receiver
  - The data is divided into packets and transmitted over 79 hop frequencies in a pseudo random pattern
  - Only transmitters and receivers that are synchronized on the same hop frequency pattern will have access to the transmitted data

- FHSS appears as short-duration impulse noise to eavesdroppers
  - The transmitter switches hop frequencies 1,600 times per second to assure a high degree of data security

Reduce interference and eavesdropping capabilities: Physical layer

Present channel monopolization by transmitters

- Physical Medium access Policies

Examples

- Bluetooth FHSS
  - Unsynchronized transmitters seldom collide
- Wi-Fi
  - Each network is instantiated over a specific frequency
- GSM
  - Each terminal transmits over a specific mobile station

Interference is still possible from external sources or overlapping channels

Reduce interference and eavesdropping capabilities: data layer

Prevent attackers from identifying the participants in a communication

- Headers need to be encrypted, and temporary identifiers should be used

Prevent eavesdroppers from understanding data link payloads

- Frames need to be encrypted
  - Usually payloads only are encrypted

Prevent attackers from forging acceptable data link frames

- Frames need to be authenticated
  - Origin authentication
    - Freshness

IEEE 802.11: Architecture (in structured networks)

Station (STA)
- Device that can connect to a wireless network
- Has a (unique) identifier
  - Media Access Control (MAC) address

Access Point (AP)
- Device that allows the interconnection between a wireless network and other network devices or networks

Wireless network
- Network formed by a set of STAs and AP that communicate using radio signals

IEEE 802.11: Structured network terminology

Basic Service Set (BSS)

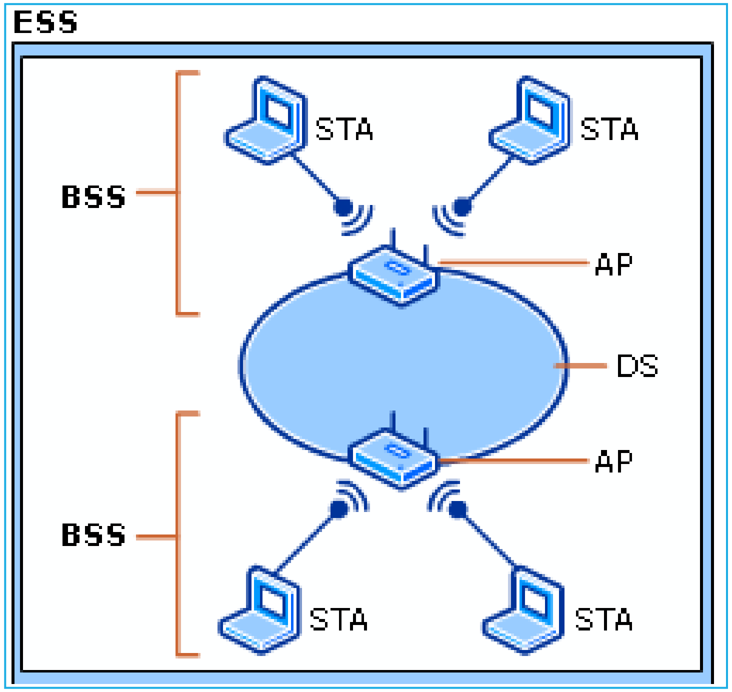
- Network formed by a set of STA associated to an AP

Extended Service Set (ESS)

- Network formed by several BSS interconnected by a Distribution System (DS)

Service Set ID (SSID)

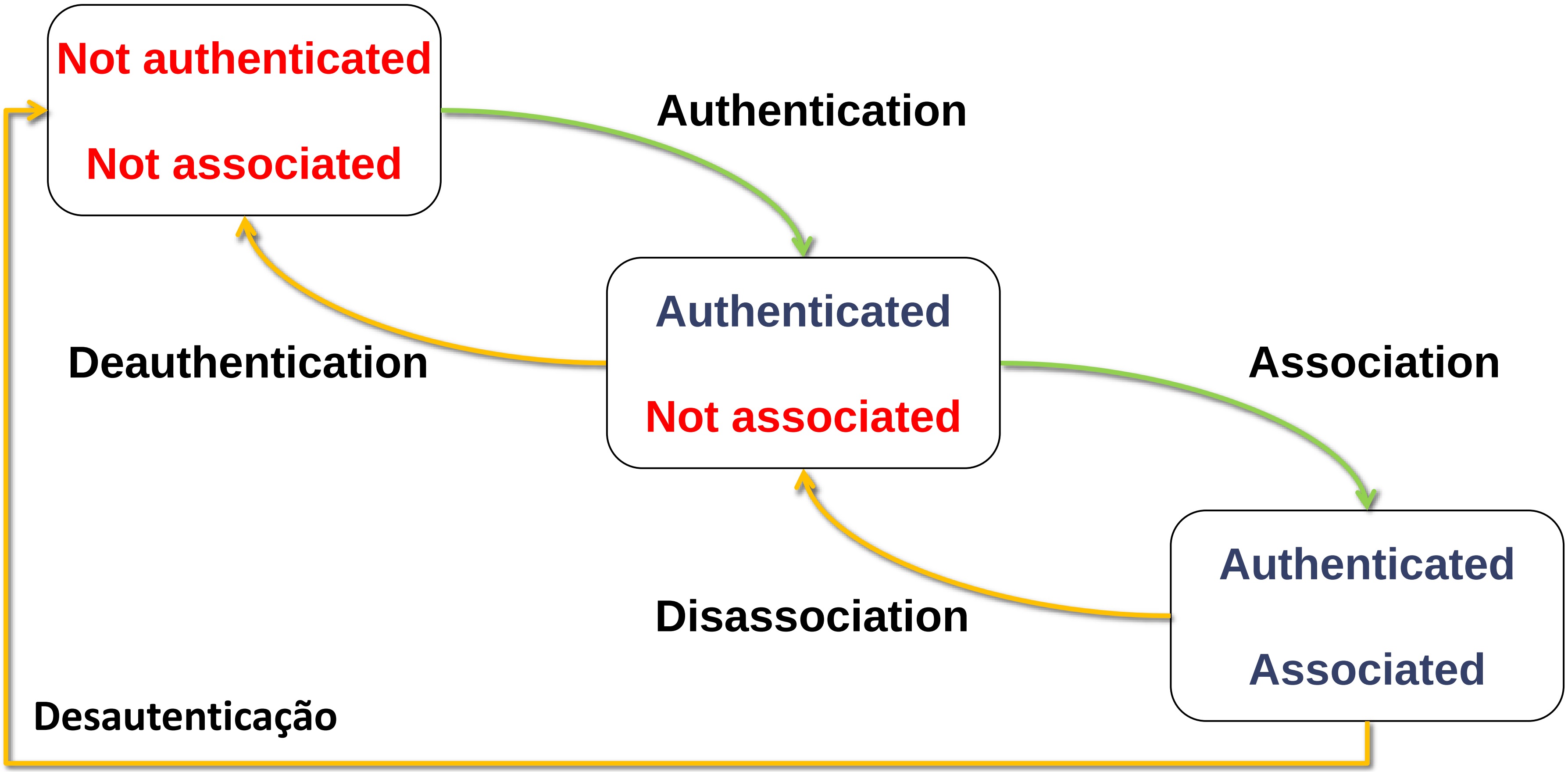
- Identifier of a wireless network served by a BSS or ESS
- The same infrastructure can use several SSID



IEEE 802.11: Structured network terminology

```
$ airport -s
            SSID BSSID             RSSI CHANNEL
         MEO-WiFi 9e:97:26:f1:65:3e -87  11
FON_ZON_FREE_INTERNET 00:05:ca:d3:32:f9 -86  11
         ZON-22D0 00:05:ca:d3:32:f8 -90  11
     Cabovisao-BB20 c0:ac:54:f8:fe:dc -84  6
FON_ZON_FREE_INTERNET 84:94:8c:ae:74:a9 -81  6
         ZON-6E50 84:94:8c:ae:74:a8 -81  6
FON_ZON_FREE_INTERNET 84:94:8c:ad:23:99 -86  2
         ZON-ED50 84:94:8c:ad:23:98 -87  2
FON_ZON_FREE_INTERNET bc:14:01:9b:d0:c9 -88  1
         ZON-D030 bc:14:01:9b:d0:c8 -88  1
```

IEEE 802.11: Authentication & Association state machine



IEEE 802.11: Frame types

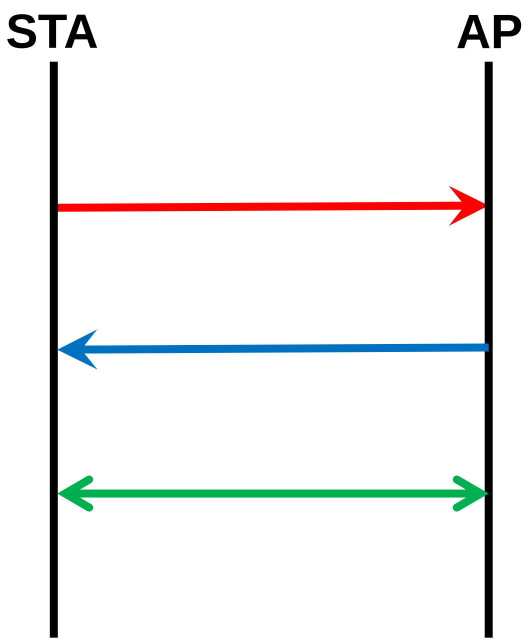
Management frames

- Beacon
- Probe Request & Response
- Authentication Request & Response
- Deauthentication
- Association Request & Response
- Reassociation Request & Response
- Disassociation

Control frames

- Request to Send (RTS)
- Clear to Send (CTS)
- Acknowledgment (ACK)

Data Frames



IEEE 802.11 data link security: Overview

Functionality \ Network Type		pre-RSN	RSN (Robust Security Network)		
		WEP	WPA		802.11i (ou WPA2)
Authentication		Unilateral (STA)	Bilateral with 802.1X (STA, AP and network)		
Key Distribution			EAP ou PSK, 4-Way Handshake		
IV Management Policy			TKIP		AES-CCMP
Data Cipher		RC4			AES-CTR
Integrity Control	Headers		Michael		AES CBC-MAC
	Payload	CRC-32	CRC-32, Michael		

Other

- SSID hiding (on beacons)
- MAC address filtering (on associations)
- (Privacy) MAC client randomization before association

IEEE 802.11: WEP (Wired Equivalent Privacy)

Optional and unilateral Authentication

- Can support multiple types simultaneously

OSA: Open System Authentication

- No authentication, just for the state transition model

SKA: Shared Key Authentication

- Challenge/response between STA and AP
- Key (password) per person (MAC address) or network
- Unilateral STA authentication
  - No AP / network authentication

Frame payload encryption

- With RC4, using 40 or 104 bit keys

Frame payload authentication with CRC-32

WEP:
Lots of security problems ...

SKA is completely insecure

- An eavesdropper gets all it needs to impersonate a victim
  - No need to discover the password
- Rogue APs cannot be detected

Same key for authentication and payload confidentiality

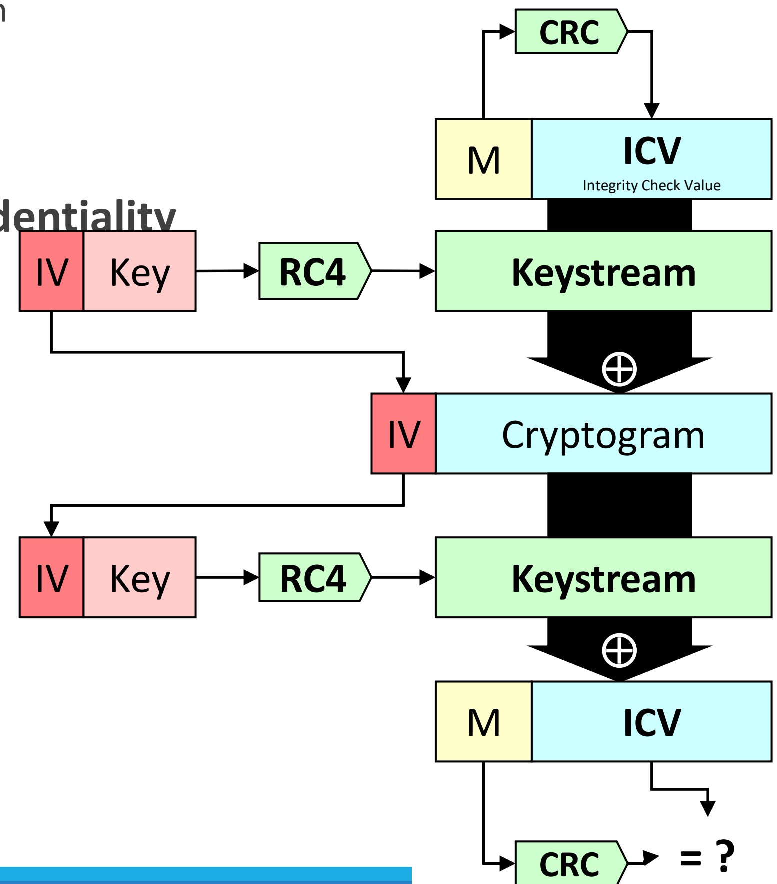
- No key distribution, keys overused

Weak integrity control

- CRC-32 is linear
- Frame deterministic modification is trivial

Mediocre IV management

- IV is too short (24 bits)
  - Easy to get cryptograms produced with the same IV
  - Same IV, same key ⇒ same keystream, cryptanalysis becomes easier
- IV is not managed at all
  - Reuse is not controlled / prevented



Fluhrer, Mantin and Shamir (FMS) Attack

A vulnerability was discovered in RC4

- Weak keys were found due to the KSA (Key Scheduling Algorithm) used
  - **Some initial keystream bits reflect key bits**

Description:

- Key_{RC4} = IV[0:2] + Key, where len(key) = 13 (or 5), total length is 104 bits
- IV is visible
- With some keys (a+3, n-1, *) with a=key byte, n = [0..256], if attacker knows:
  - first byte of plain text (p0)
  - first m bytes of key (k0..m)
- Attacker can derive m+1 bytes of the key

Result:

- can recover key after ~500K to 1M packets (<1.4GB Data)

Fluhrer, Mantin and Shamir (FMS) Attack

Attacker knows

- first byte of the cryptogram (c_0) is public (in the packet)
- first byte of plaintext (p_0) is known (SNAP header, value = 0xAA)
- first 3 bytes of key are known (IV)
- first byte of keystream $k_0 = p_0 \oplus c_0$

Process

- Assume Key = IV + [3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15]
- initialize the KSA to the 3rd round (i=3)
- Wait for vulnerable IVs (a+3, n - 1, *)
- K_i can be "recovered" using $(c_0 - j - S[i]) \bmod n$
  - S[i] = result of permutation box at pos i, n = size of S, j= index of byte
- Attacker doesn't know if K_i is correct
  - Correct value will appear more frequently
  - Result: determine the most frequently value and increase i

Mitigation of WEP problems: WPA (WiFi Protected Access)

WPA uses WEP in a safe way
- A different RC4 key per frame
- RC4 week keys are avoided
- Extra cryptographic integrity control with Michael
- IV strict sequencing for preventing frame reuse

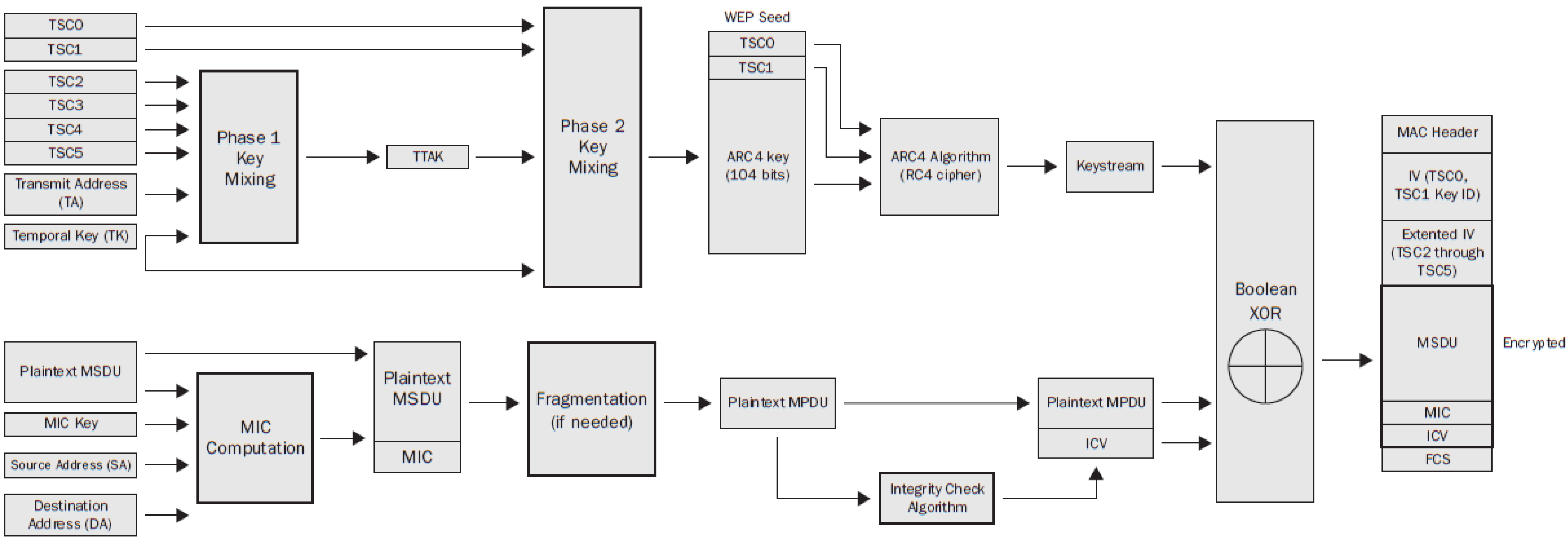
Implemented first by device drivers
- Latter on firmware

Inline with 802.11i
- The actual 802.11 security standard
- WPA can be used with 802.1X for strong, mutual authentication

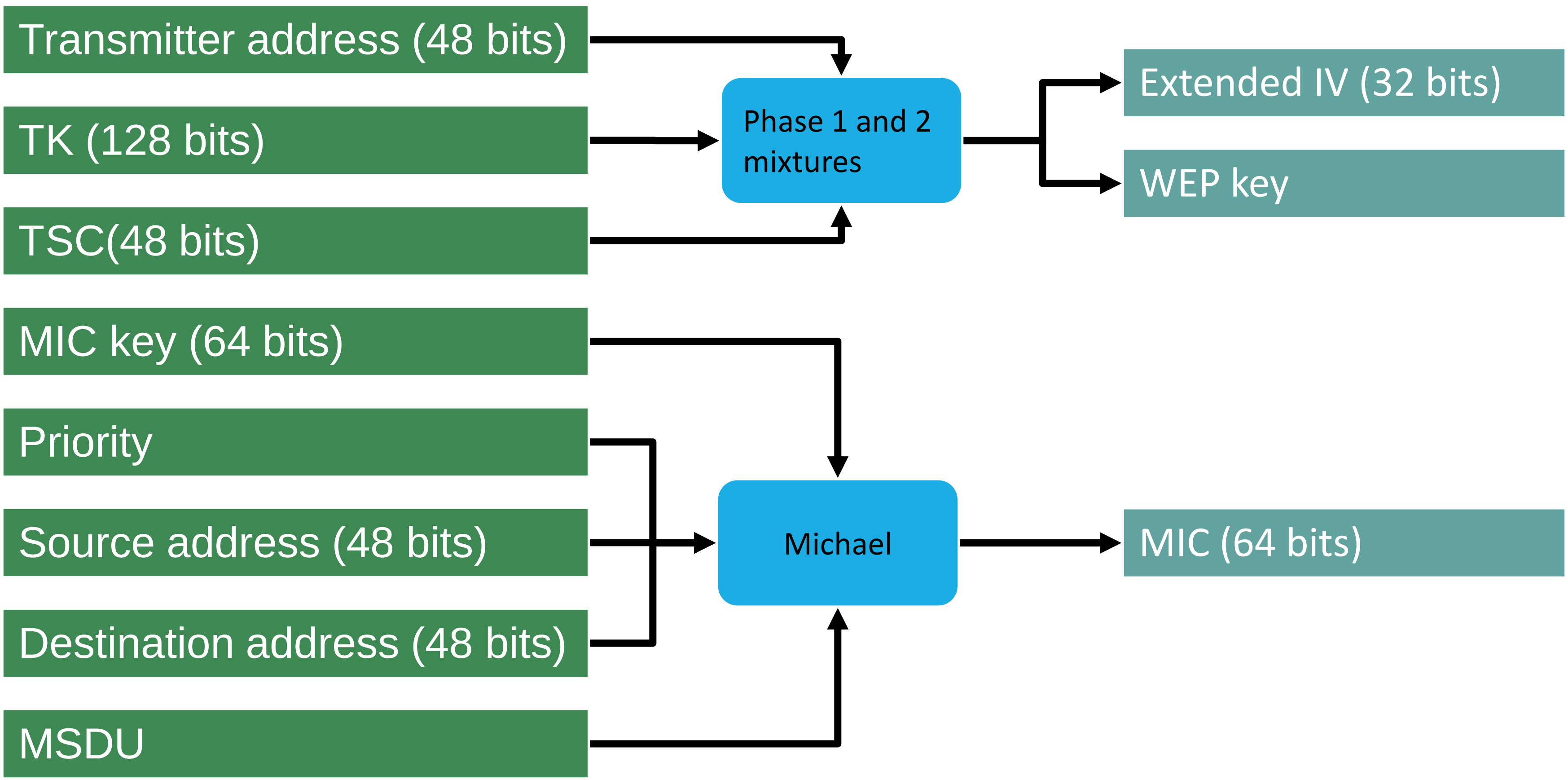
Mitigation of WEP problems: WPA (WiFi Protected Access) - TKIP

1. **Temporal Keys: to defeat social engineering attacks**
2. **Sequencing: to defeat replay & injection attacks**
3. **Key Mixing: to defeat the known IV collisions & weak-key attacks**
4. **Enhanced Data Integrity(MIC): to defeat bit-flipping & forgery attacks**
5. **TKIP Countermeasures: to address constraints of TKIP MIC**

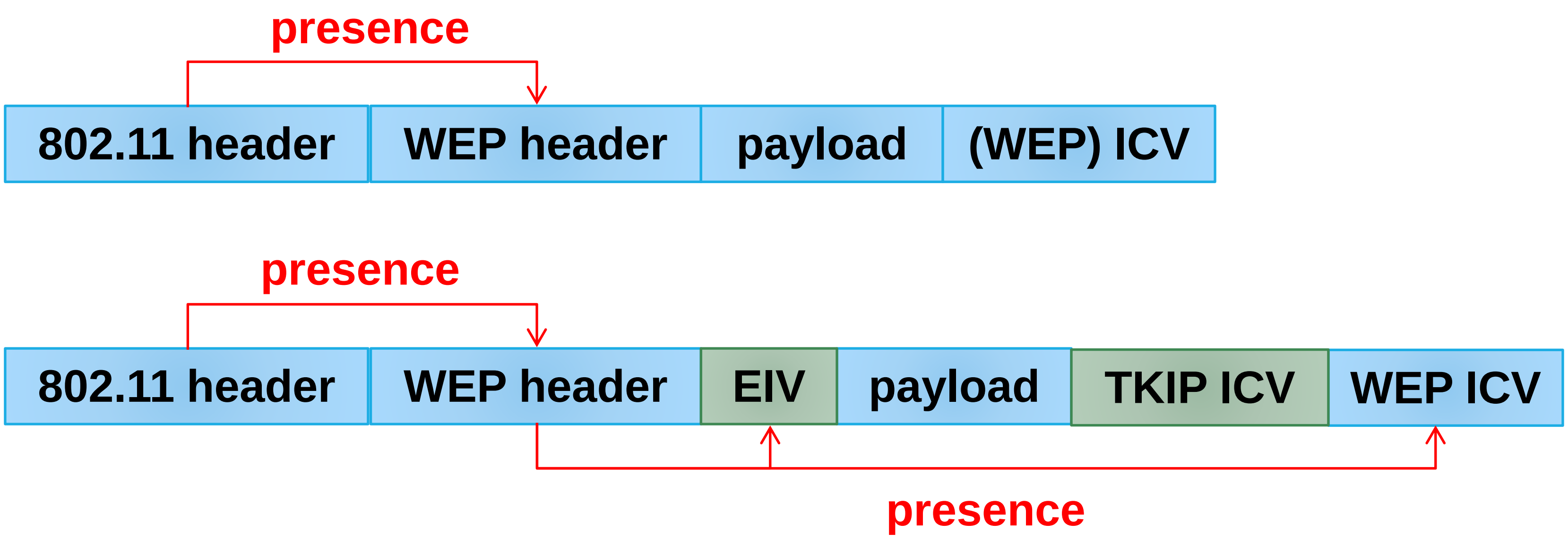
WPA:
TKIP (Temporal Key Integrity Protocol)



WPA:
TKIP (Temporal Key Integrity Protocol)



TKIP: Frame layout



Beck-Tews attack

Conditions

- the network address is known: ex, 192.168.0.0
- the network supports QoS (IEEE 802.11e) with 8 Traffic Identifiers
- the TKIP key renewal is long (3600 seconds)
- Chop-chop attack: decrypt m bytes of a packet by sending m*128 packets by brute forcing the ICV

Attack:

- Capture an ARP Request / Response: A known plaintext
  - known except: last byte of IP addrs, 8 byte MIC, 4 byte ICV
- Send packets guessing bytes. Limited to 1 packet, per TID per minute
  - Objective: Guess plaintext of MIC and ICV by analysing errors from AP
- Brute force IP addresses (2 bytes)
- Reverse MIC and find the key
  - MICHAEL is not a one way function
- Final: Obtain entire keystream valid for a given TSC

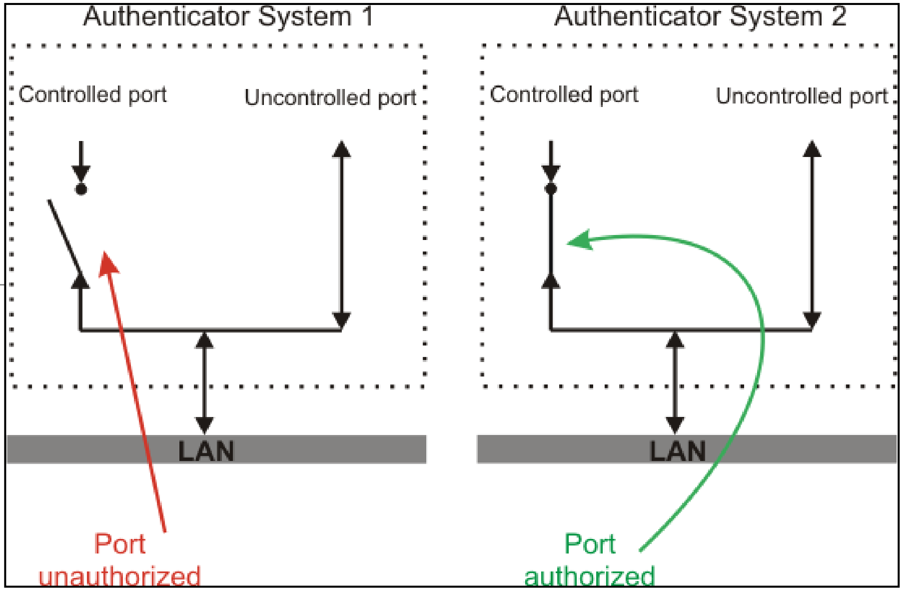
IEEE 802.1X: Port-Based Authentication

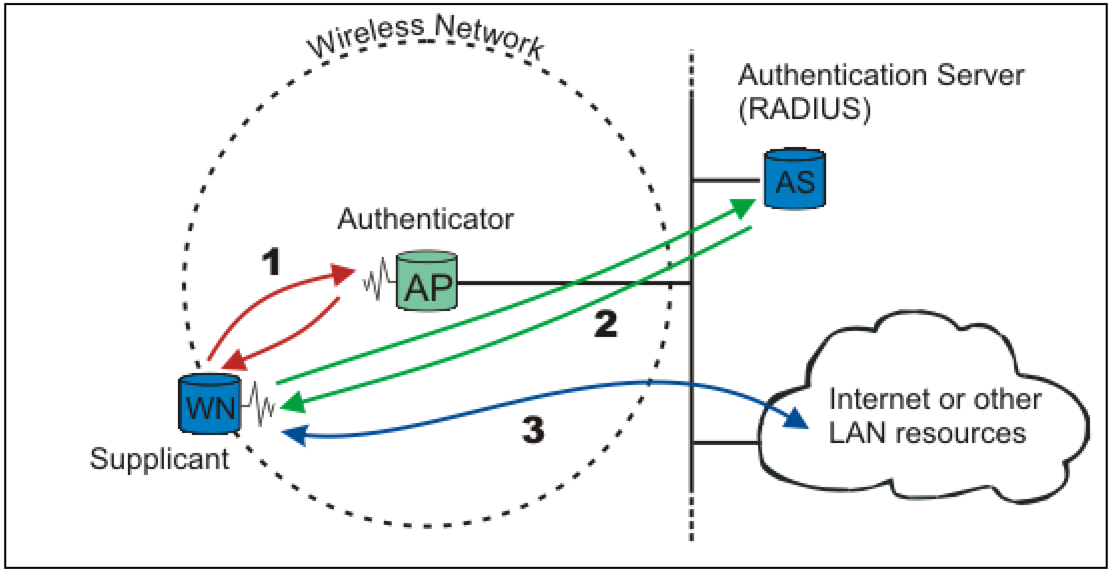
Authentication model for all IEEE 802 networks
- Layer 2 mutual authentication

Originally conceived for large networks
- University campus, etc.
- Model was extended for wireless networks

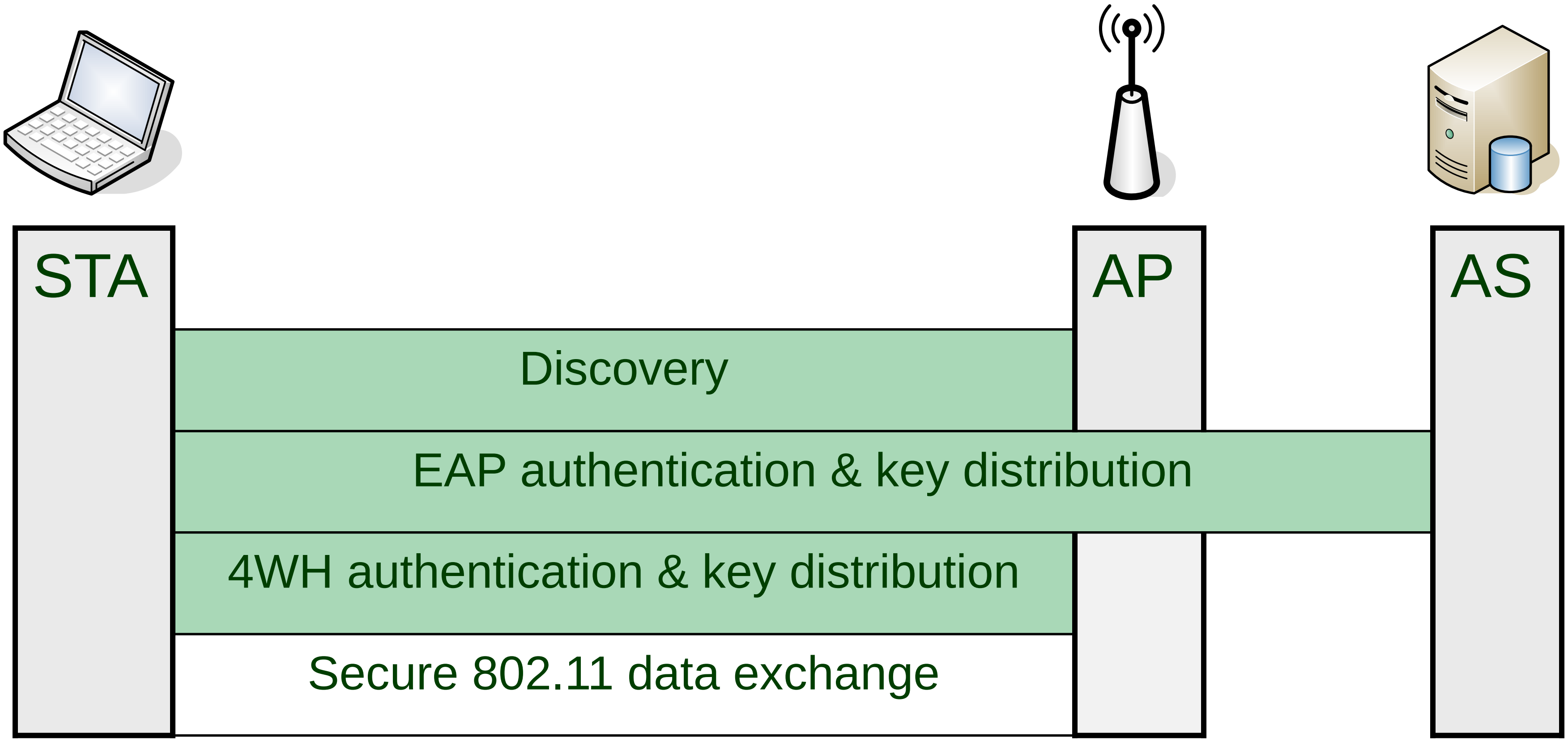
Performs key distribution
- Additional protocols focus in the remaining processes

IEEE 802.1X: Architecture

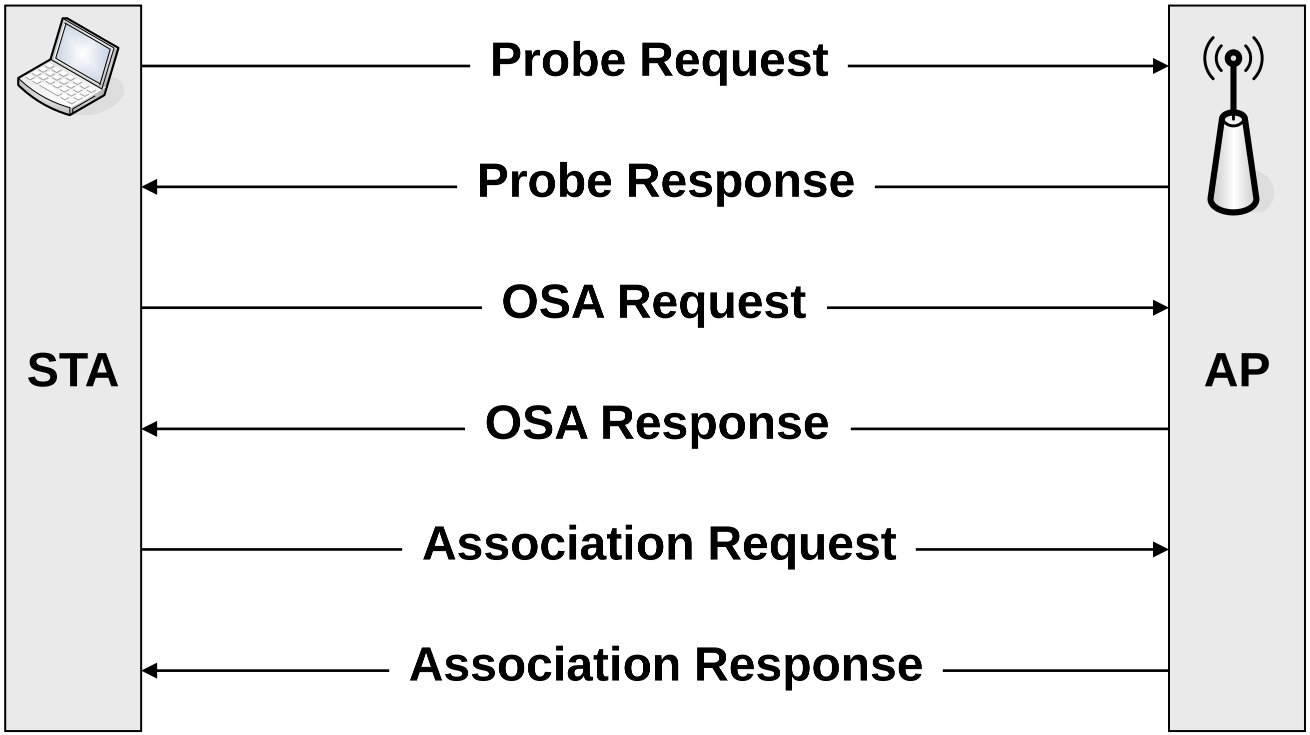




IEEE 802.1X: Operational Phases



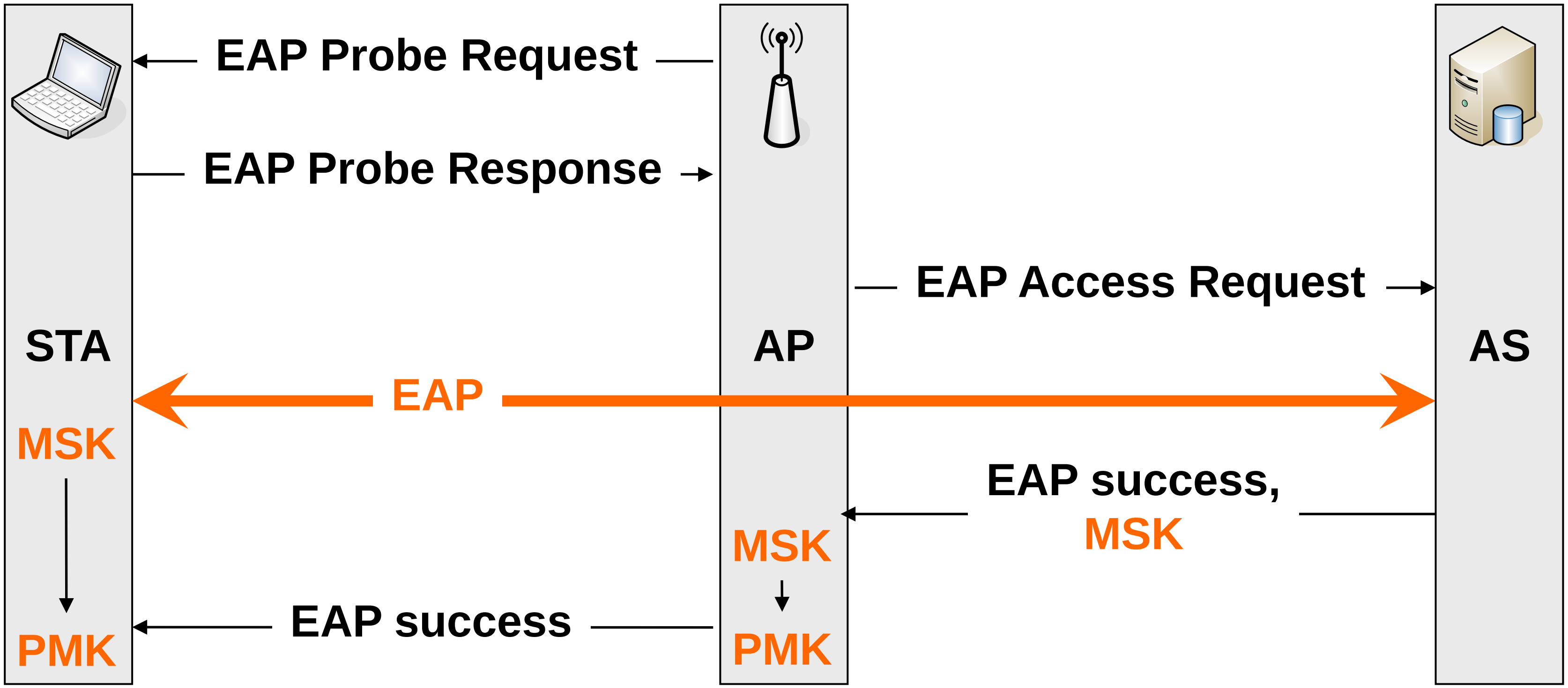
IEEE 802.1X Phase 1: Discovery (802.11 messages)



STA only got access to the AP

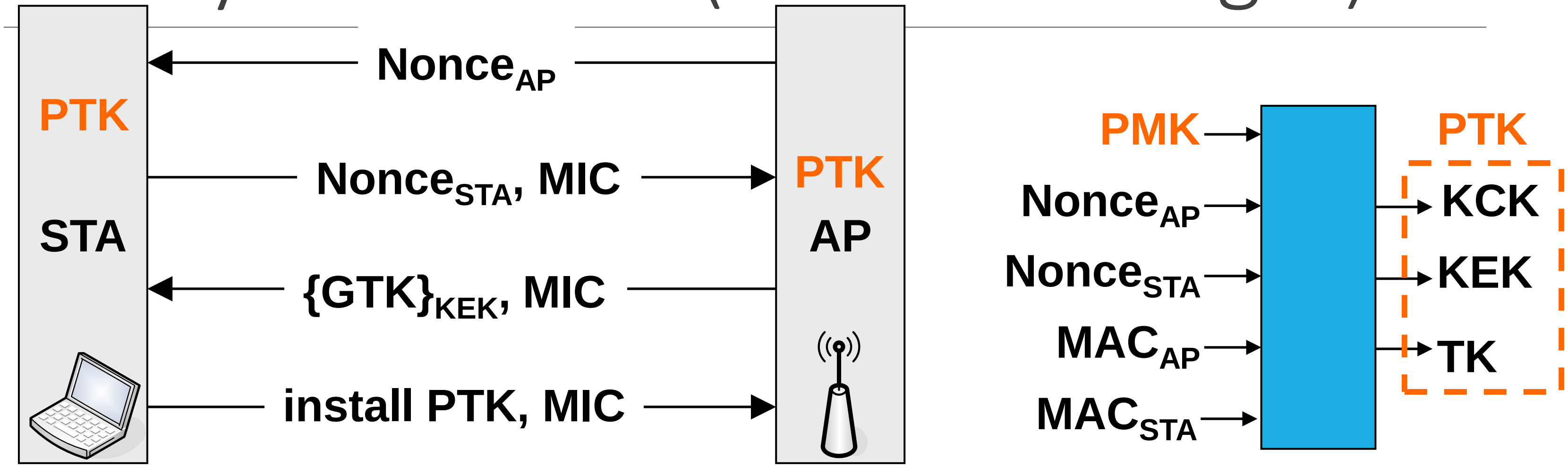
- 802.1X controlled port still closed

IEEE 802.1X Phase 2: Authentication (EAP Messages)



At the end of this phase AP and STA share crypto data
- PMK (*Pairwise Master Key*)
- But 802.1X controlled port still closed

IEEE 802.1X Phase 3: 4-Way Handshake (EAPoL Messages)



At the end AP and STA share new, fresh crypto data

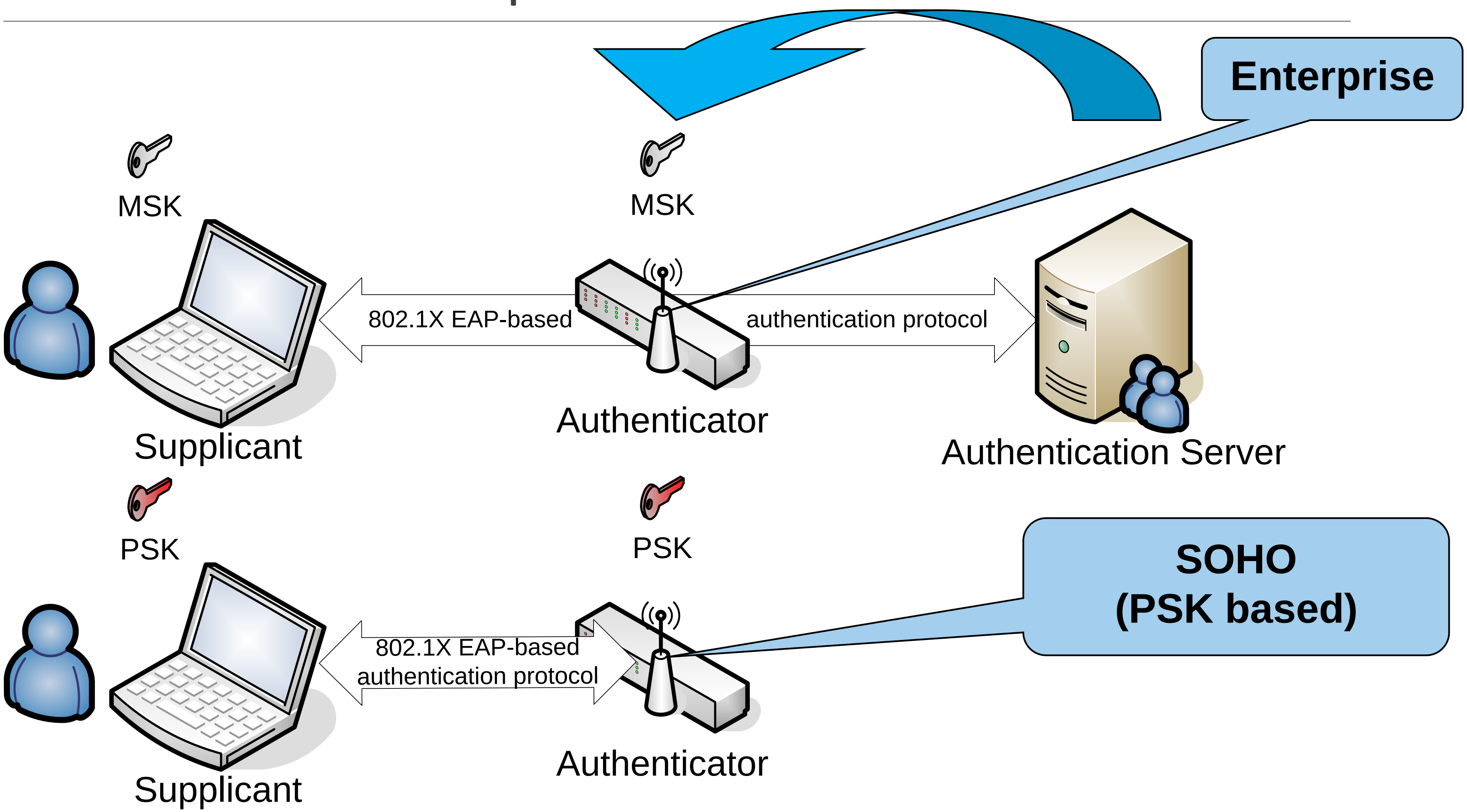
- PTK (*Pairwise Transient Key*)
- GTK (*Group Transient Key*)

Both are convinced that the peer knows PMK and PTK

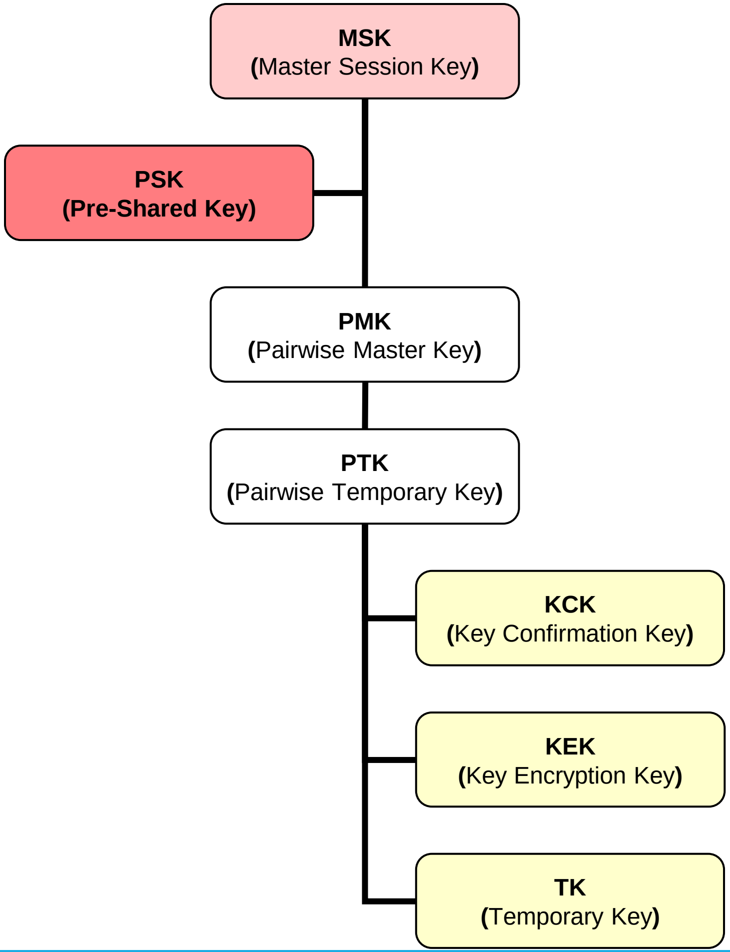
- Due to the use of MICs

802.1X controlled port is now open for unicast traffic

IEEE 802.1X: Architectural options



IEEE 802.1X: Complete key hierarchy



MSK
- Fresh outcome of an EAP protocol run
- Enterprise architecture

PSK
- Long-term AP-STA pre-shared key
- SOHO architecture

PMK
- Fresh key used for AP-STA mutual authentication and for key distribution in 4WH protocol runs

PTK
- Key used to protect AP-STA data exchanges
  - CKC / KEK: 4WH protocol
  - TK: 802.11 data frames

EAP (Extensible Authentication Protocol)

Initially conceived for PPP
- Adapted to 802.1X

AP not involved
- Relay EAP traffic
- Different EAP protocols do not imply changes in APs

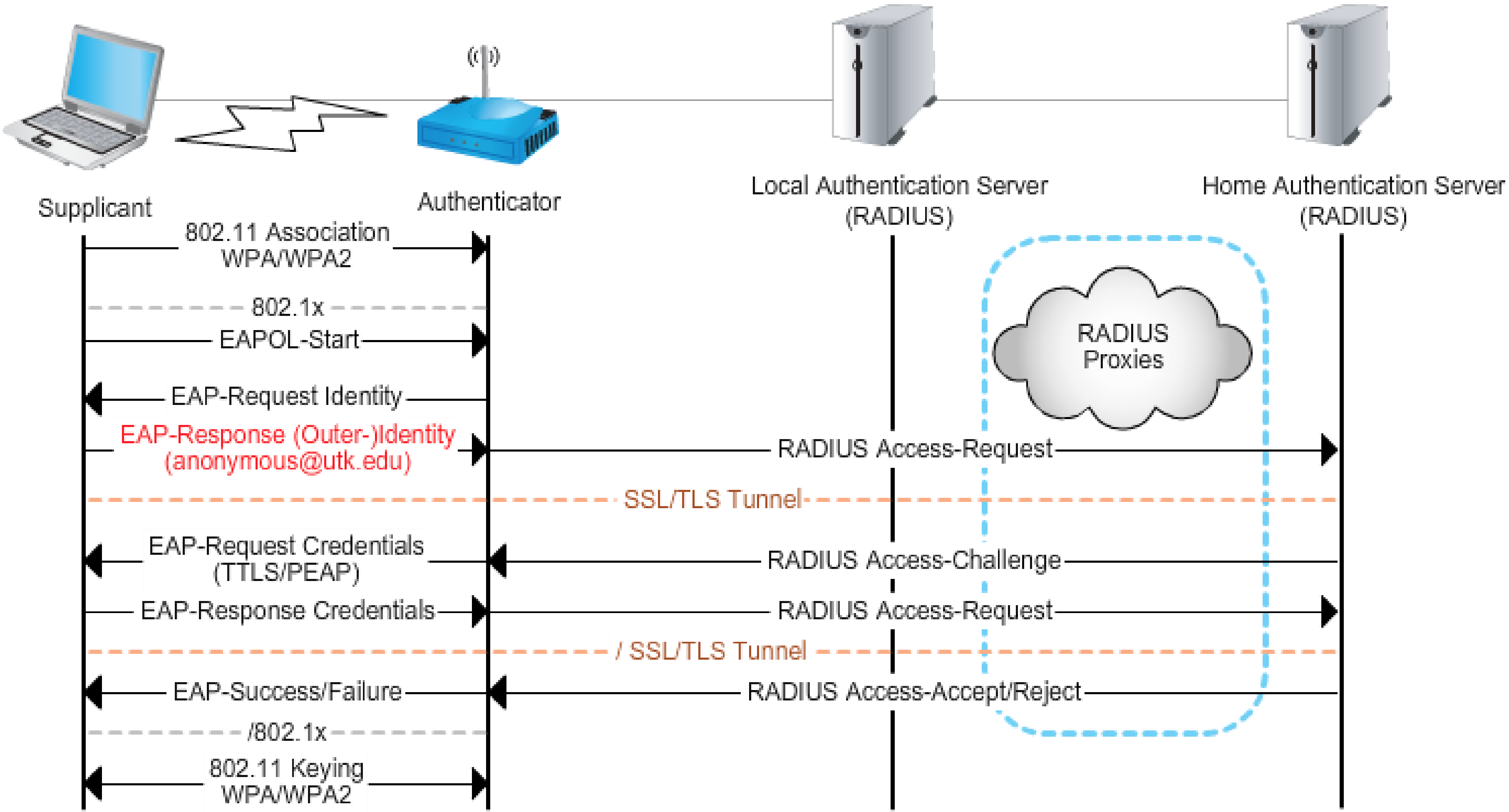
Not conceived for wireless networks
- EAP traffic not protected
- Mutual authentication not mandatory
  - An STA can be fooled by a stronger (radio level), rogue AP

Some EAP protocols for 802.1X

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
AS	N/A	digest (challenge, password)	Public Key (certificate)		
Authentication	digest (challenge, password)	digest (challenge, password)	Public Key (certificate)	EAP, Public Key (certificate)	PAP, CHAP, MS-CHAP, EAP
Key Management	No	Yes			
Risks	- Identity exposure - Dictionary attacks - Host-in-the-Middle attacks - Connection stealing	- Identity exposure - Dictionary attacks - Host-in-the-Middle attacks	Identity exposure		Possible identity exposure in phase 1

https://www.eduroam.us/node/10

Eduroam: 802.1X – PEAP - MS-CHAPv2



Available on most University of the world

- Local Authentication Servers (using RADIUS) for roaming access

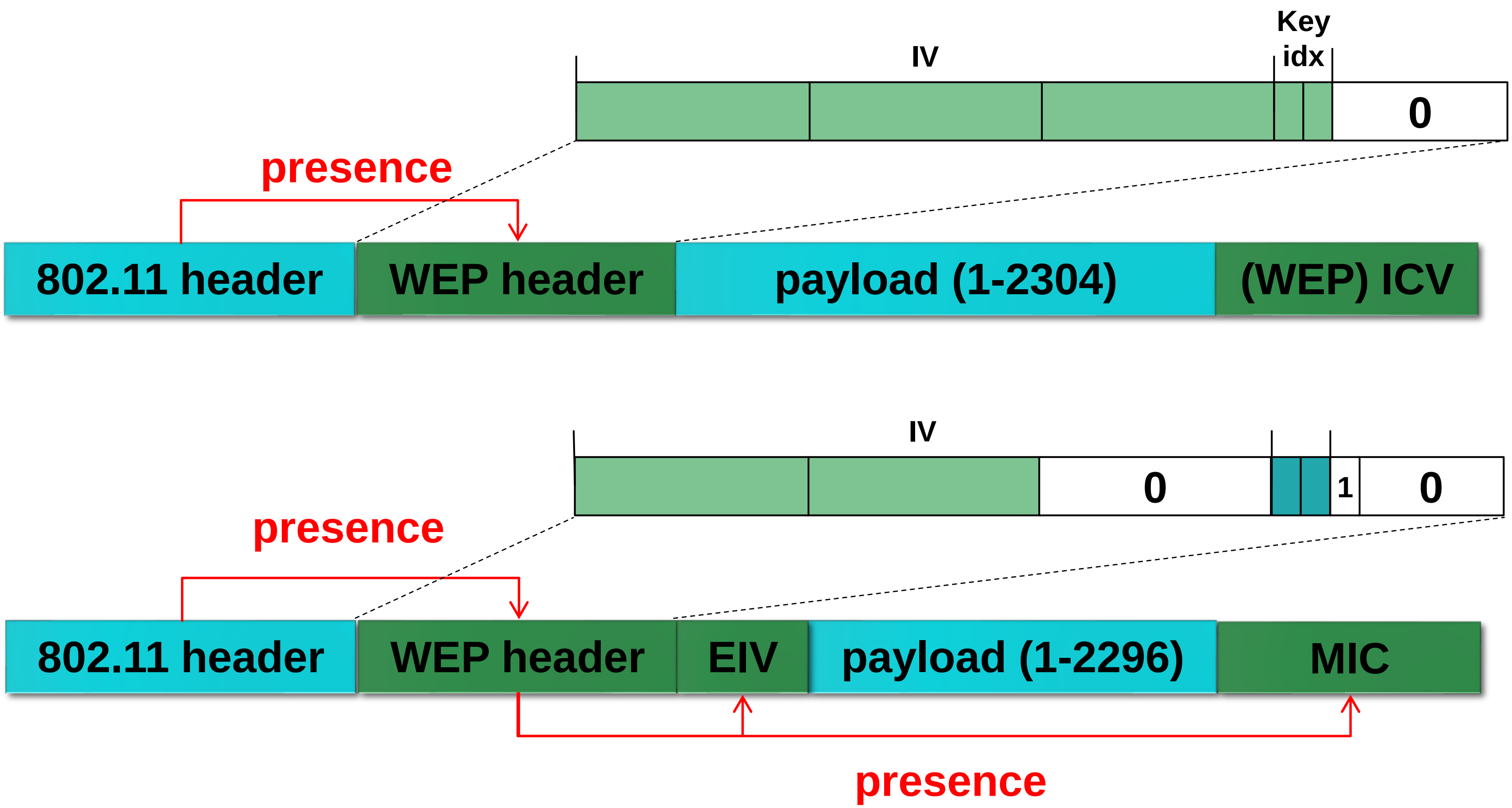
IEEE 802.11i (WPA2)

Defines Robust Security Networks (RSN)
- Those that support WPA and 802.11i

Uses advanced security mechanisms for frame protection
- Advanced Security Algorithm (AES) for payload encryption and frame integrity control

Uses 802.1X for network access authentication
- Simplified Pre-Shared Key (PSK) mode for SOHO (Small Office, Home Office) environments
- EAP-based protocol for enterprise environments

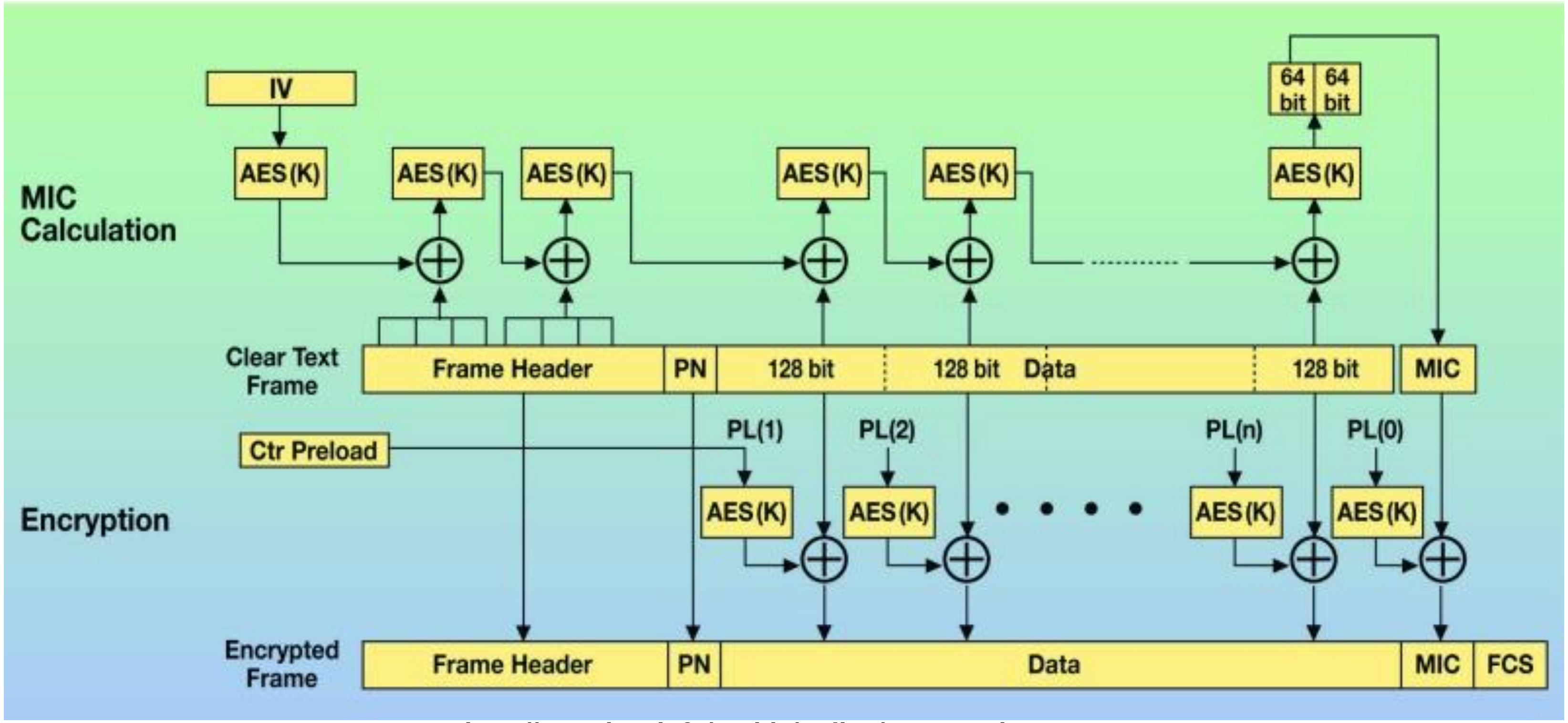
WEP vs. AES-CCMP: Frame layout



IEEE 802.11i (WPA2)

CCMP - Counter CBC-MAC Protocol

- 128bit keys, protection of headers, data, with cipher and authentication



http://2014.kes.info/archiv/online/04-5-036.htm

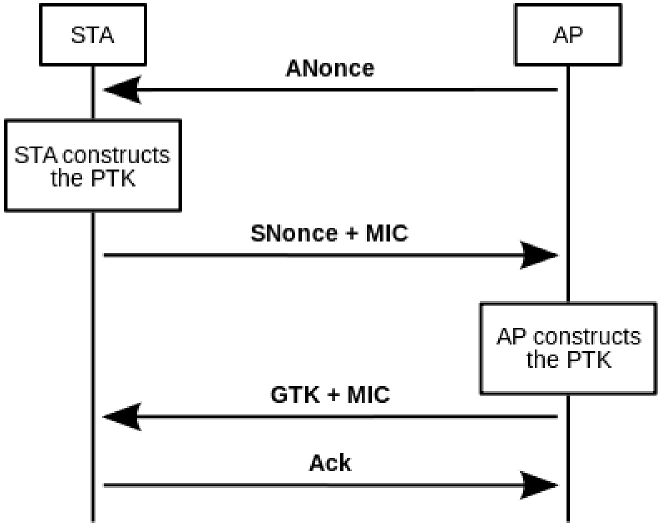
WPA2

PTK: Pairwise Transient Key

- PRF(PMK | ANonce | SNonce | AP MAC address |STA MAC address)
- PRF: Pseudo Random Function
- PMK = PSK = PBKDF2(HMAC−SHA1, password, ssid, 4096, 256)

GTK: Group Temporal Key

- Used for broadcast traffic



802.11w:
Protected Management Frames

Management frames that can be used for DoS attacks are authenticated

- Deauthentication & Deassociation requests
- Other management frames unicasted or broadcast by an AP

BIP (Broadcast Integrity Protocol)

- IGTK (Integrity GTK)
- For protecting part of the AP broadcast traffic

AS Query Request / Query Response

- Help to deal with desynchronization issues

IEEE 802.11 security: Are all the problems solved? No!

Dictionary attacks are still possible with PSK or EAP-based authentication

- And they will continue to be as long as (weak) passwords are chosen by people

Only data frames are protected

- Management frames are not protected
- Attackers can deauthenticate or disassociate a victim STA

Some problems remain at the CSMA level

- Low Congestion Window (CW) values allow attackers to get all the bandwidth

KRACK2

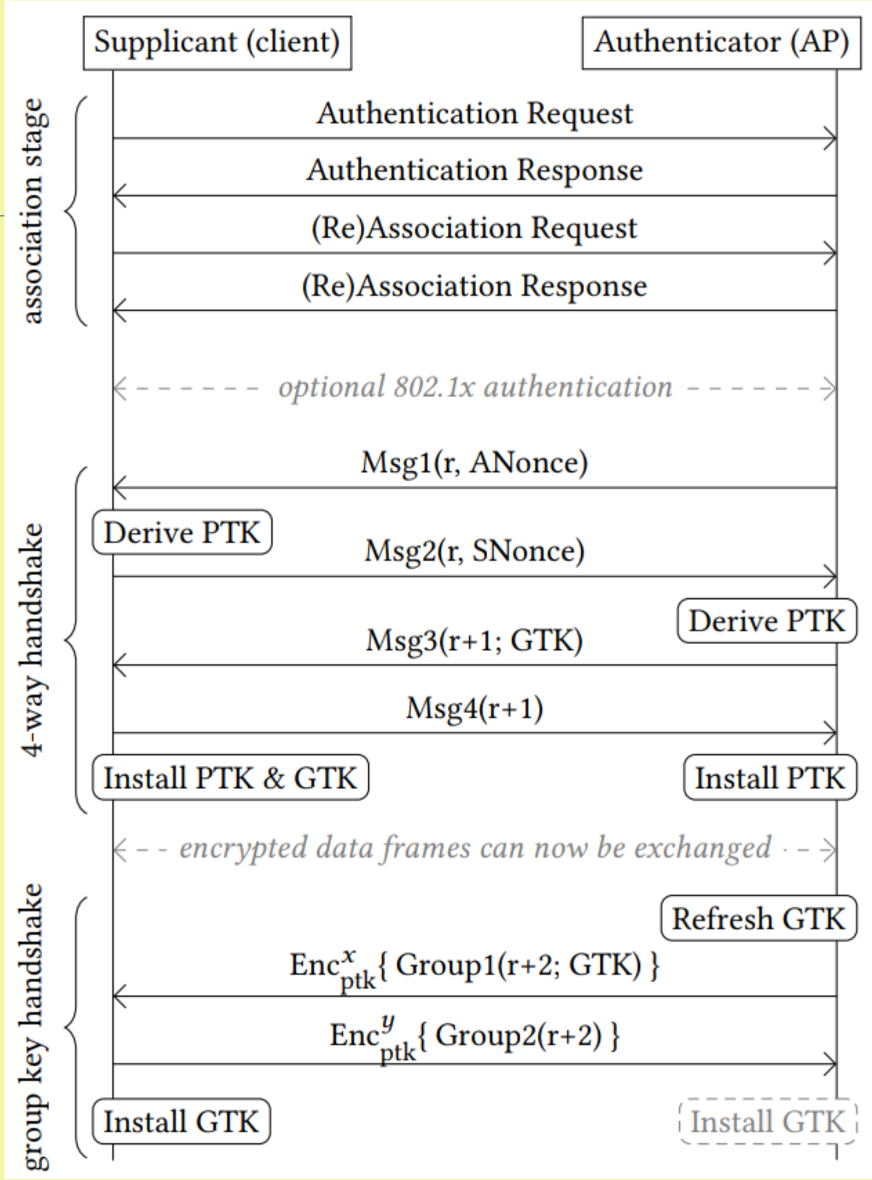
Objective: make victims reuse keys to find keystream

Vulnerability: Supplicant will always process Msg3

- Even if PTK is already installed
- In the First Frame, NONCE = 1

Attack: Block Msg4

- AP will re-transmit Msg 3
- Key is re-installed
- Data frame uses NONCE=1



KRACK2

Objective: make victims reuse keys to find keystream

Vulnerability: Supplicant will always process Msg3

- Even if PTK is already installed
- In the First Frame, NONCE = 1

Attack: Block Msg4

- AP will re-transmit Msg 3
- Key is re-installed
- Data frame uses NONCE=1