Network Security: WLAN Security

Mohit Sethi
Ericsson, Finland
Aalto University, Finland

WLAN Security - Outline

- Part 1:
  - WLAN Standards and Components
  - Joining Open WLAN
  - WPA2-PSK and four-way handshake
- Part 2:
  - WPA 3: Opportunistic Wireless Encryption (Enhanced Open)
  - WPA 3: Password Authenticated Key Exchange (PAKE : Dragonfly)
- Part 3:
  - Enterprise security - EAP

WLAN Standards

- IEEE 802.11 standard defines physical and link-layer for wireless Ethernet
- Wi-Fi is an industry alliance to promote 802.11 interoperability
- Original 802.11-1997, latest 802.11-2016, many amendments
- Physical layer:
  - Uses unlicensed bands at 2.4 GHz (microwave ovens, Bluetooth) and 5 GHz
  - Up to 14 radio channels in the 2.4 GHz band, but only about 3 non-overlapping ones
- Link layer
  - Looks like Ethernet (802.3) to layers above
  - MAC protocol differs from 802.3 because one antenna cannot detect collisions while transmitting
    → explicit ACKs needed

WLAN Components

- Access point (AP) = bridge between wireless (802.11) and wired (802.3) networks
- Wireless station (STA) = PC or other device with a wireless network interface card (NIC)
  - To be precise, AP is also a STA
- Stations are identified by globally unique 48-bit MAC address
  - MAC = Medium Access Control, don't confuse with message authentication code
  - MAC address is assigned to each network interface card (NIC) by the manufacturer, which gets them from IEEE
- Infrastructure mode = wireless stations communicate only with AP
- Ad-hoc mode = no AP; wireless stations communicate directly with each other
- We will focus on infrastructure-mode WLANs

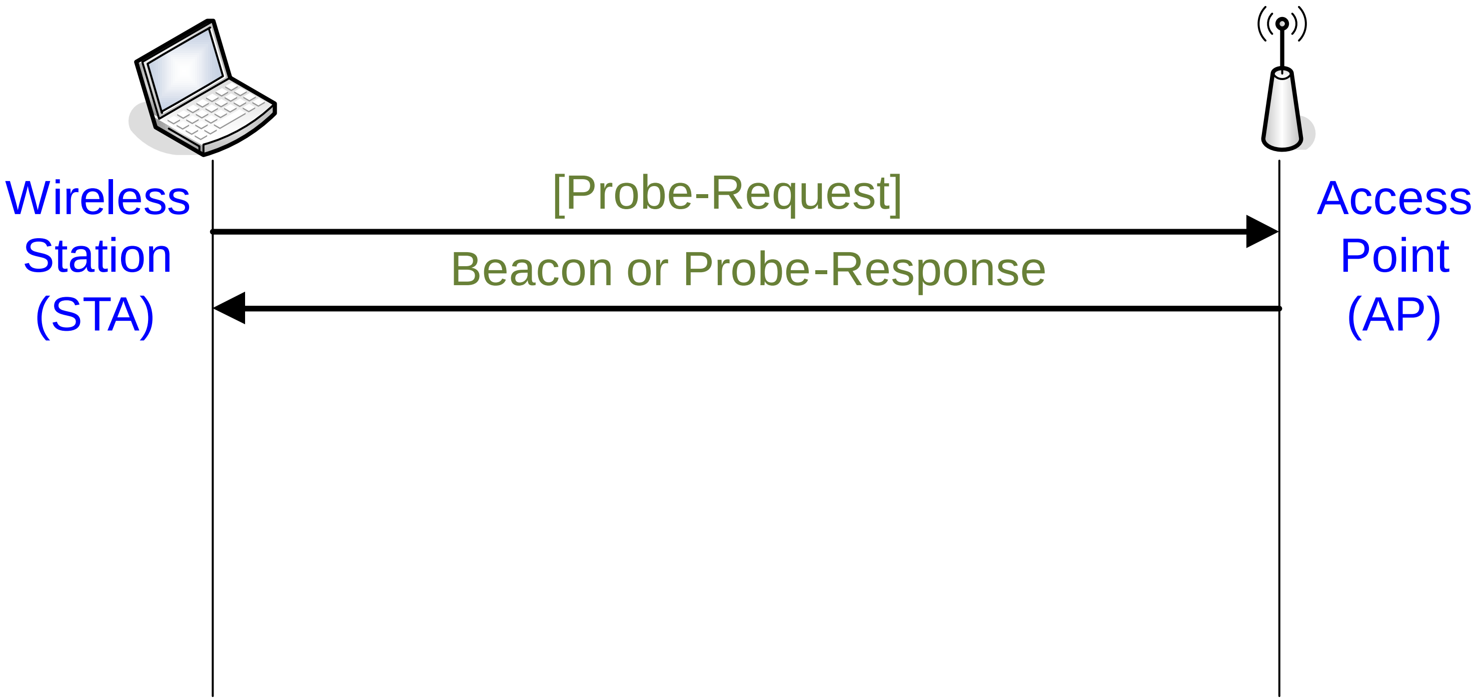
WLAN Structure

- Basic service set (BSS) = one WLAN cell (one AP + other wireless stations)
- The basic service set is identified by basic service set identifier (BSSID) = AP MAC address
- Extended service set (ESS) = multiple cells where the APs have the same service set identifier (SSID)
- The wired network is called distribution network in the standard; typically it is wire Ethernet
- APs in the same ESS can belong to the same IP network segment, or to different ones

Joining an open WLAN

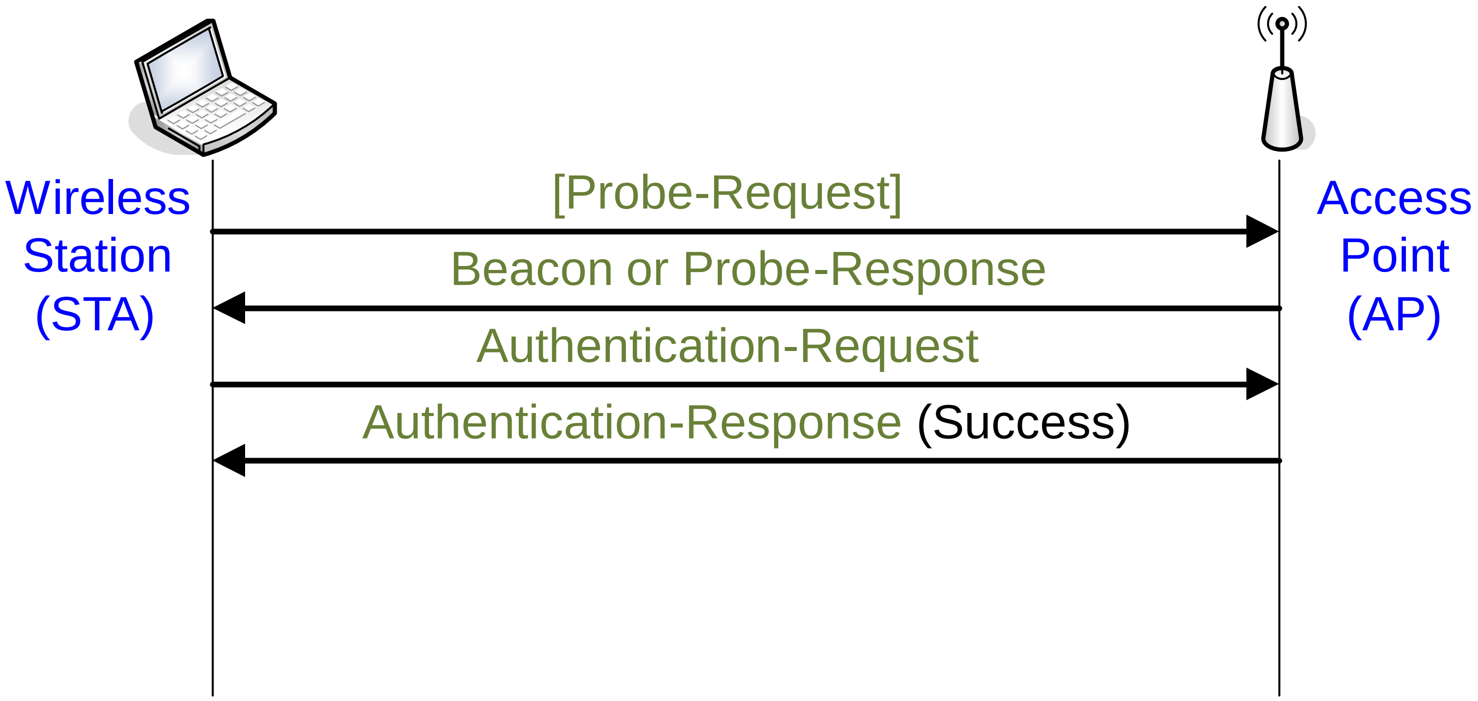
Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off



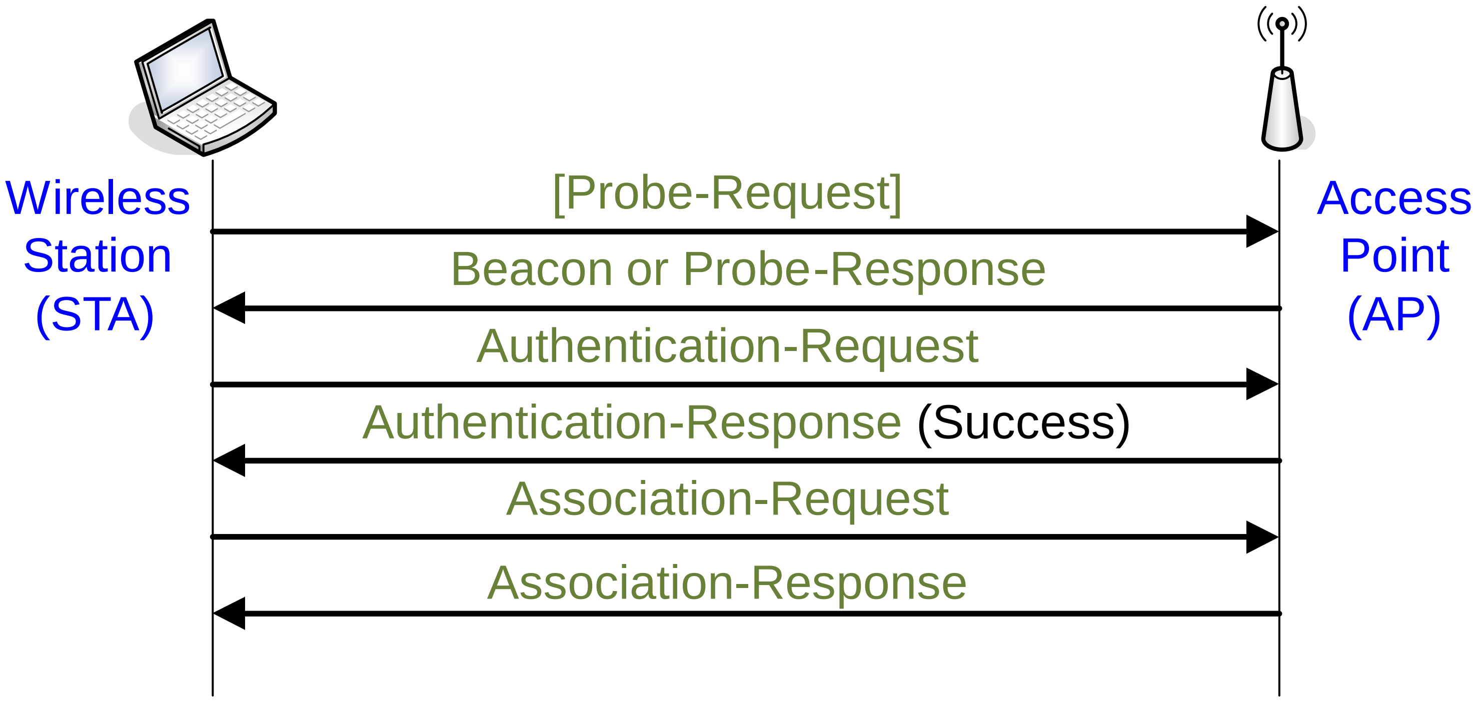
Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off



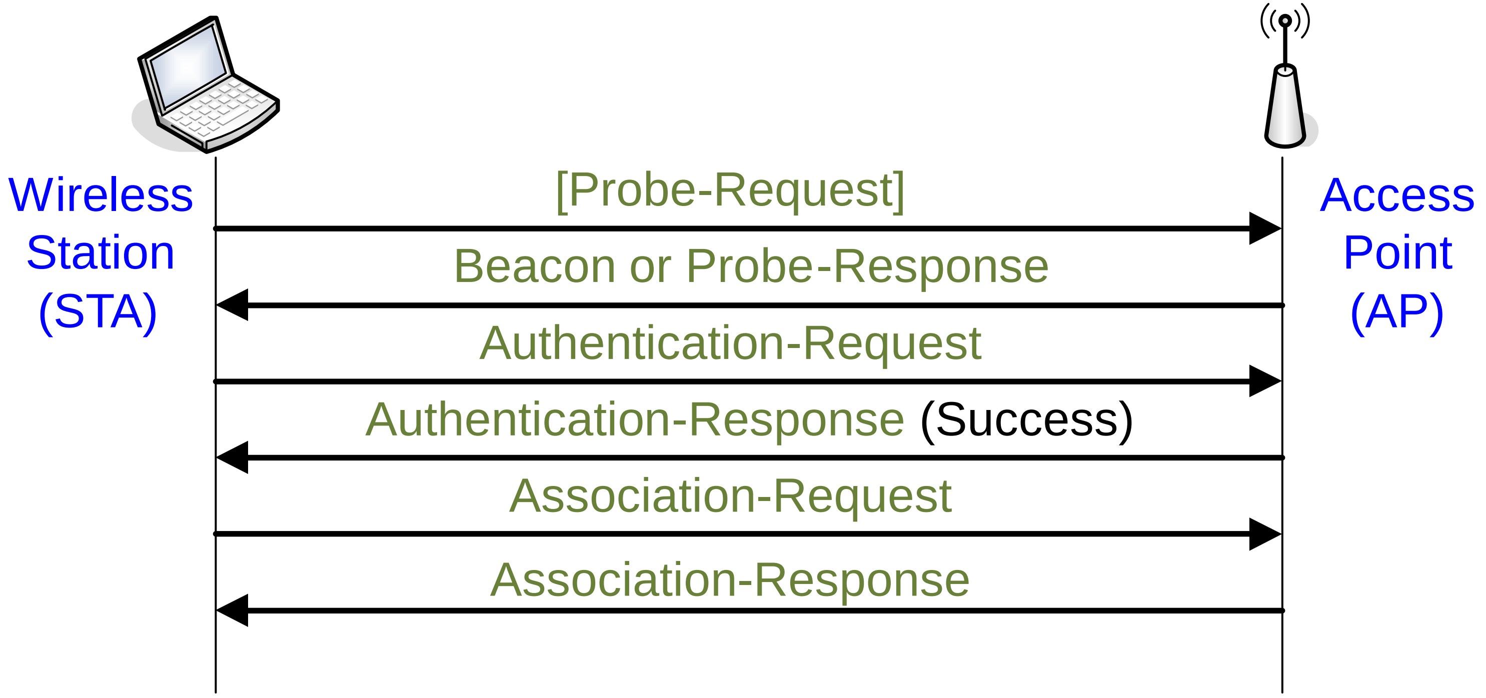
Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off



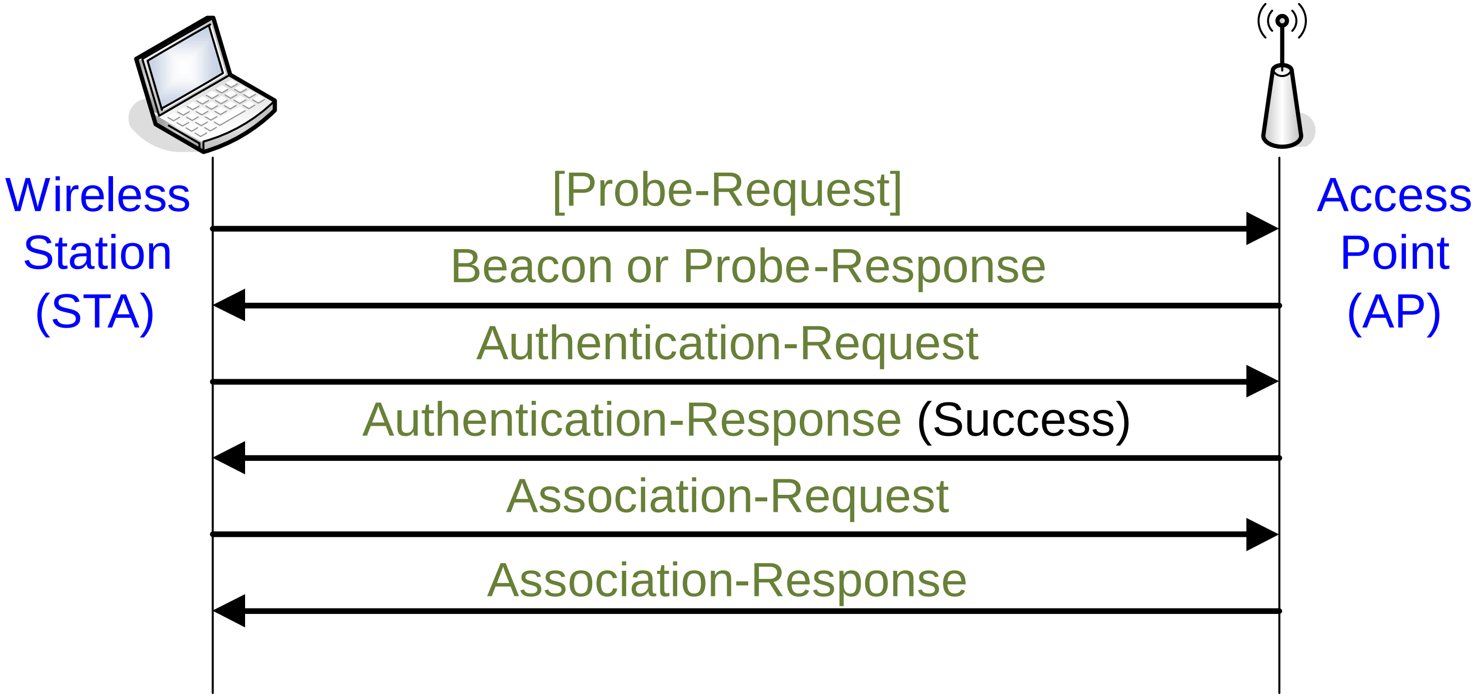
Joining an open WLAN

- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off
- STA must specify SSID to the AP in association request



Joining an open WLAN

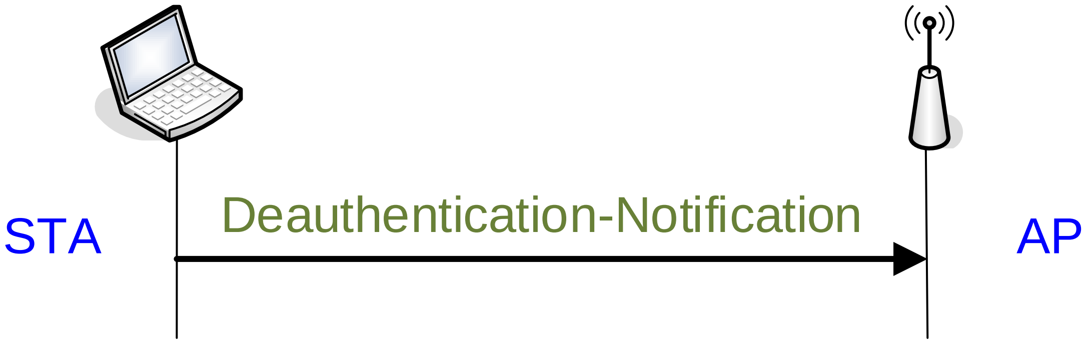
- AP sends beacons, usually every 50 ms
- Beacons usually include the SSID but broadcast can be turned off
- STA must specify SSID to the AP in association request



- Open system authentication = **no authentication**, empty authentication messages

Leaving a WLAN

- Both STA and AP can send a Disassociation Notification or Deauthentication Notification
- Include reason codes
  - – station inactivity
  - – station leaving

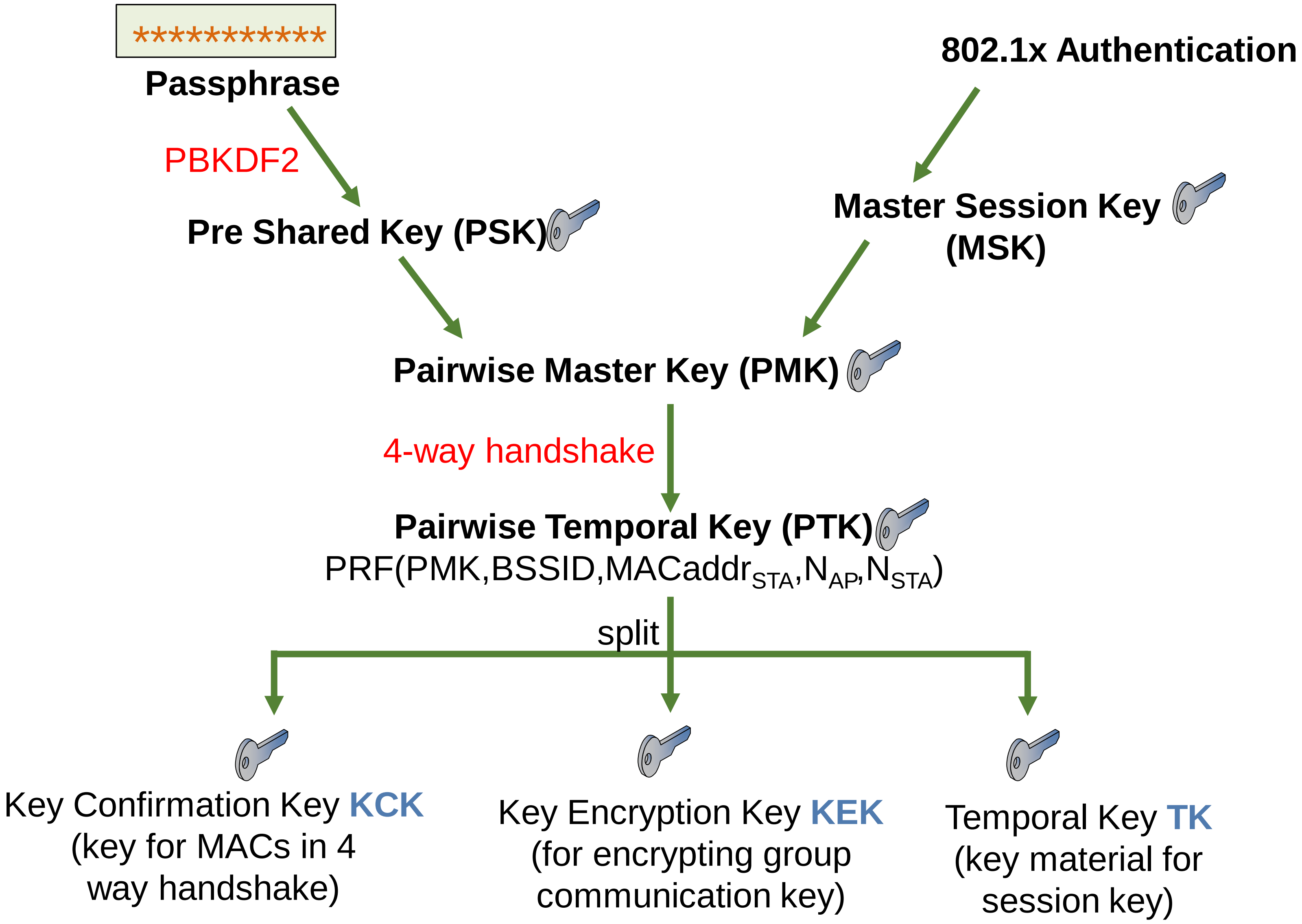


Real WLAN security: WPA2-PSK

Real WLAN Security

- **Wireless Protected Access 2 (WPA2)**
  - WPA2 is the Wi-Fi alliance name for the 802.11i amendment to the IEEE standard, which is now part of 802.11-2016
  - Robust security network (RSN) = name in the IEEE standard
  - Uses 802.1X for access control
  - Uses EAP for authentication and key exchange, eg. EAP-TLS
  - Confidentiality and integrity protocol AES-CCMP

RSN Key Hierarchy



****

Passphrase

PBKDF2

Pre Shared Key (PSK)

802.1x Authentication

Master Session Key (MSK)

Pairwise Master Key (PMK)

4-way handshake

Pairwise Temporal Key (PTK)

PRF(PMK,BSSID,MACaddr$_{STA}$,N$_{AP}$,N$_{STA}$)

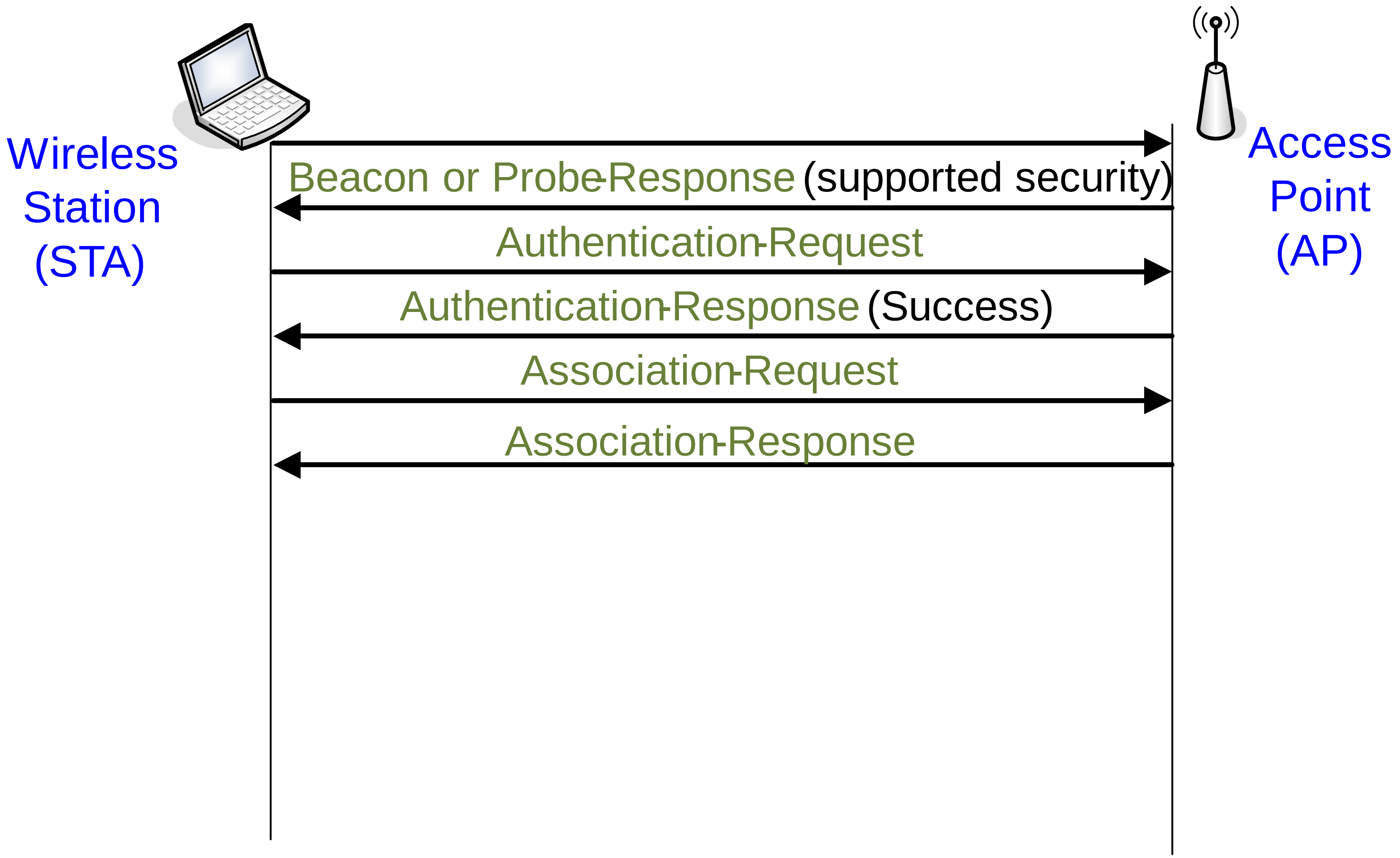
split

Key Confirmation Key **KCK**
(key for MACs in 4 way handshake)

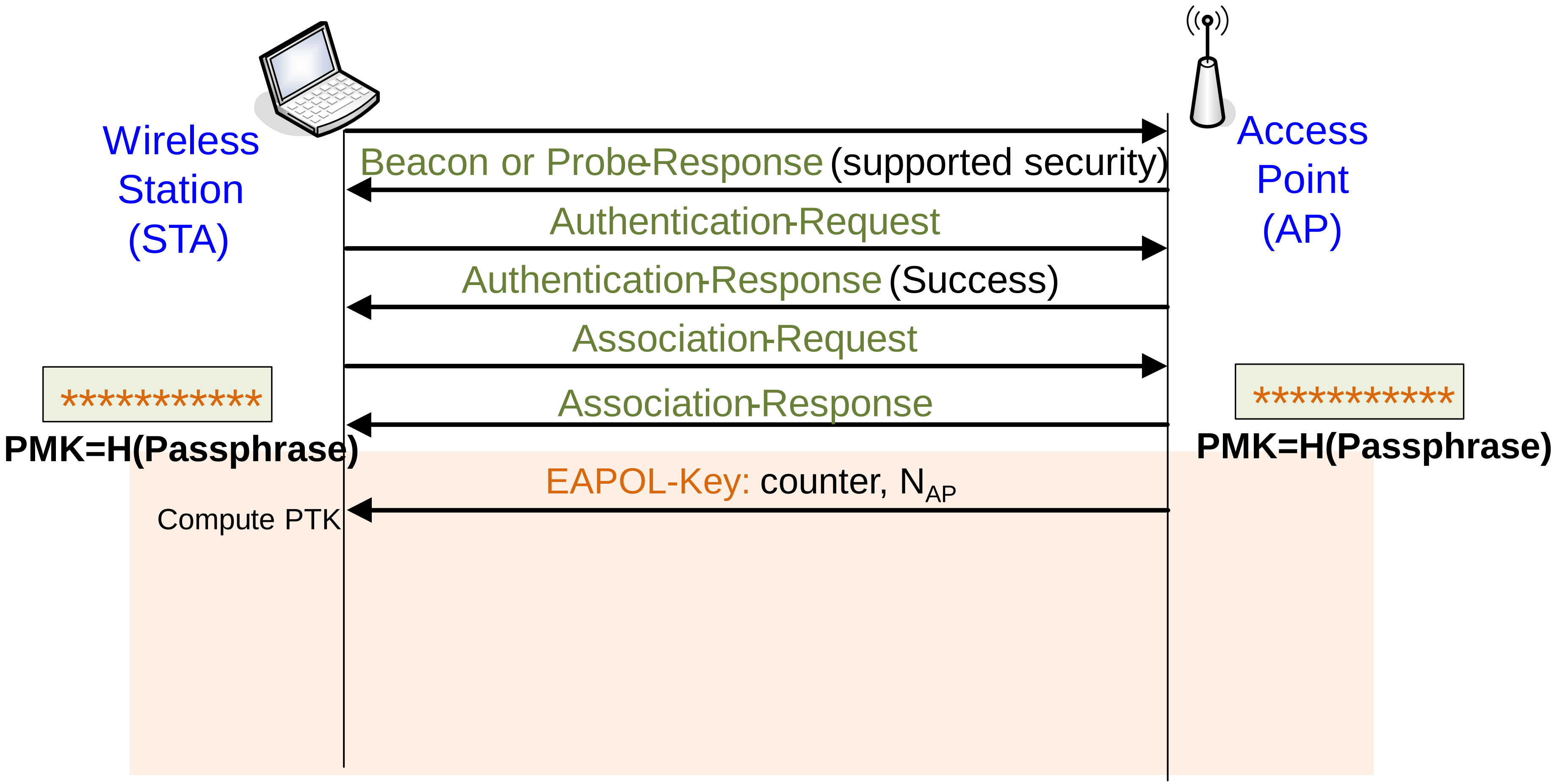
Key Encryption Key **KEK**
(for encrypting group communication key)

Temporal Key **TK**
(key material for session key)

WPA2 – Four-way handshake

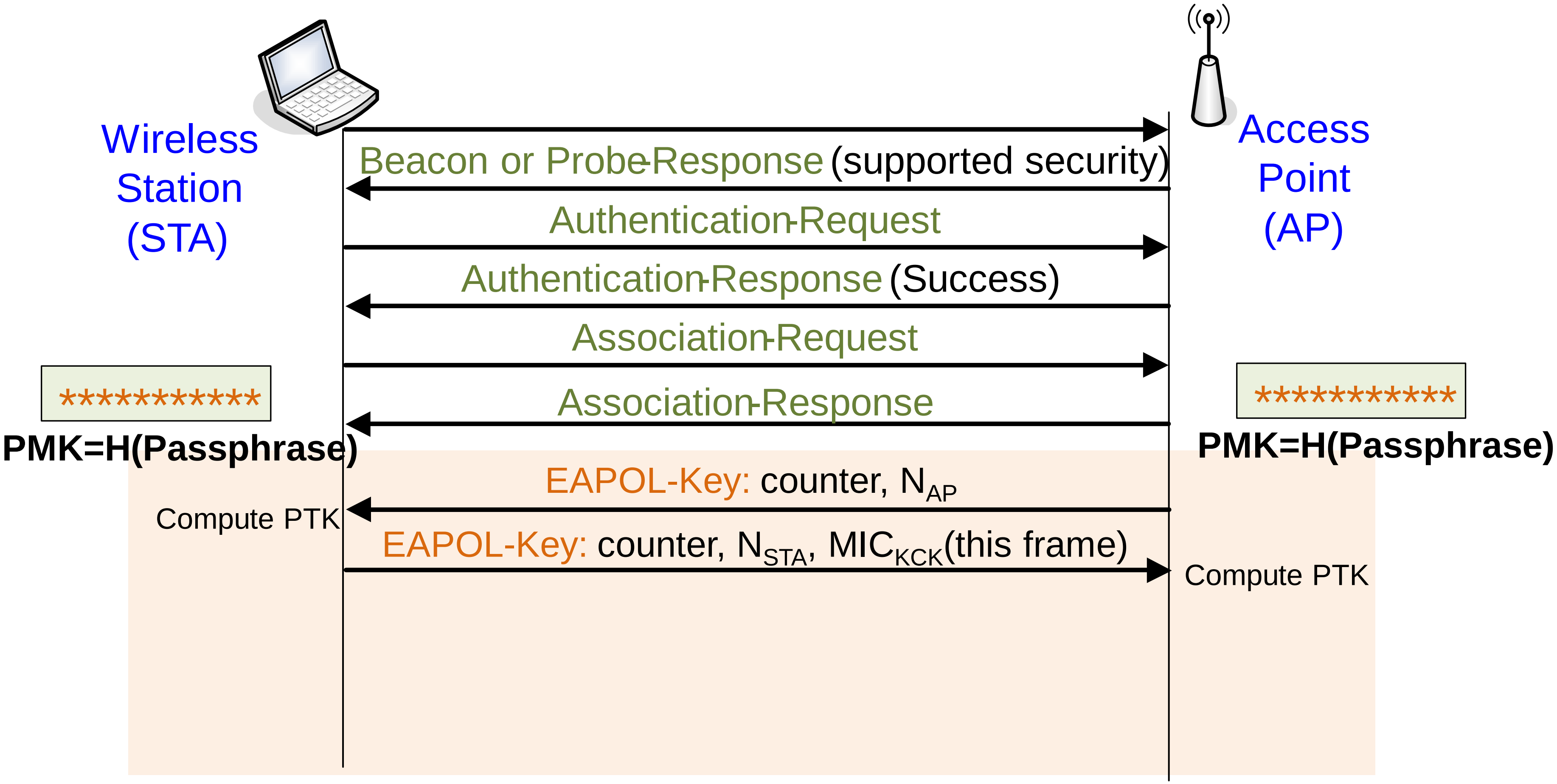


WPA2 – Four-way handshake



PMK = key derived from Passphrase/802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,MACaddr_{AP},MACaddr_{STA},N_{AP},N_{STA})
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC

WPA2 – Four-way handshake



Wireless Station (STA)

Access Point (AP)

Beacon or Probe Response (supported security)

Authentication Request

Authentication Response (Success)

Association Request

Association Response

****

PMK=H(Passphrase)

****

PMK=H(Passphrase)

EAPOL-Key: counter, N_{AP}

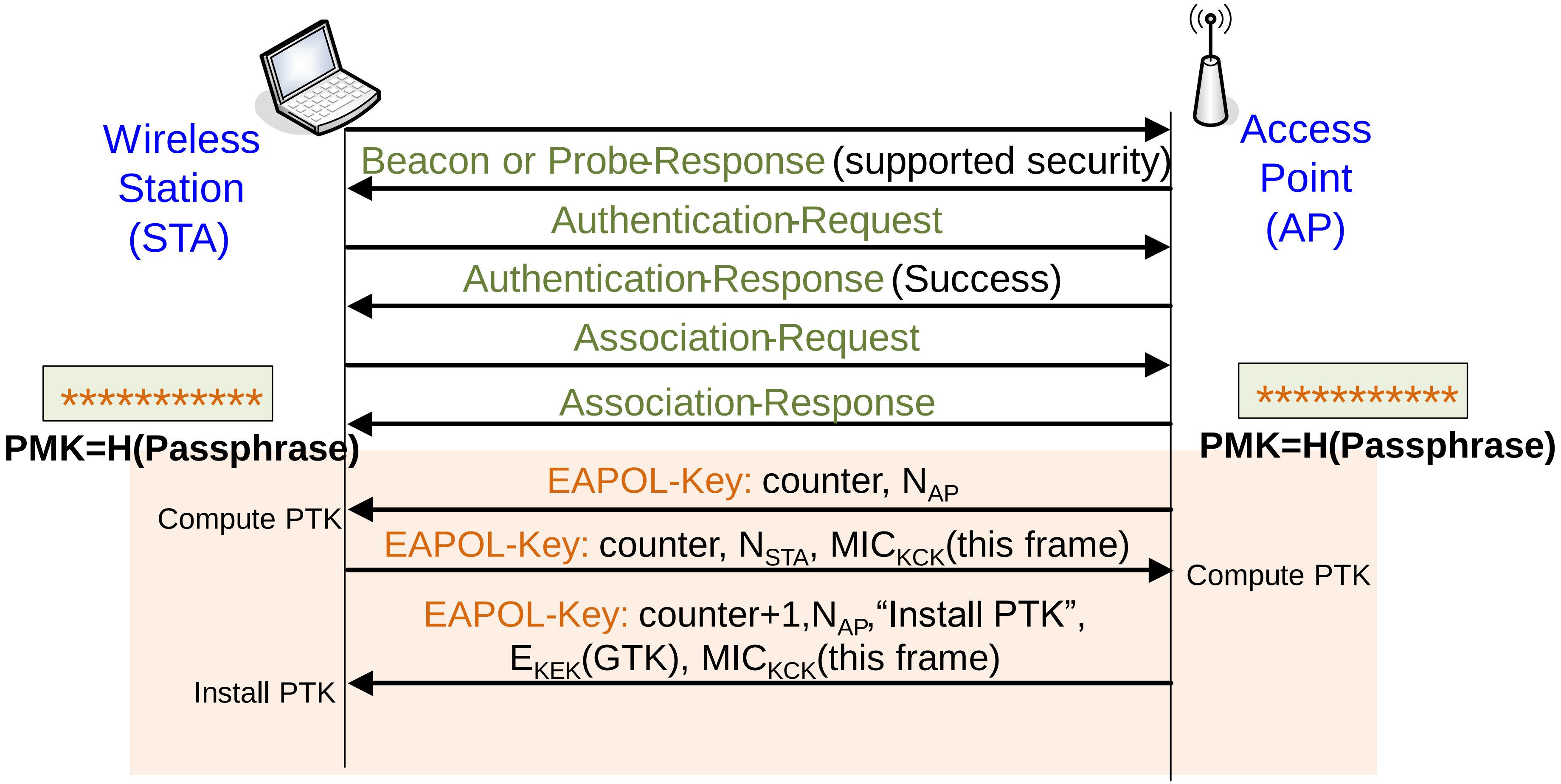
Compute PTK

EAPOL-Key: counter, N_{STA}, MIC_{KCK}(this frame)

Compute PTK

PMK = key derived from Passphrase/802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,$MACaddr_{AP}$,$MACaddr_{STA}$,N_{AP},N_{STA})
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC

WPA2 – Four-way handshake



Wireless Station (STA)

Access Point (AP)

Beacon or Probe Response (supported security)

Authentication Request

Authentication Response (Success)

Association Request

Association Response

****

PMK=H(Passphrase)

****

PMK=H(Passphrase)

EAPOL-Key: counter, N_{AP}

Compute PTK

EAPOL-Key: counter, N_{STA}, MIC_{KCK}(this frame)

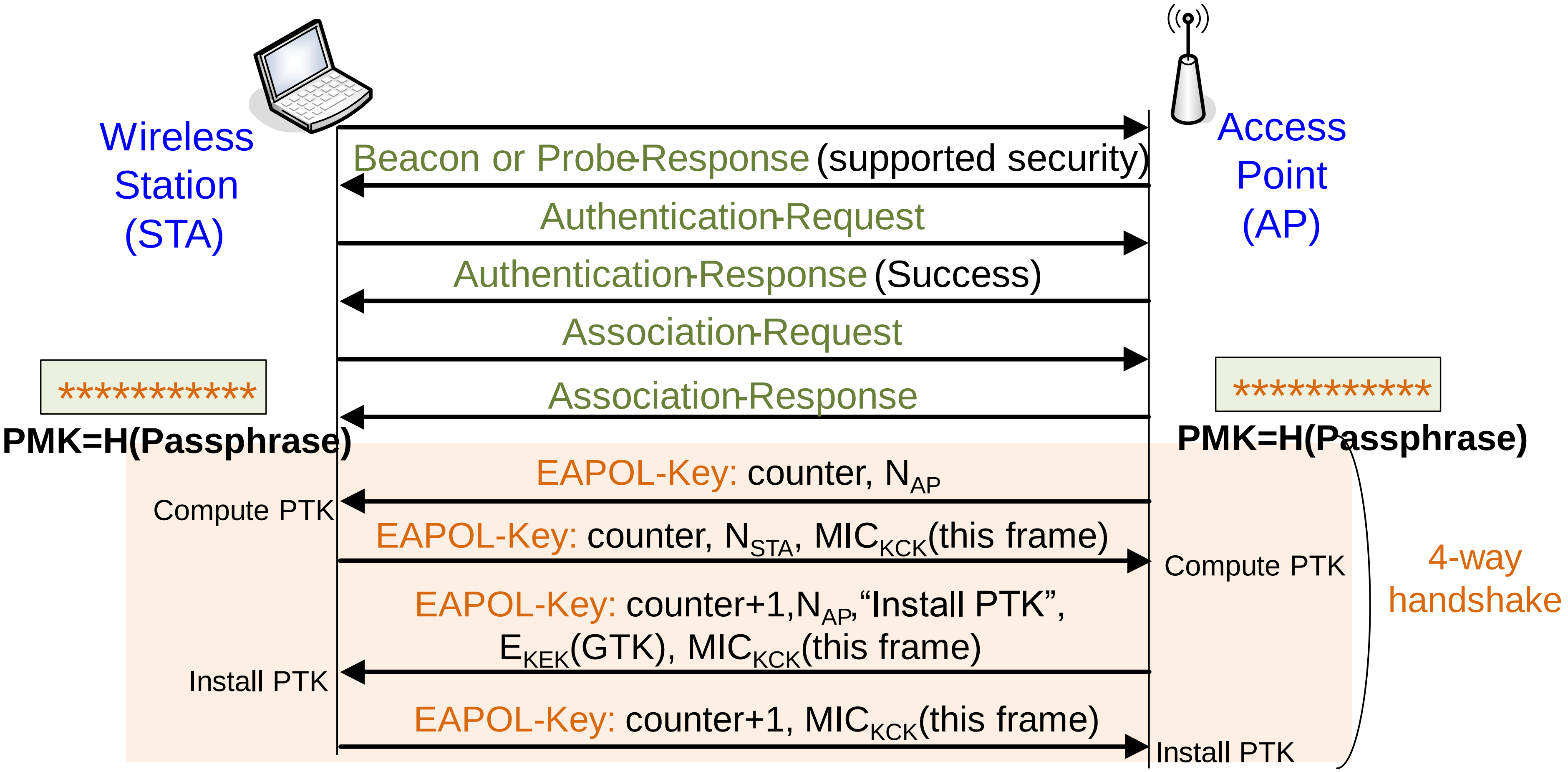
Compute PTK

EAPOL-Key: counter+1,N_{AP},“Install PTK”, E_{KEK}(GTK), MIC_{KCK}(this frame)

Install PTK

PMK = key derived from Passphrase/802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,$MACaddr_{AP}$,$MACaddr_{STA}$,N_{AP},N_{STA})
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC

WPA2 – Four-way handshake



Wireless Station (STA)

Access Point (AP)

Beacon or Probe-Response (supported security)

Authentication-Request

Authentication-Response (Success)

Association-Request

Association-Response

****

PMK=H(Passphrase)

****

PMK=H(Passphrase)

EAPOL-Key: counter, N_{AP}

Compute PTK

EAPOL-Key: counter, N_{STA}, MIC_{KCK}(this frame)

Compute PTK

EAPOL-Key: counter+1,N_{AP},“Install PTK”, E_{KEK}(GTK), MIC_{KCK}(this frame)

Install PTK

EAPOL-Key: counter+1, MIC_{KCK}(this frame)

Install PTK

4-way handshake

PMK = key derived from Passphrase /802.1x auth
counter = replay prevention, reset for new PMK
PRF = pseudo-random function
PTK = PRF(PMK,$MACaddr_{AP}$,$MACaddr_{STA}$,N_{AP},N_{STA})
KCK, KEK = parts of PTK
MIC = message integrity check, a MAC

Next Video

- Part 2:
  - WPA 3: Opportunistic Wireless Encryption (Enhanced Open)
  - WPA 3: Password Authenticated Key Exchange (PAKE : Dragonfly)
- Part 3:
  - Enterprise security - EAP