Network Security: WLAN Security

Tuomas Aura

Outline

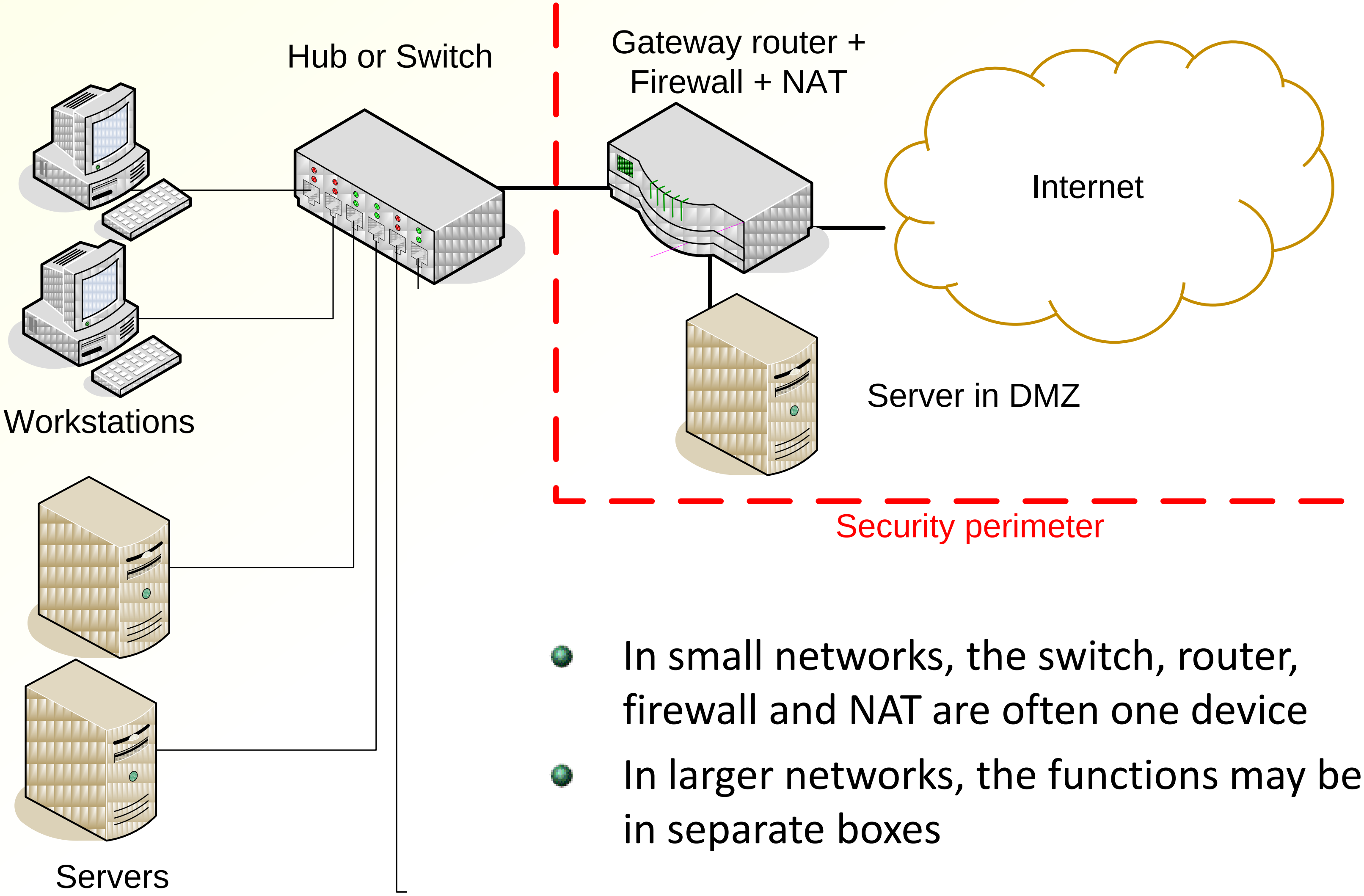
- Wireless LAN technology
- Threats against WLANs
- Weak security mechanisms and WEP
- 802.1X, WPA, 802.11i, WPA2
- WLAN mobility

Wireless LAN technology

Wireless LAN (WLAN) standards

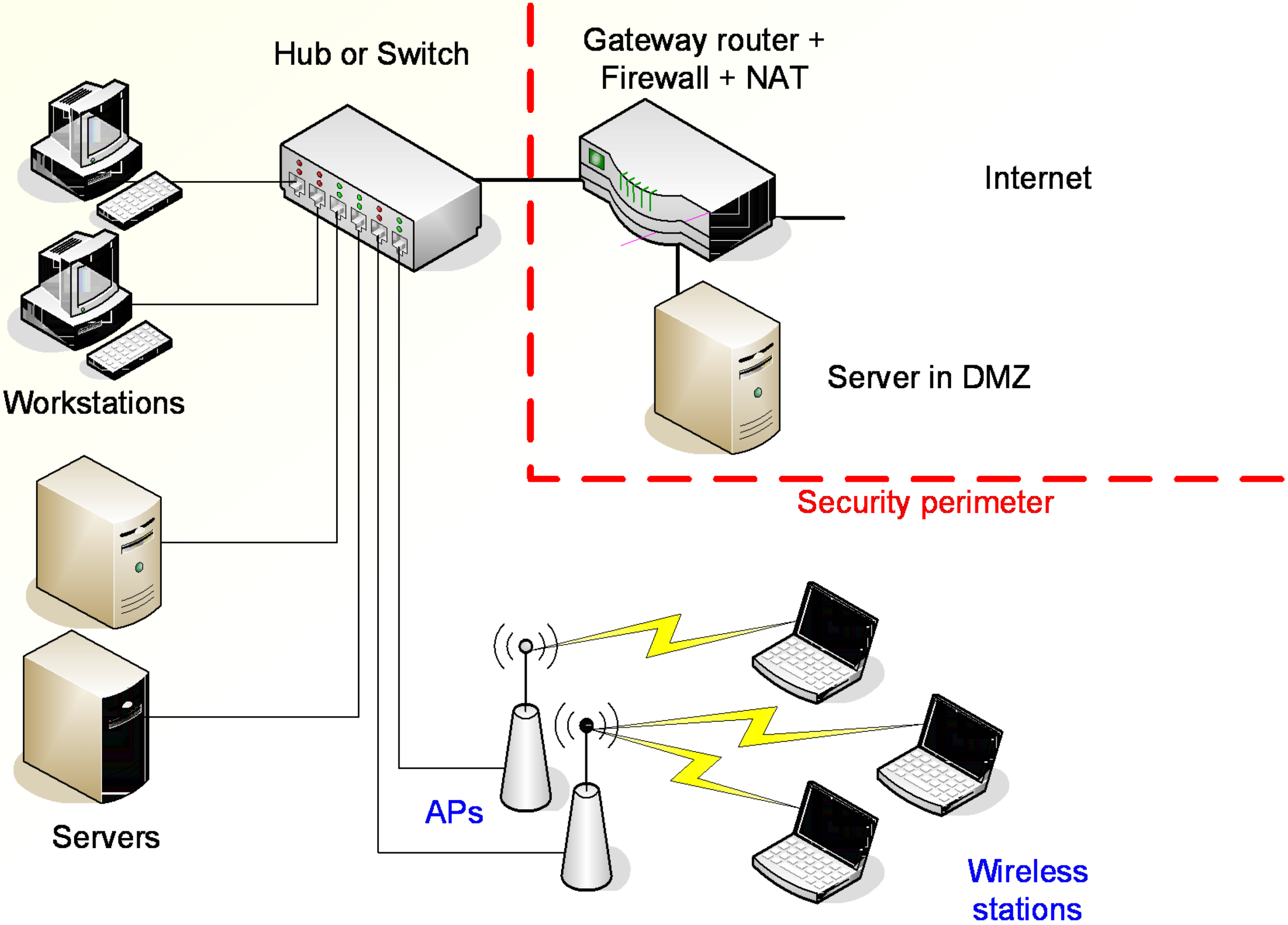
- IEEE 802.11 standard defines physical and link layers for wireless Ethernet LANs
- Wi-Fi is an industry alliance to promote 802.11 interoperability
- Original 802.11-1997, 802.11-2007, 802.11n
- Stations identified by 48-bit MAC addresses
  - Globally unique MAC address assigned to each NIC by the manufacturer

Small-business LAN



- In small networks, the switch, router, firewall and NAT are often one device
- In larger networks, the functions may be in separate boxes

Small-business WLAN



Wireless LAN components

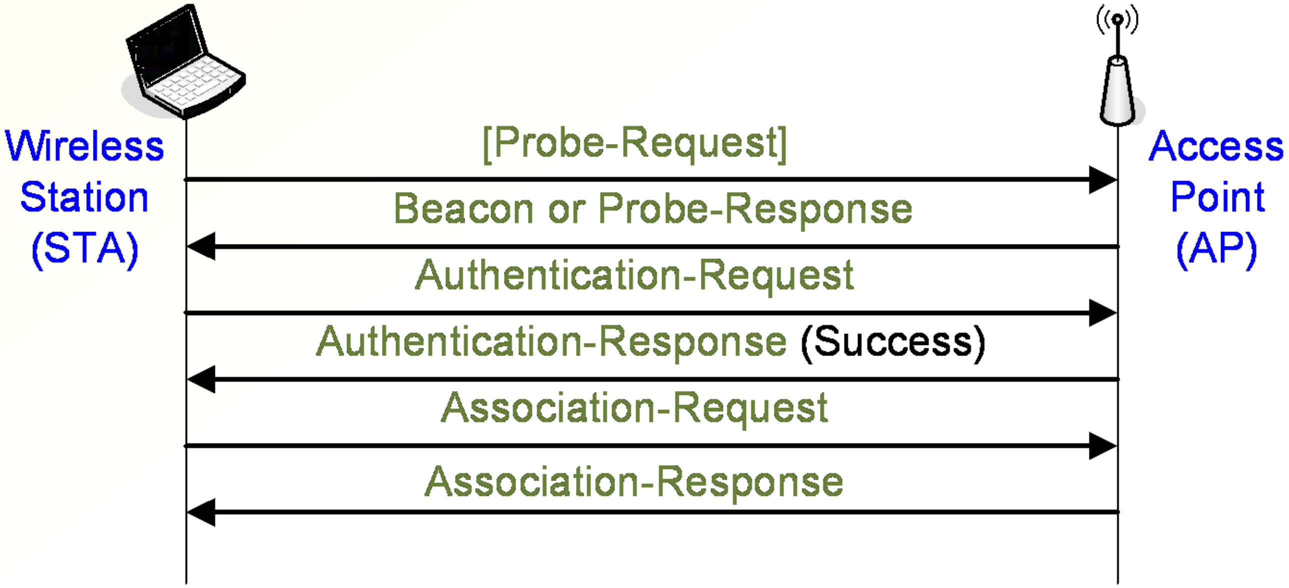
- Access point (AP) = bridge between wireless (802.11) and wired (802.3) networks
- Wireless station (STA) = PC or other device with a wireless network interface card (NIC)
- Infrastructure mode = wireless stations communicate only with AP
- Ad-hoc mode = no AP; wireless stations communicate directly with each other
- We will focus on infrastructure-mode WLANs

Wireless LAN structure

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

Joining a wireless LAN

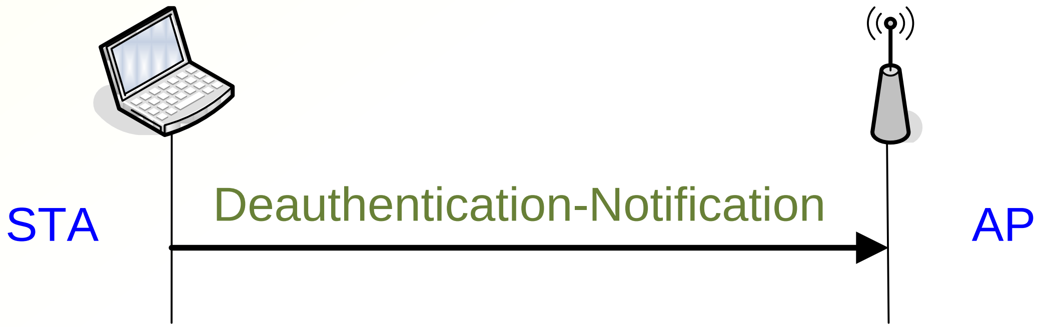
- AP sends beacons, usually every 50-100 ms
- Beacons usually include the SSID but the SSID broadcast can be turned off
- STA must specify SSID to the AP in association request



- Open System authentication = no authentication, empty messages

Leaving a wireless LAN

- Both STA and AP can send a Disassociation Notification or Deauthentication Notification



Threats against WLANs

Exercise: WLAN threat analysis

- List as many threats against wireless LANs as you can think of. What kind of unwanted things can happen?
  - Consider home, small-business, corporate and university networks, Internet cafes and commercial hotspot operators
- Prioritize the threats roughly by how serious they are. Which threats can be ignored and which not?

Wireless LAN threats

- Signal interception — sniffing
- Unauthorized network access — access to intranet or Internet access without payment
- Access-point misconfiguration
- Unauthorized APs — unauthorized ingress routes may bypass firewall
- Denial of service — logical attacks with spoofed signaling, signal jamming
- AP spoofing — stronger signal attracts STAs

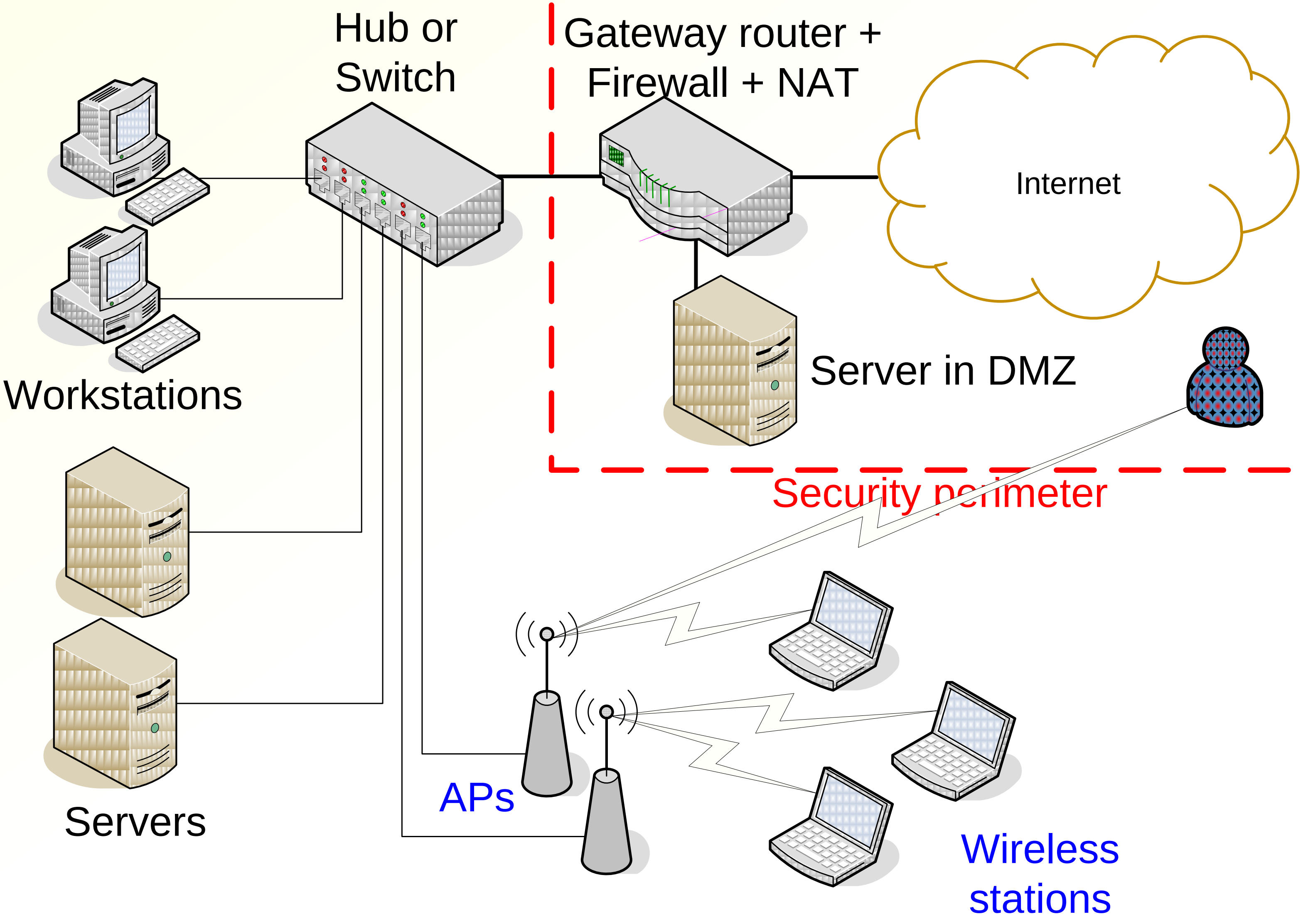
Signal interception

- The radio signal is not confined to a physical building → Attacker can sniff traffic outside the building, e.g. in the parking lot
- Directional high-gain antenna can intercept WLAN signal from hundreds of meters away

Unauthorized network access

- Discussion:
  - Would you mind your neighbors accessing your home AP?
  - Would a university, a company or a commercial WLAN AP operator want to control access?
- Wardriving:
  - Hobbyists drive around the city looking for open hotspots and create maps of open WLANs that can be used for Internet access
  - Tools: http://www.wardrive.net/wardriving/tools/

Attacker in a small-business WLAN



AP configuration

- Many different ways to configure access points:
  - Web page (home equipment)
  - SNMP (professional equipment)
  - serial cable
  - Telnet
- Default passwords — hackers can change the configuration or replace firmware
- Hub broadcasts — AP connected to a hub leaks wired-to-wired traffic

Unauthorized access points

- Unauthorized access points installed by employees are often badly administered:
  - No access control enabled; anyone can connect
  - Direct access to the intranet behind firewall

→ Attacker can use unauthorized APs as an ingress route

- Solutions:
  - Sweeps: walk or drive around premises and look for AP beacons — now a standard corporate practice
  - Scan for AP SNMP and web interfaces
- Similar to unauthorized modems

Denial of service

- Logical attacks:
  - Spoofed deauthentication or disassociation message causes the AP or STA to lose state
- AP capacity exhaustion:
  - Typical AP handles data fast but association and authentication slower → flood AP with false authentications to prevent honest nodes from associating
- Radio jamming:
  - Either jam the who radio channel or selectively break some frames

AP spoofing

- Clients are configured to associate automatically with APs that advertise specific SSIDs
- Attack: fake AP broadcasts cyclically all known hotspot, hotel, airport and big-company SSIDs

  → clients will associate with it automatically thinking they are at the hotspot
  → easy MitM attack on all IP packets

WLAN security goals

- Wireless LAN security protocols have following goals:
  - Data confidentiality and integrity — prevent sniffing and spoofing of data on the wireless link
  - Access control — allow access only for authorized wireless stations
  - Accounting — hotspot operators may want to meter network usage
  - Authentication — access control and accounting usually depend on knowing the identity of the wireless station or user
  - Availability — do not make denial-of-service attacks easy (radio jamming is always possible)
- Not all problems have been solved

Weak security mechanisms and WEP

Discussion: common recommendations

- The following security measures are often recommended to WLAN administrators:
  - Disable the SSID broadcast
  - Maintain a list of authorized MAC addresses and block unauthorized ones from the network
  - Select AP locations in the middle of the building (not close to windows), use directional antennas and line walls and windows with metal foil to minimize the signal leakage to the outside of the building
- How much security do these measures bring?
- How expensive are they?

Weak WLAN security mechanisms

- Disabling the SSID broadcast — attacker can sniff the SSID when other clients associate
- ACL of authorized MAC addresses — attacker can sniff and spoof another client's MAC address
- AP locations, directional antennas and metal foil to keep signal inside a building — attacker can use a directional antenna with high gain

→ Weak mechanisms are rarely worth the trouble

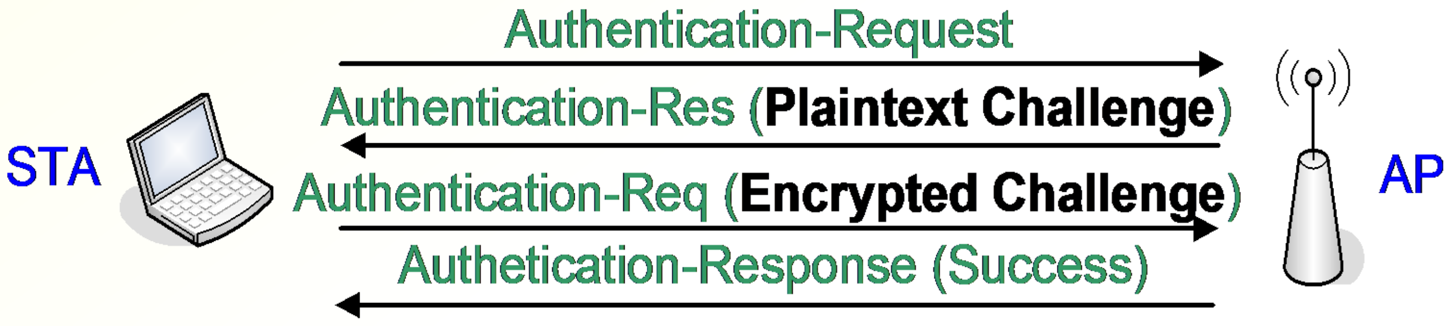
WEP encryption

- In original 802.11-1997 standard, no longer is use
- WEP = Wired Equivalent Privacy;
  goal was security equivalent to a wired LAN
- Encryption and integrity check for data frames;
  management frames unprotected
- RC4 stream cipher with a static 40-bit pre-shared key and 24-bit initialization vector

  (128-bit WAP = 104-bit key + 24-bit IV)
- Integrity check value (ICV) =
  CRC checksum encrypted with RC4
- Multiple cryptographic weaknesses make WEP vulnerable to attacks; now gives no security

802.11 shared-key authentication

- Alternative to open-system authentication in 802.11-1997, never really used
- AP authenticates STA: STA encrypts a challenge with the WEP algorithm and preshared key


Authentication-Request
Authentication-Res (Plaintext Challenge)
STA
Authentication-Req (Encrypted Challenge)
AP
Authetication-Response (Success)

- Unidirectional entity authentication only; no connection to message authentication
- AP may require WEP encryption and authentication or only one of them

WEP security weaknesses

- 40-bit keys → brute-force cracking
- Static keys → cannot change keys often
- 24-bit IV → IV reuse; dictionary attack; all IV values exhausted in 5 hours or less on a busy AP
- IV generation not specified → reuse possible even earlier
- CRC+RC4 for ICV → possible to modify data
- No protection for management frames → disassociation and deauthentication attacks
- Authentication not bound to the session → man-in-the-middle and replay attacks
- Authentication based on RC4 → attacker learns key stream and can spoof responses
- Weak IV attacker against RC4 → cracking of 104-bit WEP keys

Need for Link-Layer Security?

- Wireless LAN security protocols provide link-layer security only; not end-to-end protection

  → Good for corporate APs, access control to LAN

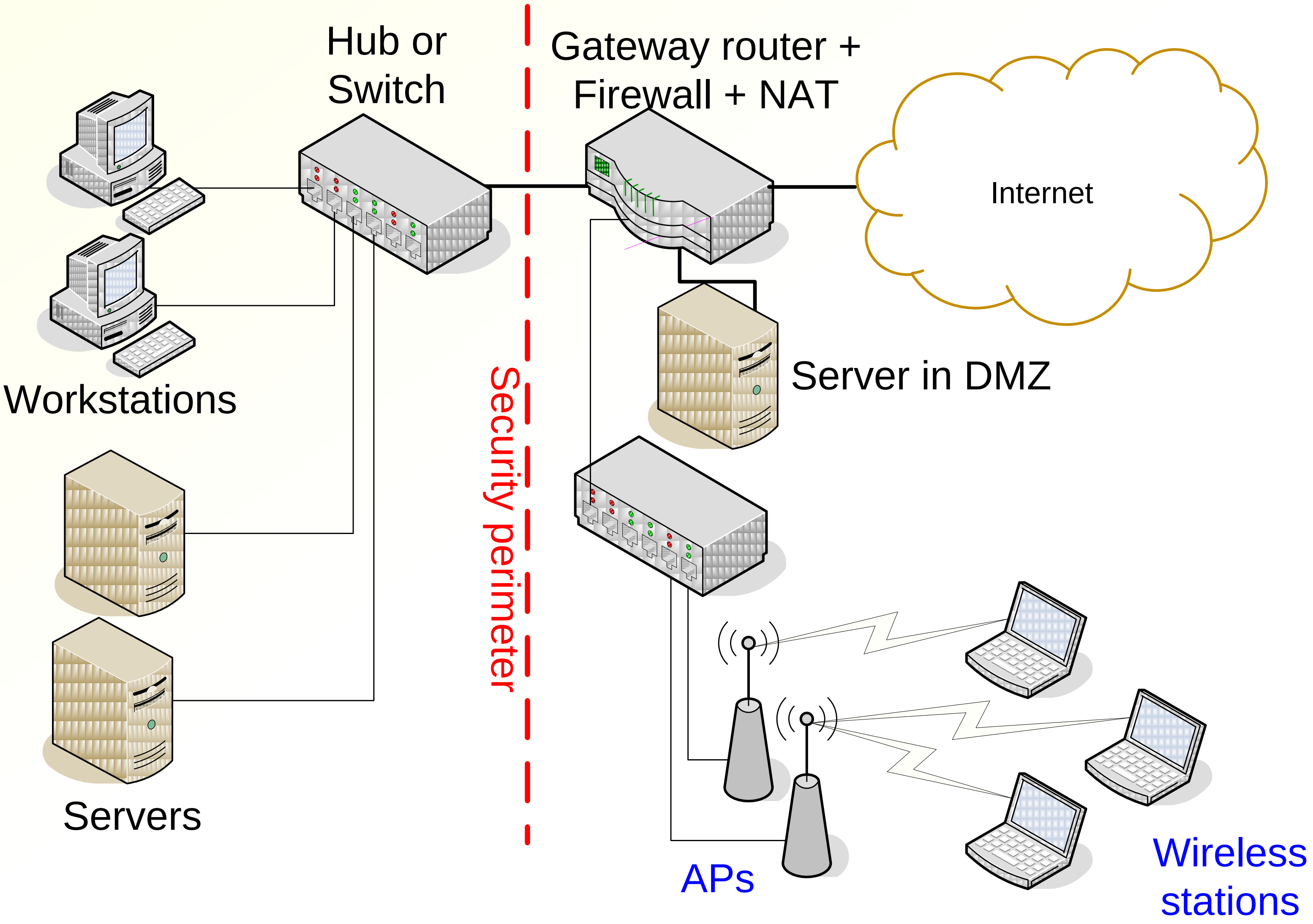
  → Good for commercial WLAN operators, access control for paying customers

  → Irrelevant for road warriors at wireless hotspots and at other untrusted networks

- Alternative: treat WLAN as insecure and use end-to-end security, such as IPSec or VPN

  e.g. Aalto vs. Aalto Open

Alternative Architecture



Need for WLAN Access Control?

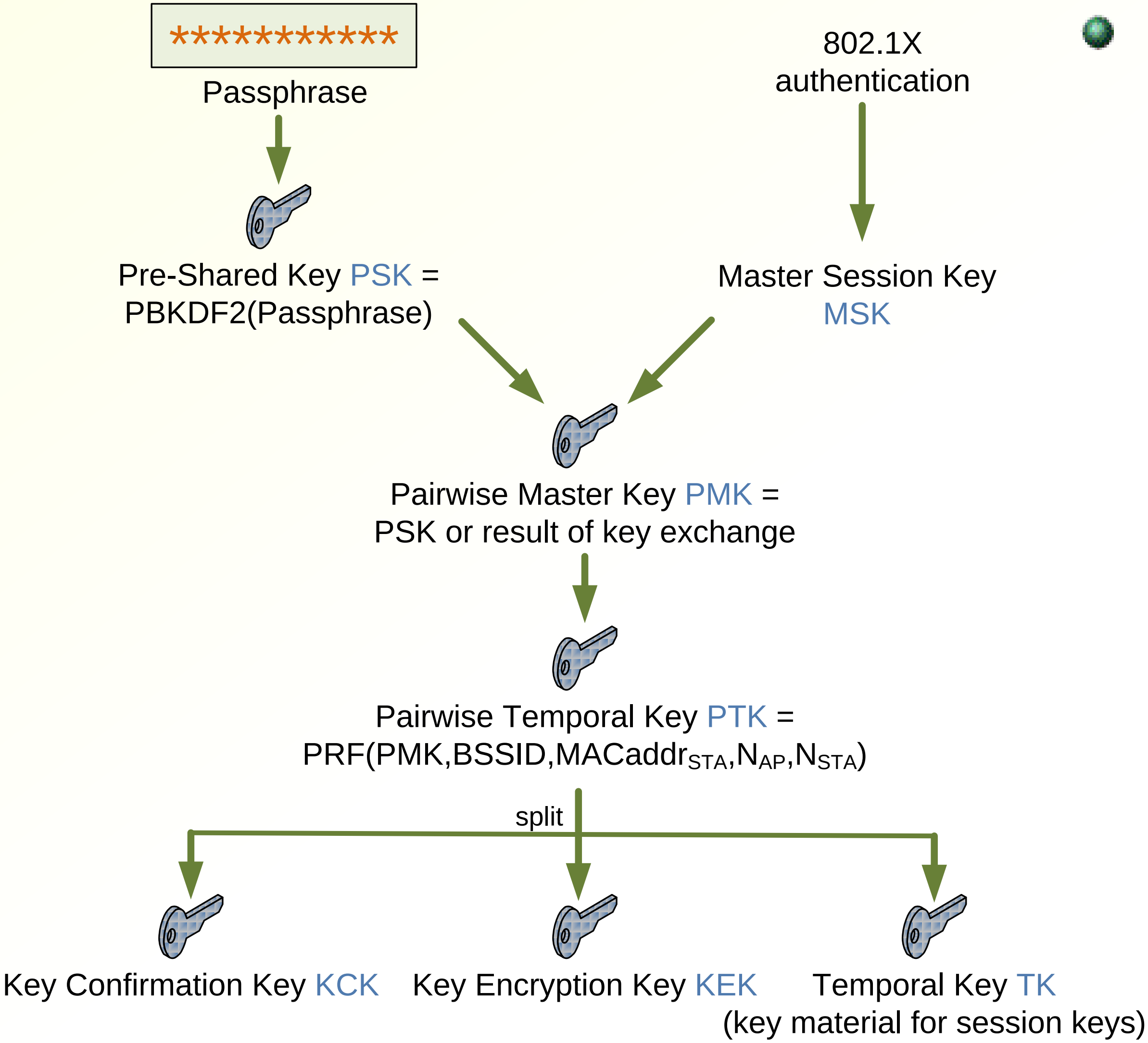
- Arguments for controlling access:
  - Open WLAN allows hackers to access the corporate or home LAN; firewall protection bypassed;
    "like having an Ethernet socket in the parking lot"
  - Unauthorized users consume network resources without paying
  - Contract with ISP may not allow open APs
  - Liability issues if the unauthorized users send spam or access illegal content
- Arguments for open access:
  - Good service for customers and visitors
  - End-to-end security needed anyway
  - Little lost by giving away excess bandwidth; authorized users can be given better QoS
- New access points and virtual LANs (VLAN) allow combination of the two on the same equipment

802.1X, WPA, WPA2

Real WLAN security mechanisms

- Wireless Protected Access 2 (WPA2)
  - WPA2 is the Wi-Fi alliance name for the 802.11i amendment to the IEEE standard, now part of 802.11-2007
  - 802.11i name robust security network (RSN)
  - 802.1X for access control
  - EAP authentication and key exchange, eg. EAP-TLS
  - New confidentiality and integrity protocols TKIP and AES-CCMP
  - Requires new hardware for AES
- Wireless Protected Access (WPA)
  - Defined by Wi-Fi alliance; available before the 11i standard
  - 802.1X; EAP-TLS
  - Supports only TKIP encryption = RC4 with frequently changing keys and other enhancements
  - Firmware update to older AP or NIC often sufficient

802.11i key hierarchy



****

Passphrase

802.1X
authentication

Pre-Shared Key PSK =
PBKDF2(Passphrase)

Master Session Key
MSK

Pairwise Master Key PMK =
PSK or result of key exchange

Pairwise Temporal Key PTK =
PRF(PMK,BSSID,MACaddr$_{STA}$,N$_{AP}$,N$_{STA}$)

split

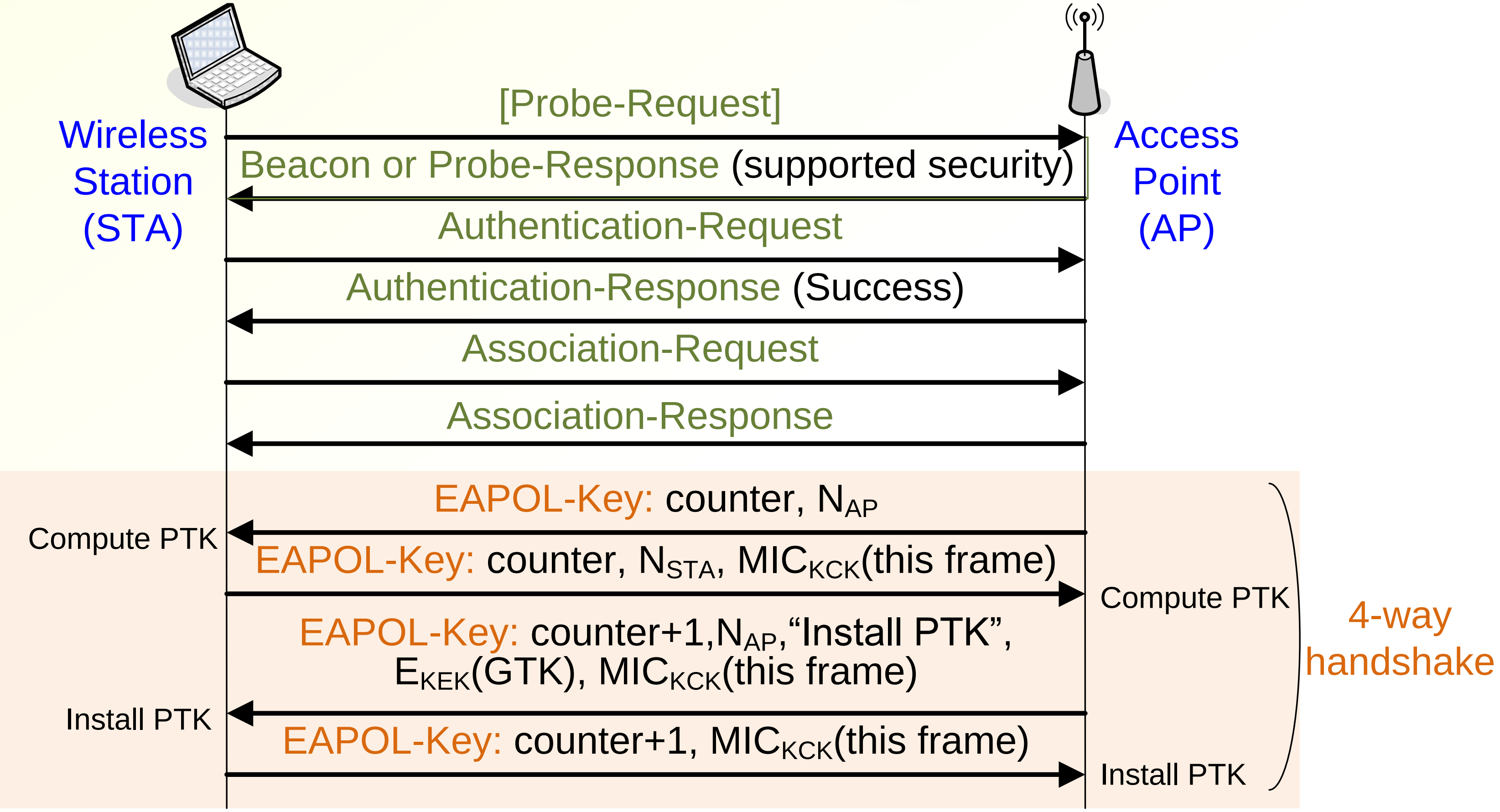
Key Confirmation Key KCK

Key Encryption Key KEK

Temporal Key TK
(key material for session keys)

- Two alternative ways of obtaining keys:
  - Preshared key (PSK) authentication= WPA2-PSK = WPA2-Personal
  - 802.1X authentication= WPA2-EAP = WPA2-Enterprise
  - Difference to WPA-* only in minor details and algorithms

WPA2-PSK and 4-way handshake



Wireless Station (STA)

Access Point (AP)

[Probe-Request]

Beacon or Probe-Response (supported security)

Authentication-Request

Authentication-Response (Success)

Association-Request

Association-Response

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

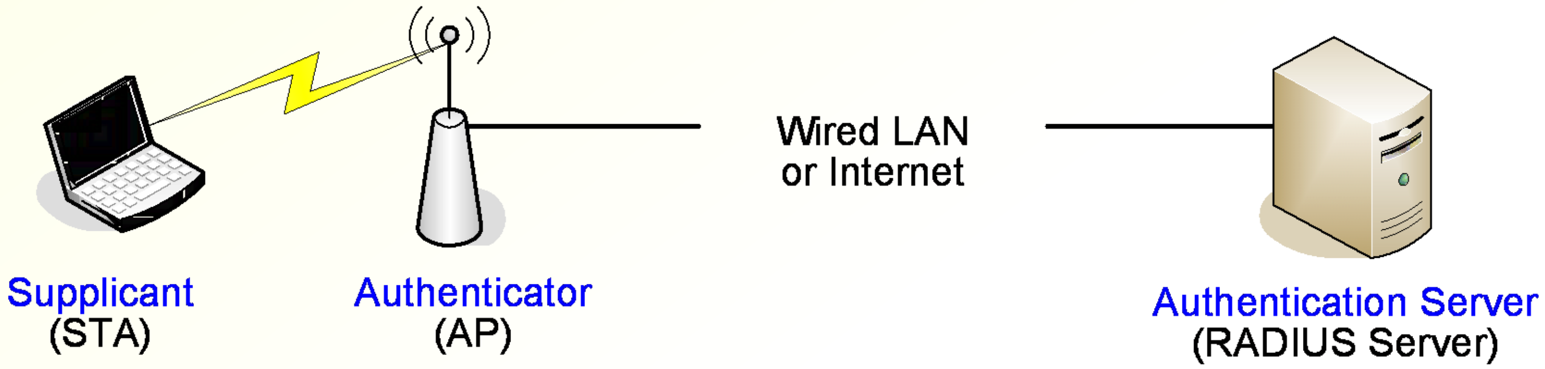
4-way handshake

PMK = key derived from Passphrase
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
GTK = Group Temporal Key

IEEE 802.1X

- Port-based access control — originally intended for enabling and disabling physical ports on switches and modem banks
- Conceptual controlled port at AP
- Uses Extensible Authentication Protocol (EAP) to support many authentication methods;
  usually EAP-TLS
- Starting to be used in Ethernet switches, as well

802.11/802.1X architecture

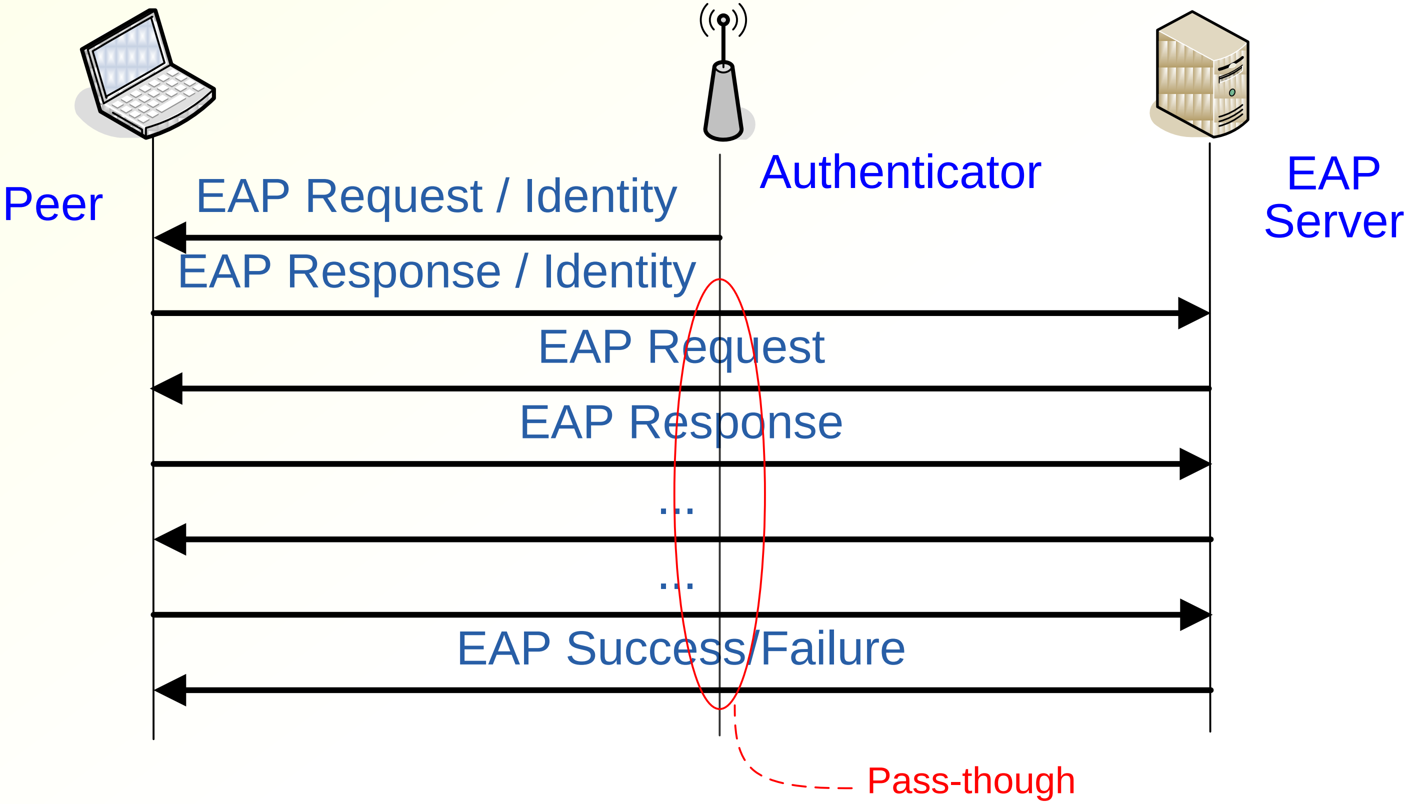


- Supplicant wants to access the wired network via the AP
- Authentication Server (AS) authenticates the supplicant
- Authenticator enables network access for the supplicant after successful authentication

EAP

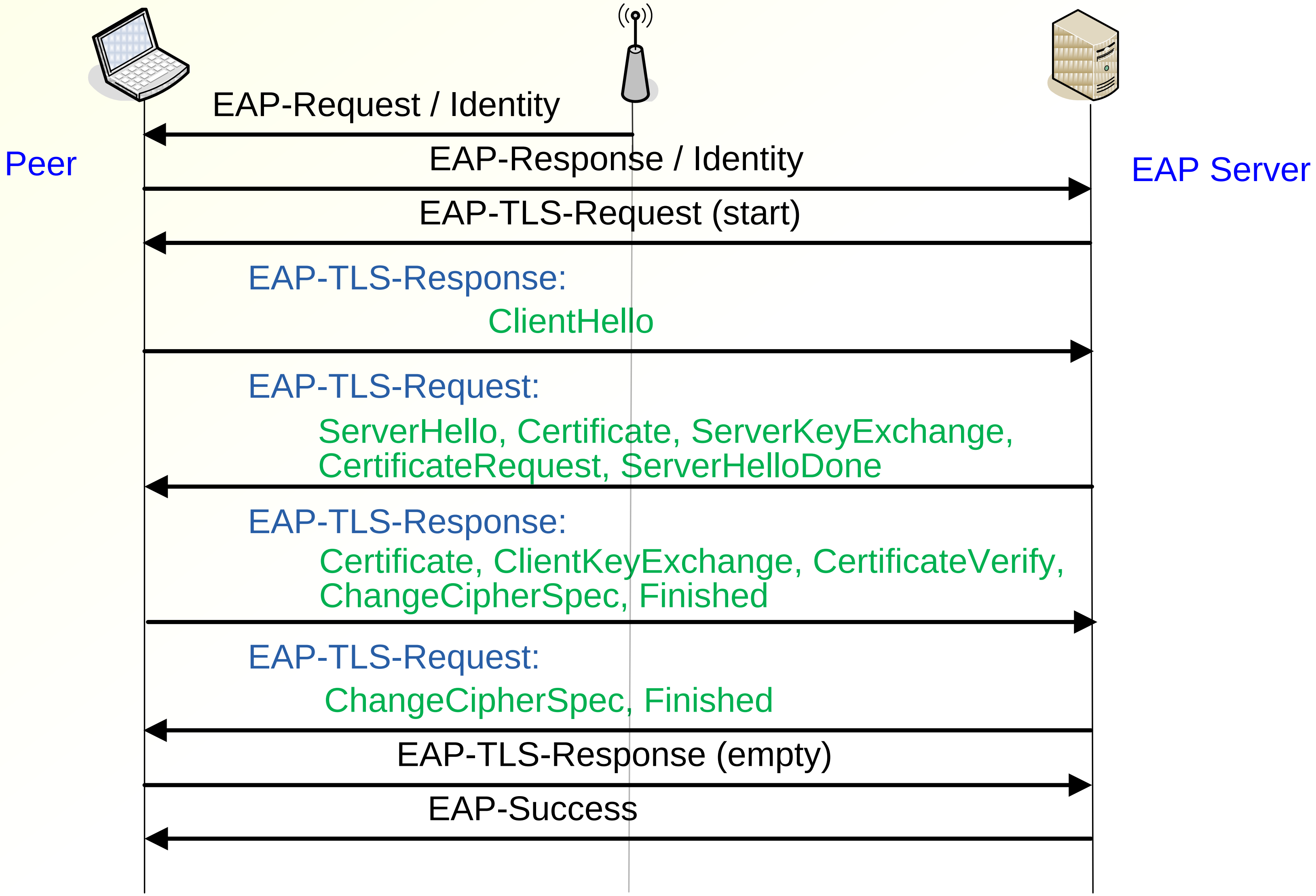
- Extensible authentication protocol (EAP) defines generic authentication message formats: Request, Response, Success, Failure
- Originally designed for authenticating dial-up users with multiple methods
- Security is provided by the authentication protocol carried by EAP, not by EAP itself
- EAP supports many authentication protocols: EAP-TLS, LEAP, PEAP, EAP-SIM, ...
- Used in 802.1X between supplicant and authentication server
- EAP term for supplicant is peer, reflecting the original idea that EAP could be used for mutual authentication between equal entities

EAP protocol



- Request-response pairs
- User identified by network access identifier (NAI): username@realm
- Allows multiple rounds of request–response, e.g. for mistyped passwords

EAP-TLS Protocol



Peer

EAP Server

EAP-Request / Identity

EAP-Response / Identity

EAP-TLS-Request (start)

EAP-TLS-Response:
ClientHello

EAP-TLS-Request:
ServerHello, Certificate, ServerKeyExchange,
CertificateRequest, ServerHelloDone

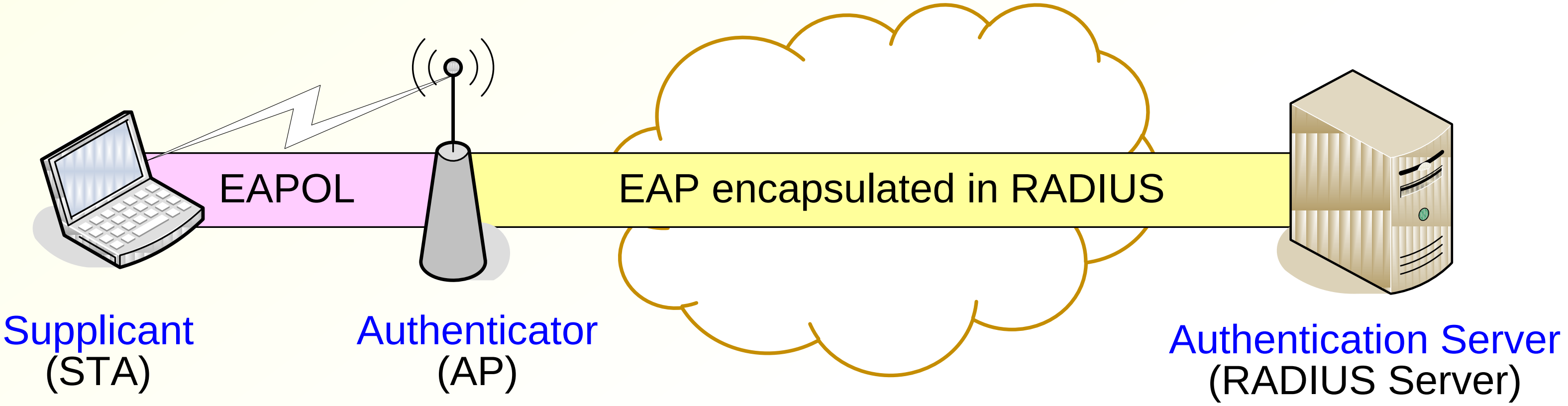
EAP-TLS-Response:
Certificate, ClientKeyExchange, CertificateVerify,
ChangeCipherSpec, Finished

EAP-TLS-Request:
ChangeCipherSpec, Finished

EAP-TLS-Response (empty)

EAP-Success

EAP encapsulation in 802.1X and WLAN



- On the wire network, EAP is encapsulated in RADIUS attributes
- On the 802.11 link, EAP is encapsulated in EAP over LAN (EAPOL)
- In 802.1X, AP is a pass-through device: it copies (most) EAP messages without reading them

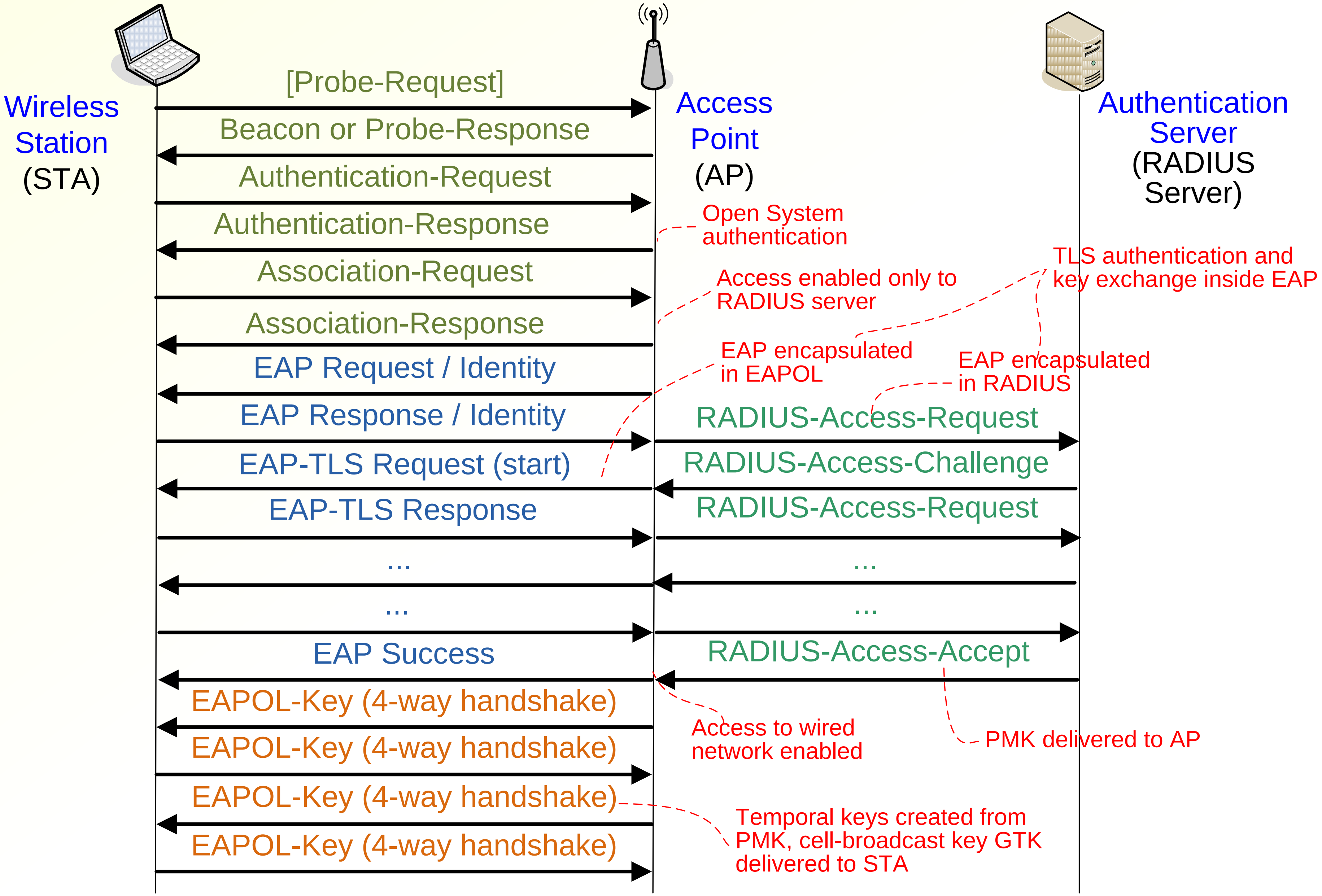
RADIUS

- Remote access dial-in user service (RADIUS)
  - Originally for centralized authentication of dial-in users in distributed modem pools
- Defines messages between the network access server (NAS) and authentication server:
  - NAS sends Access-Request
  - Authentication server responds with Access-Challenge, Access-Accept or Access-Reject
- In WLAN, AP is the NAS
- EAP is encapsulated in RADIUS Access-Request and Access-Challenge; as many rounds as necessary

RADIUS security

- AP and authentication server share a secret
- Responses from authentication server contain an authenticator; requests from AP are not authenticated
- Authenticator = MD5 hash of the message, AP's nonce and the shared secret
- Per-station key material is sent to the AP encrypted with the shared secret
- Radius uses a non-standard encryption algorithms but no problems found so far (surprising!)

EAP protocol in context



Wireless Station (STA)

Access Point (AP)

Authentication Server (RADIUS Server)

[Probe-Request]

Beacon or Probe-Response

Authentication-Request

Authentication-Response

Association-Request

Association-Response

EAP Request / Identity

EAP Response / Identity

EAP-TLS Request (start)

EAP-TLS Response

...

...

EAP Success

EAPOL-Key (4-way handshake)

EAPOL-Key (4-way handshake)

EAPOL-Key (4-way handshake)

EAPOL-Key (4-way handshake)

RADIUS-Access-Request

RADIUS-Access-Challenge

RADIUS-Access-Request

...

...

RADIUS-Access-Accept

Open System authentication

Access enabled only to RADIUS server

TLS authentication and key exchange inside EAP

EAP encapsulated in EAPOL

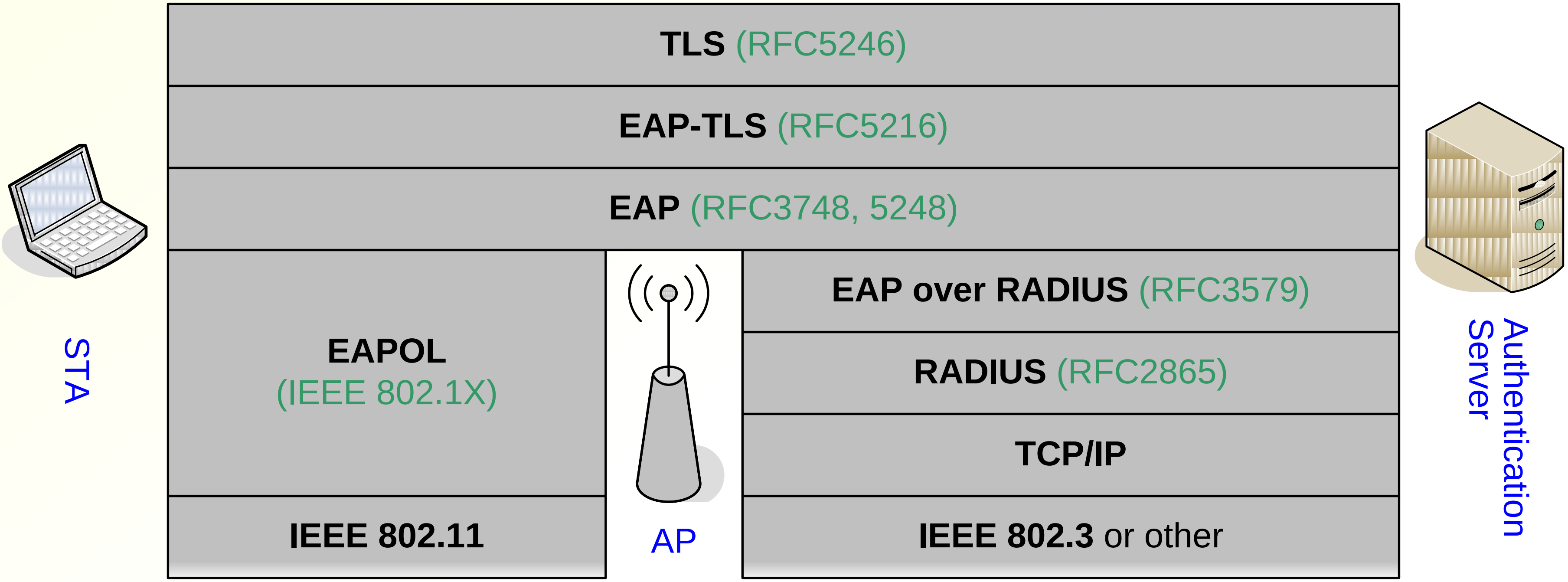
EAP encapsulated in RADIUS

Access to wired network enabled

PMK delivered to AP

Temporal keys created from PMK, cell-broadcast key GTK delivered to STA

802.1X protocol stack



TLS (RFC5246)

EAP-TLS (RFC5216)

EAP (RFC3748, 5248)

EAPOL (IEEE 802.1X)

EAP over RADIUS (RFC3579)

RADIUS (RFC2865)

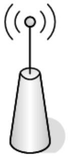
TCP/IP

IEEE 802.11

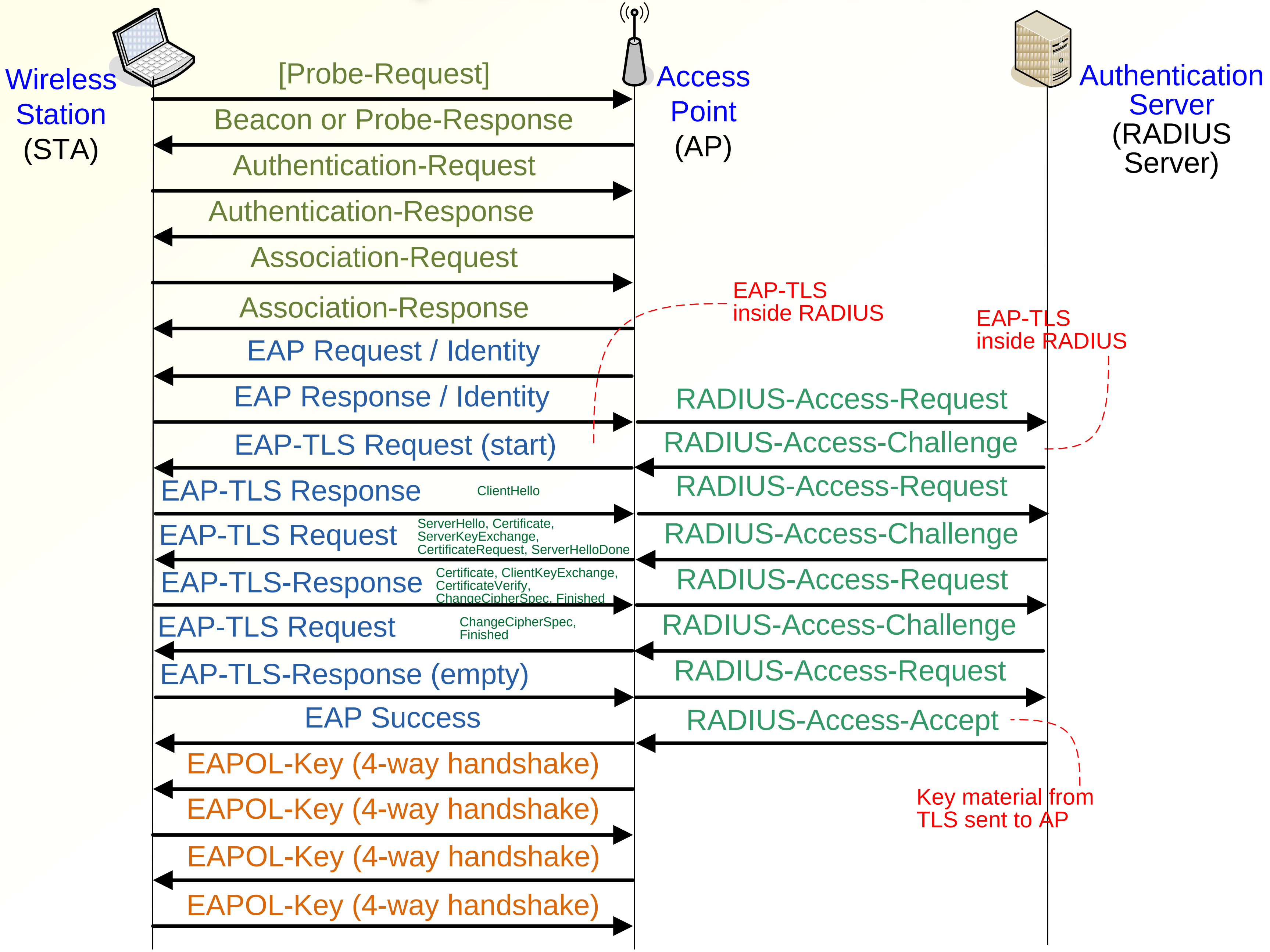
IEEE 802.3 or other

- Excessive layering?

Terminology

			
TLS	Client		Server
EAP/AAA	Peer	Authenticator	EAP server / Backend authentication server
802.1X	Supplicant	Authenticator	Authentication server (AS)
RADIUS		Network access server (NAS)	RADIUS server
802.11	STA	Access point (AP)	

Full WPA/802.11i Authentication



Wireless Station (STA)

Access Point (AP)

Authentication Server (RADIUS Server)

[Probe-Request]

Beacon or Probe-Response

Authentication-Request

Authentication-Response

Association-Request

Association-Response

EAP Request / Identity

EAP Response / Identity

EAP-TLS Request (start)

EAP-TLS Response ClientHello

EAP-TLS Request ServerHello, Certificate, ServerKeyExchange, CertificateRequest, ServerHelloDone

EAP-TLS-Response Certificate, ClientKeyExchange, CertificateVerify, ChangeCipherSpec, Finished

EAP-TLS Request ChangeCipherSpec, Finished

EAP-TLS-Response (empty)

EAP Success

EAPOL-Key (4-way handshake)

EAPOL-Key (4-way handshake)

EAPOL-Key (4-way handshake)

EAPOL-Key (4-way handshake)

RADIUS-Access-Request

RADIUS-Access-Challenge

RADIUS-Access-Request

RADIUS-Access-Challenge

RADIUS-Access-Request

RADIUS-Access-Challenge

RADIUS-Access-Request

RADIUS-Access-Accept

EAP-TLS inside RADIUS

EAP-TLS inside RADIUS

Key material from TLS sent to AP

Authentication Latency

- 7-8 round trips between AP and STA for EAP-TLS
  - 7 roundtrips when TLS session reused (cf. 4 with PSK)
  - Probe-Request / Probe-Response alternative to Beacon → 1 more round trip
  - Messages with many long certificates may need to be fragmented → more round trips
- 3–4 round trips between AP and authentication server
  - 3 roundtrips when TLS session reused
- Typical authentication latency >1 second every time STA roams between APs → need optimizations

Session protocol: AES-CCMP

- AES Counter Mode-CBC MAC Protocol is used for encryption and integrity in 802.11i/RSN
- Advanced Encryption Standard (AES)
- CCMP = Counter Mode + CBC MAC
  → AES counter mode encryption
  → CBC MAC for integrity protection
- Requires new hardware

Session protocol: TKIP

- Temporal Key Integrity Protocol (TKIP) can be implemented with pre-WPA2 hardware and a firmware update
- Still RC4 but WEP vulnerabilities fixed:
  - New message integrity algorithm — Michael
  - New encryption key for each frame
  - 48-bit IV constructed to avoid RC4 weak keys
  - IV used as sequence counter to prevent replays
- Recent cryptographic attacks against TKIP! Time to start using only WPA2

WPA/802.11i security - goals and reality

- Authentication and access control prevents unauthorized network access
- Mutual authentication prevents association with rogue access points
- CCMP encryption prevents data interception on wireless link
- Strong integrity check prevents data spoofing on wireless link
- Deauthentication and disassociation attacks still possible
  - Difficult to fix because of the layering

Link-layer mobility in WLAN

Wireless LAN roaming

- Moving between APs is slow
  - Many roundtrips to a remote authentication server
  - Many messages between STA and AP, channel acquisition time for each message can be long on a busy WLAN
  - Complex protocol layering leads to unnecessary messages
- How to speed up the handover?

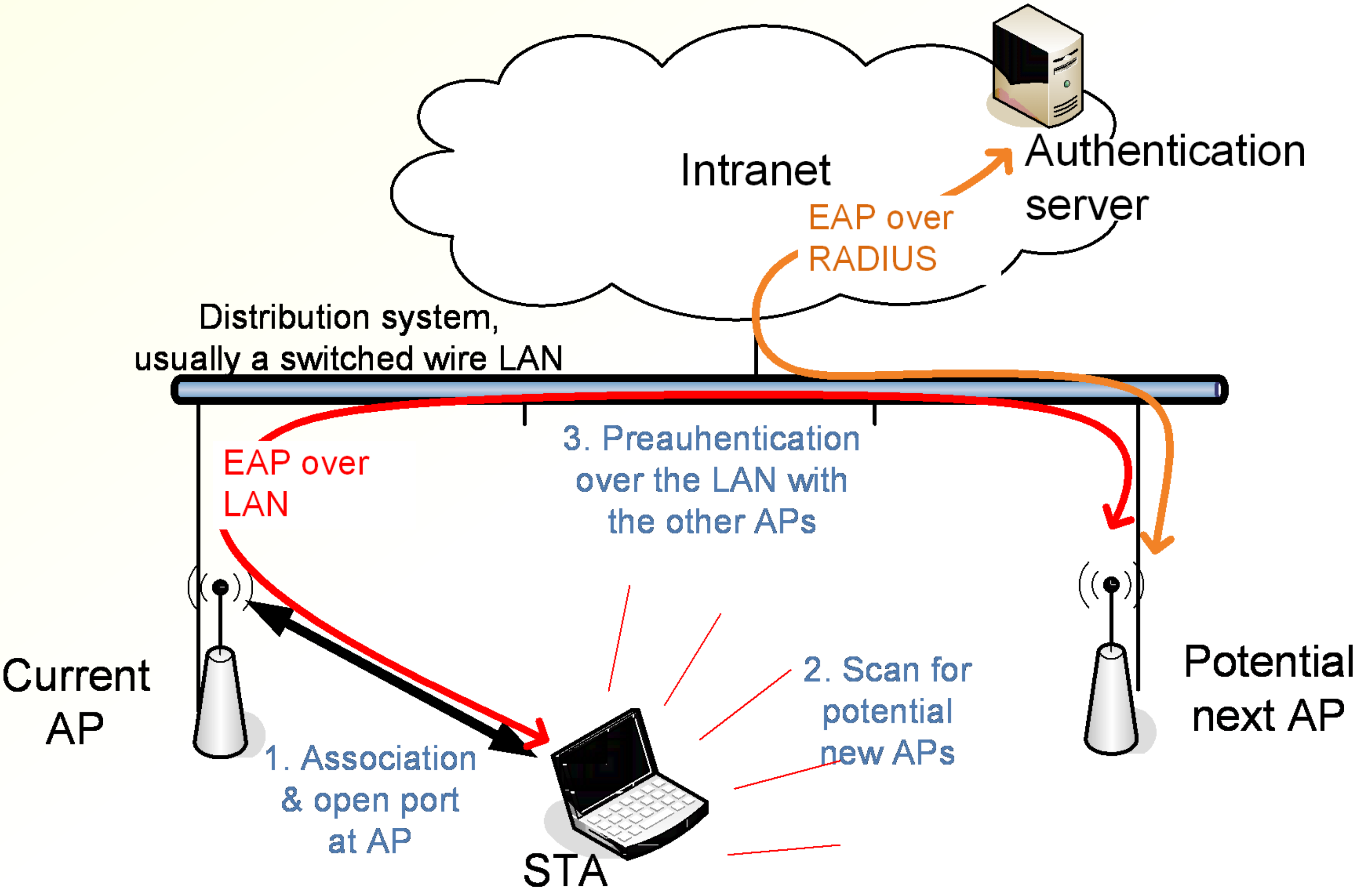
PMK caching

- AP and STA may cache previous pair-wise master keys (PMK) and reuse them if the same client returns to the same AP
- Only a 4-way handshake between STA and AP needed after (re)association to create new session keys from the PMK
- Key identifiers to identify PMK
- STA may send a list of key identifiers in (re)association request; AP selects one in Message 1 of the 4-way handshake
- Standardized in 802.11i, now in 802.11-2007/WPA2

Wireless switch

- Proprietary roaming solution from equipment manufacturers
- Moving parts of the authenticator to a switch
- Client STA assumes AP has cached PMK even if it has never authenticated to that AP
  - called ”opportunistic PMK caching”
- Switch pushes PMK to all APs, or AP pulls key on demand

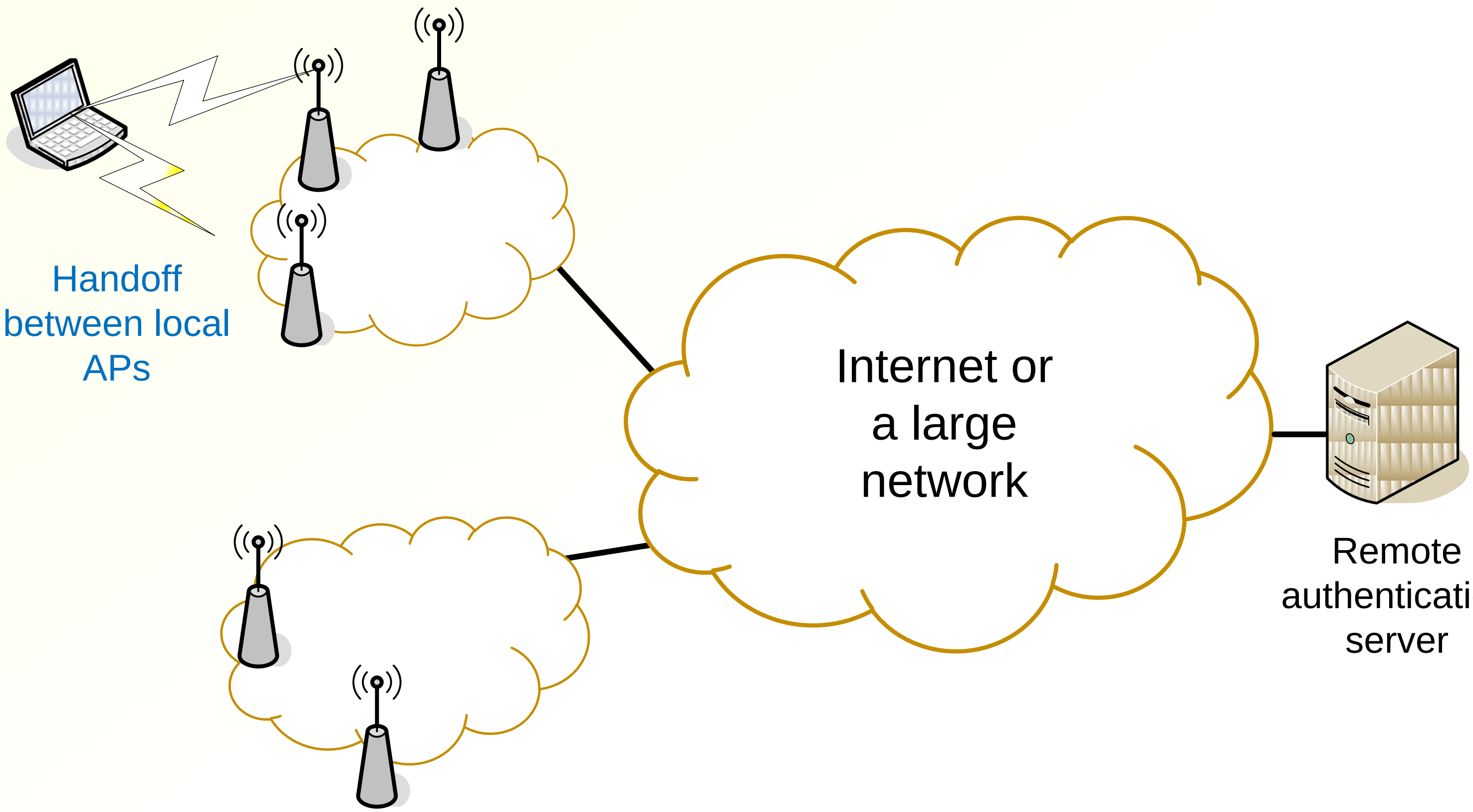
802.1X preauthentication


Intranet
Authentication server
EAP over RADIUS
Distribution system, usually a switched wire LAN
EAP over LAN
3. Preauhentication over the LAN with the other APs
Current AP
Potential next AP
2. Scan for potential new APs
1. Association & open port at AP
STA

802.1X preauthentication

- Client STA scans for potential new APs and authenticates to them before deassociation from the old AP
  - AP advertises the preauthentication capability in its beacon
- STA communicates with the new AP over the LAN, via the old AP
  - STA uses the BSSID (= MAC address) of the new AP as the destination address of the frames it sends to the new AP → new AP must be on the same IP segment
- AP caches the PMK, just as if the STA had associated with it previously
- Finally, STA reauthenticates to the new AP

Local handoff problem


Handoff between local APs
Internet or a large network
Remote authentication server

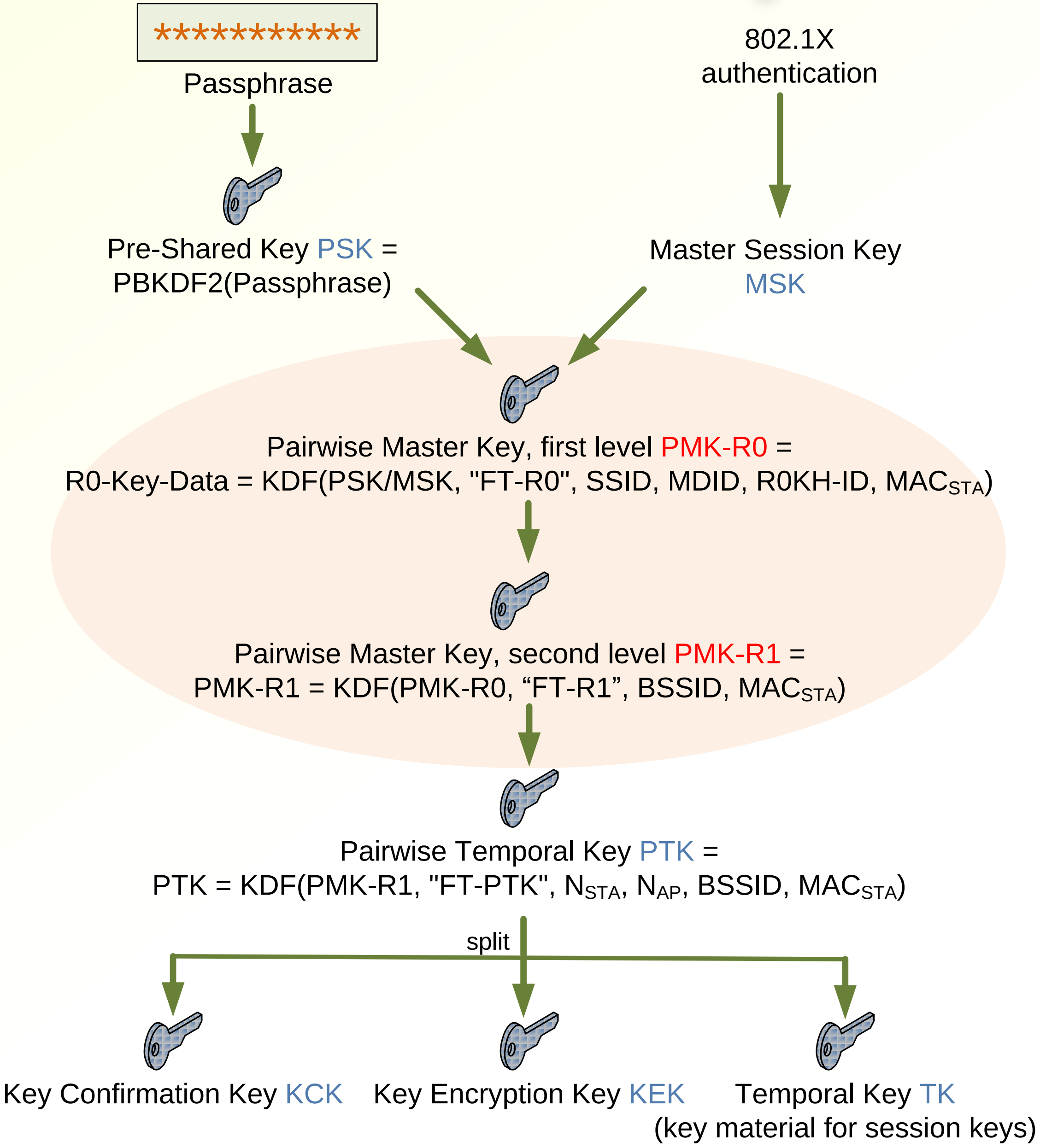
- Even local handoffs require connection to the AS, which may be far away

802.11r fast BSS transition

- Amendment 802.11r adds mechanisms for fast handover
  - With PSK or cached MSK, piggyback the 4-way handshake on 802.11 authentication and association messages → only 2 roundtrips between STA and AP
  - Mobility domain = group of APs close to each other + local "server" that helps in local handoffs
  - AP advertises capability for fast BSS transition, and a mobility domain identifier
  - Key hierarchy within the mobility domain: local server (R0KH) holds first-level key (PMK-R0), which is used to derive second-level keys (PMK-R1) for APs (R1KH) in the same domain
    → avoid contacting a remote authentication server
  - In practice:

    R0KH = wireless switch, R1KH = AP
  - Also, prereservation of resources for QoS (see 802.11e) done in parallel with the 4-way handshake

802.11r key hierarchy



****

Passphrase

802.1X authentication

Pre-Shared Key PSK = PBKDF2(Passphrase)

Master Session Key MSK

Pairwise Master Key, first level PMK-R0 =
R0-Key-Data = KDF(PSK/MSK, "FT-R0", SSID, MDID, R0KH-ID, MAC$_{STA}$)

Pairwise Master Key, second level PMK-R1 =
PMK-R1 = KDF(PMK-R0, “FT-R1”, BSSID, MAC$_{STA}$)

Pairwise Temporal Key PTK =
PTK = KDF(PMK-R1, "FT-PTK", N$_{STA}$, N$_{AP}$, BSSID, MAC$_{STA}$)

split

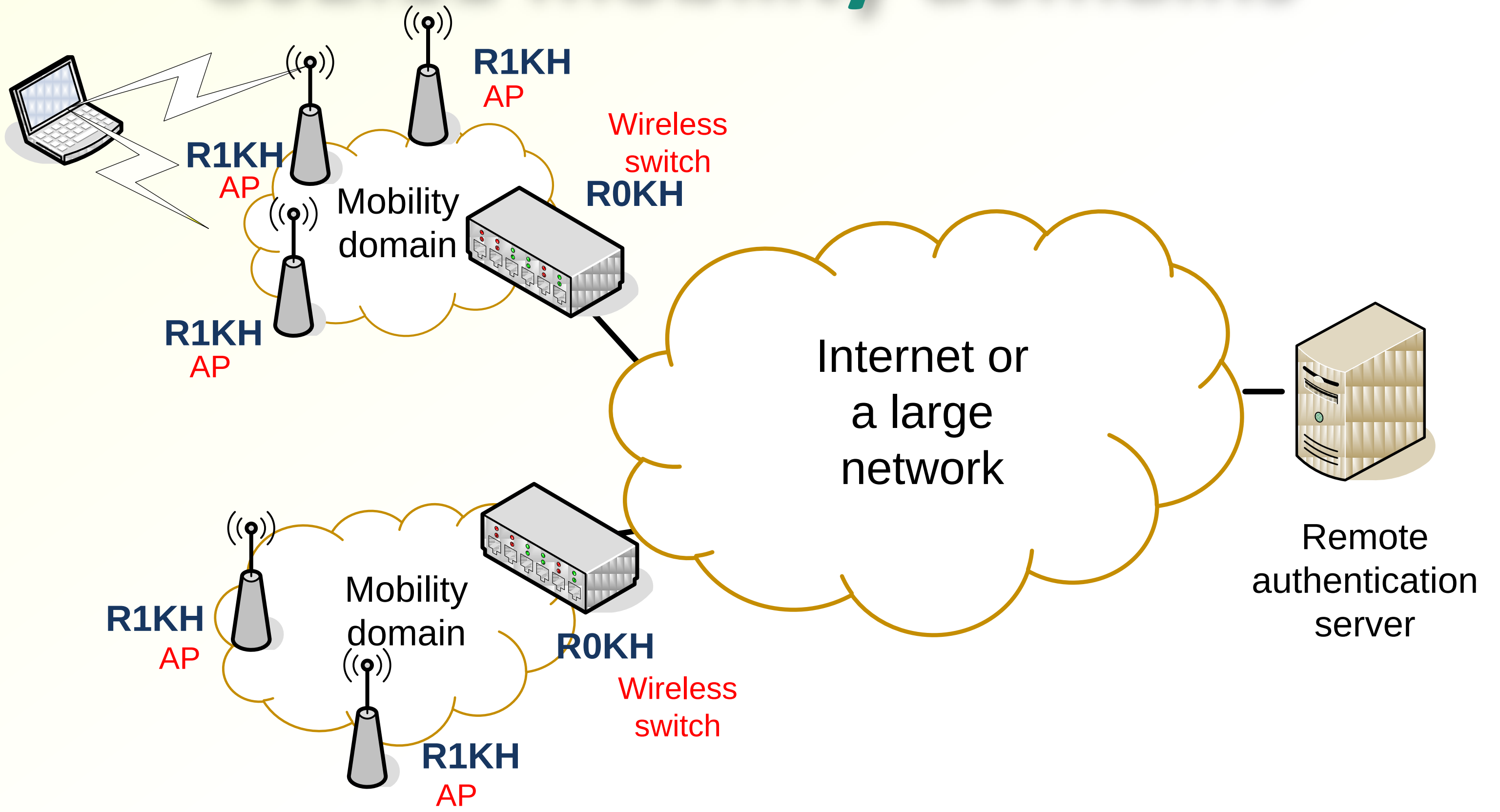
Key Confirmation Key KCK

Key Encryption Key KEK

Temporal Key TK
(key material for session keys)

- PMK-R0 = key shared by STA and the mobility domain (wireless switch); derived from PSK or EAP MSK
- PMK-R1 = key shared by STA and AP; derived locally from PMK-R0
- AP only knows PMK-R1, STA knows PMK-R0 and can compute PMK-R1 for each new AP

802.11 mobility domains



- Handoff within a mobility domain is supported by the local R0KH
- EAP with AS only when moving between mobility domains
- 802.11r specifies the key hierarchy and communication between STA and AP; the protocol between APs and the R0KH is not standardized

Other roaming solutions

- L3 tunneling between wireless switches:
  hides IP address changes from the mobile
- Inter-technology handovers
  (e.g. wire LAN—WLAN—3G)
- Mobility protocols on network-layer or higher to support mobility between IP segments and between network technologies
- Handover latency in layer 3 is even bigger an issue than in link-layer mobility
  - Delays ok for roaming but not for interactive voice
- Layer-3 mobility protocols: Mobile IP/IPv6, NEMO, MOBIKE, HIP

Password authentication for WLAN

Universal access method (UAM)

- Web-based authentication
- Used mostly in wireless hotspots for credit-card payment or checking user account
- Redirect new users to authentication server when they try open a web browser

  Methods of redirection:

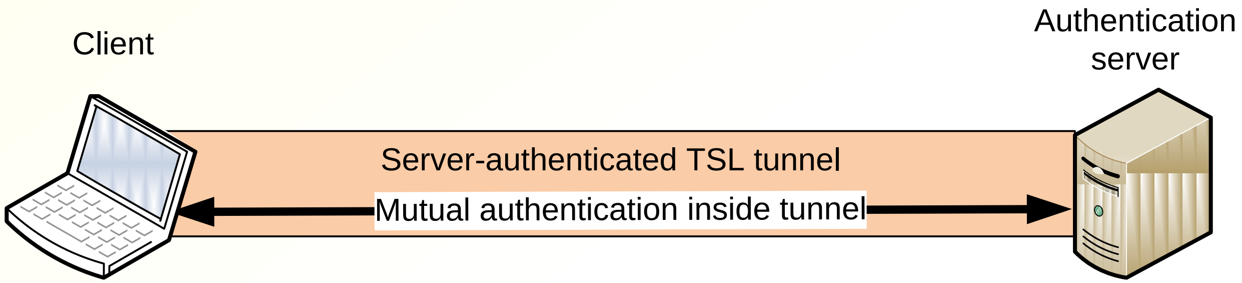
  - Spoofed HTTP redirection
  - DNS spoofing
  - Redirection of IP packets at switch
- Add authenticated users MAC addresses to whitelist

LEAP, PEAP, EAP-TTLS

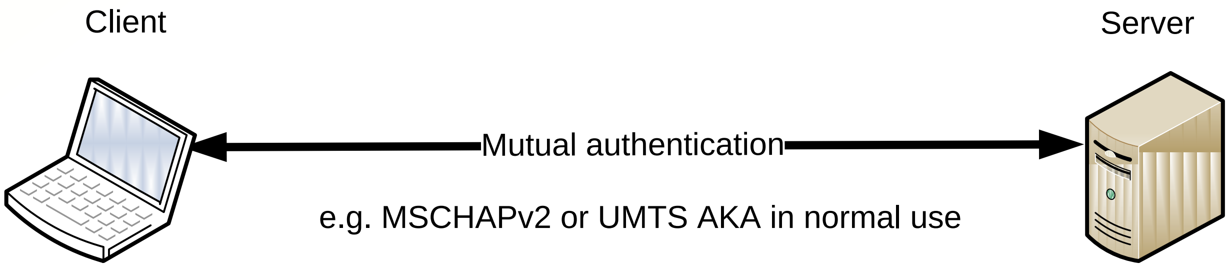
- Idea: authenticate the server with TLS, then the client inside the encrypted tunnel
- Lightweight Extensible Authentication Protocol (LEAP) by Cisco — insecure and no longer used
- Protected EAP (PEAP) by Microsoft
  - Round 1: EAP-TLS with server-only authentication
  - Do not send EAP-Success; instead, start encryption and move to round 2
  - Round 2: any EAP authentication method (e.g. MSCHAPv2) with mutual authentication
- Inner authentication could be any EAP method. In practice, WPA stations support EAP-PEAP-MSCHAPv2
- Password authentication inside encrypted tunnel
- EAP-Success message is also authenticated
- Some identity protection:
  - PEAP encrypts the EAP-Request-Identity message
    → user identity in round 2 is hidden
  - Client may send machine identity in round 1
- Another similar proposal: EAP-TTLS

Tunnelled authentication problem (1)

- PEAP and EAP-TTLS clients authenticate the server with TLS
- Server authenticates the client inside the TLS tunnel with MSCHAPv2, TLS, UMTS AKA, or any other protocol — authentication may be mutual

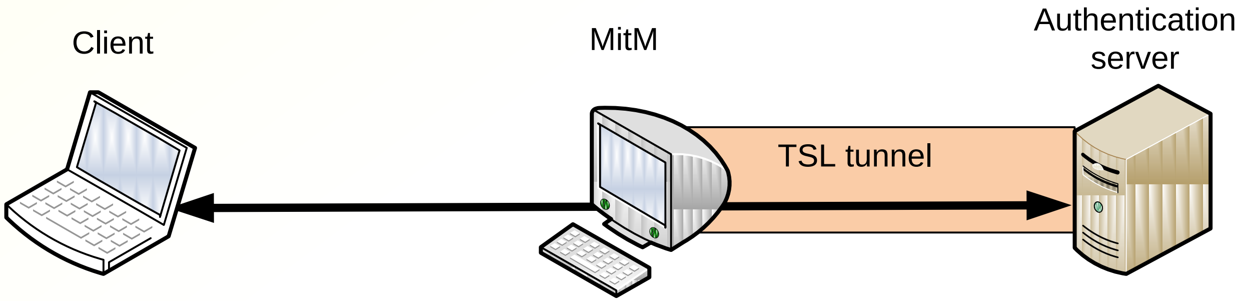

Client
Authentication server
Server-authenticated TSL tunnel
Mutual authentication inside tunnel

- Session key is provided by the TLS tunnel — session keys from the inner authentication are not used
- BUT… the same inner authentication methods are used also without TLS tunnelling



Tunnelled authentication problem (2)

- Attacker can pretend to be a server in the no-tunnel version and forward his authentication inside a tunnel [Asokan, Niemi, Nyberg 2003]
- Easy for UMTS AKA — attacker can pretend to be a 3G base station
- More difficult for MSCHAPv2 — attacker needs to be a server on the intranet to which the client connects



Exercises

- Why is WPA-Enterprise not widely used in home wireless networks, wireless hotspots or Internet cafes?
- How could the network attachment and access control protocols be further optimized to reduce latency?
- Is WLAN security alternative or complementary to end-to-end security such as TLS?
- Explain how each of the security weaknesses in WEP arises from the protocol and algorithm details