

Network Security: WLAN Security

Tuomas Aura

T-110.5241 Network security
Aalto University, Nov-Dec 2012

Outline

- Wireless LAN technology
- Threats against WLANs
- Weak security mechanisms and historical WEP
- Real WLAN security: WPA2
- Password-based user authentication
- WLAN mobility

Wireless LAN technology

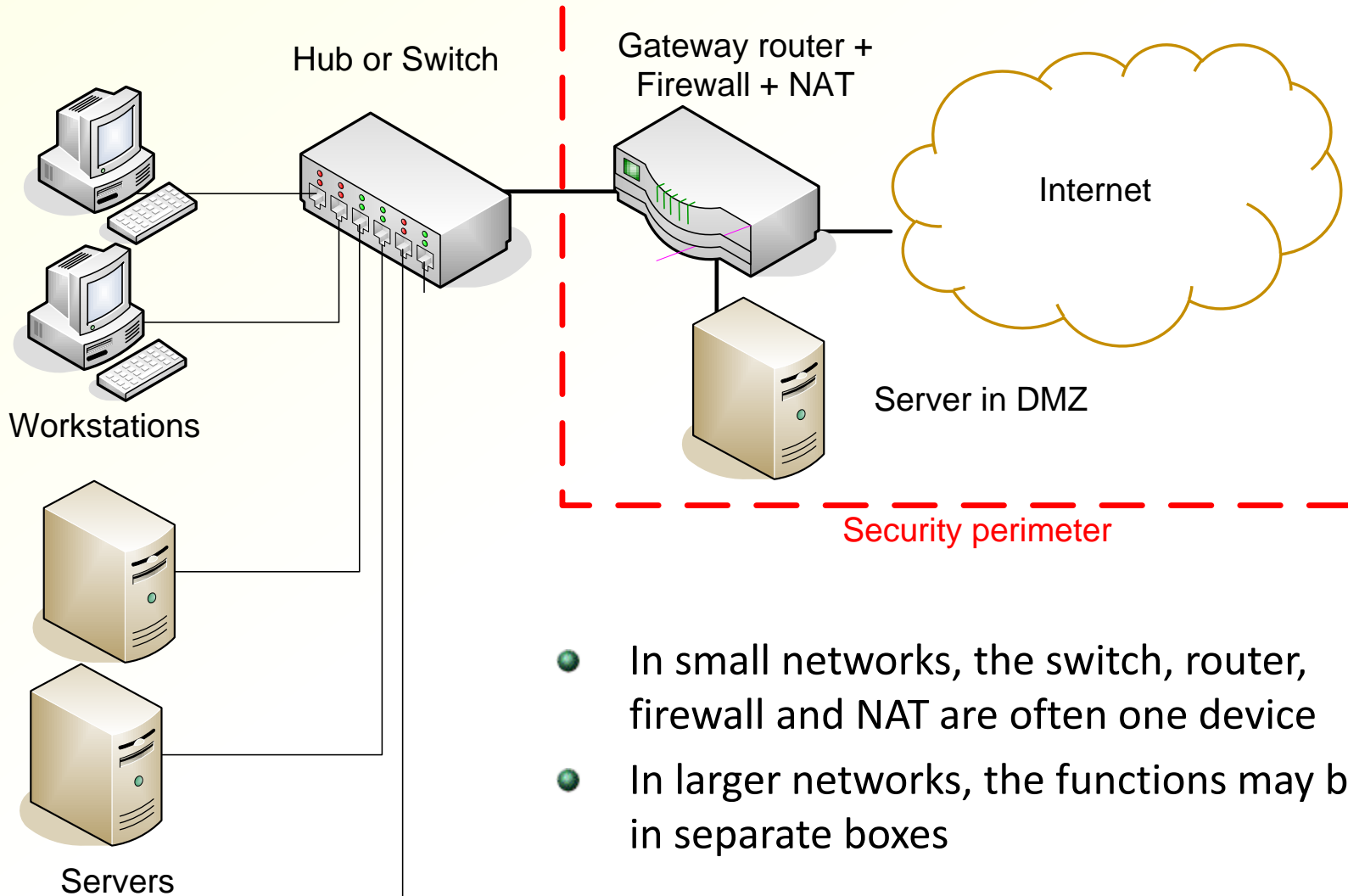
Wireless LAN (WLAN) standards

- 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 network interface card (NIC) by the manufacturer

802.11 technology overview

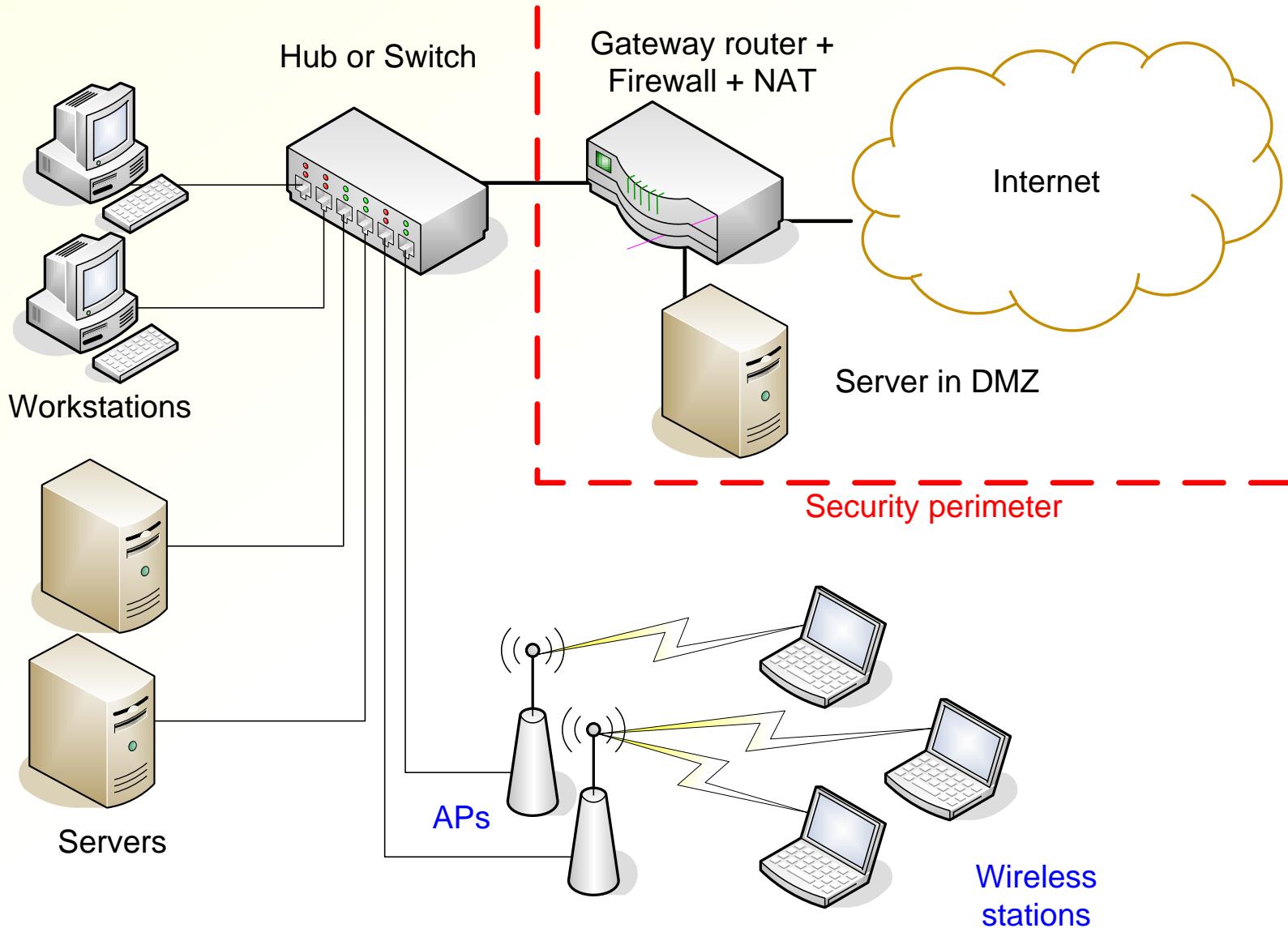
- Physical layer:
 - Uses unlicensed bands at 2.4 GHz (microwave ovens, Bluetooth) and 5 GHz
 - Up to 14 radio channels, but only 2–4 non-overlapping ones
- Link layer
 - Looks like Ethernet (802.3) to layers above
 - MAC protocol differs from 802.3 because one antenna cannot detect collisions while transmitting
→ explicit ACKs needed

Small-business LAN

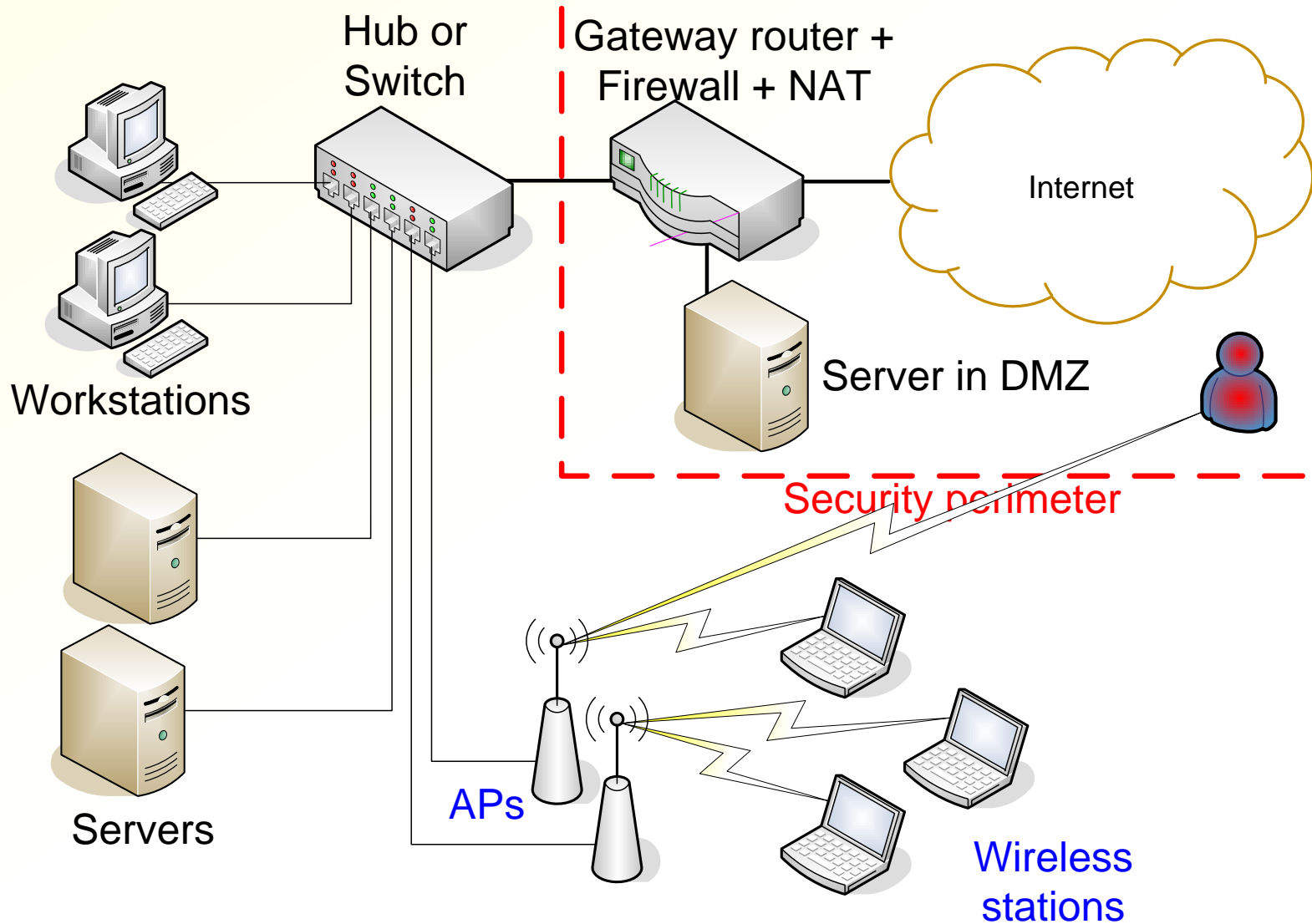


- In small networks, the switch, router, firewall and NAT are often one device
- In larger networks, the functions may be in separate boxes

Small-business WLAN



Main WLAN security threat



Wireless LAN components

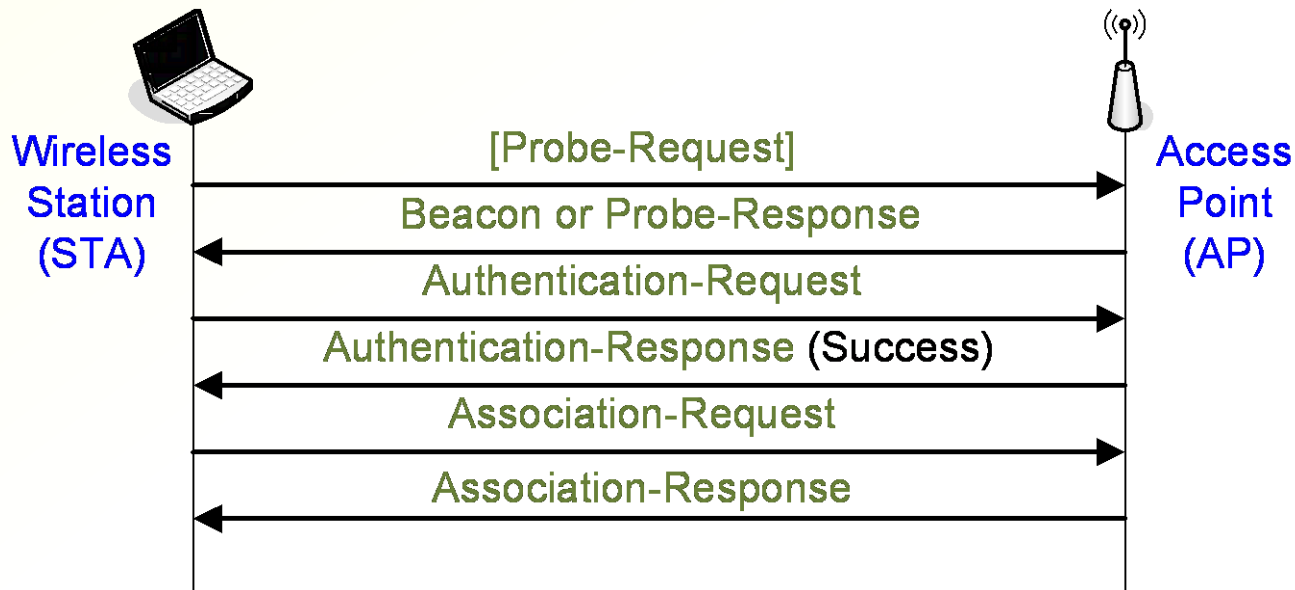
- **Access point (AP)** = bridge between wireless (802.11) and wired (802.3) networks
- **Wireless station (STA)** = PC or other device with a wireless network interface card (NIC)
 - To be precise, AP is also a STA
- **Infrastructure mode** = wireless stations communicate only with AP
- **Ad-hoc mode** = 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

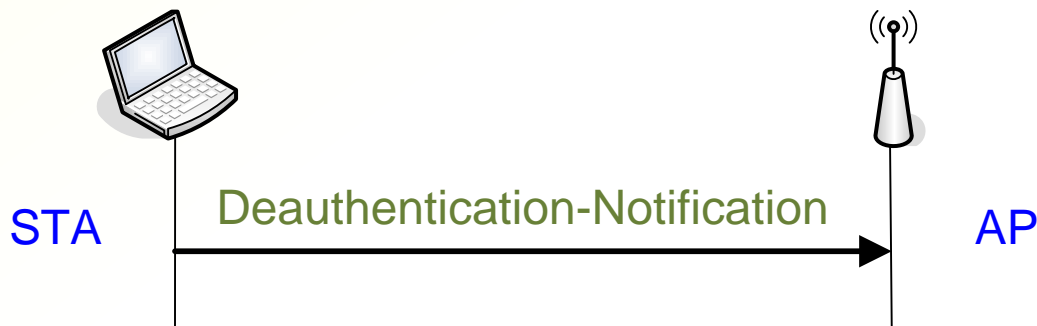
- AP sends **beacons**, usually every 50-100 ms
- Beacons usually include the SSID but the **SSID broadcast** can be turned off
- STA must specify SSID to the AP in association request



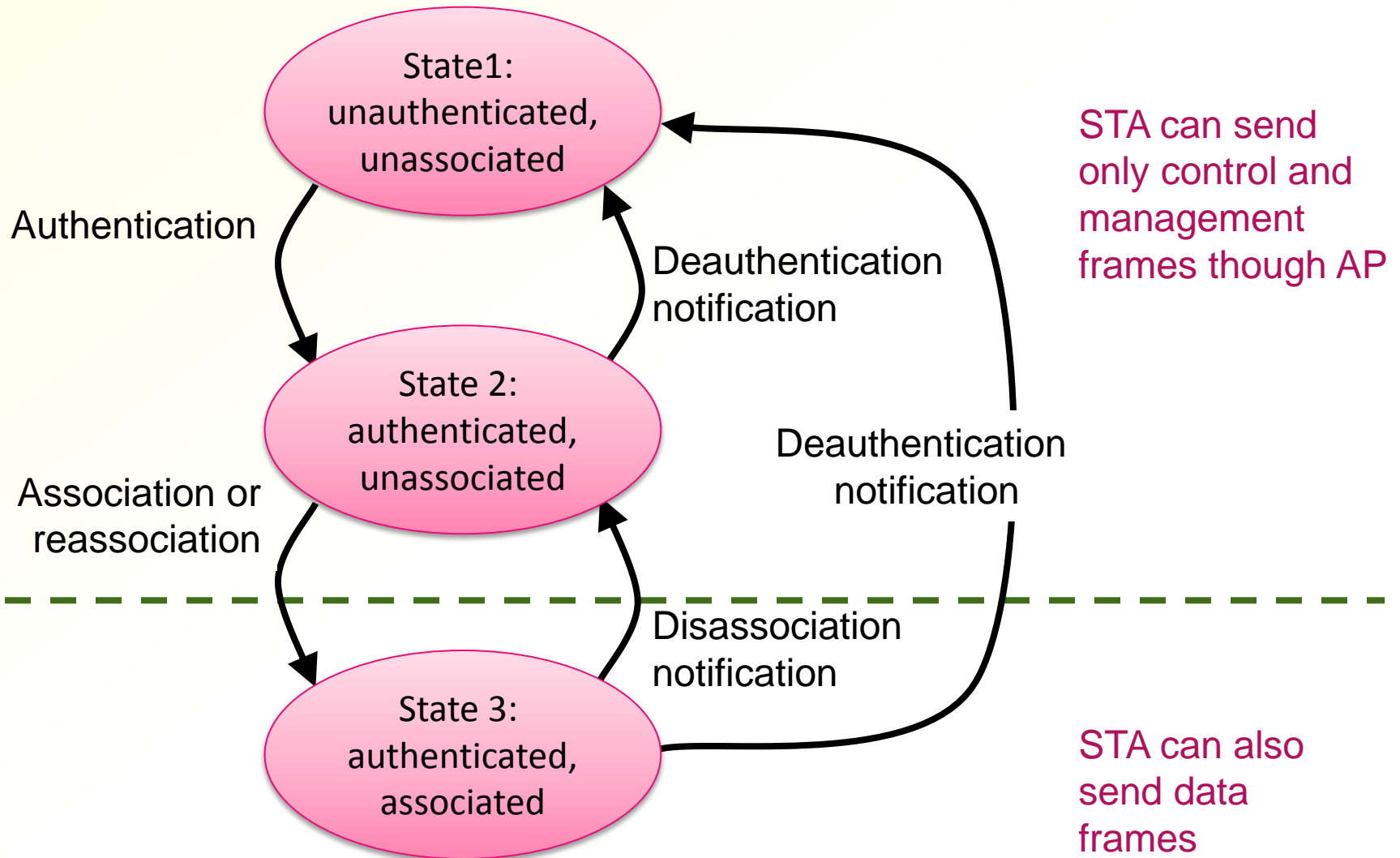
- Open System authentication = **no authentication**, empty authentication messages

Leaving a wireless LAN

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



802.11 association state machine



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 authorization or payment
- Access-point misconfiguration
- Unauthorized APs — unauthorized ingress routes to intranet may bypass firewall
- Denial of service — logical attacks with spoofed signaling, signal jamming
- AP spoofing — stronger signal attracts STAs

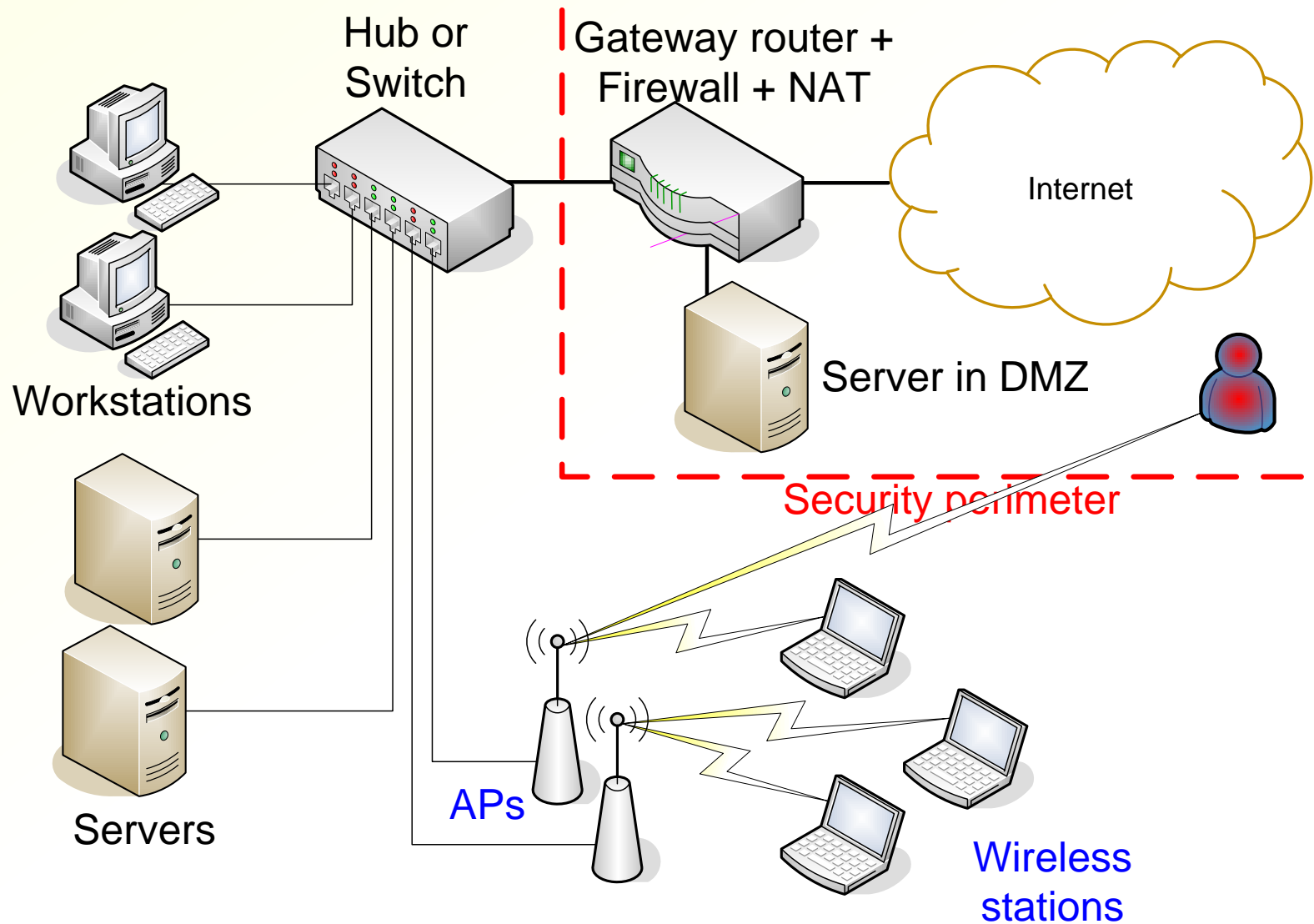
Signal interception

- 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?
- Using unprotected WLAN for Internet access is now legal in Finland
- **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

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 to access the intranet
- Solutions:
 - **AP sweeps**: walk or drive around premises and look for AP beacons — now a standard corporate practice
 - Scan for SNMP and web admin interfaces in the intranet
 - Some high-end APs have built-in feature for unauthorized AP detection
- Similar to unauthorized modems in the old days

Denial of service

- Logical attacks:
 - **Spoofer 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 whole 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 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 historical WEP

Good to know

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

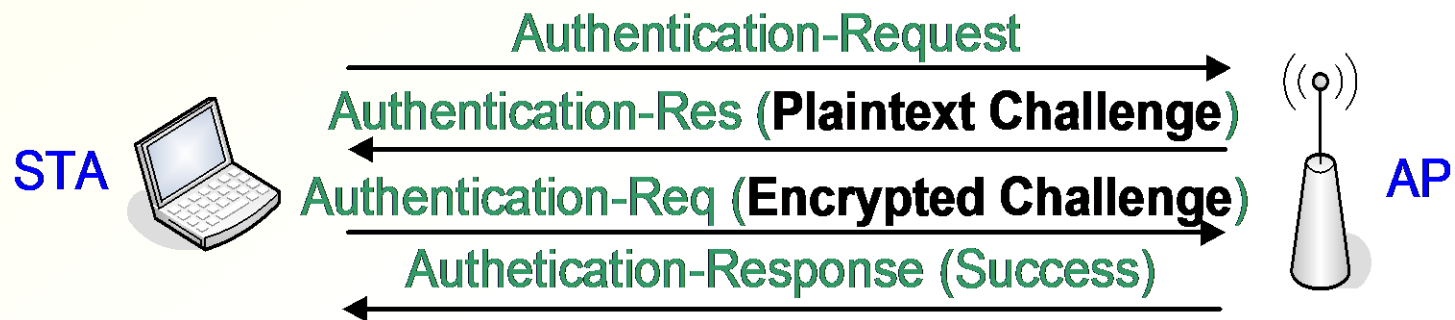
- **Disabling the SSID broadcast** — attacker can sniff the SSID when other clients associate
 - **ACL of authorized MAC addresses** — attacker can sniff and spoof another client's MAC address
 - **AP locations, directional antennas and metal foil to keep signal inside a building** — hard to build a Faraday cage, and attacker can use a directional antenna with high gain
- Weak security mechanisms are rarely worth the trouble

Historical 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; today 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



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

WEP keys

- WEP keys are configured manually; no other mechanism specified in 802.11
- STA can store 4 keys simultaneously; every frame header contains a 2-bit key id
- AP and all stations may share the same key, or AP may have a different key for each client STA (**per-station keys**)
 - No effect on client STA implementation
 - AP implementation much more complex with per-station keys → rarely implemented before WPA

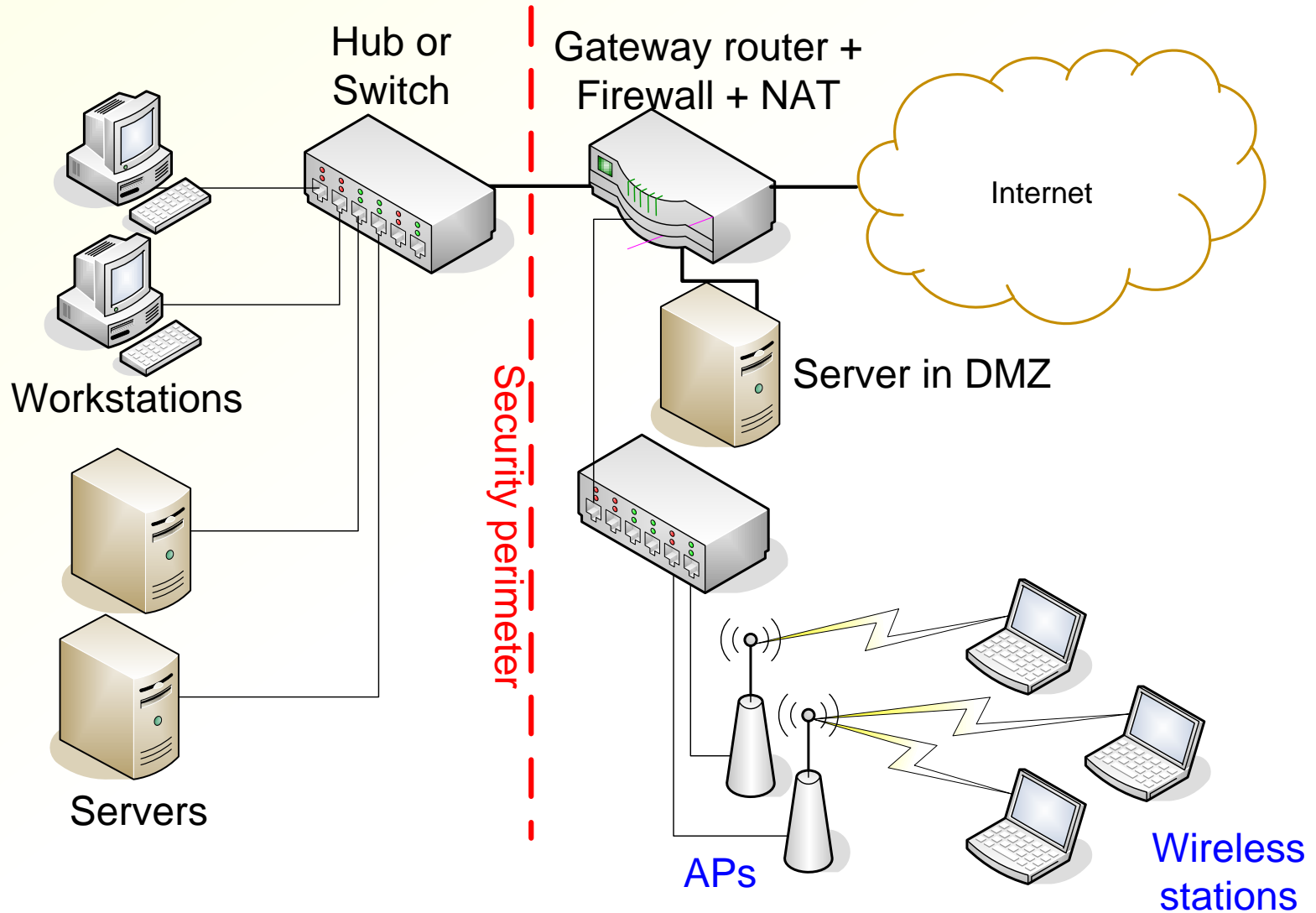
WEP security weaknesses

- 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

Is link-layer security needed?

- 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



Is WLAN access control needed?

- 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 providing public service
 - 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
- High-end access points and virtual LANs (VLAN) make it possible to configure two SSIDs on the same physical AP, one for authenticated intranet access and one for open Internet access

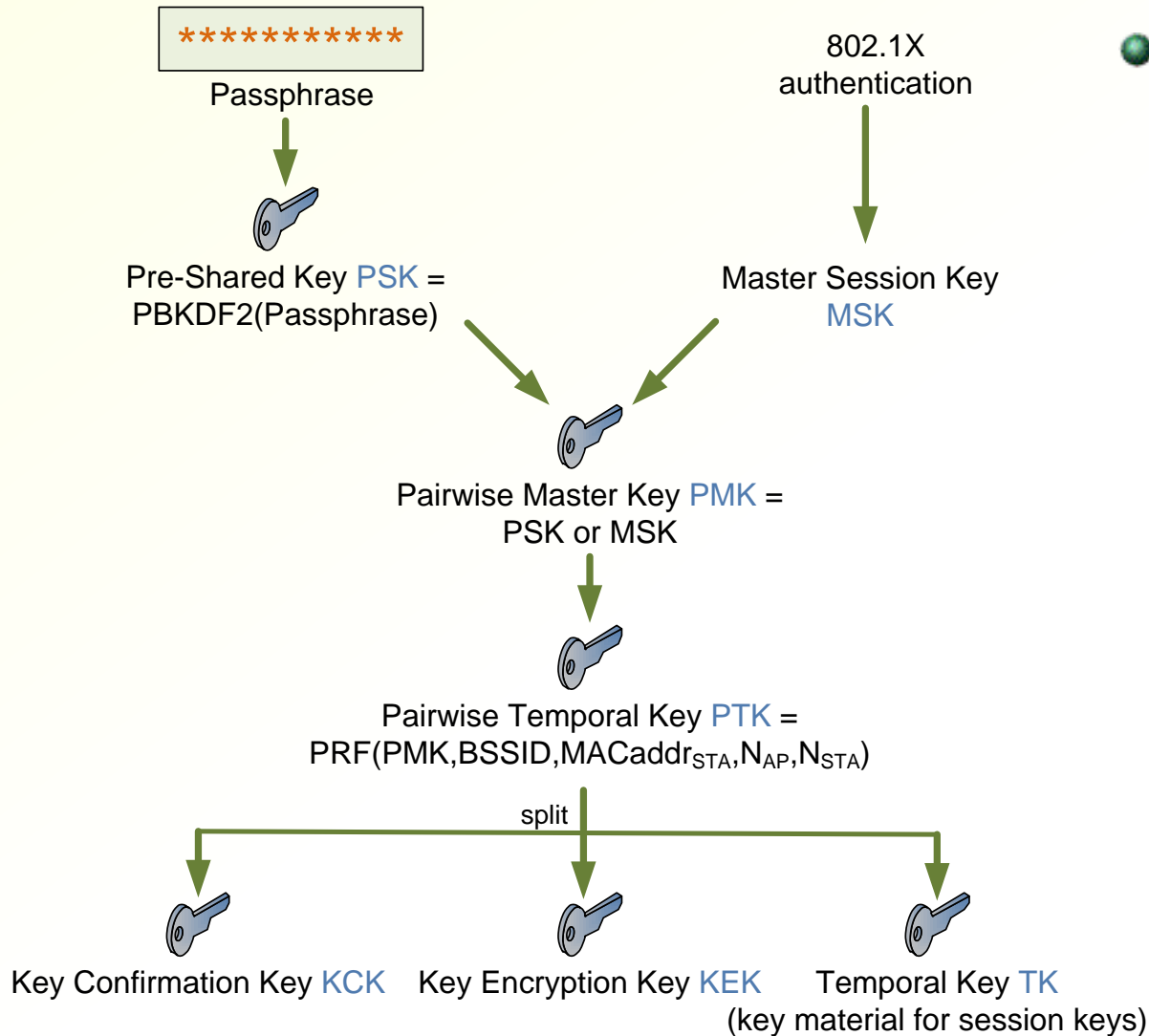
Real WLAN security: WPA2

The most important part

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 defines **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
 - AES requires new hardware
- **Wireless Protected Access (WPA)**
 - Defined by Wi-Fi alliance for transition period before the 11i standard and AES hardware support
 - Supports only TKIP encryption = RC4 with frequently changing keys and other enhancements
 - Firmware update to older AP or NIC often sufficient
 - **Security of TKIP and WPA is now considered broken**

RSN key hierarchy

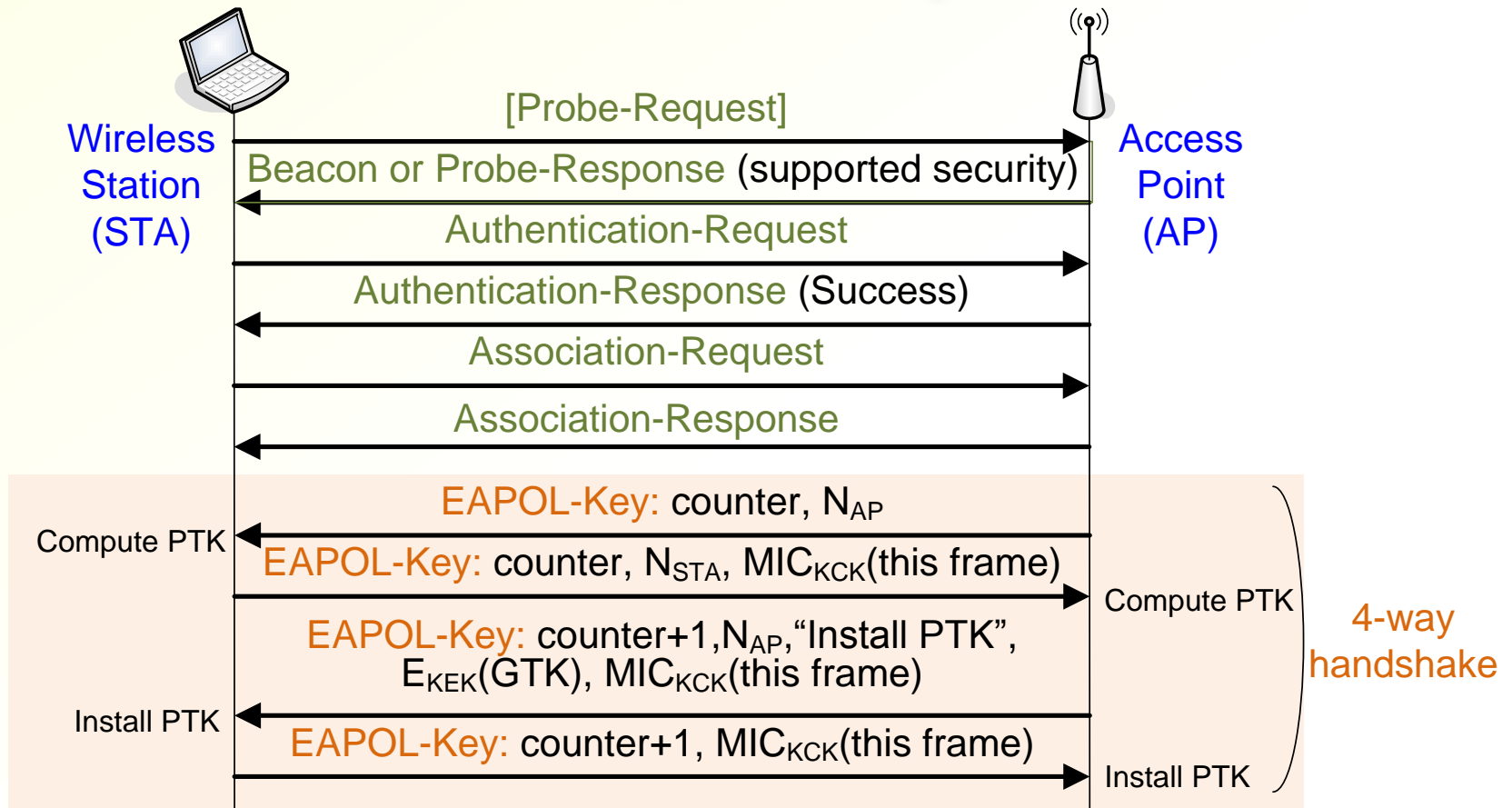


- Two alternative ways to obtain keys:
 - **Preshared key (PSK)** authentication = WPA2-PSK = WPA2-Personal
 - **802.1X** authentication = WPA2-EAP = WPA2-Enterprise
 - WPA-* differs from WPA2-* only in minor details and in crypto algorithms

RSN key hierarchy

- Pairwise keys between AP and STA:
 - Pairwise master key (PMK)
 - Temporal keys derived from PMK
 - data encryption and integrity keys
 - EAPOL-Key encryption and integrity keys
- 4-message protocol of EAPOL-Key messages is used to refresh temporal keys
 - Key computed as a hash of PMK, new nonces, and AP and STA MAC addresses
- Group keys for group and broadcast communication

WPA2-Personal, 4-way handshake

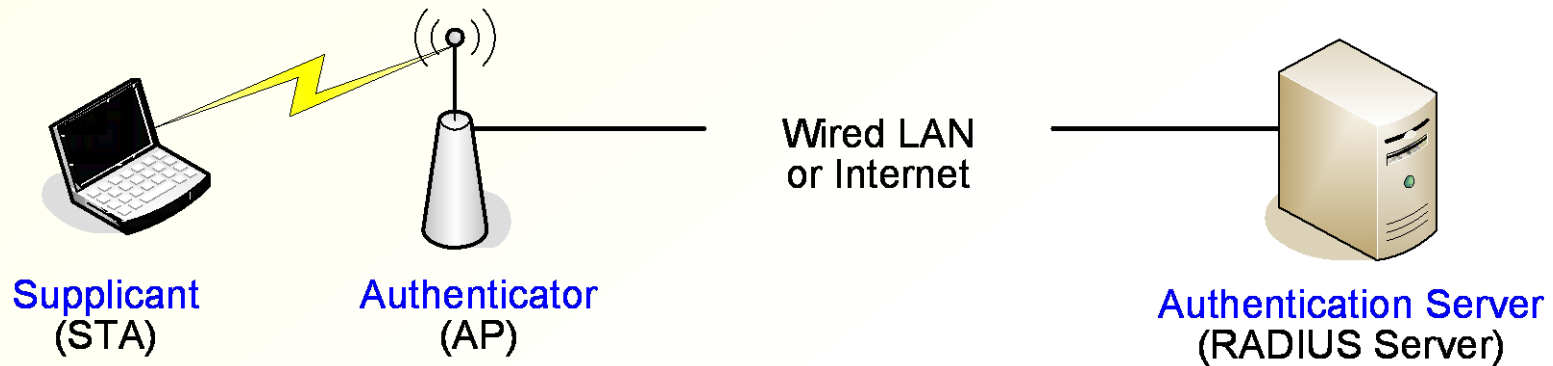


PMK = key derived from Passphrase
 counter = replay prevention, reset for new PMK
 PRF = pseudo-random function
 $PTK = PRF(PMK, MACaddr_{AP}, MACaddr_{STA}, N_{AP}, N_{STA})$
 KCK, KEK = parts of PTK
 MIC = message integrity check, a MAC
 GTK = Group Temporal Key

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

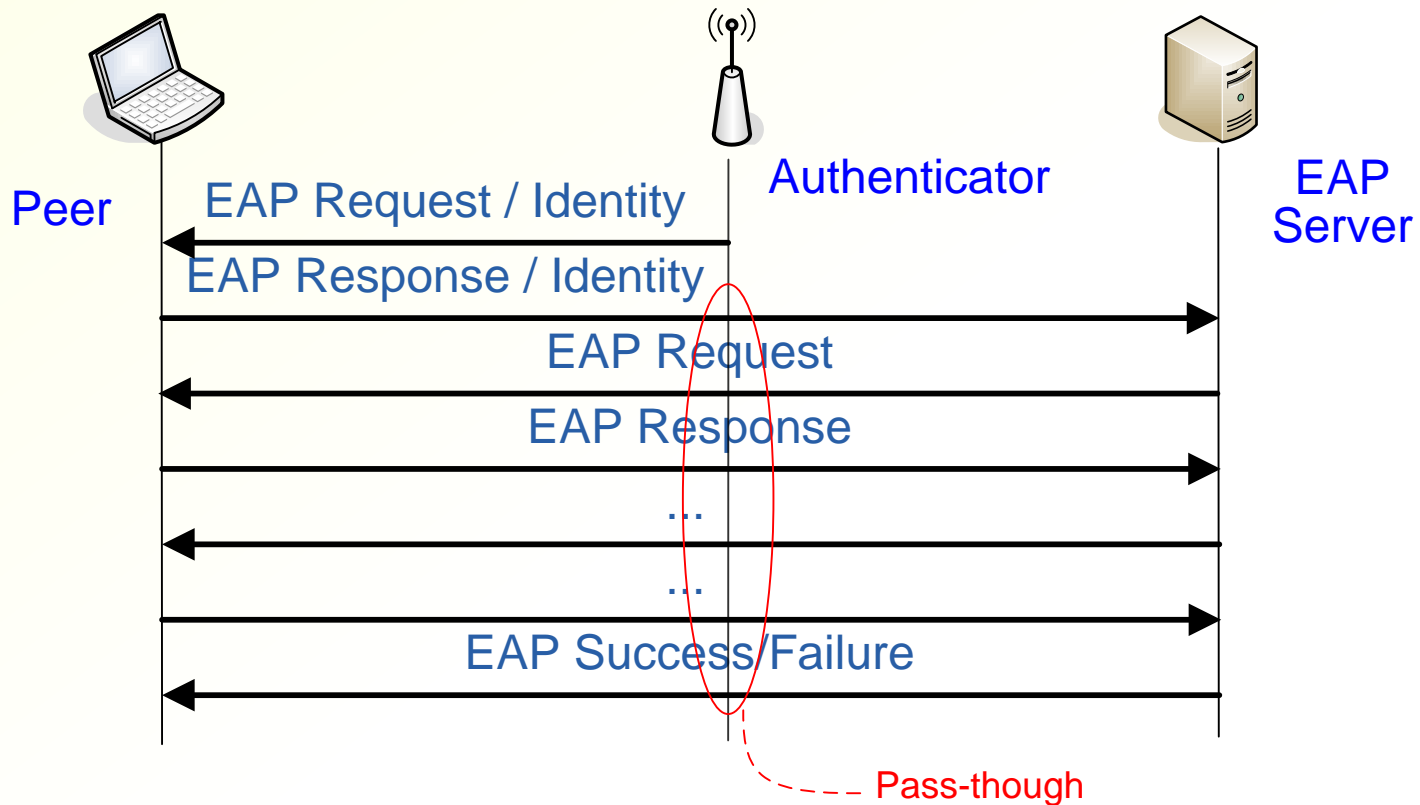


- **Supplicant** wants to access the wired network via the AP
- **Authentication Server (AS)** authenticates the supplicant
- **Authenticator** enables network access for the supplicant after successful authentication

EAP

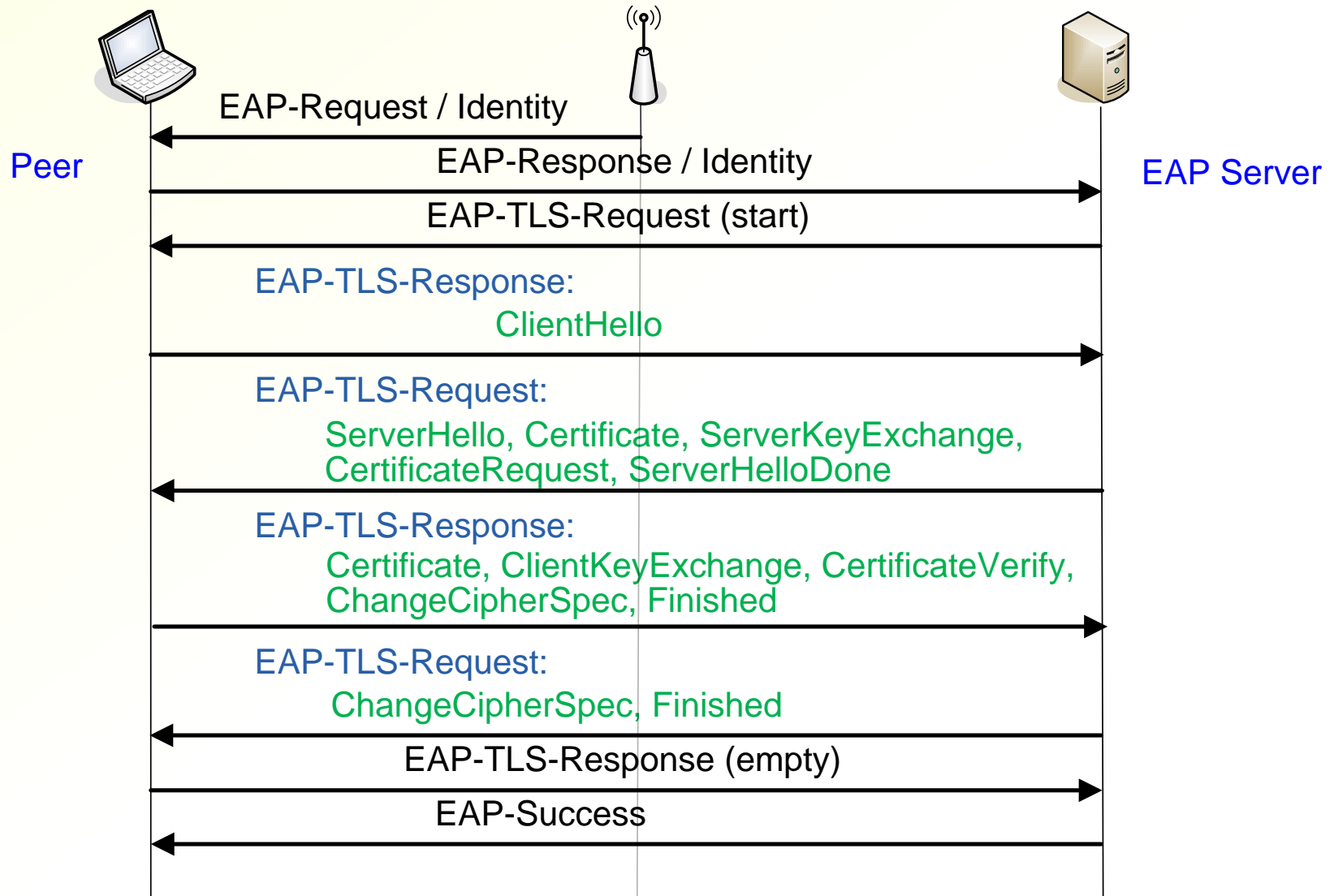
- Extensible authentication protocol (EAP) defines generic authentication message formats: Request, Response, Success, Failure
- Originally designed for authenticating dial-up users with multiple methods
- Security is provided by the authentication protocol carried in EAP, not by EAP itself
- EAP supports many authentication protocols: EAP-TLS, 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

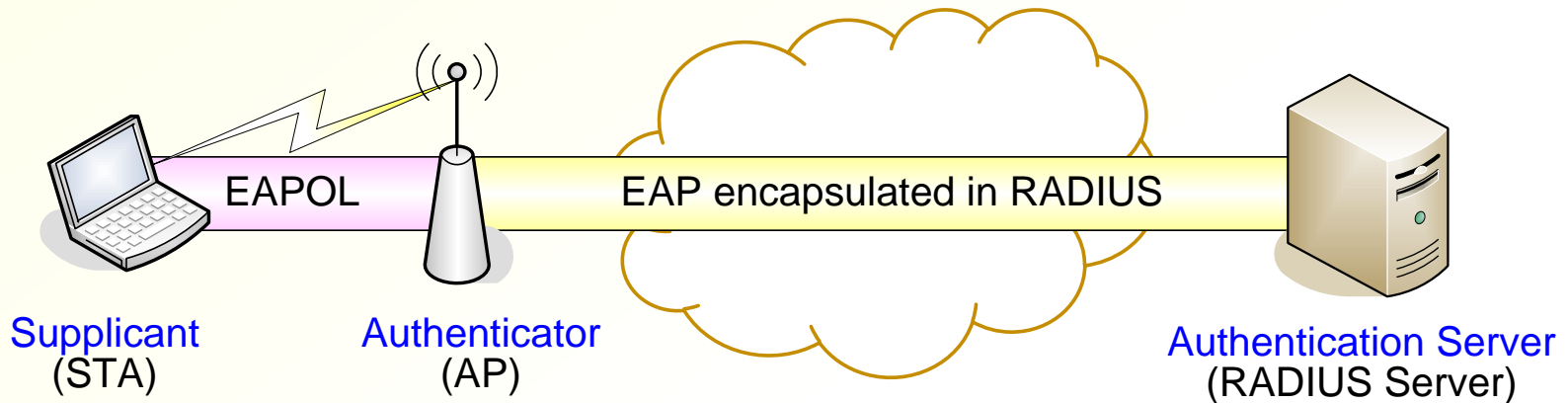


- Request-response pairs
- User identified by **network access identifier (NAI)**: username@realm
- Allows multiple rounds of request–response, e.g. for mistyped passwords

EAP-TLS Protocol



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

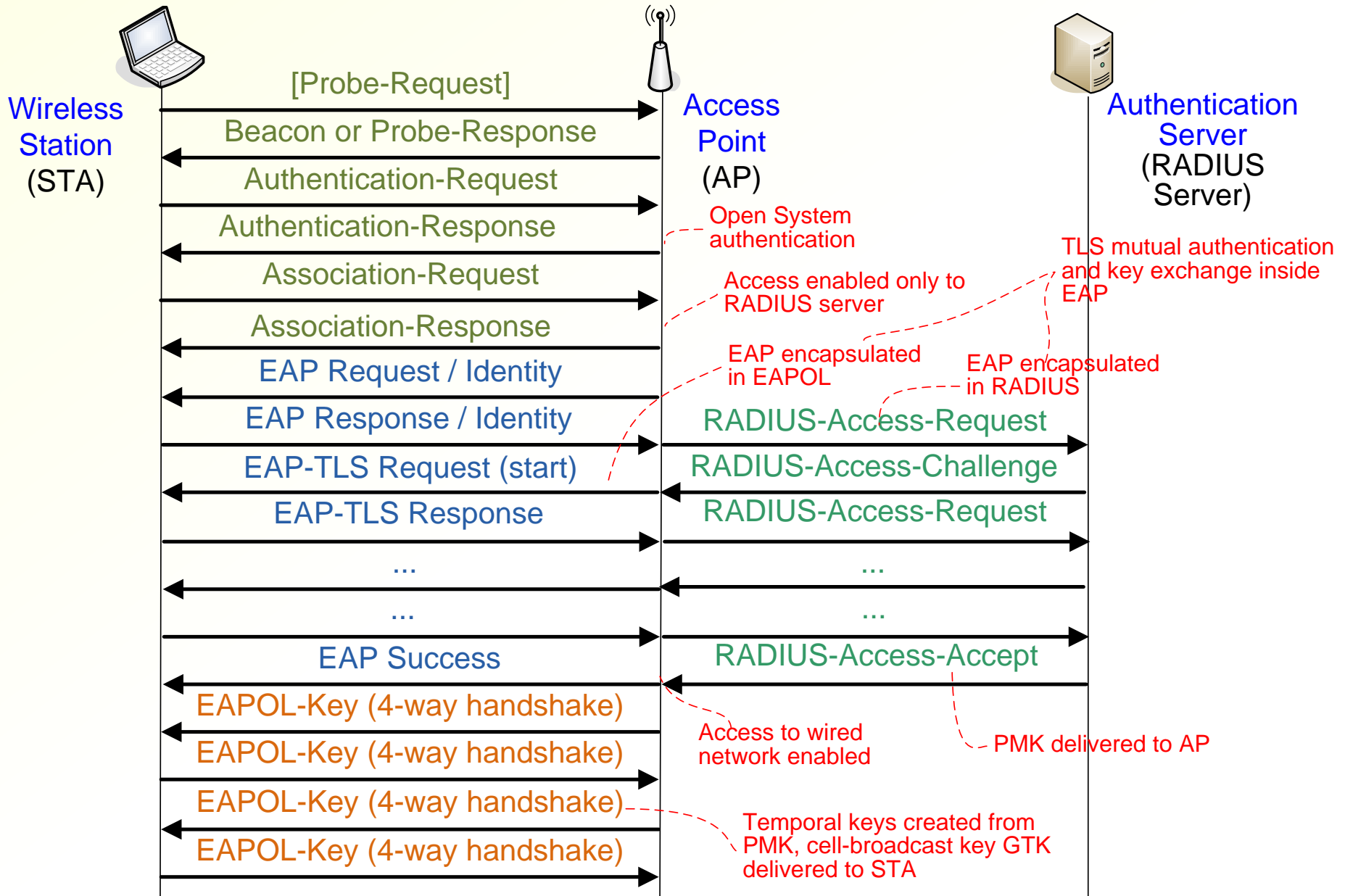
RADIUS

- 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

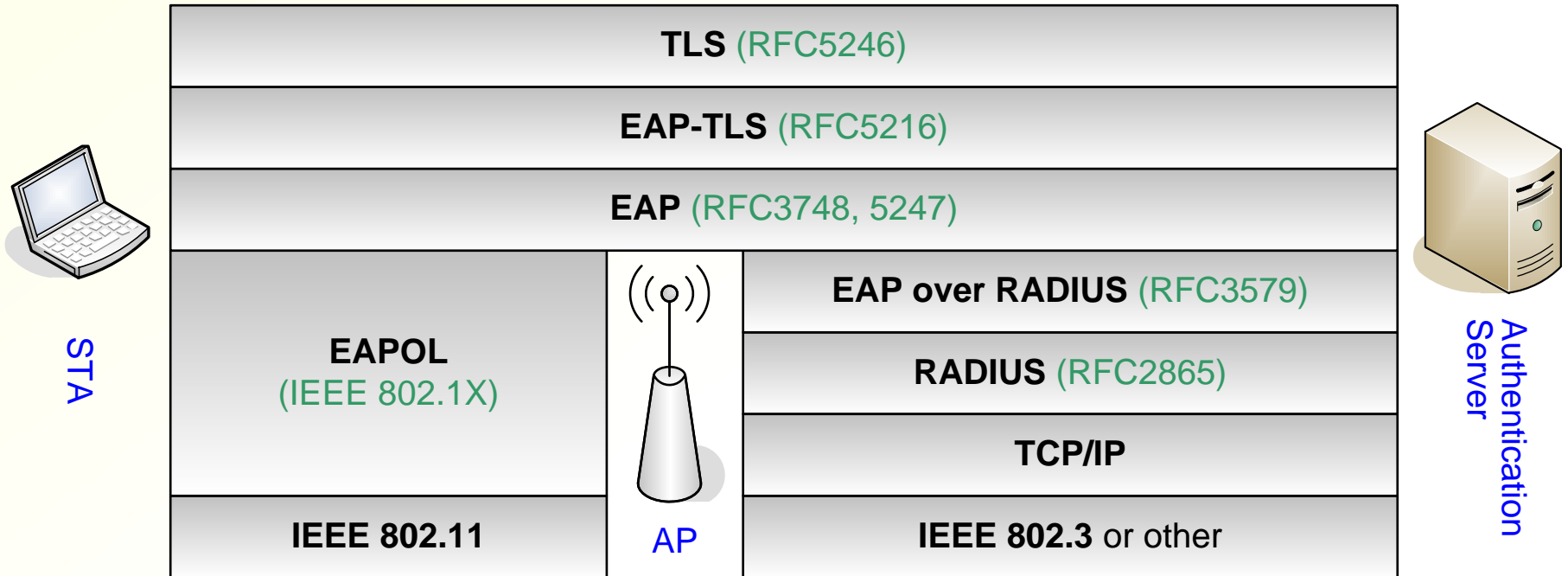
RADIUS security

- AP and authentication server share a secret
- Responses from authentication server contain an authenticator; requests from authenticator (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!)
 - Important to use a **long** (≥ 16 characters) **random** shared secret to prevent offline cracking; no need to memorize it

EAP protocol in context






802.1X stack and specifications

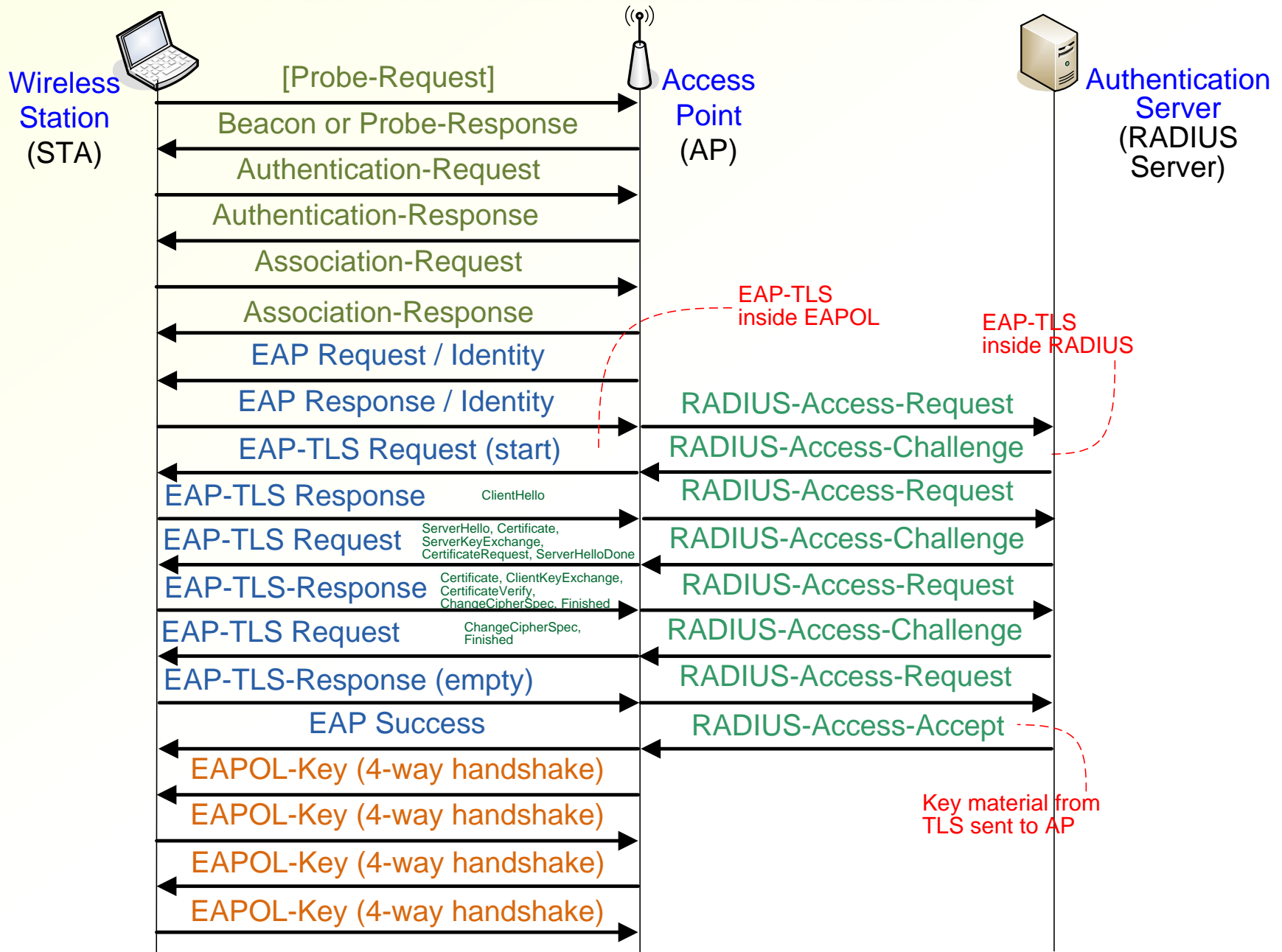


- Excessive layering?

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 WPA2 Authentication



Authentication Latency

- ~7 round trips between AP and STA for EAP-TLS
 - One less 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
- 4 round trips between AP and authentication server
 - One less when TLS session reused
- Typical authentication latency >1 second every time STA roams between APs → optimizations needed!

Session protocol: AES-CCMP

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

Session protocol: TKIP (now outdated)

- Temporal Key Integrity Protocol (TKIP)
- Designed for transition period when pre-WPA network cards were used with firmware update
- Still using 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
- **Now outdated:**
 - **Cryptographic attacks against TKIP make it insecure! Time to start using only WPA2**

What does WPA2 achieve?

- 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

Password authentication for WLAN

Captive portal

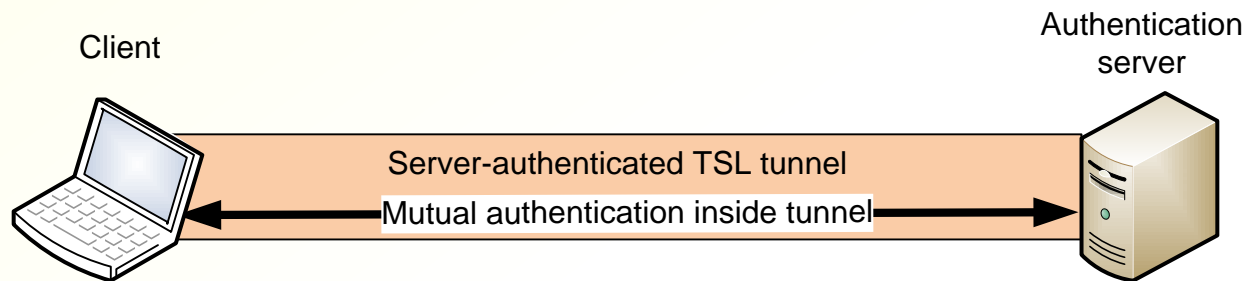
- Web-based authentication for network access; also called **universal access method (UAM)**
 - Used in hotels and wireless hotspots for credit-card payment or password authentication
- **New users are directed to an authentication web page (“captive portal”) when they open a web browser**
 - Redirection usually based on spoofed HTTP redirection; sometimes DNS spoofing or IP-layer interception
- Authenticated users’ MAC addresses are added to a whitelist to allow Internet access

PEAP, EAP-TTLS

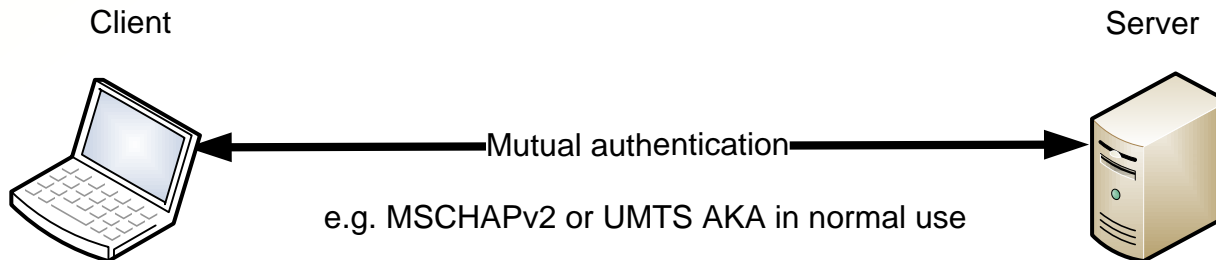
- General idea: authenticate the server with TLS, then the client inside the encrypted tunnel
- Protected EAP (PEAP) by Microsoft
 - Round 1: EAP-TLS with server-only authentication
 - Instead of EAP-Success, start encryption and move to round 2
 - Round 2: any EAP authentication method with mutual authentication
- EAP-PEAP-MSCHAPv2 (also called PEAPv0 or just PEAP): in practice, the authentication in round 2 is MSCHAPv2
- What does PEAP achieve:
 - Password authentication takes place inside an encrypted tunnel → prevents offline password cracking from MSCHAPv2 messages
 - EAP-Response-Identity sent twice, both in inner and outer EAP layer; outer layer may use the string “anonymous” for identity protection
- Similar protocols: LEAP by Cisco (insecure and no longer used) and EAP-TTLS by Funk Software/Juniper

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

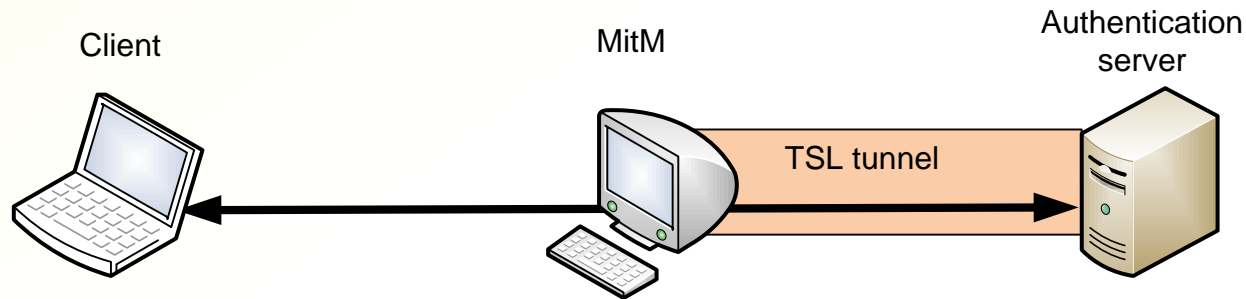


- Session key is provided by the TLS tunnel — session keys from the inner authentication are not used
- BUT... the same inner authentication methods are used also without TLS tunnelling



Tunnelled authentication problem (2)

- Attacker can pretend to be a server in the no-tunnel scenario and forward the authentication into 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 legitimate server to which the client connects



Link-layer mobility in WLAN

Additional reading

Reassociation and IAPP

- When STA moves between APs, it sends **Reassociation Request**
 - Association Request includes the old AP address
 - New AP may contact the old AP over the wire network to delete the old association there
 - Old AP may forward to the new AP any packets that still arrive there
- **Inter-access point protocol (IAPP)**
 - Protocol for communication between APs over the wire network
 - Draft specification 802.11f in 2003, **never standardized**

Wireless LAN roaming

- Moving between APs is slow: may require full association and WPA2-Enterprise authentication
 - 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?

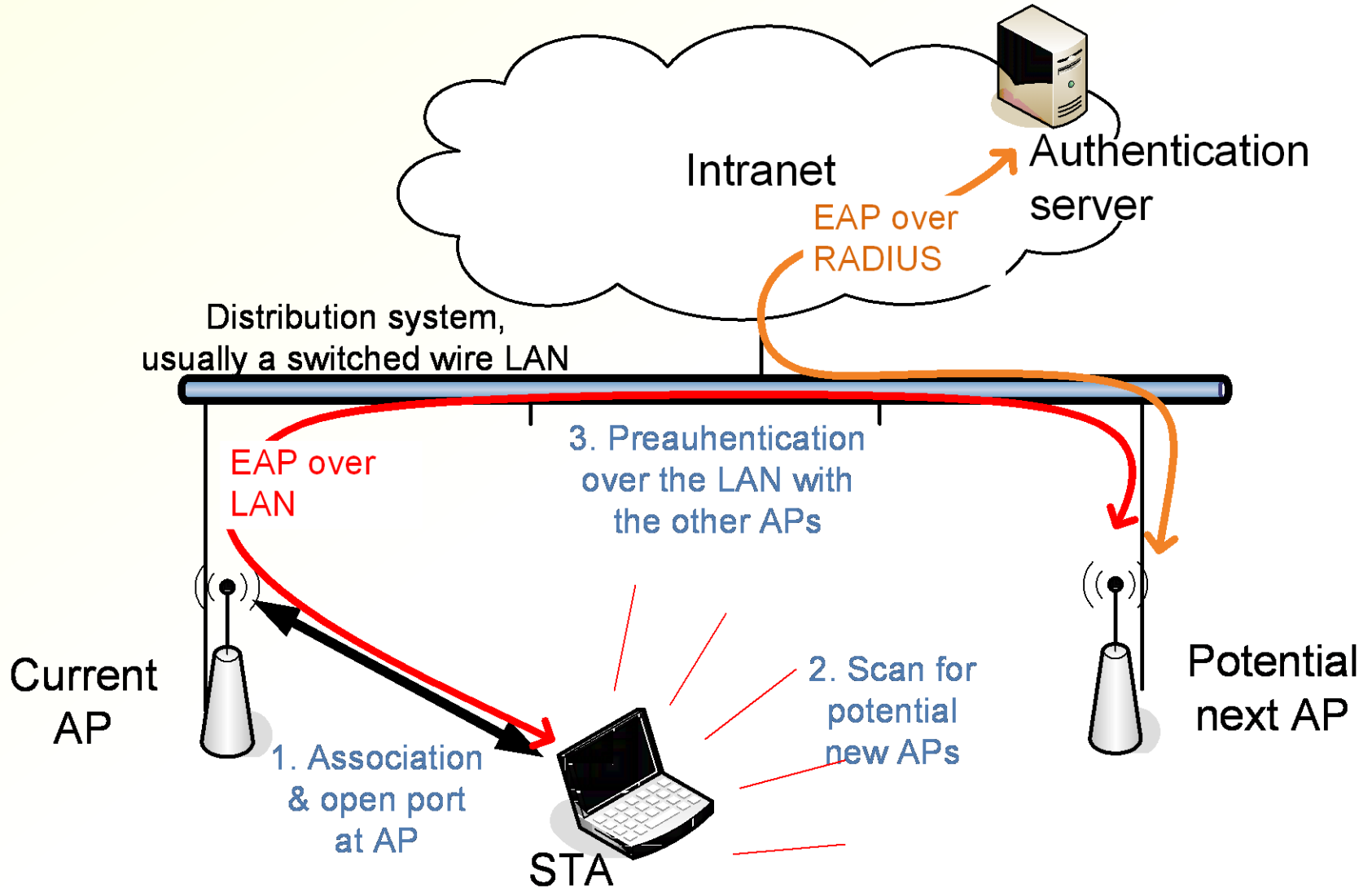
PMK caching

- 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 WPA2

Wireless switch

- Proprietary roaming solution from network equipment manufacturers
- Authenticator moved partly to a switch
- Switch pushes PMK to all or selected APs, or AP pulls key on demand
- Client STA assumes AP has cached PMK even if it has never authenticated to that AP
 - called "opportunistic PMK caching"

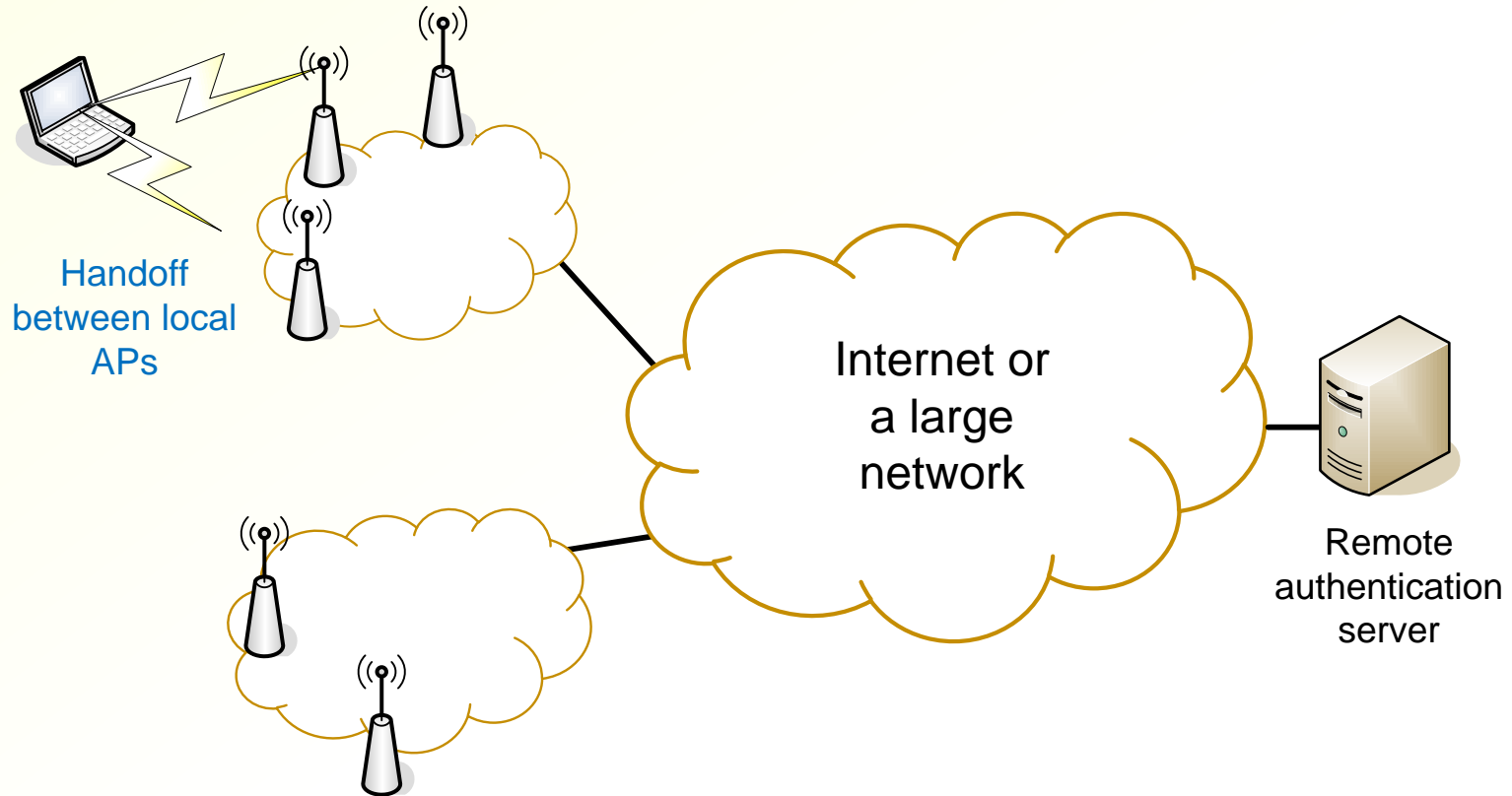
802.1X preauthentication



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 wire 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

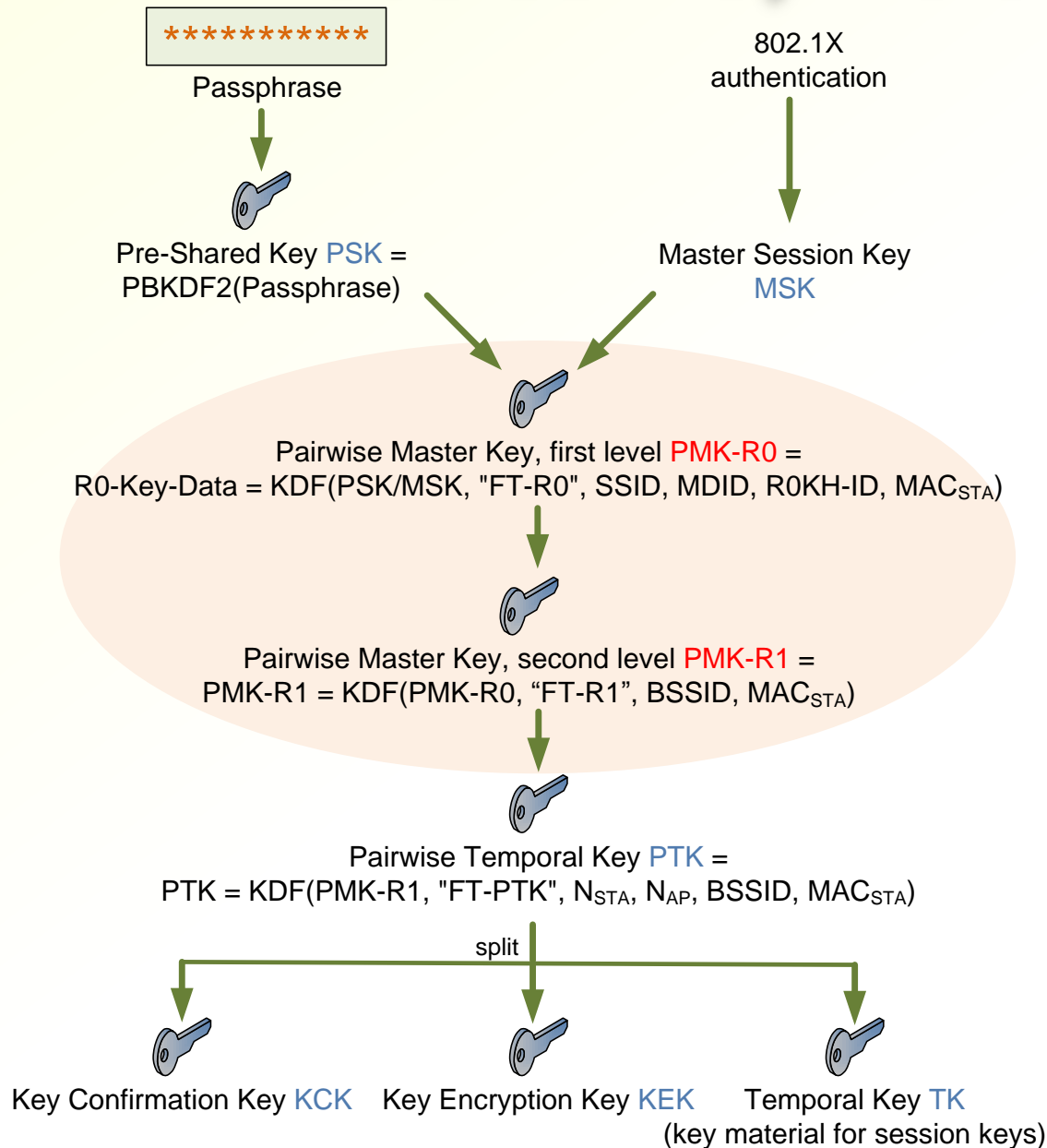


- Even local handoffs require connection to the AS, which may be far away

802.11r fast BSS transition

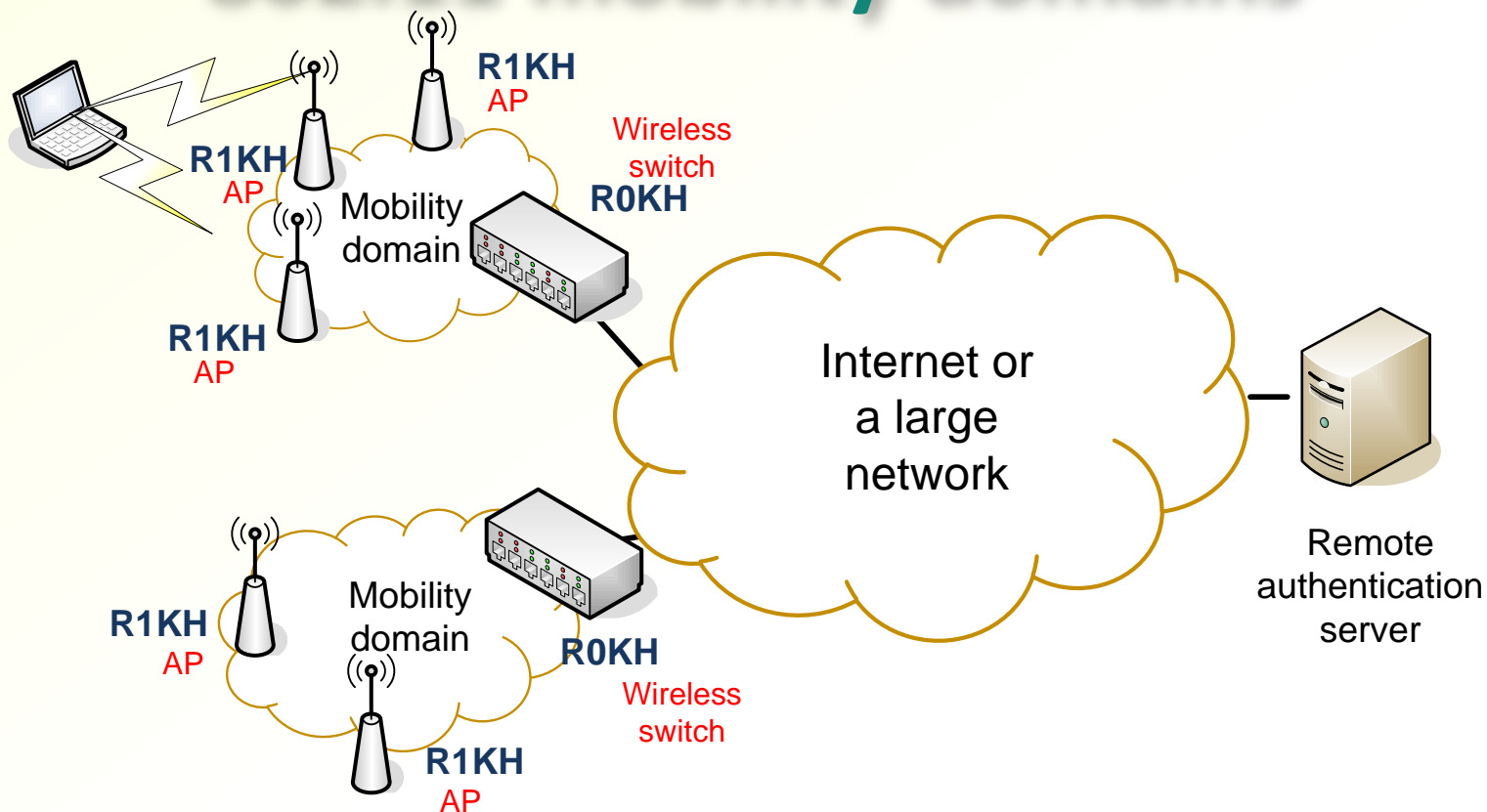
- Amendment 802.11r adds mechanisms for fast handover
 - With PSK or cached MSK, piggyback the 4-way handshake on 802.11 authentication and association messages → only 2 roundtrips between STA and AP
 - Mobility domain = group of APs close to each other + local “server” that helps in local handoffs
 - 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, pre-reservation of resources for QoS (see 802.11e) done in parallel with the 4-way handshake

802.11r key hierarchy



- **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

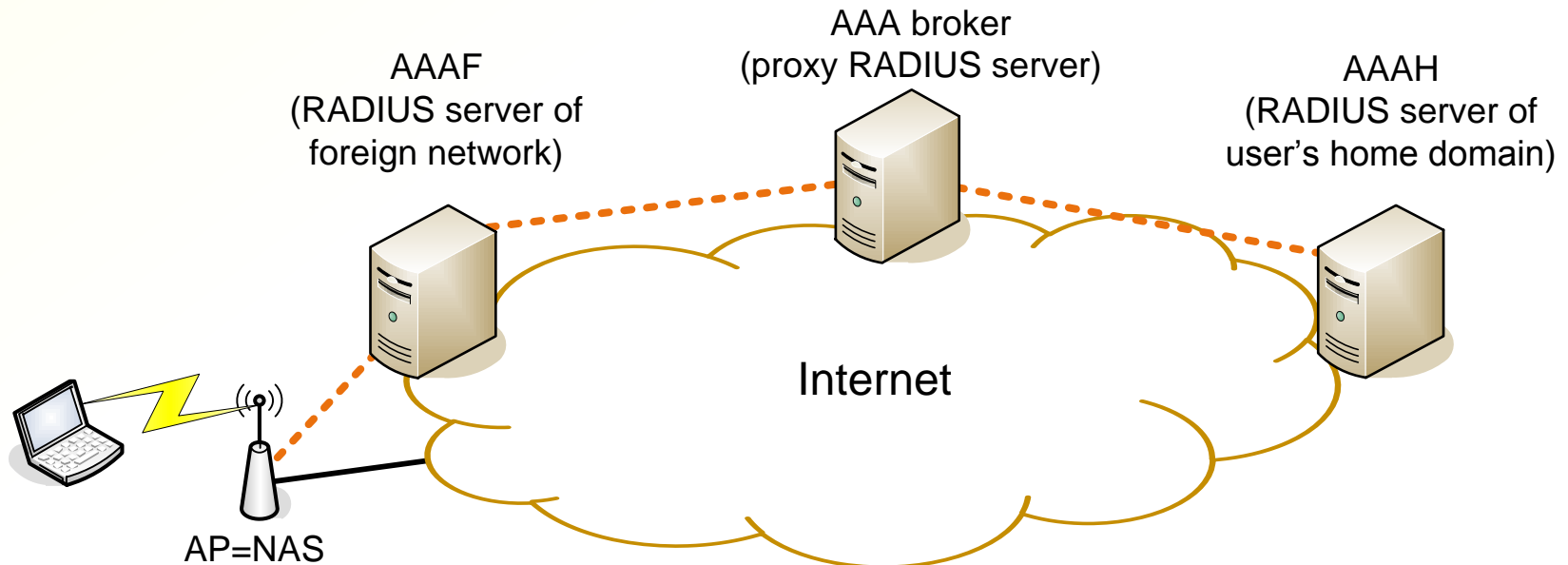
802.11 mobility domains



- 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

AAA

- Authentication, authorization and accounting (AAA)
 - Architecture and protocols for managing network access
 - Standard protocols: **DIAMETER** (newer), **RADIUS** (still widely used)
- Roaming support:
 - **Visited AAA** (VAAA) acts as a proxy for **home AAA** (HAAA)
 - **AAA brokers** can be used to create roaming federations



Eduroam

- **Eduroam** is a federation for wireless roaming between educational institutions
 - User is registered at the home university, which as a RADIUS server (AAAH)
 - National educational and research network (NREN), e.g. Funet, operates a national roaming broker
 - National broker are connected to a regional broker for international roaming
- EAP authentication: **user's home institution determines the EAP authentication method**
 - Aalto uses PEAP
- Users identified by NAI: `username@realm`
 - NAI for Aalto users: `username@aalto.fi` or `firstname.lastname@aalto.fi` (seems to vary between users)
 - In PEAP, the outer NAI only needs to have only correct realm, but Aalto seems to require the username to be correct

Related reading

- Gollmann, Computer security, 3rd ed., chapters 19.5–19.6
- Stallings, Network security essentials, 4th ed. chapter 6.1–6.2

Exercises

- Is WLAN security alternative or complementary to end-to-end security such as TLS?
- Why is WPA-Enterprise not widely used in home wireless networks, wireless hotspots or Internet cafes?
- Why are password-based methods needed for authorizing WLAN access?
- UAM intercepts the first web request made by the user. What reliability issues might this cause?
- Can the UAM access control be circumvented? How secure can it be made? Can the password be leaked?
- If a cellular network operator wants to offer wireless hotspot access to its customers, how could the SIM card be used for authorizing WLAN access from the phones?
- How could the network attachment and access control protocols be further optimized to reduce latency? Which standards bodies would need to be involved?