Wireless network security

Security of IT infrastructure

Michal Rjaško

Why is security more of a concern in wireless?

- Physical (in)security
  - Physical connections between devices are replaced by logical associations
  - Sending and receiving messages do not need physical access to the network infrastructure
- Broadcast communications
  - Transmission can be overheard by anyone in range
  - Anyone can generate transmission
    - Which will be received by devices in range
    - Which will interfere with other nearby transmissions and may prevent their correct reception (jamming)

Why is security more of a concern in wireless?

- Eavesdropping is easy
- Sending fake messages is easy
- Replaying previously recorded messages is easy
- Illegitimate access to the network and its services is easy
- Denial of service is easily achieved by jamming
- Pretending to be someone else is easy

Wireless communication security requirements (1)

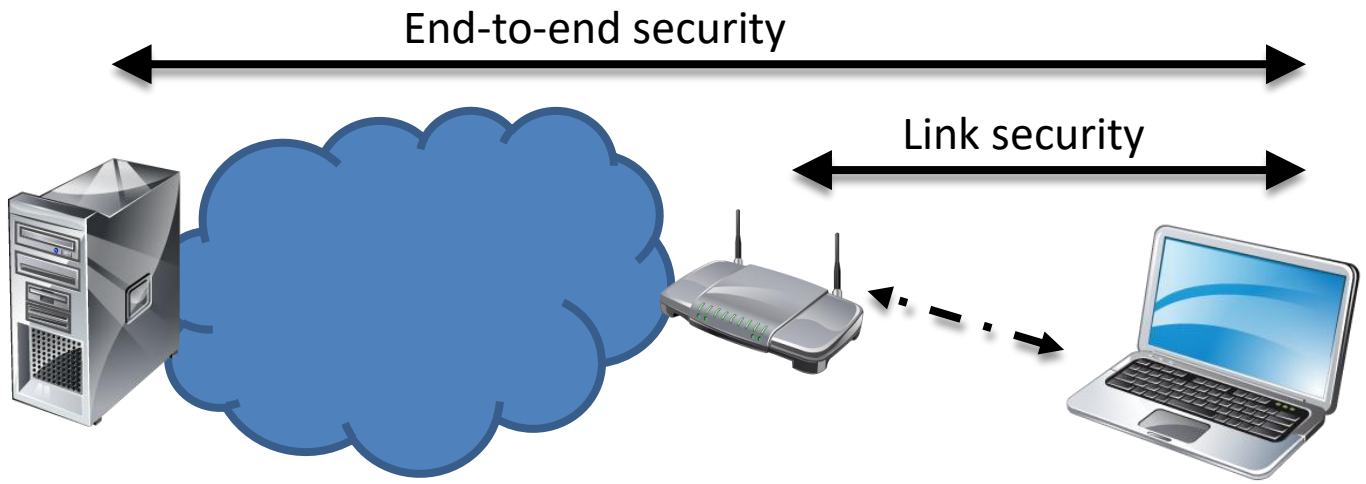
Design for mobile devices

- Low power consumption
  - Minimize computation complexity of algorithms
  - Minimize network communication
- Limited computational power in IoT devices
- Cryptographic and other security-related algorithms must be simple
- Need to minimize communications overhead for security protocols

Wireless communication security requirements (2)

- Confidentiality
  - Messages sent over wireless links must be encrypted
- Authenticity
  - Origin of messages received over wireless links must be verified
- Replay detection
  - Freshness of messages received over wireless links must be verified
- Integrity
  - Integrity of messages received over wireless links must be verified
- Access control
  - Access to the network should be provided only to legitimate entities
  - Access control must be permanent, not only when device joins the network
- Protection against jamming

Link versus end-to-end security



- End-to-end security
  - Provided by network (e.g. IPsec, VPN), transport (TLS) or application layer (e.g. application specific)
- Link security
  - Provided by link layer (802.11 WEP, WPA, 802.11i)

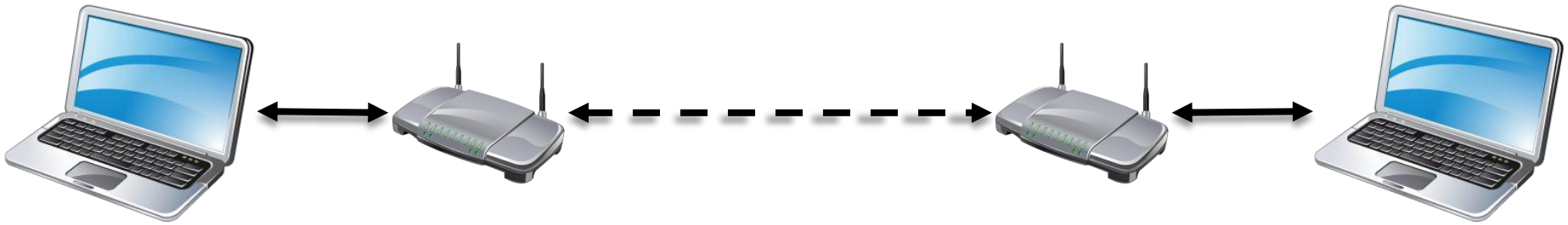
Introduction to Wifi

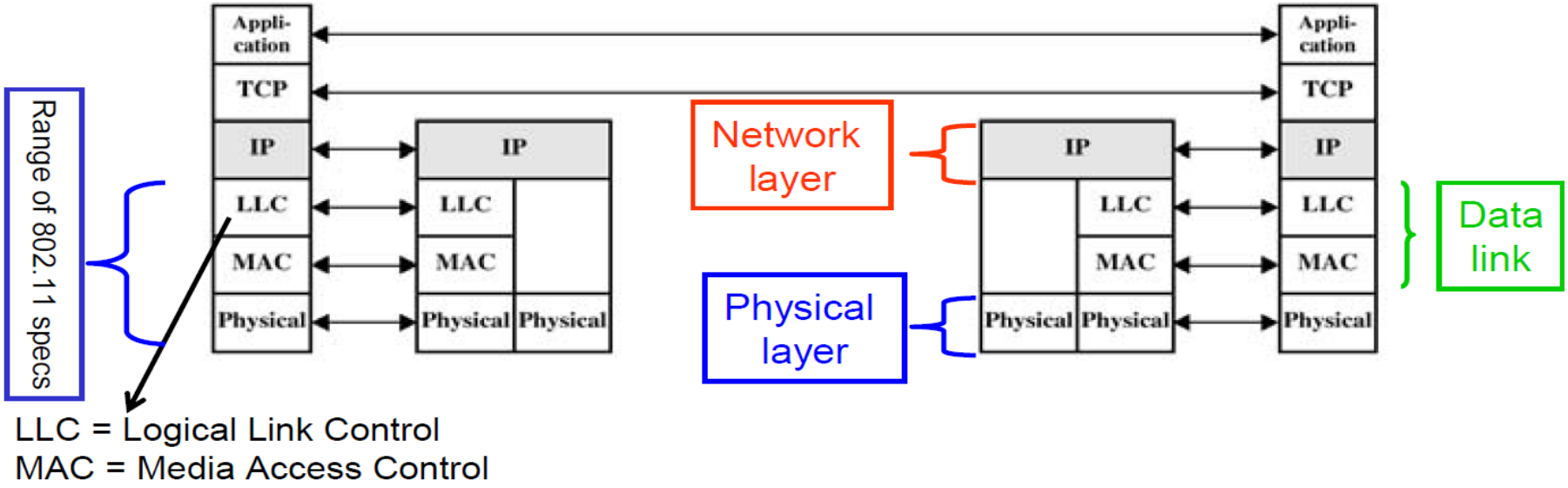
- Standard 802.11 in 1997
  - Original speed 1 – 2 Mb/s
- Specifies 1st and 2nd layer in OSI model
  - Physical layer
  - Data layer
- Compatibility of devices is guaranteed by WECA (Wireless Ethernet Compatibility Alliance)
  - Certification
  - Now Wi-Fi Alliance

Introduction to Wifi

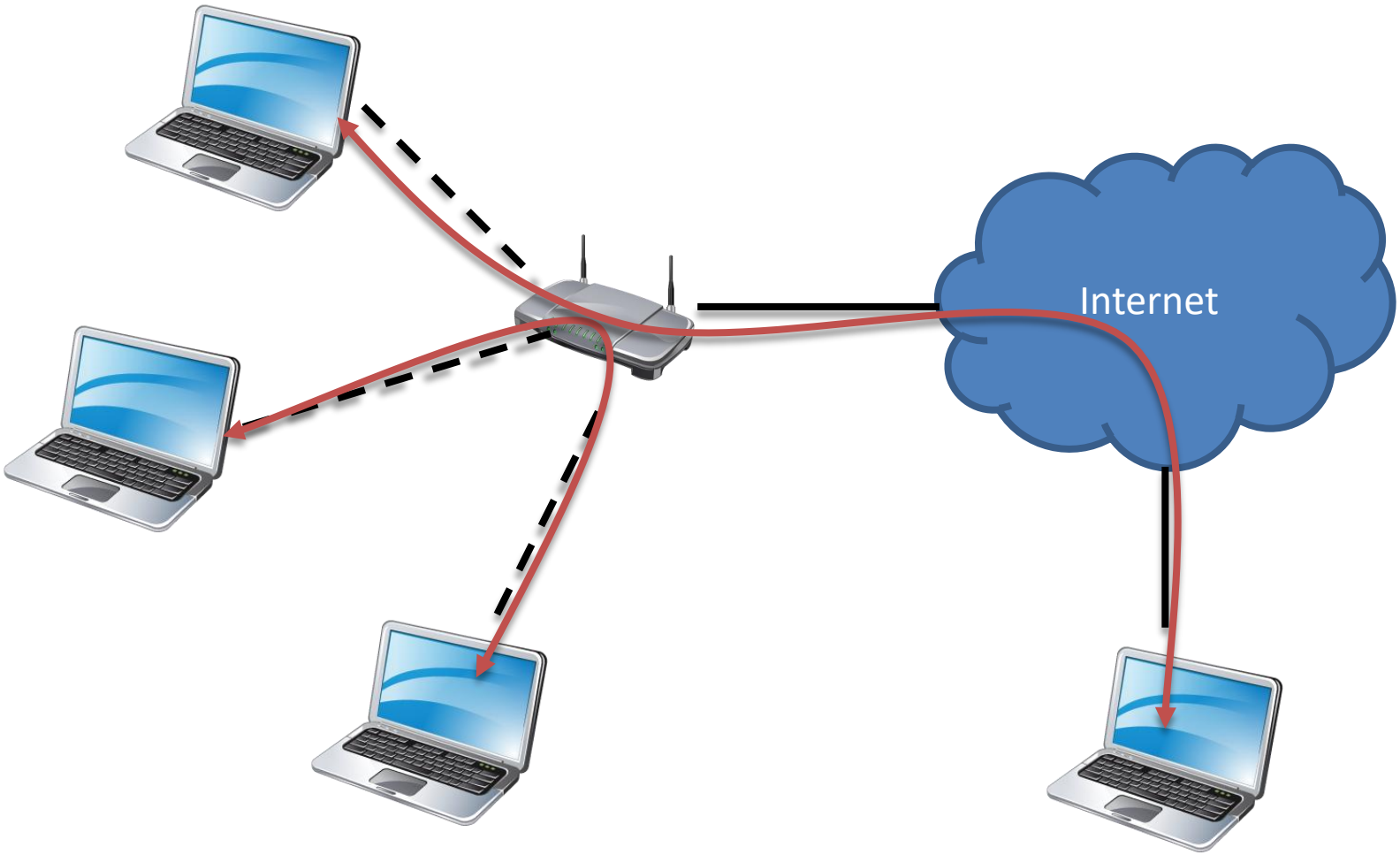
- Two types of devices
  - Wireless stations (STA)
    - Computer, PDA, smartphone, tablet, glasses, watch, ...
  - Access point (AP)
    - Bridge between wireless and wired network
    - Composed of
      - Radio
      - Wired network interface
      - Bridging software
    - Multiple mobile devices are connected to the network via one access point

Introduction to Wifi



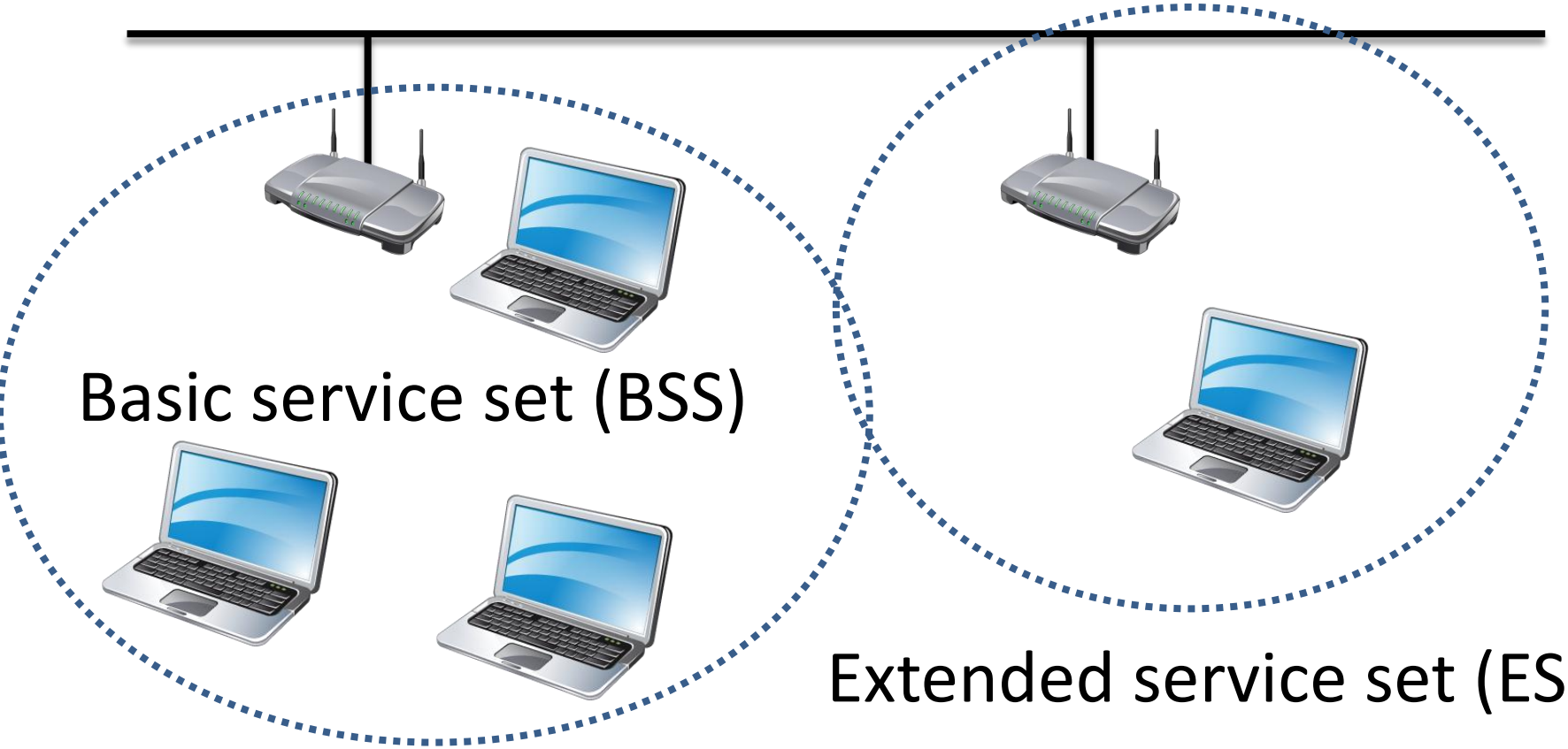


Introduction to Wifi



Introduction to Wifi

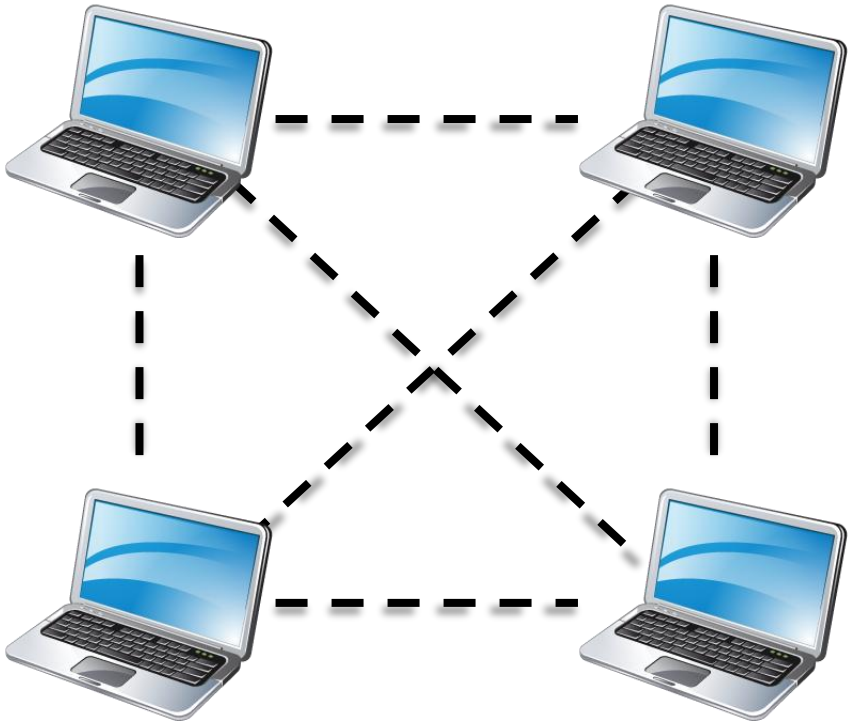
Infrastructure mode



- SSID (Service Set Identifier) is attached to each packet
- Multiple APs with the same SSID are ESS

Introduction to Wifi

Ad-hoc mode



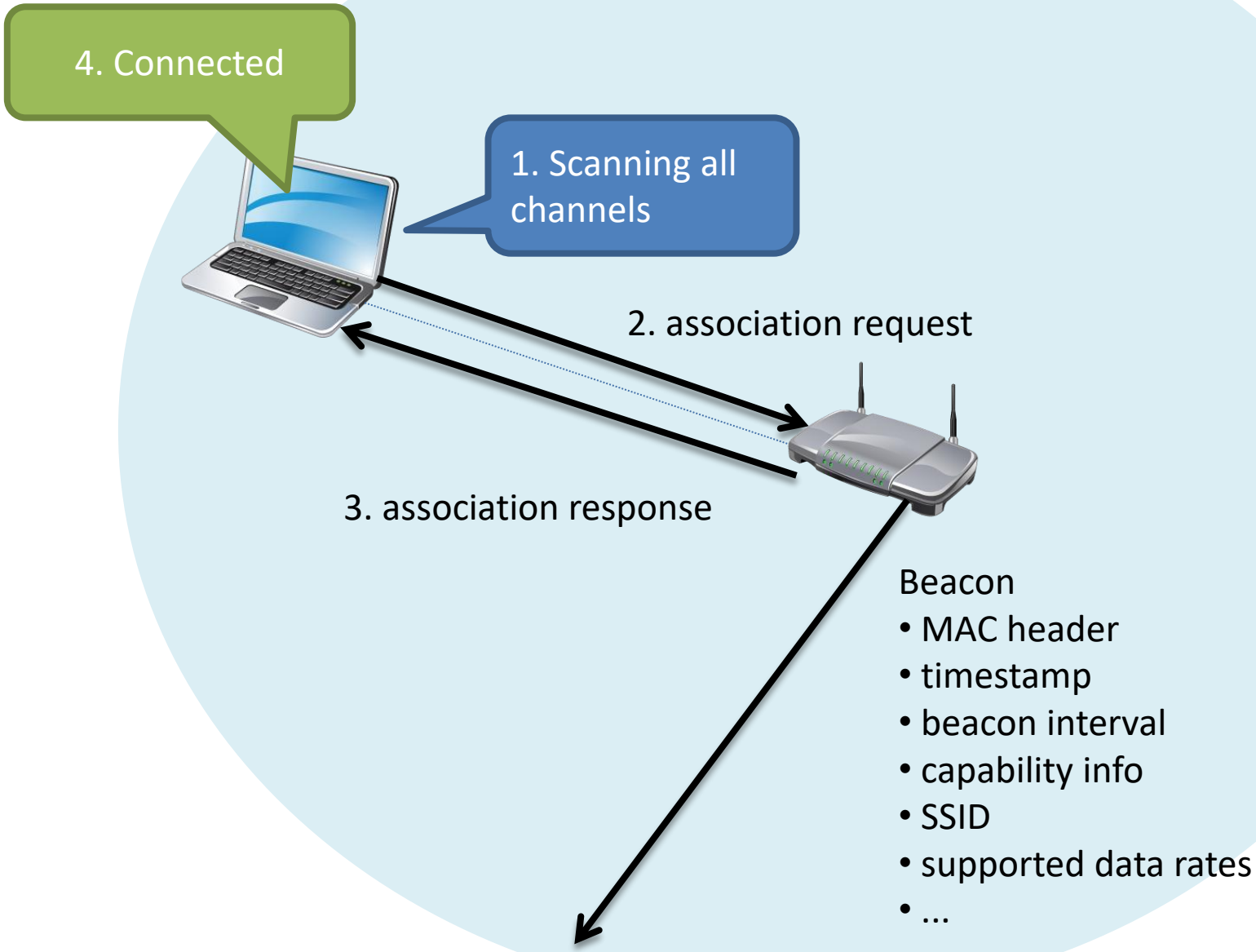
WiFi standards

- **IEEE 802.11 (1997)**
  - **2,4 GHz, 1-2Mb/s**
  - **WEP**
- IEEE 802.11b (1999)
  - 2,4 GHz, 11Mb/s
- IEEE 802.11g (2003)
  - 2,4 GHz, 54 Mb/s
- **IEEE 802.11i (2004)**
  - **WPA, WPA2**
- IEEE 802.11a (1999)
  - 5GHz, 54 Mb/s
- IEEE 802.11e (2005)
  - QoS (Quality of Service)
- IEEE 802.11f (2003)
  - Inter-Access Point Protocol
- IEEE 802.11n (2009)
  - More than 100 Mb/s, 5GHz and 2,4 GHz
- …
- 2019 WPA3

WiFi – Access control types

- No access control (unsecured networks)
- Access control based on MAC address
  - It's easy to falsify MAC address
- Hidden SSID
  - AP need not to broadcast SSID
  - Connecting to network requires SSID
  - Attacker can eavesdrop SSID
- Access control based on a shared secret (key) between station and AP
- 802.1x, EAP, RADIUS

Connecting to unsecured network



802.11 WEP
Wired Equivalent Privacy

- Part of standard 802.11
- Goal:
  - Make WiFi at least as secure as a wired LAN (with no particular protection mechanisms)
  - WEP was never intended to achieve strong security
- Services:
  - Access control to network
  - Message confidentiality
  - Message integrity

Wireless communication security requirements and WEP



Confidentiality

- Messages sent over wireless links must be encrypted



Authenticity

- Origin of messages received over wireless links must be verified



Replay detection

- Freshness of messages received over wireless links must be verified



Integrity

- Integrity of messages received over wireless links must be verified



Access control

- Access to the network should be provided only to legitimate entities
- Access control must be permanent, not only when device joins the nework



Protection against jamming

WEP – Access control

- Based on a shared secret key
- Key is shared between all
  - Stations
  - Access points
- All connected stations are able to decrypt messages sent by other stations
- The key is usually manually placed into all stations and APs
  - Nightmare for administrators of large networks

WEP – access control

Two types of access control

- Without authentication
  - Everyone can connect to AP
  - However, messages are encrypted, thus STA must know the shared key
- Shared key authentication
  - (see next slide)
- At first glance it seems that the second type is more secure
  - In fact it’s quite the opposite (details later)

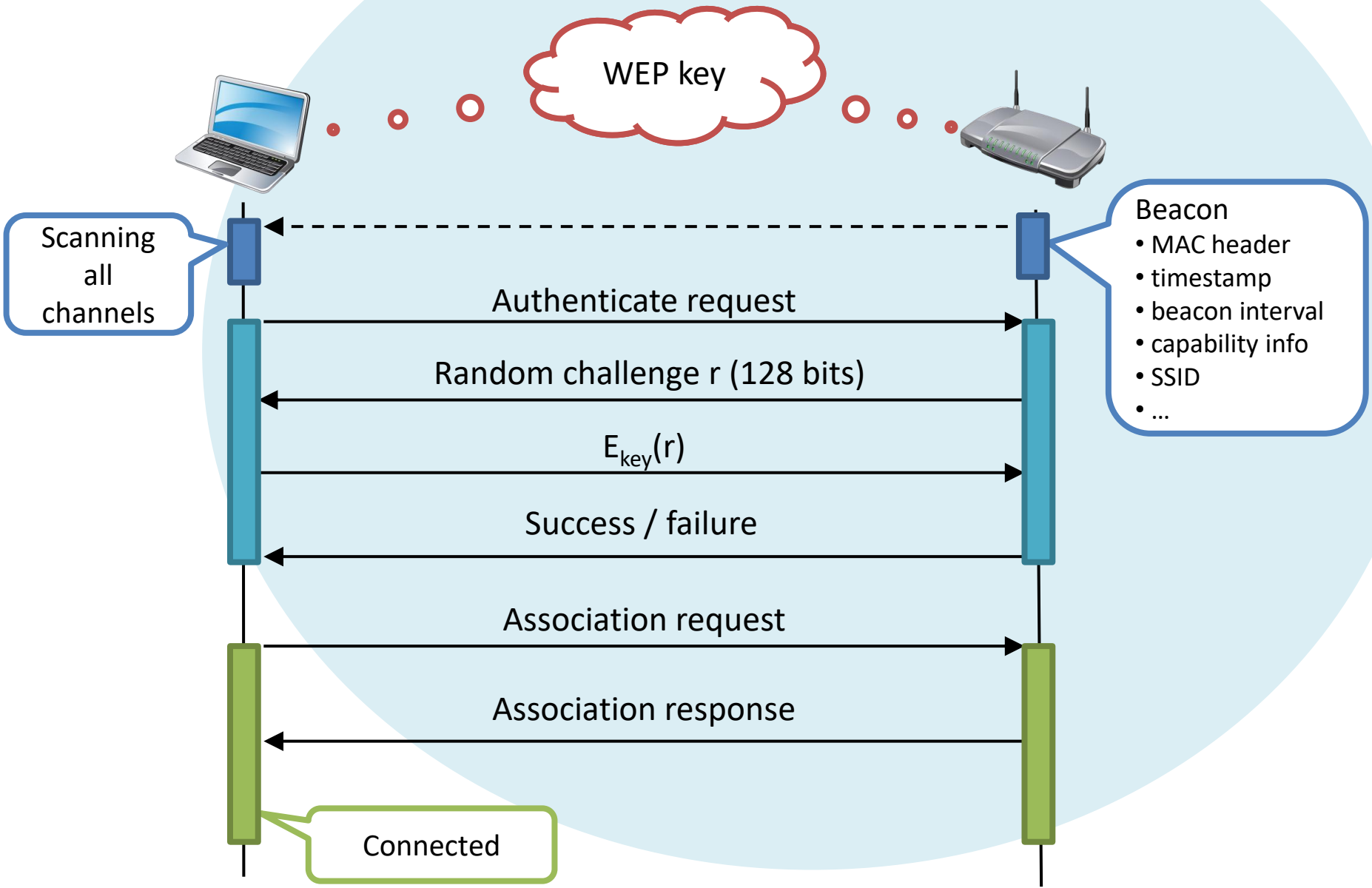
WEP – access control

Shared key authentication

- Before connecting to the network, station must authenticate itself
- Authentication is based on simple „challenge-response“ protocol:
  - STA → AP: authenticate request
  - AP → STA: authenticate challenge (r) //r has 128 bits
  - STA → AP: authenticate response ($e_{key}(r)$)
  - AP → STA: authentication success/failure

- When STA is authenticated, STA can send „association request“ and AP will reply
- If authentication fails, connection is refused

Connecting to a network secured by WEP



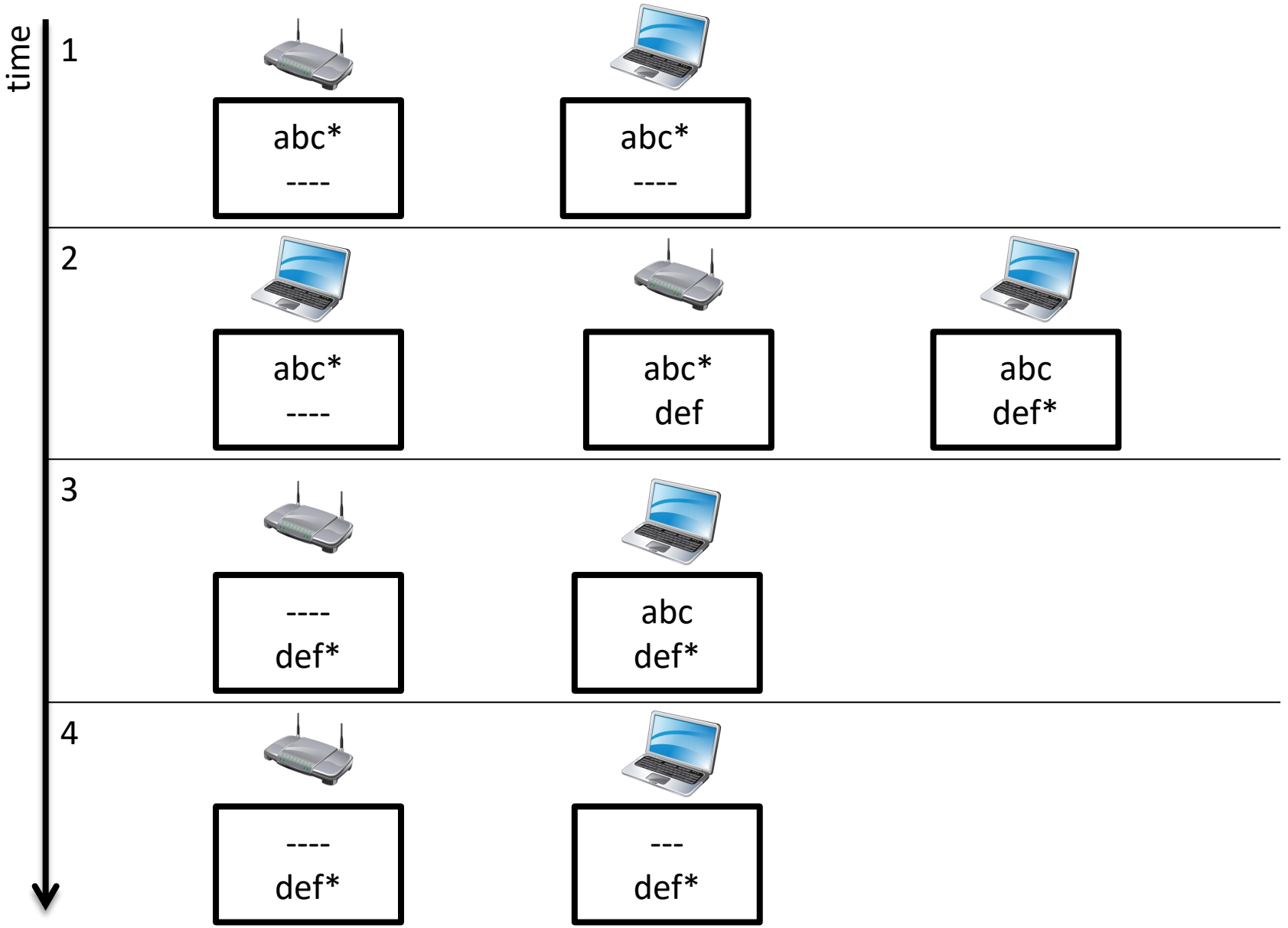
WEP – confidentiality

- Messages are encrypted using RC4 (stream cipher from 1987, designed by Ron Rivest)
  - Process of encryption:
    - For each message
      - RC4 is initialized with the shared key (40-bits / 104 bits)
      - RC4 produces pseudo-random stream of bits (“key stream”)
      - The key stream is XORed with the message
    - Deciphering is similar
  - It is important to XOR each message with different “key stream”
    - RC4 is thus initialized with the shared key and initialization vector IV
      - Shared key is the same for each message
      - 24-bit IV is changing with each message

WEP - keys

- Shared key is known for all stations in a group
  - If someone leaves the group, the key must be changed
- Original standard requires 64 bit key for RC4
  - 40 bits were reserved for the secret key and 24 bits for initialization vector
  - After releasing key-length restrictions in USA also 128 bit key was standardized, from which 104 bits are for secret key and 24 bits are for initialization vector
- In case of large networks, it is impossible to change the secret key in all stations at once
- WEP supports multiple secret keys
  - One key is active – it is used for message encryption
  - Any key can be used to decrypt messages
  - Each message contains key ID that allows the receiver to find out which key should be used for decryption

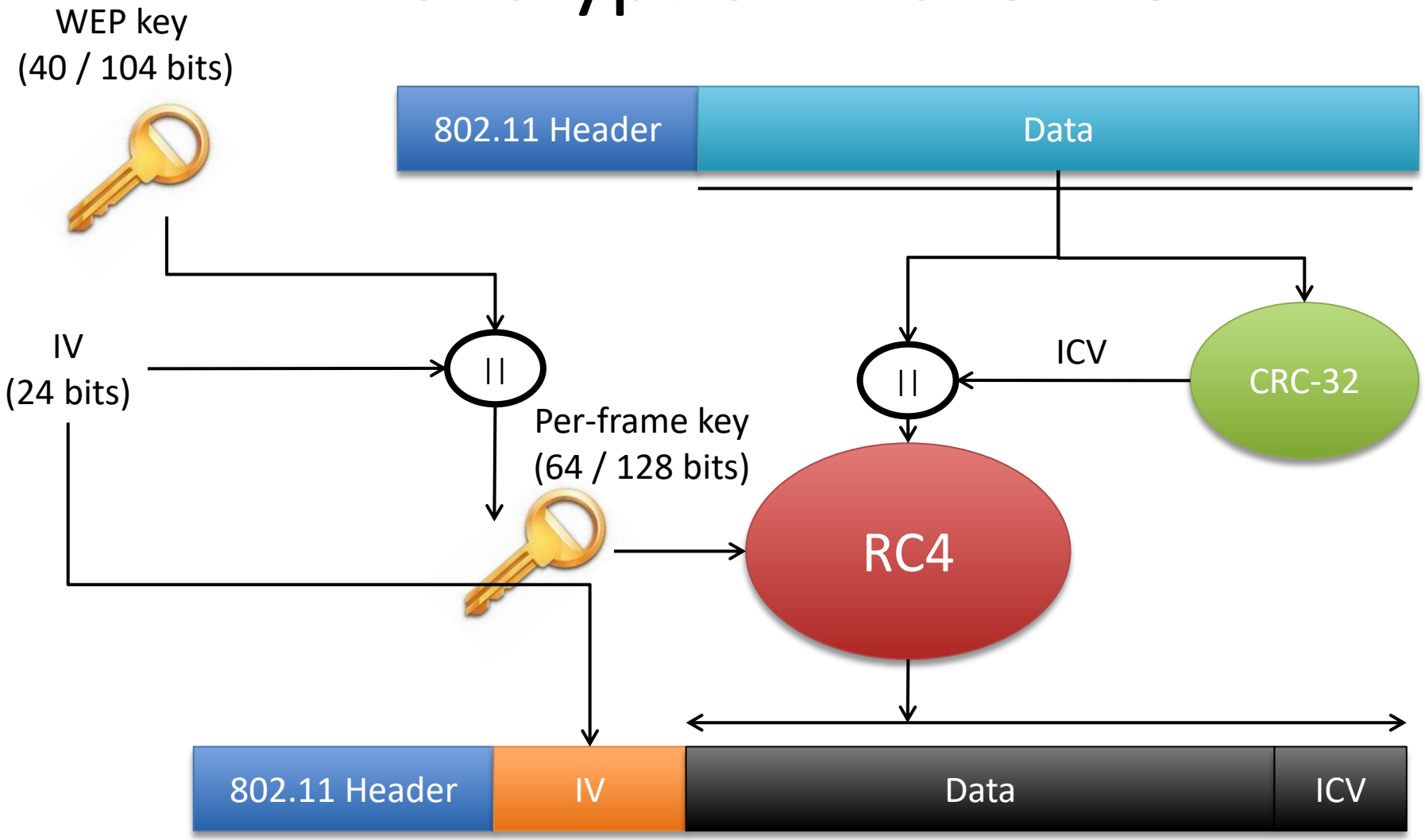
WEP – the key change process



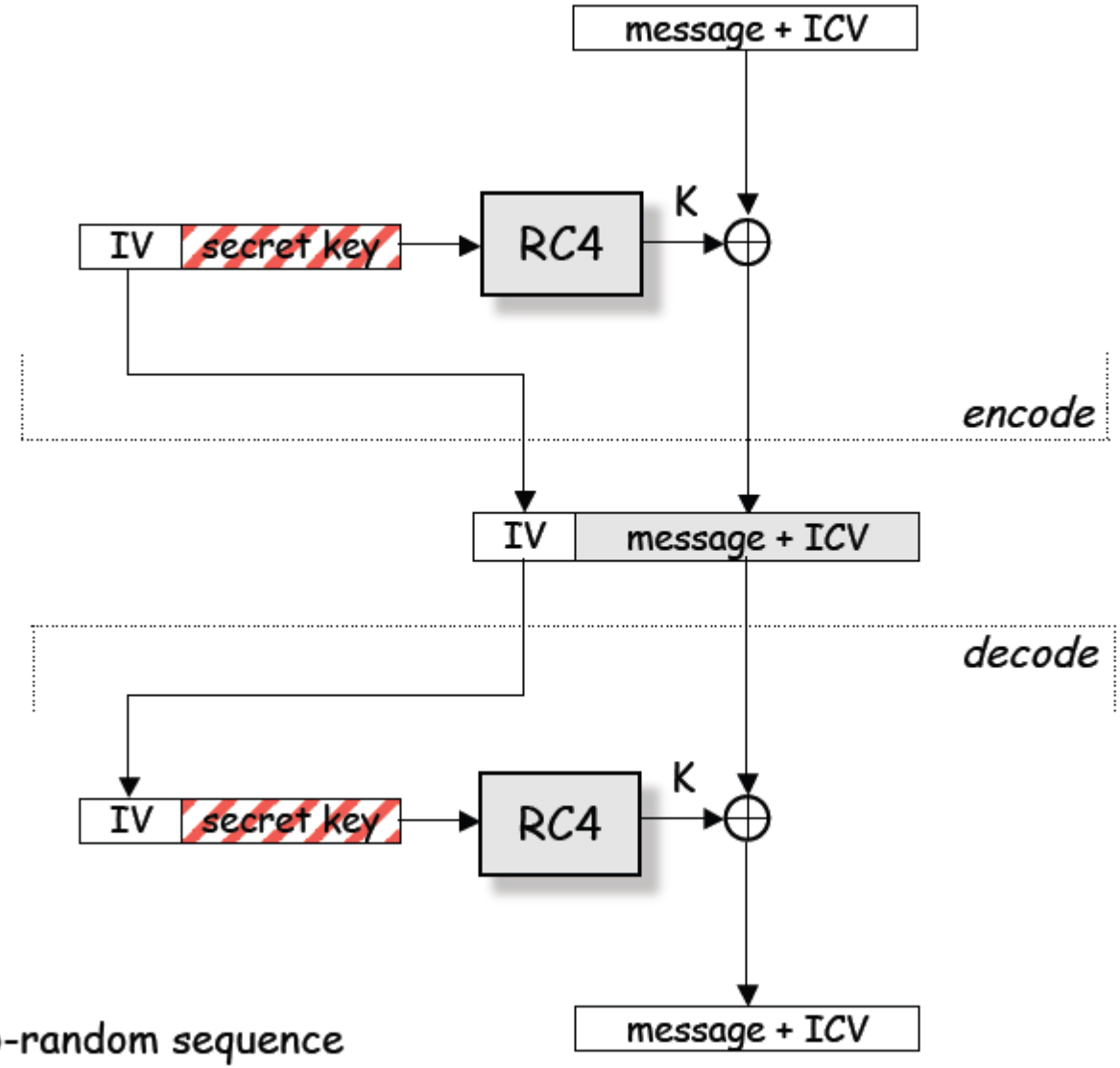
WEP – Integrity

- Integrity control by encrypted CRC (Cyclic Redundancy Check)
  - First, ICV (integrity check value) is computed and attached to the end of message
    - ICV has 32 bits
  - Message and ICV are then encrypted
- CRC is based on cyclic self-correcting codes
  - It's designed to detect / correct common errors produced by noise over communication channel
  - Need not to detect intentional errors

WEP encryption – overview



WEP – encryption / decryption



K: pseudo-random sequence

WEP – security flaws

- Authentication is one-way only
  - AP is not authenticated to the station
  - Station risks communication with malicious AP
- The same secret key is used for authentication and encryption
  - Weakness in any of the protocols can be used to break the key

WEP – security flaws

- No „session key“ is established during authentication
  - Access control is not permanent
  - Once a station is authenticated to the AP, an attacker can send malicious messages using the MAC address of STA
  - correctly encrypted messages cannot be produced by the attacker, but reply of previously overheard messages is still possible

WEP – security flaws

STA can be impersonated:

- Recall the challenge-response protocol for authentication:
  - ...
  - AP → STA: r //r has 128 bits
  - STA → AP: IV||(r $\oplus$ K)
  - …

  Where K is 128-bit key stream from RC4 initialized on IV and the shared key
- An attacker can compute:

  r $\oplus$ (r $\oplus$ K) = K
- Then it can use K to impersonate STA later
  - ...
  - AP → attacker: r'
  - Attacker → AP: IV||r' $\oplus$ K
  - …

WEP – security flaws

- WEP has no replay protection at all
  - 802.11 does not specify how to compute IV, whether it must be incremented after each message
- The attacker can manipulate messages despite the ICV mechanism and encryption:
  - CRC is linear with respect to XOR:
    - $CRC(X \oplus Y) = CRC(X) \oplus CRC(Y)$
  - Attacker observes $(M||CRC(M)) \oplus K$, where K is a key stream from RC4
  - For each ΔM, the attacker can compute $CRC(\Delta M)$
  - Hence, the attacker can compute:

$$((M||CRC(M)) \oplus K) \oplus (\Delta M||CRC(\Delta M)) =$$
$$((M \oplus \Delta M)||(CRC(M) \oplus CRC(\Delta M))) \oplus K =$$
$$((M \oplus \Delta M)||CRC(M \oplus \Delta M)) \oplus K$$

WEP – security flaws

- IV reuse
  - IV space is too small – 24 bits
    - 16,777,216 possible values
    - After around 17 mil., all IVs are reused
    - A busy AP at 11 Mbps can use whole IV space in 7 hours
  - The same IV used in two messages M_1, M_2 means, that they were encrypted with the same key stream K
    - Hence, the attacker can compute
      - $C_1 \oplus C_2 = (K \oplus M_1) \oplus (K \oplus M_2) = M_1 \oplus M_2$

WEP – security flaws

- Weak RC4 keys
  - For some seed values (called weak keys), the beginning of the RC4 output is **not really random**
  - If a weak key is used, first few bytes of the output reveals a lot of information about the key
  - Some IV values produce weak keys for RC4
    - The attacker will know that, since IV is sent in clear
  - WEP encryption can be broken by capturing a few million messages

WEP – lesson learnt

- Engineering security protocols is difficult
  - One can combine otherwise strong building blocks in a wrong way and obtain insecure system at the end
    - Example 1:
      - Stream ciphers alone are OK
      - Challenge-response protocols for entity authentication are OK
      - But they shouldn't be combined with the same key
    - Example 2:
      - Encrypting a message digest to obtain an ICV doesn't work if the message digest function is linear with respect to the encryption function
- Avoid the use of WEP (if possible)

Overview of IEEE 802.11i

- After the collapse of WEP, IEEE started to develop a new security architecture – 802.11i
- Main novelties in 802.11i with respect to WEP
  - Access control model is based on 802.1X (EAP, Radius)
    - Possibility to use strong cryptographic protocols as TLS
  - Authentication process results in a shared session key (prevents session hijacking)
  - Different functionalities (encryption, integrity) use different keys derived from the session key using one way function
  - Better integrity control
  - Better encryption

IEEE 802.11i standard

- Defines the concept RSN (Robust Security Network)
  - Integrity protection and encryption is based on AES
  - Nice solution but incompatible with old hardware
  - Known as WPA2 (WiFi Protected Access 2)
- Defines also protocol TKIP (Temporal Key Integrity Protocol)
  - Encryption based on RC4, but WEP problems have been avoided
  - Integrity protection based on Michael
  - Ugly solution, but works on old hardware
  - Known as WPA (WiFi Protected Access)

802.11 – Security solutions
comparison

	WEP	WPA	WPA2
Access control	pre-shared key	802.1X / pre-shared key	802.1X / pre-shared key
Authentication	-	EAP / pre-shared key	EAP / pre-shared key
Encryption	RC4	TKIP (RC4)	AES

802.11 – Security solutions comparison

	WEP	WPA	WPA2
Cipher	RC4	RC4	AES
Key size	40 (104) bits	128 bits encryption 64 bits authentication	128 bits
IV size	24 bits	48 bits	48 bits
Integrity protection	CRC-32	Michael	CBC-MAC
Header integrity	-	Michael	CBC-MAC
Replay protection	-	Sequential IV	Sequential IV
Key management	-	EAP (802.1x)	EAP (802.1x)

IEEE 802.11i
Access control

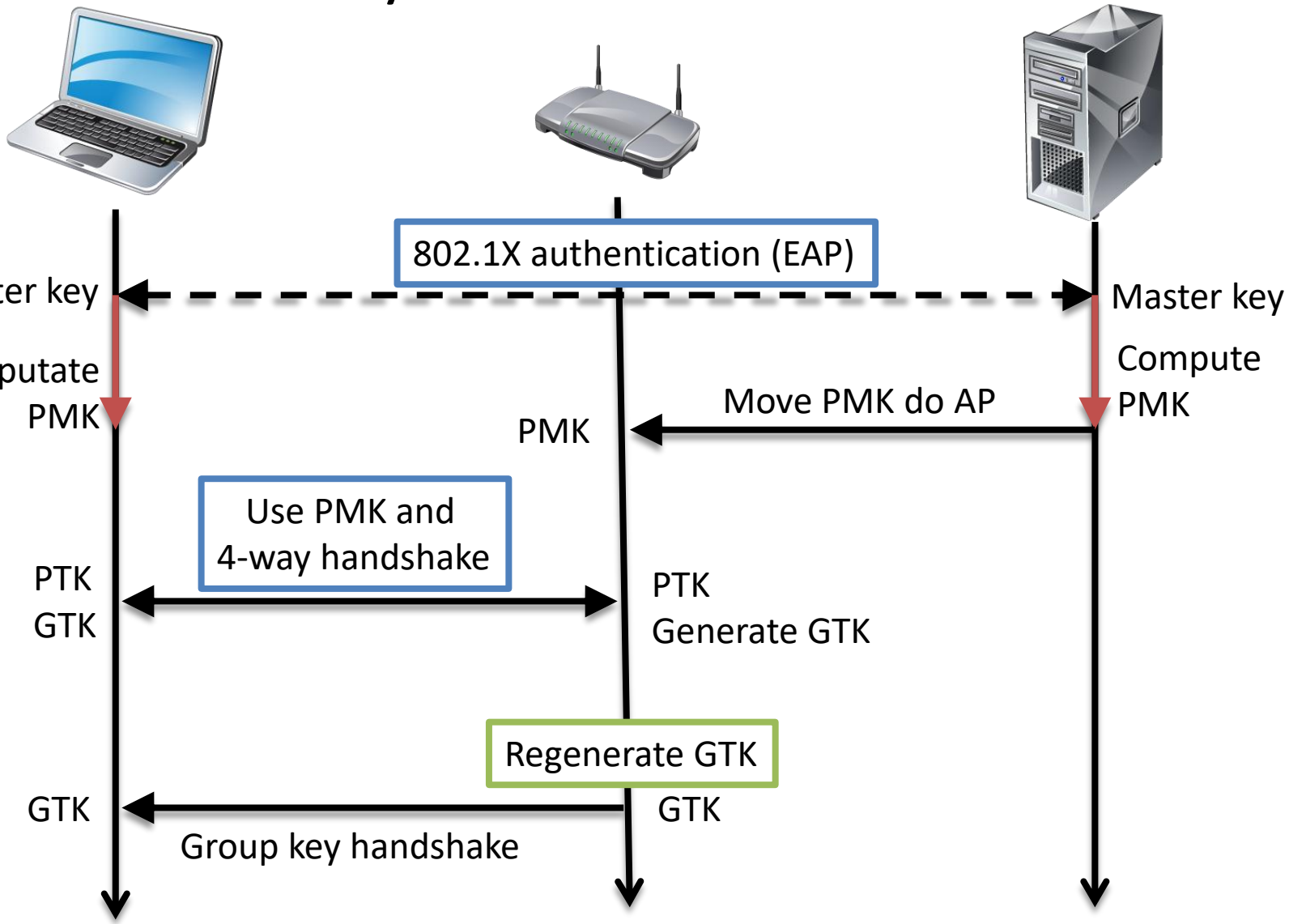
- Personal use
  - Shared key as in WEP
  - WPA-PSK, WPA2-PSK
- Enterprise use
  - 802.1X (EAP, Radius)
  - WPA-Enterprise, WPA2-Eterprise
  - Result of the authentication protocol is a master key (MK) between the station and authentication server.
    - Master key is valid only for the particular session

IEEE 802.11i
Key initialization

- Automatic: utilizes 802.1X
  - After 802.1X, station and authentication server compute Pairwise Master Key (PMK) from the Master Key (MK)
  - Authentication server sends PMK to AP
  - Station and AP use PMK to generate **PTK** (Pairwise Transient Key)
    - Used to encrypt message between AP and one STA
    - Computed using 4-way handshake protocol
  - Then AP generates GTK (Group Transient Key)
    - Used to encrypt broadcast messages from AP to all STAs
- Manual
  - WPA/WPA2-PSK (personal)
  - PMK is computed from the pre-shared key, otherwise the same as automatic

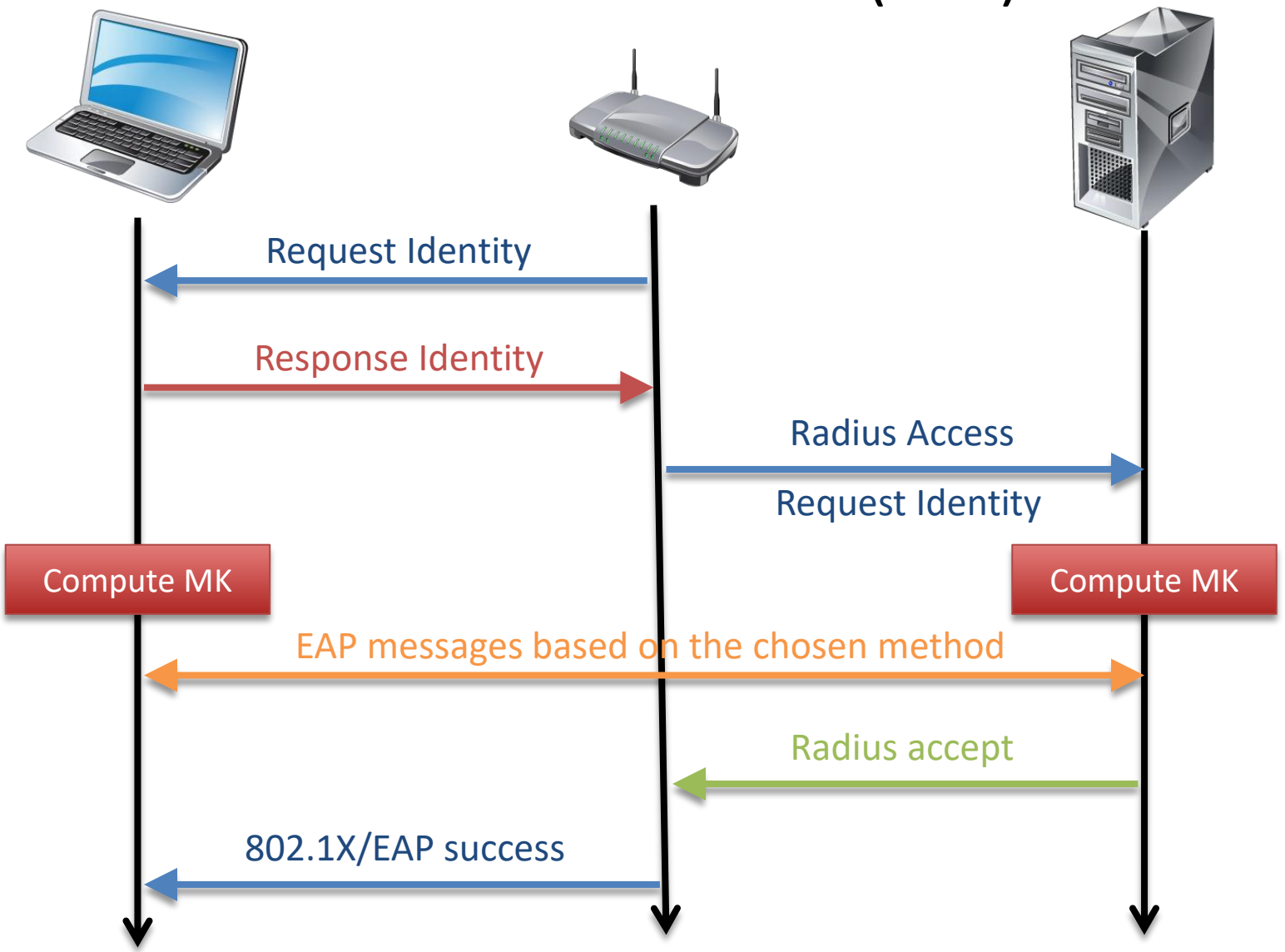
WPA / WPA2

Key initialization



WPA / WPA2 Enterprise

802.1X authentication (EAP)



4-way handshake protokol

Initiated by AP and used for

- Verification that both sides know PMK
- Exchange random values to be used in the generation of PTK
- Send GTK

MIC_{KIK} – Message Integrity Code (computed using key-integrity key (which is derived form PTK))

KeyReplayCtr – used for replay protection

AP: Generate random A_r

AP → STA: A_r | KeyReplayCtr

STA: Generate random S_r
Compute PTK from A_r, S_r, PMK

STA → AP: S_r | KeyReplayCtr | MIC_{KIK}

AP: Compute PTK and verify MIC
Generate GTK

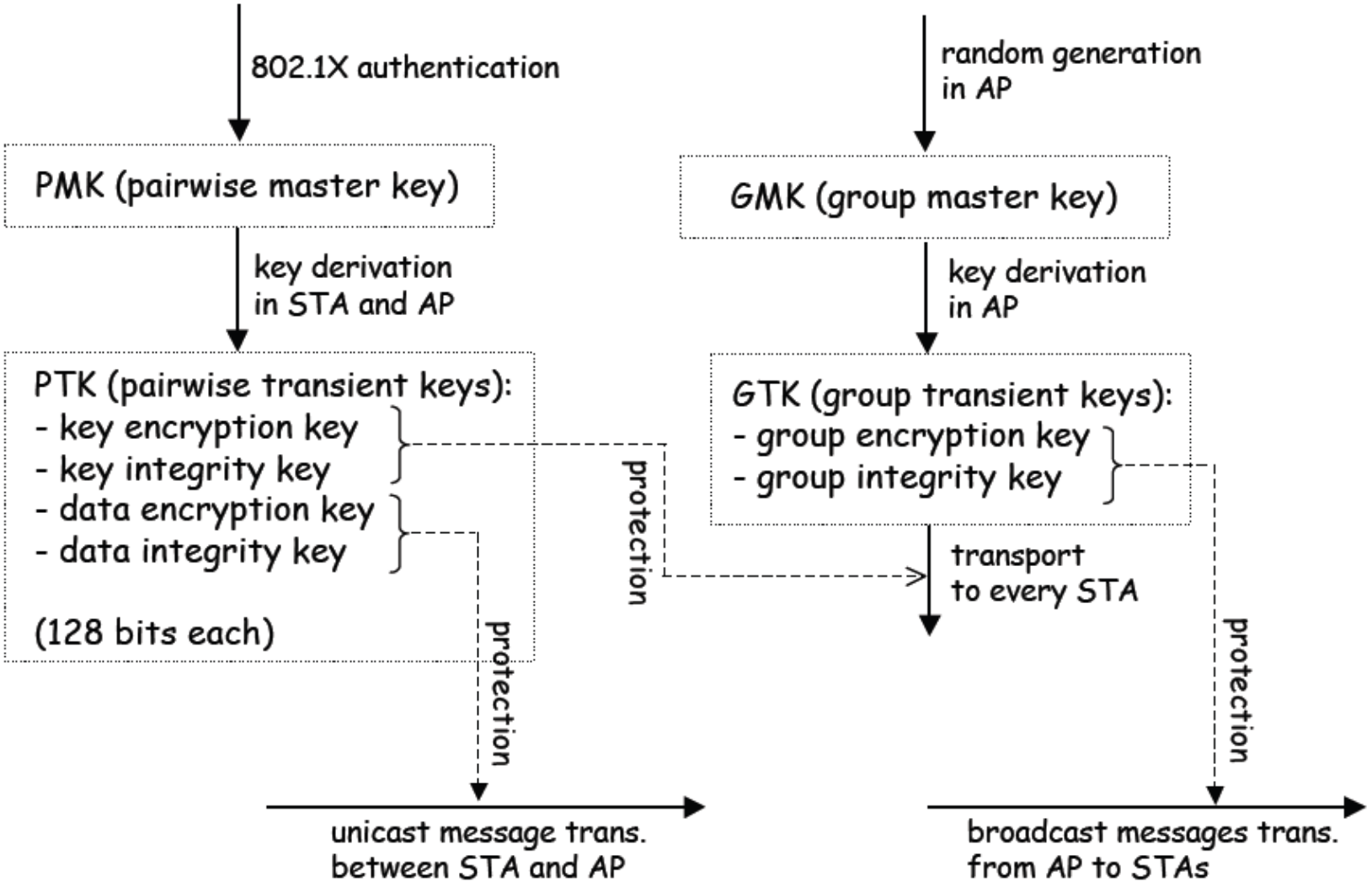
AP → STA: A_r | KeyReplayCtr+1
| $\{GTK\}_{KEK}$ | MIC_{KIK}

STA: Verify MIC and install keys

STA → AP: KeyReplayCtr+1 | MIC_{KIK}

AP: Verify MIC and install keys

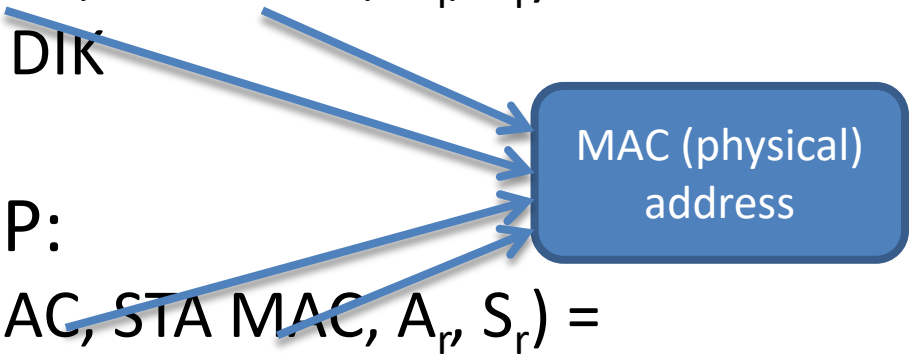
IEEE 802.11i
key hierarchy



4-way handshake protokol

PTK computation

- In case of TKIP:
  - Prf-512(PMK, AP MAC, STA MAC, A_r, S_r) =
    = KEK | KIK | DEK | DIK
- In case of AES-CCMP:
  - Prf-384(PMK, AP MAC, STA MAC, A_r, S_r) =
    = KEK | KIK | DE&IK



Prf-512 / Prf-384 – pseudo-random function with output length 512 / 384 bits.

IEEE 802.11i - Summary



Detection

Negotiation

802.1X authentication

802.11i key initialization

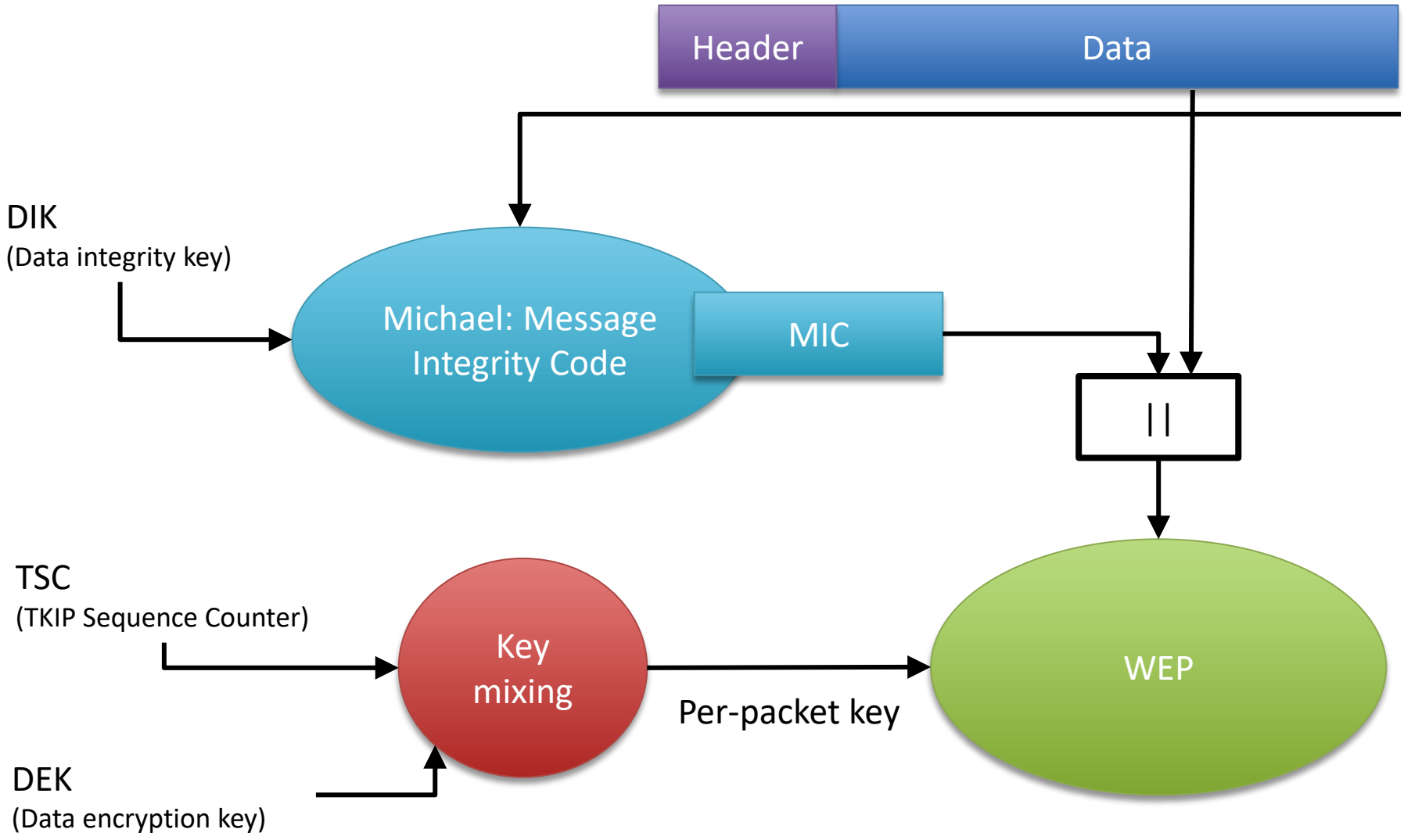
RADIUS – key distribution

Data protection TKIP / AES-CCMP

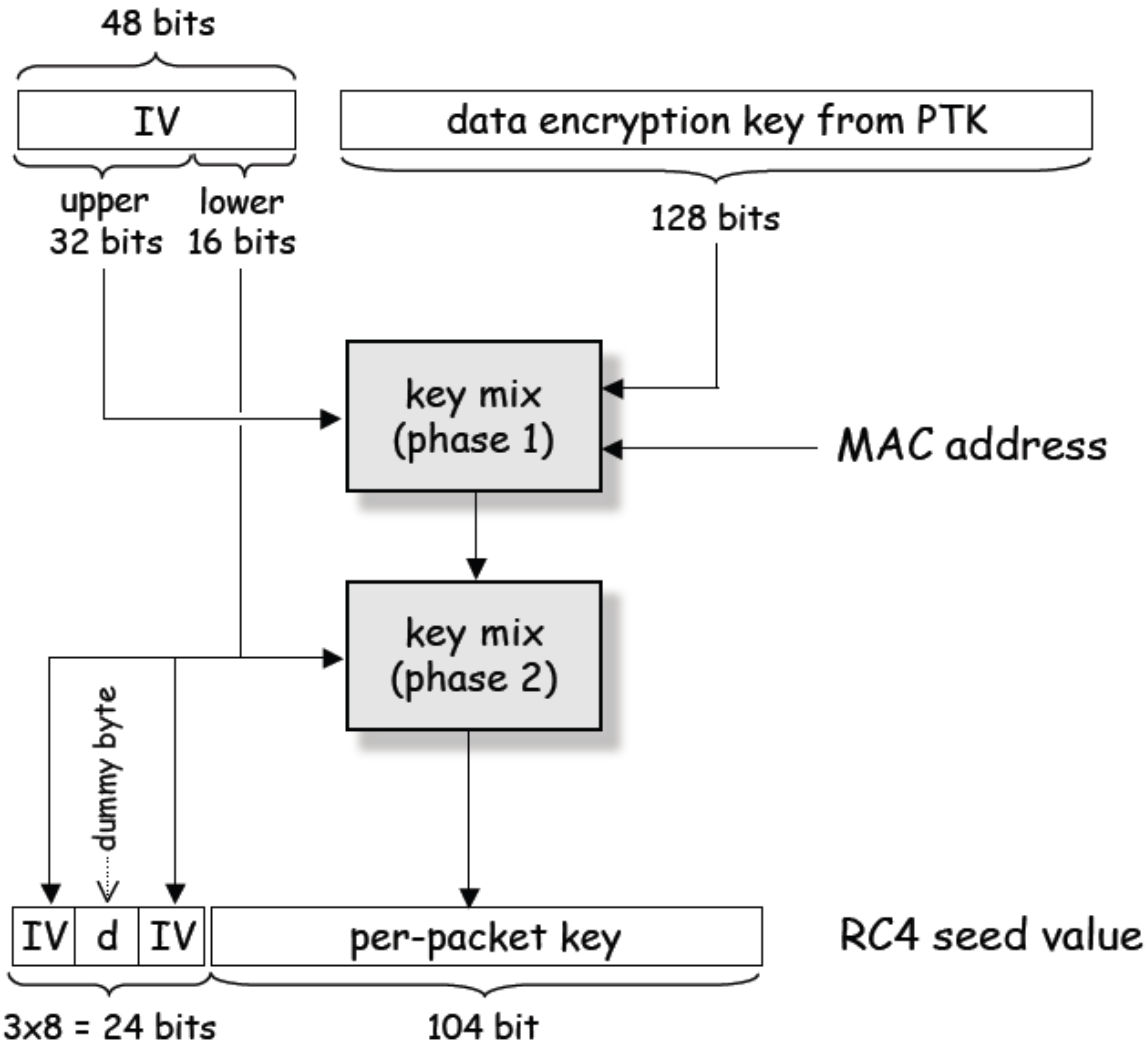
WPA – Encryption
TKIP

- Runs on old hardware, which supports RC4
- 128 bit secret key
- Weaknesses from WEP are eliminated
  - New integrity protection – Michael
    - Generates nonlinear 8 byte MIC (Message Integrity Code) together with 32 bit CRC
  - IV is 48-bit TKIP sequence counter (TSC)
    - Replay protection, with a new session key TSC is set to 0 and incremented with each message

TKIP - encryption



TKIP – keys for RC4

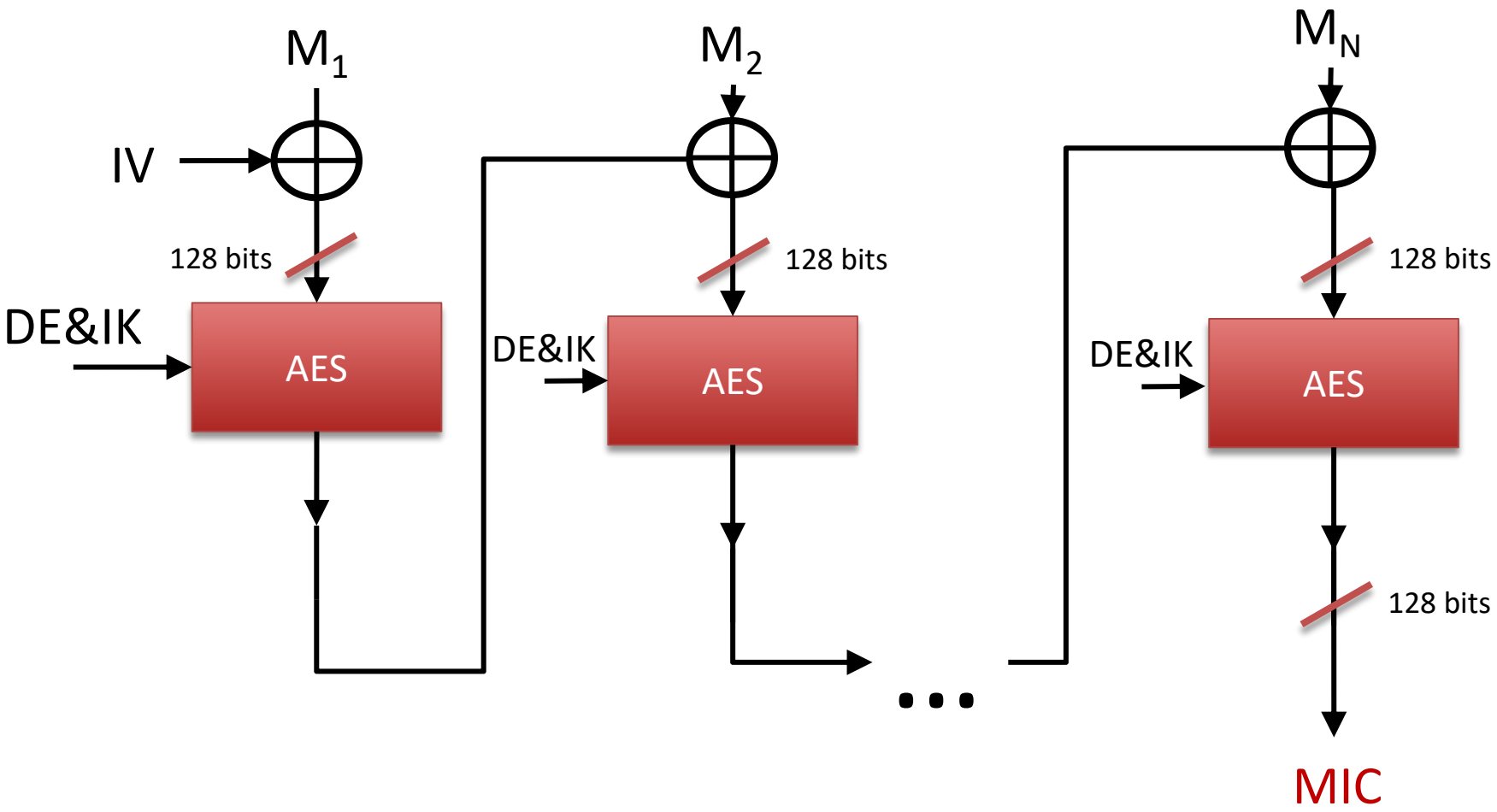


WPA2
AES-CCM

- WPA2 is based on AES with key length 128 bits
- CCM means CTR mode and CBC-MAC
  - Integrity control based on CBC-MAC (with AES as a block cipher)
  - Encryption runs in CTR mode (with AES)
- Same key for encryption and authentication but with different IV
- Incompatible with WEP, needs new hardware.

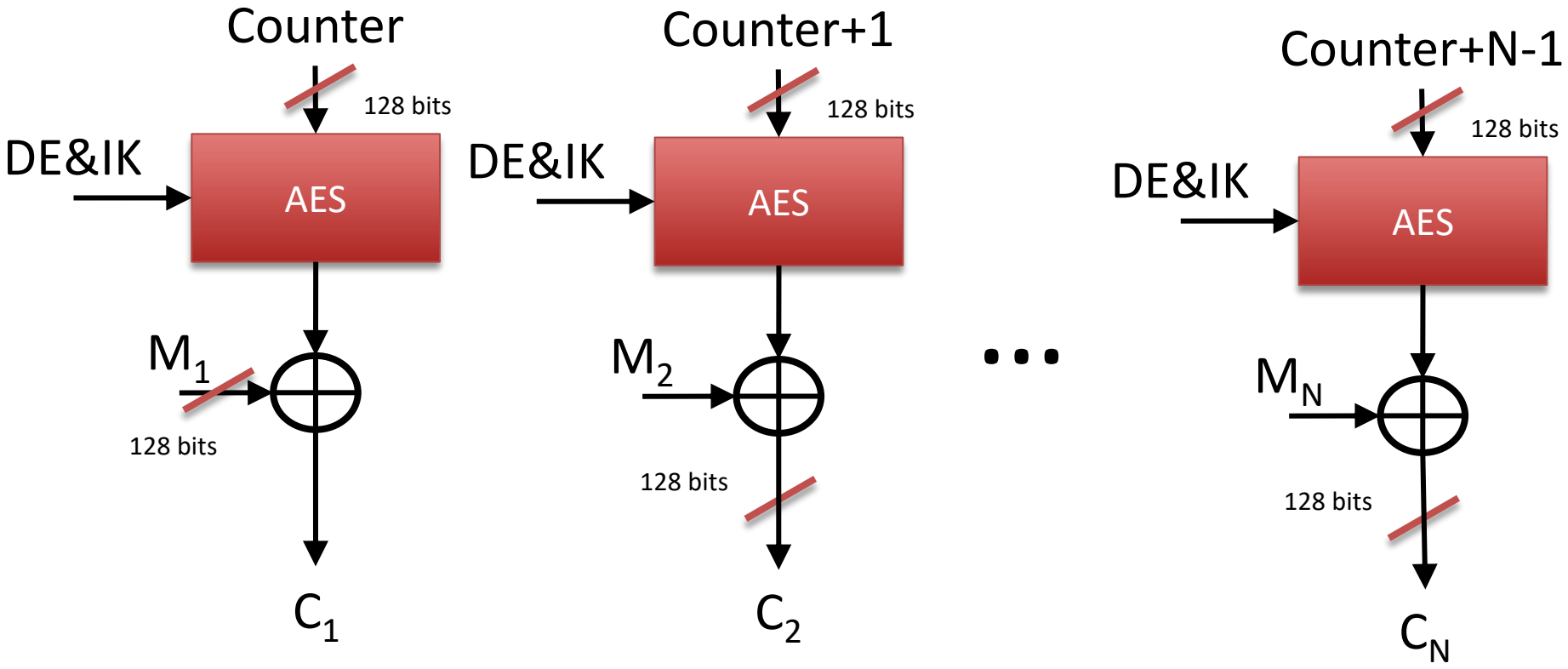
WPA2 integrity control

CBC-MAC



WPA2 encryption

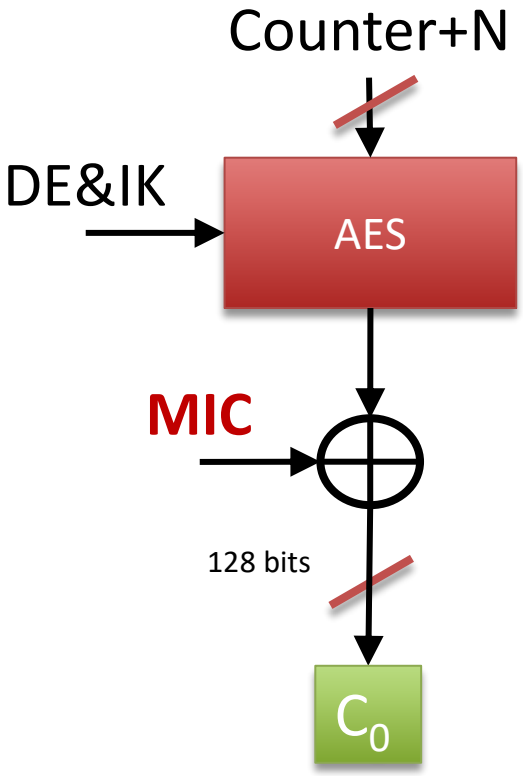
Counter mode





WPA2 encryption

Counter mode (2)





Wireless communication security requirements and WPA2

- ✓ Confidentiality
  - Messages sent over wireless links must be encrypted
- ✓ Authenticity
  - Origin of messages received over wireless links must be verified
- ✓ Replay detection
  - Freshness of messages received over wireless links must be verified
- ✓ Integrity
  - Integrity of messages received over wireless links must be verified
- ✓ Access control
  - Access to the network should be provided only to legitimate entities
  - Access control must be permanent, not only when device joins the nework
- ✗ Protection against jamming

WPA2 and 4-way handshake problems

- No forward secrecy in WPA2-PSK
  - The PTK is derived from the PMK
  - The PMK is derived from the password and random values exchanged during 4-way handshake

  => Session keys are derivable from the long-term secret

WPA2 and 4-way handshake problems

Attacker may guess password offline for WPA2-PSK (using e.g. dictionary attack)

- Attacker captures the 4-way handshake, he itercepts:
  - SSID (network name), MAC addresses (AP + client), Nonces (A_r, S_r), MIC (message integrity code)
  - everything needed to verify a password guess is observable
- Attacker guesses a password and computes:
  1. PMK = PBKDF2(password, SSID, MACs)
  2. PTK = PRF-384(PMK, A_r, S_r, MAC_{AP}, MAC_{CLIENT})
  3. Use PTK to compute MIC and check if is the same as camputerd

WPA2 problems

- WPA2-Enterprise
  - Can provide forward secrecy
  - Can be resistant to offline attacks
  - But may not, it depends on the configuration (which EAP / TLS protocols and ciphers are used)
- The WPA2 does not provide encryption for open networks

KRACK attack on WPA2

- https://www.krackattacks.com/ (2017)
- Vulnerability in 4-way handshake implementation:
  - If AP does not receive the 4th message, it resends the 3rd
    - This can normally happen when response from STA is lost during transmission
  - Hence, STA installs PTK and GTK every time it receives 3rd message
    - Also resets counter in data encryption protocol
      - Possible replay attack
    - Couter mode of AES -> when couter is reset, messages are encrypted using the same key stream

Evil Twin attack

- Not really a bug in WPA2 but a consequence of how clients connects to networks with the same SSID
  - An attacker creates a fake access point (same SSID and same settings)
  - Client connects to it e.g. because of stronger signal
- WPA2-PSK: attacker captures 4-way handshake
  - May guess password using offline dictionary attack
  - Phishing portal (if user connects to open twin instead)
    - “Wrong password, please login here”
- WPA2-Enterprise:
  - Warning with „invalid certificate“ is shown, but client accepts it
  - Attacker runs fake authentication server and captures authentication exchange (challenge-response),
  - May guess password offline.

WPA2 vs WPA3

Several improvements for the state-of-the-art security

- Enterprise mode
  - AES-256 in GCM mode
  - HMAC with SHA-384
- Personal mode
  - Still supports AES-128 in CCM mode
- Simultaneous Authentication of Equals (SAE)
  - Variant of Dragonfly Key Exchange
    - Password based authentication and key exchange
    - Mitigates security issues posed by weak passwords
    - Prevents offline cracking (even if Evil Twin captures data)
  - Based on Diffie-Hellman key exchange (over elliptic curves)
    - Provides forward secrecy
  - Dragonblood attack: https://wpa3.mathyvanhoef.com/
    - Problems with sidechannel attacks, downgrade attacks, …
- OWE (Opportunistic Wireless Encryption)
  - Diffie-Hellman key exchange for open networks
  - No certificates, possible man in the middle

WPA3 key exchange

- WPA2: “prove you know the password by deriving the same key”
- WPA3: “we both prove knowledge of the password via a secure key exchange, without ever exposing anything reusable”
  - two main stages:
    1. SAE handshake (authentication + key agreement)
    2. 4-way handshake (key confirmation + session setup)

WPA3 – SAE (very roughly)

1. STA → AP: (Group ID, Random S_1, P_1)
   - Group ID – identification of used DLOG group
   - S_1 – random scalar
   - P_1 – curve point: $P_1 = r_1 \cdot PWE$
     - Random scalar r_1, PWE = Hash(password + MACs + …) → curve point
2. AP → STA: (Random S_2, P_2)
   - P_2 – curve point: $P_2 = r_2 \cdot PWE$

STA and AP compute the shared key K from S_1, P_1, S_2, P_2

- Because the ECDH problem is hard, attacker is not able to compute the shared key without knowing PWE

3. STA → AP: Confirm value C_1
   - C_1 = H(K, S_1, P_1, S_2, P_2, MAC_{AP}, MAC_{STA}, “client”)
   - AP verifies
4. AP → STA: Confirm value C_2
   - C_2 = H(K, S_1, P_1, S_2, P_2, MAC_{AP}, MAC_{STA}, “access point”)

WPA3 – 4-way handshake

- Same protocol as in WPA2, but
  - A key can be installed only once
  - duplicate “install PTK” events are ignored
  - State machine describing the protocol is stricter
    - handshake messages tied to strict states
    - replayed message ≠ trigger reinstall

Conclusion

- In general, attacking wireless networks is easier than attacking wired networks
  - The attacker does not need to have physical access to the network infrastructure
- Original protection of WiFi networks – WEP
  - Big security flaws, do not use
- Security standard 802.11i
  - Access control based on 802.1X
  - Better key management
  - TKIP (WPA)
    - Runs on old hardware
    - Utilizes RC4
    - Eliminates weaknesses of WEP
  - AES-CCMP (WPA2)
    - CTR mode and CBC-MAC
    - Requires new hardware
- WPA3 on the way, still has some concerns, but generally better

Wi-Fi Protected Setup (WPS) Insecurities (home nets)



- A standard that attempts to allow easy establishment of a secure wireless home network
- The standard allows four usage modes aimed at a home network user adding a new device to the network:
  - PIN Method (e.g., enter the PIN on AP into the client)
  - Push-Button-Method (a user simultaneously pushes a button on the AP and the client)
  - Near-Field-Communication Method (bring the client close to the AP)
  - USB Method
- In December 2011 researcher Stefan Viehböck reported a design and implementation flaw that makes brute-force attacks against PIN-based WPS feasible to perform on WPS-enabled Wi-Fi networks
  - A successful attack on WPS allows unauthorized parties to gain access to the network

- **The only effective workaround is to disable WPS**
  - **Impossible on some APs**

Wi-Fi Protected Setup (WPS)

- WPS using PIN
  - 8 digit PIN, the last digit is checksum
  - 7 unknown digits = 10 000 000 combinations
- When STA attempts to gain access
  - AP reports validity of first and second halves separately
  - number of guesses need is reduces to
    10 000 + 1 000 = 11 000
    - Can be performed in few hours at most
- AP should slow or disable WPS after several wrong guesses
  - Not implemented in some devices