Bezpečnosť bezdrôtových sietí

Bezpečnosť IT infraštruktúry

Michal Rjaško

Hrozby bezdrôtových sietí

- Fyzická (ne)bezpečnosť
  - Fyzické spojenia sú v bezdrôtových sieťach nahradené logickými spojeniami
  - Posielanie a prijímanie správ nepotrebuje fyzický prístup k sieťovej infraštruktúre
- Vysielanie v štýle „broadcast“
  - Vysielanie môže ktokoľvek v dosahu odpočuť
  - Ktokoľvek môže vysielať
    - vysielanie bude prijaté zariadeniami v dosahu, prípadne
    - vysielanie bude interferovať s iným vysielaním (rušenie)

Hrozby bezdrôtových sietí

- Odpočúvanie je ľahké
- Posielanie falošných správ je jednoduchšie
- Opakovanie správ je ľahké
- Ľahšie je získať nepovolený prístup k sieti a jej službám
- Rušením ľahko spôsobíme nedostupnosť siete
- Tváriť sa ako niekto iný je ľahšie

Požiadavky na bezpečnosť bezdrôtových sietí (1)

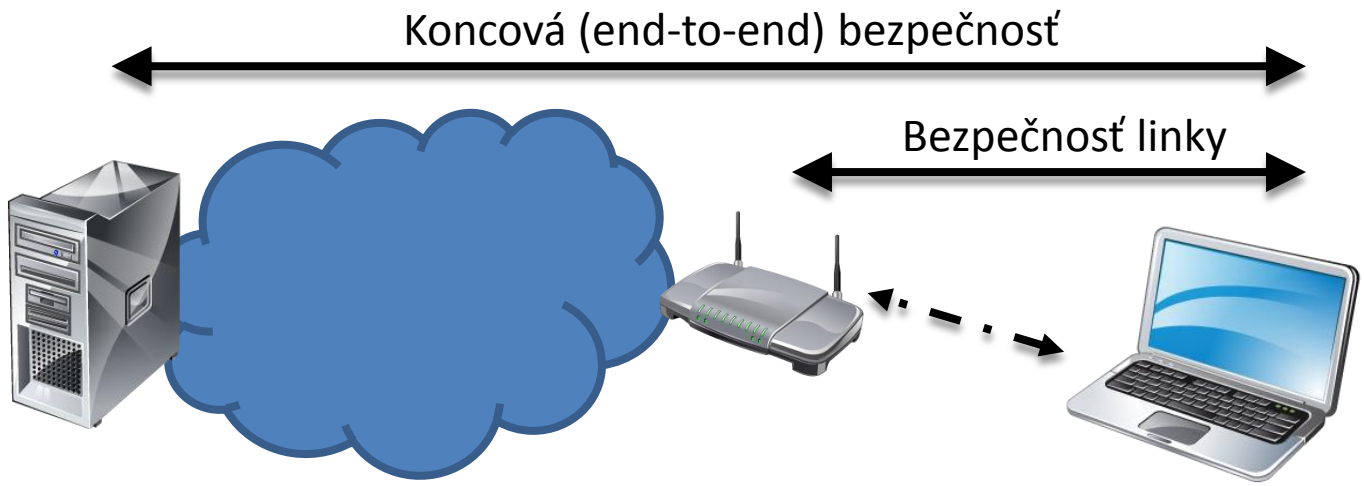
Wifi často využívajú mobilné zariadenia, kde

- Vyžadujeme nízku spotrebu energie, t.j. treba
  - Minimalizovať výpočtovú náročnosť algoritmov
  - Minimalizovať sieťovú komunikáciu
- Kryptografické a bezpečnostné algoritmy musia byť jednoduché
- Bezpečnostné protokoly musia mať malé dodatočné náklady na komunikáciu a výpočty

Požiadavky na bezpečnosť bezdrôtových sietí (2)

- Dôvernosť
  - Vysielané správy musia byť šifrované
- Autenticita
  - Overenie identity druhej strany
  - Overovanie pôvodu prijatých správ.
- Nemožnosť opakovať odpočuté správy
  - Kontrola čerstvosti prijatých správ
- Integrita správ
  - Kontrola integrity prijatých správ
- Riadenie prístupu
  - Prístup k sieti by mal byť povolený iba oprávneným účastníkom
  - Permanentná kontrola prístupu, nie iba pri nadväzovaní spojenia.
- Ochrana proti rušeniu

Linková vs. koncová bezpečnosť



- Koncová bezpečnosť
  - Zabezpečuje sa na sieťovej (IPsec, VPN), transportnej (SSL) alebo aplikačnej vrstve
- Bezpečnosť linky
  - Zabezpečuje ju linková vrstva (802.11 WEP, WPA, 802.11i)

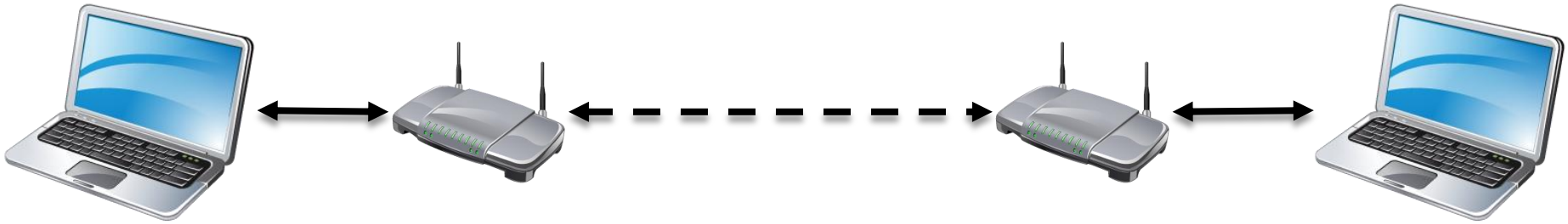
Úvod do Wifi

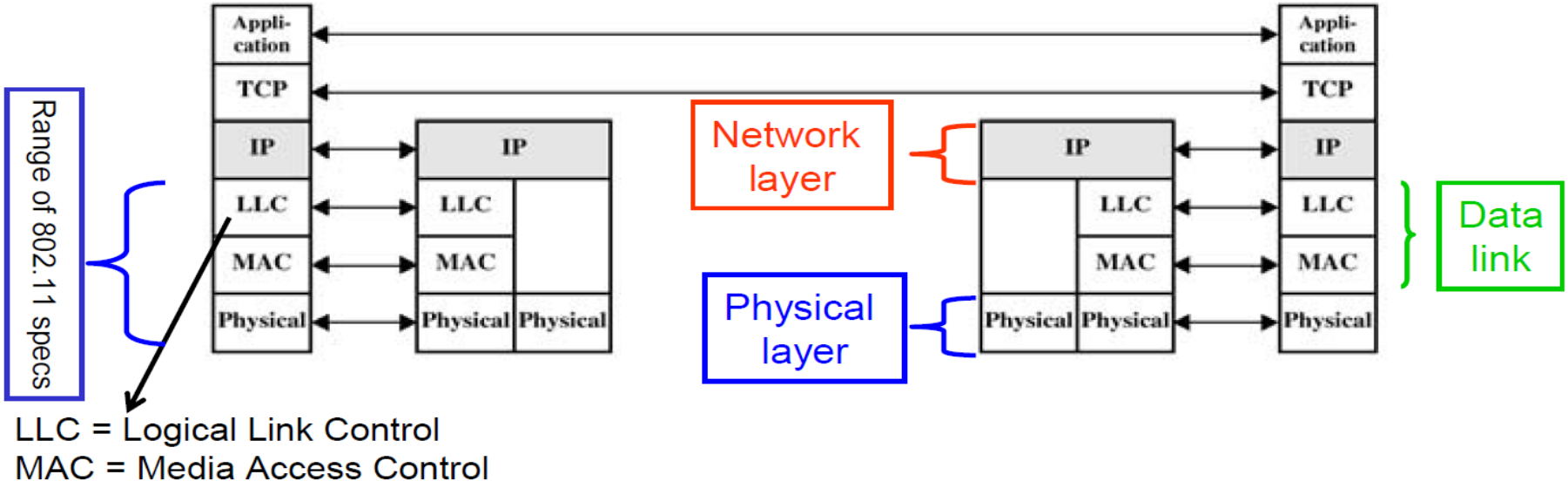
- Štandard 802.11 z roku 1997
  - Pôvodná rýchlosť 1 – 2 Mb/s
- Špecifikuje 1. a 2. vrstvu v OSI modely
  - Fyzickú vrstvu
  - Dátovú vrstvu
- Kompatibilitu zariadení zabezpečuje združenie WECA (Wireless Ethernet Compatibility Alliance)
  - Certifikácia kompatibility
  - Po novom Wi-Fi Alliance

Úvod do Wifi

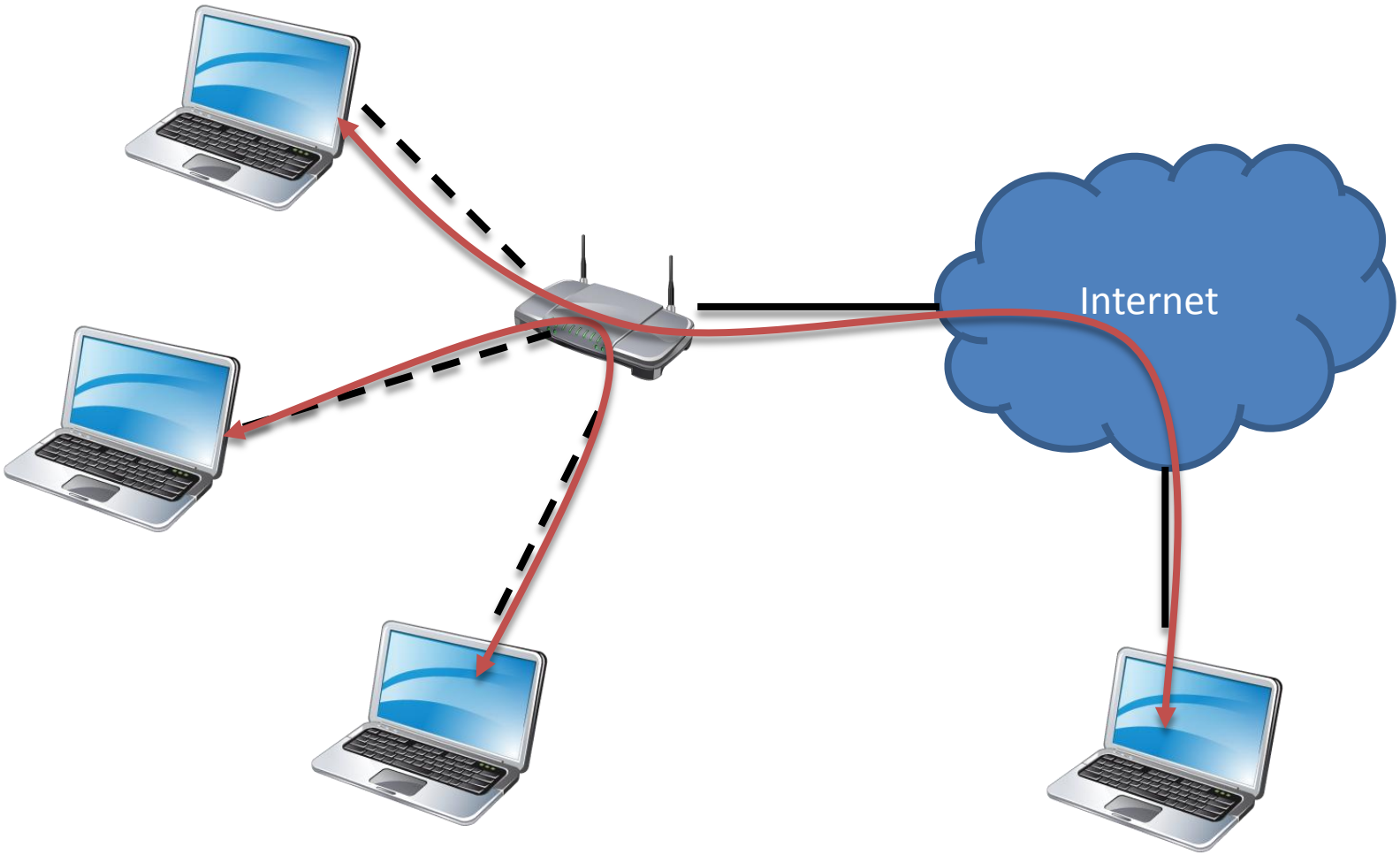
- Dva druhy zariadení
  - Bezdrôtové stanice (STA)
    - Počítač, PDA, mobil, tablet, okuliare, hodinky, ...
  - Access point (AP)
    - Most medzi bezdrôtovou a drôtovou sieťou
    - Zvyčajne obsahuje
      - Vysielač
      - Drôtové pripojenie
      - Software na premostenie pripojení
    - Cez jeden access point sa do siete pripája viacero zariadení

Úvod do Wifi



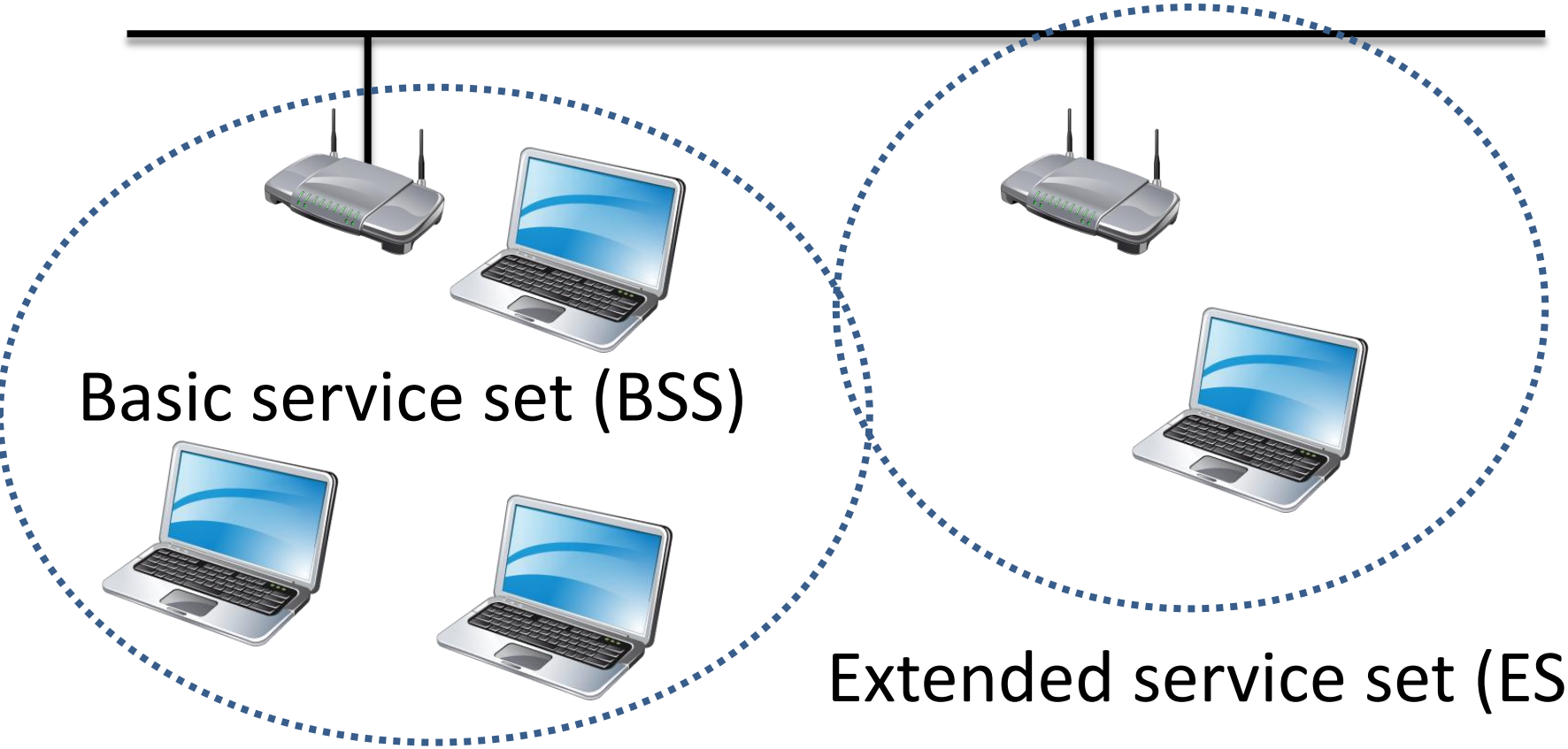

Appli-cation
TCP
IP
LLC
MAC
Physical
IP
LLC
MAC
Physical
Physical
Appli-cation
TCP
IP
LLC
MAC
Physical
IP
LLC
MAC
Physical
Physical
Range of 802.11 specs
Network layer
Physical layer
Data link
LLC = Logical Link Control
MAC = Media Access Control

Úvod do Wifi



Úvod do Wifi

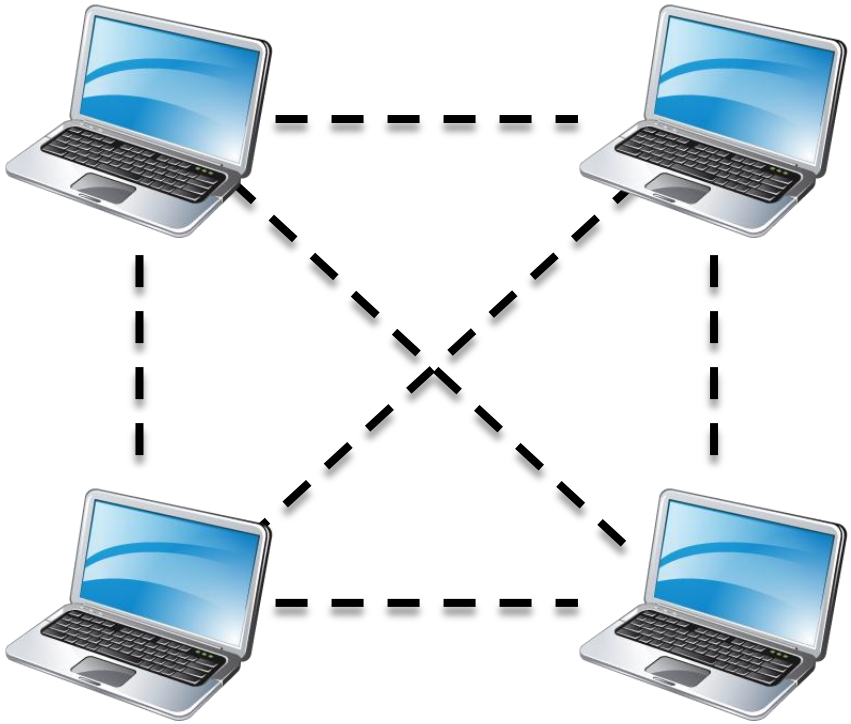
Infrastructure mode



- SSID (Service Set Identifier) je pripojené ku všetkým packetom v rámci BSS
- Viac AP s rovnakým SSID tvorí ESS

Úvod do Wifi

Ad-hoc mode



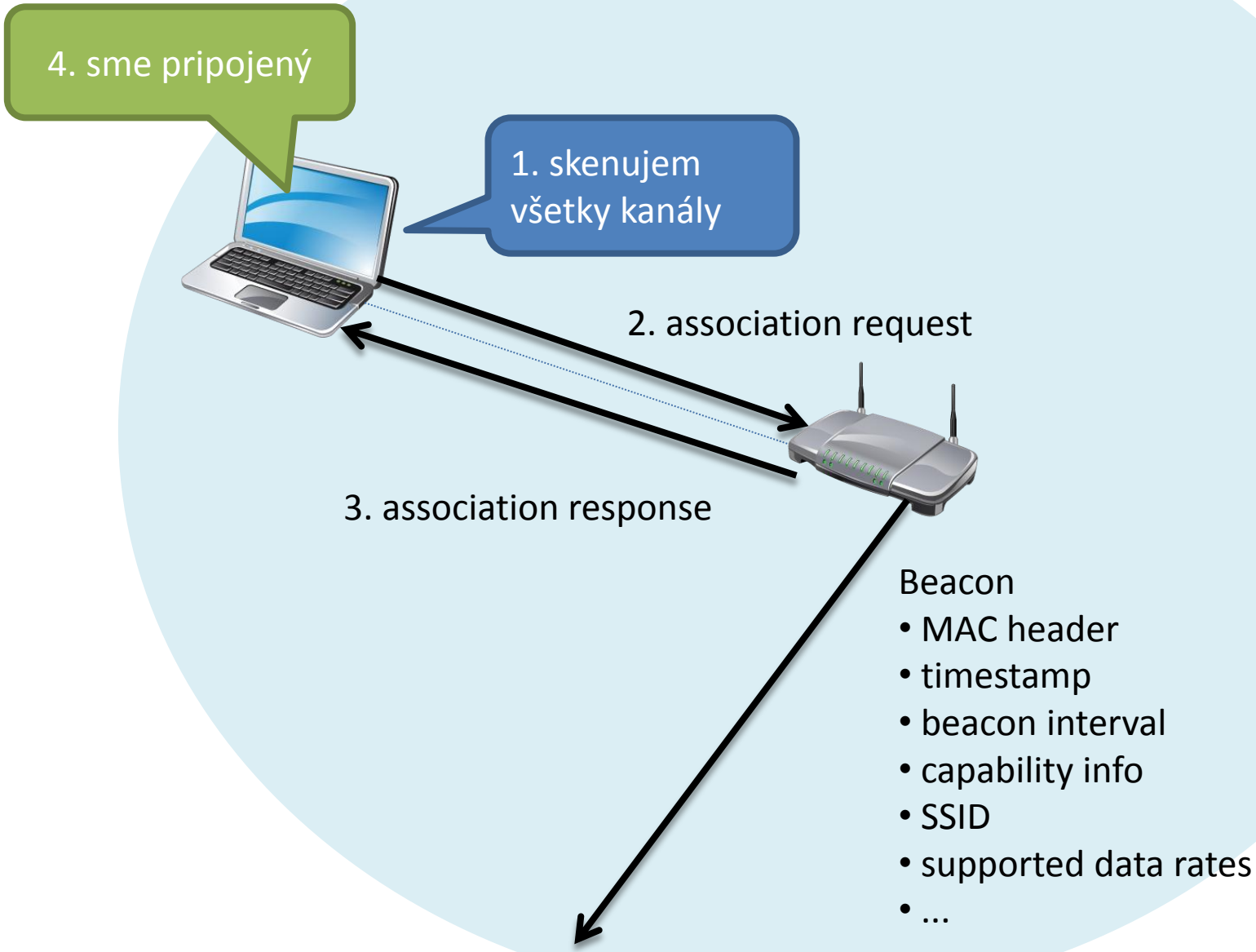
WiFi štandardy

- **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 (prechod medzi 2 AP)
- IEEE 802.11n (2009)
  - Viac ako 100 Mb/s, 5GHz aj 2,4 GHz

WiFi – Druhy kontroly prístupu

- Bez kontroly prístupu (nezabezpečené siete)
- Kontrola prístupu na základe fyzickej (MAC) adresy
  - MAC adresu je možné ľahko odpočuť a zmeniť
- Kontrola prístupu na základe SSID
  - AP nemusí vysielať SSID
  - Pre pripojenie do siete musíme poznať SSID
  - Útočník môže počas pripájania SSID odpočuť
- Kontrola prístupu na základe zdieľaného tajomstva (kľúča) medzi stanicou a AP
- 802.1x, EAP, RADIUS

Pripojenie do nezabezpečenej siete



802.11 WEP
Wired Equivalent Privacy

- Súčasť štandardu 802.11
- Cieľ:
  - Urobiť WiFi bezpečné aspoň ako je drôtová LAN sieť
  - Silná bezpečnosť nie je v prípade WEP cieľom
- Poskytuje:
  - Kontrolu prístupu k sieti
  - Dôvernosť správ
  - Integritu správ

Požiadavky na bezpečnosť bezdrôtových sietí a WEP

Dôvernosť

- **Vysielané správy musia byť šifrované**

Autenticita

- Overenie identity druhej strany
- Overovanie pôvodu prijatých správ

Nemožnosť opakovať odpočuté správy

- Kontrola čerstvosti prijatých správ

Integrita správ

- **Kontrola integrity prijatých správ**

Riadenie prístupu

- **Prístup k sieti by mal byť povolený iba oprávneným účastníkom**
- Permanentná kontrola prístupu, nie iba pri nadväzovaní spojenia.

Ochrana proti rušeniu

WEP – Kontrola prístupu

- Prebieha na základe zdieľaného tajného kľúča
- Kľúč je zdieľaný zvyčajne medzi všetkými
  - Stanicami
  - Prístupovými bodmi
- Všetky pripojené stanice sú v zásade schopné dešifrovať správy z ostatných staníc
- Zvyčajne sa kľúč manuálne vkladá do staníc aj do AP
  - Nočná mora administrátorov veľkých sietí

WEP – Kontrola prístupu

Dva druhy kontroly prístupu

- Bez autentizácie
  - Hocikto sa môže k pripojiť k AP
  - Posielané správy sa však následne šifrujú, STA teda musí poznať kľúč
- Autentizácia na základe zdieľaného kľúča „Shared key authentication“
  - (viď. ďalší slide)
- Na prvý pohľad sa môže zdať že druhý spôsob je bezpečnejší
  - V skutočnosti je to skôr naopak (detaily neskôr)

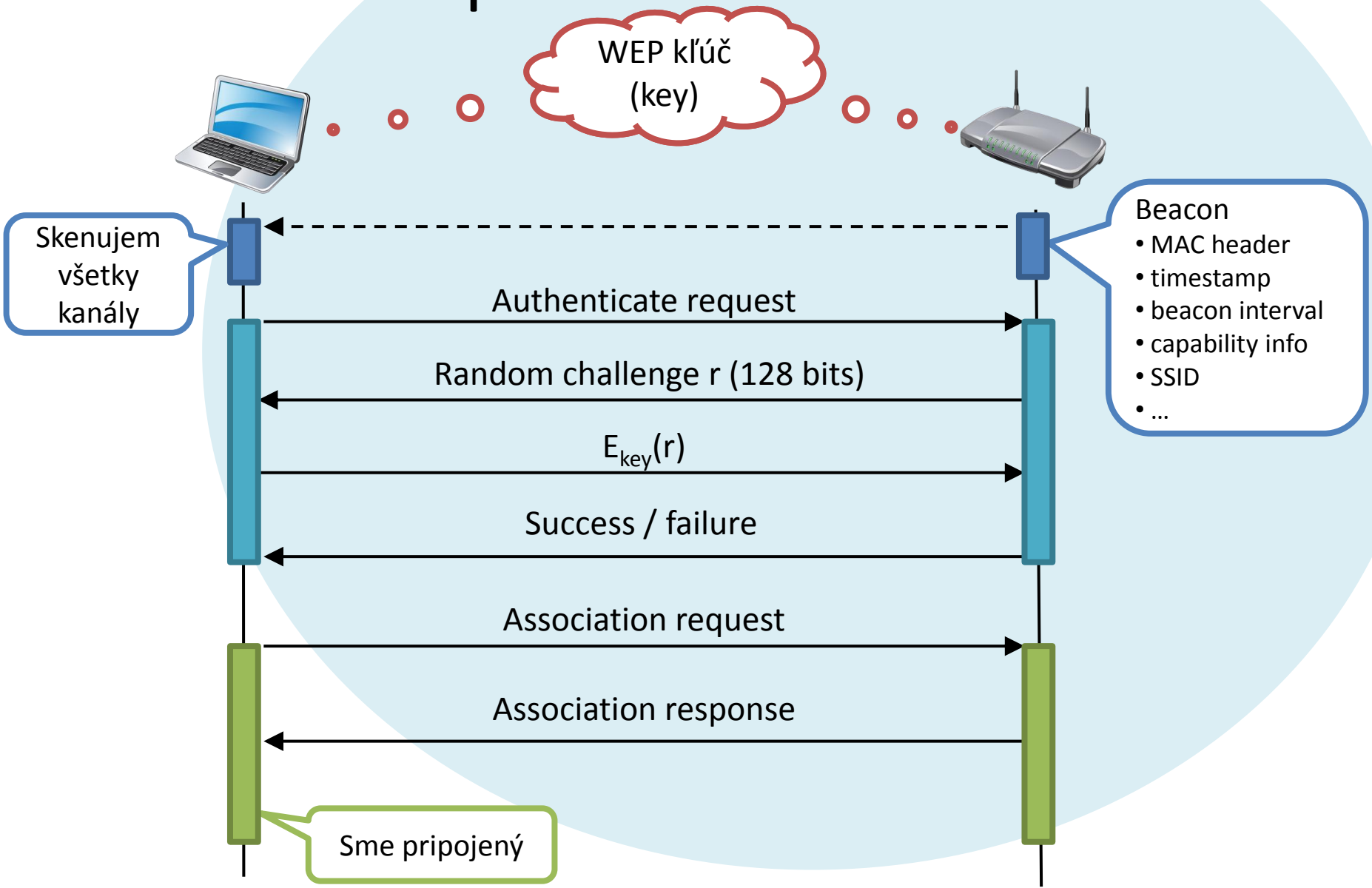
WEP – Kontrola prístupu

Shared key authentication

- Pred pripojením sa musí stanica autentizovať
- Autentizácia prebieha v jednoduchom „challenge-response“ protokole:
  - STA → AP: authenticate request
  - AP → STA: authenticate challenge (r) //r má 128 bitov
  - STA → AP: authenticate response ($e_{key}(r)$)
  - AP → STA: authentication success/failure

- Akonáhle je STA autentizované, STA môže poslať „association request“ a AP mu odpovie
- Ak autentizácia zlyhá, pripojenie nie je možné

Pripojenie do siete zabezpečenej pomocou WEP



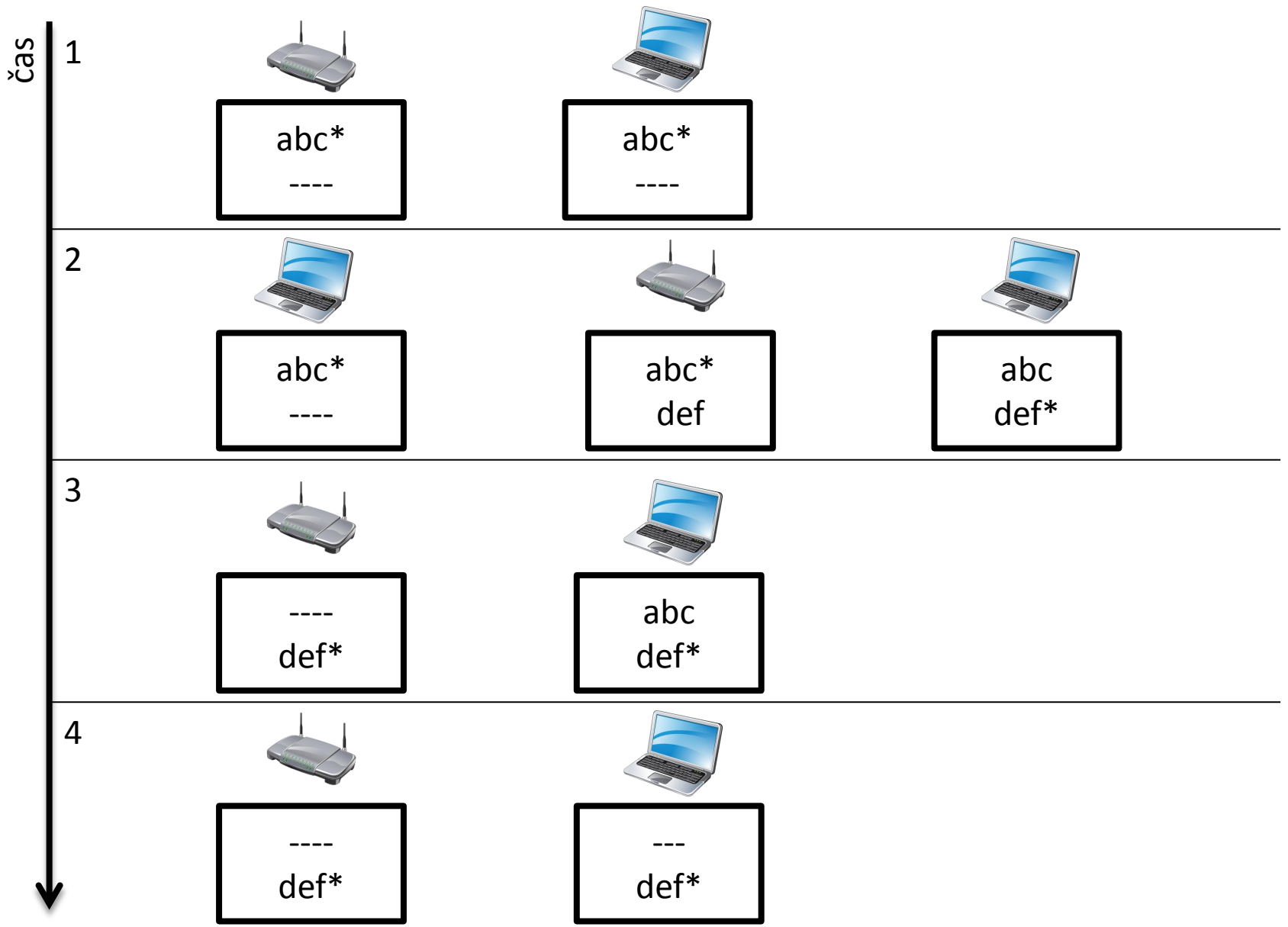
WEP – Dôvernosť

- Šifrovanie prebieha pomocou RC4 (prúdová šifra z roku 1987, navrhol ju Ron Rivest)
  - Priebeh šifrovania:
    - Pre každú zasielanú správu
      - RC4 je inicializovaná zdieľaným kľúčom (40-bitov / 104 bitov)
      - RC4 produkuje pseudo-náhodný prúd bitov (“key stream”)
      - Tento prúd je XORovaný so správou
    - Dešifrovanie je analogické
  - Je dôležité, aby bola každá správa XORovaná s iným prúdom bitov (“key stream”)
    - RC4 je teda inicializovaná kľúčom a inicializačným vektorom IV
      - Kľúč je rovnaký pre každú správu
      - 24-bitový IV sa mení pri každej posielanej správe

WEP - kľúče

- Zdieľaný kľúč pozná celá skupina používateľov.
  - Ak niekto zo skupiny odíde, je potrebné ho vymeniť.
- Pôvodný štandard počíta so 64 bitovým kľúčom pre RC4
  - 40 bitov bol zdieľaný tajný kľúč a 24 bitov sa ponechalo na inicializačný vektor
  - Po uvoľnení reštrikcií USA bol štandardizovaný aj 128 bitový kľúč, z toho 104 bitov je zdieľaný tajný kľúč a 24 bitov je inicializačný vektor
- V prípade veľkých sieti je nemožné vymeniť kľúč naraz na všetkých staniciach
- WEP podporuje viacero zdieľaných kľúčov
  - Jeden z kľúčov je aktívny, používa sa na šifrovanie správ
  - Na dešifrovanie sa môže použiť aj iný ako aktívny kľúč
  - Správa obsahuje ID kľúča, na základe ktorého príjemca použije správny dešifrovací kľúč

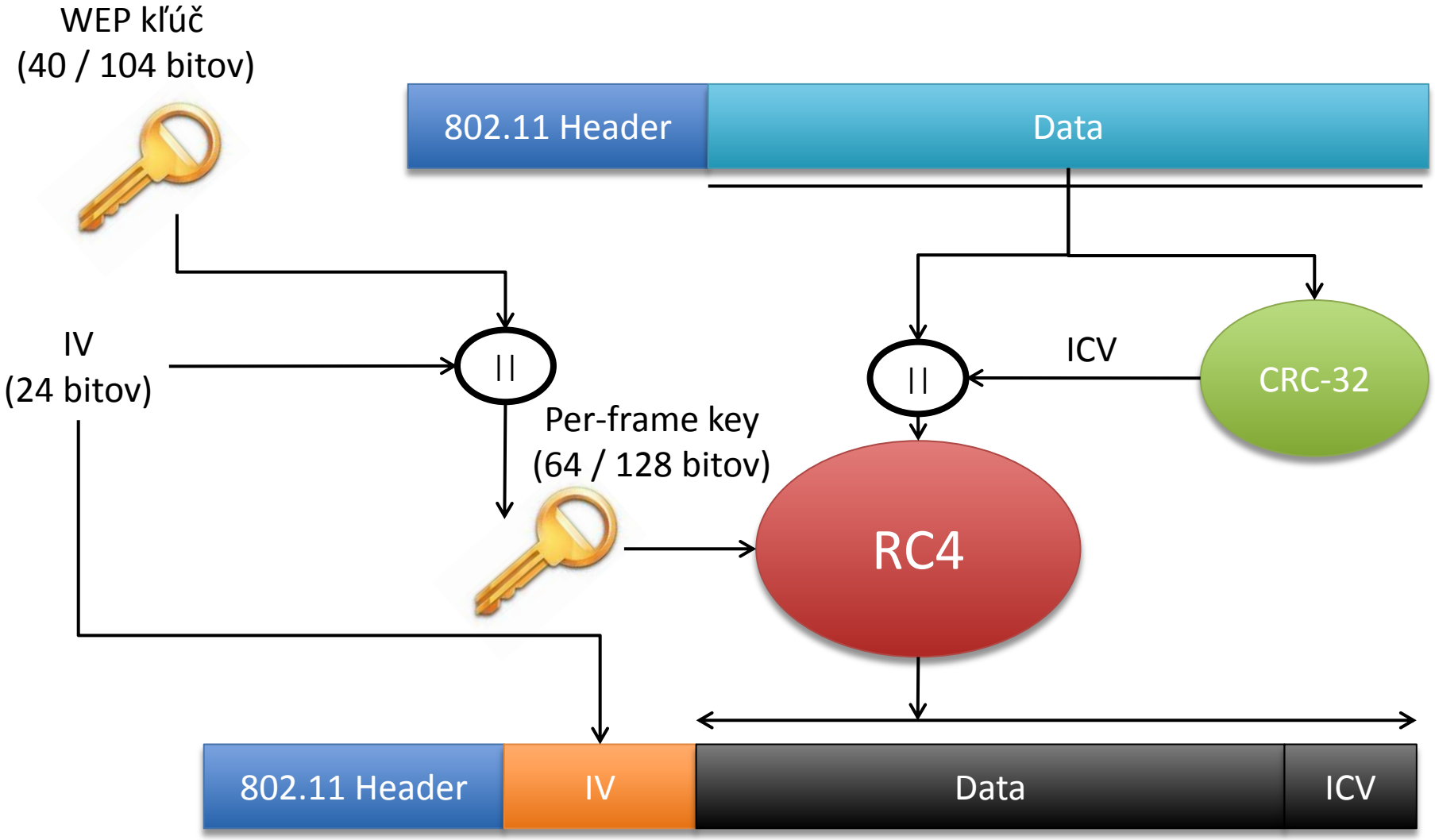
WEP – zmena kľúča



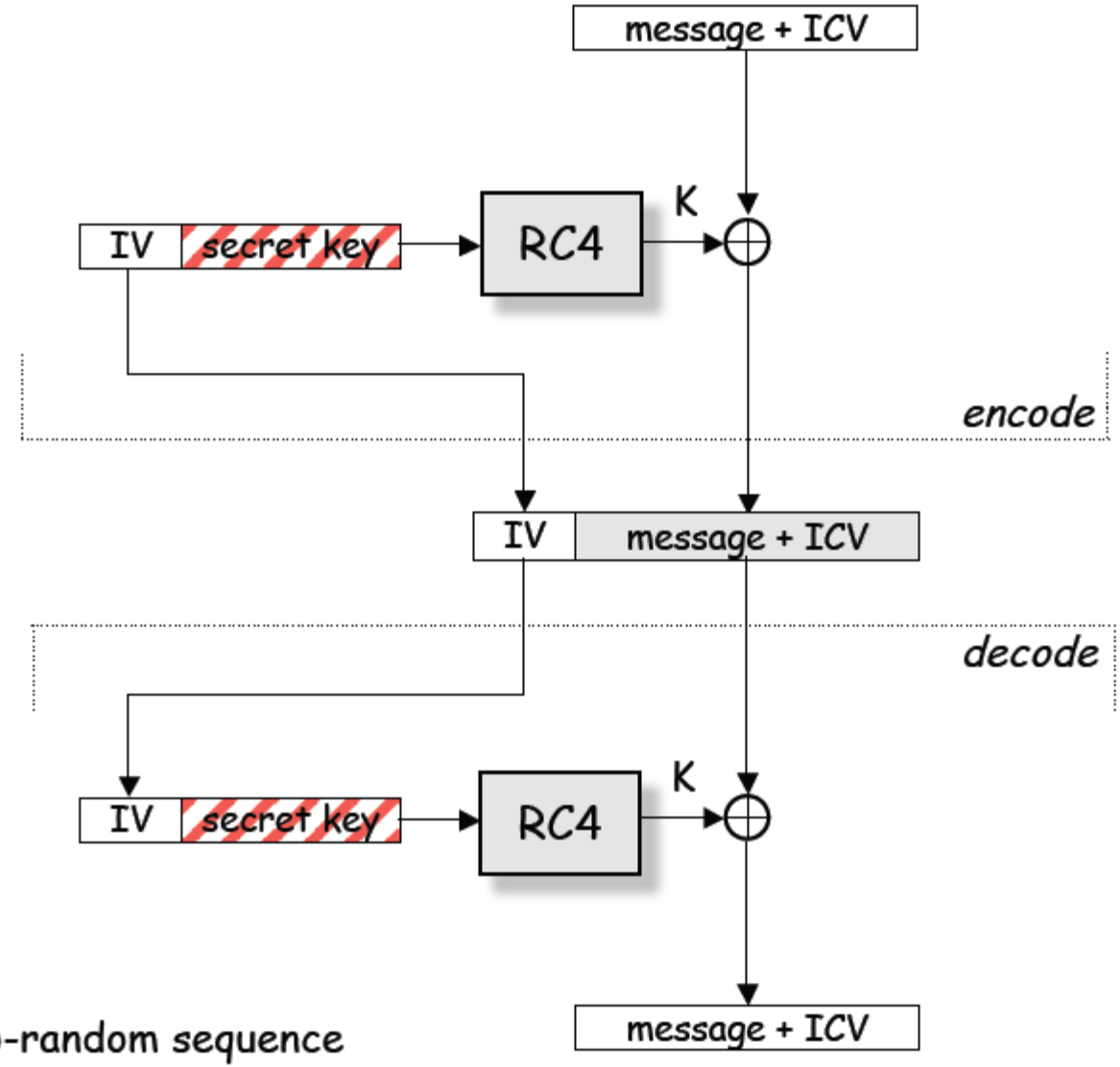
WEP – Integrita

- Kontrola integrity prebieha na základe zašifrovaného CRC (Cyclic Redundancy Check) kontrolného súčtu
  - Vypočíta sa ICV (integrity check value) a pripojí sa na koniec správy
    - Veľkosť ICV je 32 bitov
  - Správa a ICV sú zašifrované
- CRC je postavené na cyklických samo-opravných kódoch
  - je navrhnuté tak, aby odhalilo / opravilo štandardné chyby spôsobené šumom pri komunikácii
  - nemusí odhaliť zámerne urobené chyby

WEP šifrovanie – náhľad



WEP – šifrovanie / dešifrovanie



K: pseudo-random sequence

WEP – bezpečnostné problémy

- Autentizácia je iba jednosmerná
  - AP nie je pre stanicu autentizovaný
  - Stanica riskuje, že komunikuje so zlým AP
- Rovnaký tajný kľúč je použitý aj na kontrolu prístupu aj na šifrovanie
  - Problém v jednom z protokolov môže viesť k odhaleniu kľúča

WEP – bezpečnostné problémy

- Pri kontrole prístupu nie je vytvorený tzv. „session key“.
  - Kontrola prístupu je iba jednorazová
  - Akonáhle je stanica pripojená k AP, útočník môže posielať správy s použitím MAC adresy stanice
  - Vytvoriť správne zašifrované správy je ťažšie, útočník však môže opakovať odpočuté správy.

WEP – bezpečnostné chyby

Útočník sa môže vydávať za akúkoľvek stanicu:

- Spomínaný challenge-response protokol na autentizáciu:
  - ...
  - AP → STA: r //r má 128 bitov
  - STA → AP: IV||(r ⊕ K)
  - …

  Kde K je 128-bitový prúd z RC4 inicializovanej na IV a WEP kľúči
- Útočník správy ľahko odpočuje, teda môže vypočítať:

  r ⊕ (r ⊕ K) = K
- Následne môže použiť K a vydávať sa za STA
  - ...
  - AP → útočník: r’
  - Útočník → AP: IV||r’ ⊕ K
  - …

WEP – bezpečnostné chyby

- WEP nemá žiadnu ochranu voči útokom opakovaním
  - 802.11 neurčuje ako sa má IV vypočítať, či sa má po každej správe zvýšiť
- Útočník môže manipulovať so správou, napriek kontrole integrity cez ICV a jeho následnému zašifrovaniu:
  - CRC je lineárna vzhľadom na XOR:
    - $CRC(X \oplus Y) = CRC(X) \oplus CRC(Y)$
  - Útočník odpočuje $(M||CRC(M)) \oplus K$
  - Pre každé ΔM, útočník vie vypočítať $CRC(\Delta M)$
  - Útočník teda môže vypočítať:

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

WEP – bezpečnostné chyby

- Opakované použitie IV
  - Priestor IV je príliš malý – 24 bitov
    - 16,777,216 možných hodnôt
    - Po 17 mil. správach sa teda IV opakujú
    - V prípade vyťažených sietí sa priestor IV vyčerpá v priebehu niekoľkých hodín
  - Rovnaké IV v dvoch správach M_1, M_2 znamená, že boli šifrované použitím rovnakého „key stream“ K
    - vieme teda vypočítať
      - $C_1 \oplus C_2 = (K \oplus M_1) \oplus (K \oplus M_2) = M_1 \oplus M_2$

WEP – bezpečnostné chyby

- Slabé kľúče pre RC4
  - Pre niektoré inicializačné hodnoty nie je počiatočná časť prúdu generovaného RC4 dostatočne náhodná
  - Ak sa použije zlá inicializačná hodnota, niekoľko úvodných bajtov prúdu môže odhaliť informácie o kľúči
  - V prípade vhodne zvoleného IV môže dôjsť k použitiu zlej inicializačnej hodnoty
    - útočník to rozpozná, keďže IV je prenášané v otvorenom tvare
  - Šifrovanie vo WEP môže byť rozbité po odpočutí niekoľko miliónov správ

WEP - ponaučenie

- Navrhnúť bezpečnostný protokol je ťažké
  - Nesprávna kombinácia inak bezpečných protokolov môže skončiť zle
    - Príklad 1:
      - Prúdové šifry sú OK
      - Challenge-response protokol na kontrolu prístupu je OK
      - Nemali by byť kombinované s rovnakým kľúčom
    - Príklad 2:
      - Zašifrovanie správy spolu s jej odtlačkom ako kontrola integrity je OK
      - Avšak neplatí to ak je odtlačková funkcia lineárna vzhľadom na použité šifrovanie
- Ak je to možné, nepoužívať WEP

Štandard IEEE 802.11i

- Po odhalení problémov vo WEP, IEEE začala vyvíjať novú bezpečnostnú architektúru – 802.11i
- Hlavné vylepšenia v 802.11i oproti WEP
  - Kontrola prístupu na základe 802.1X (EAP, Radius)
    - Možnosť využitia silných kryptografických protokolov ako TLS
  - Výsledkom autentizačného procesu je aj „session key“ (ochrana pred session hijacking)
  - Rôzne funkcionality využívajú rôzne kľúče, ktoré sú odvodené zo zdieľaného kľúča na základe jednosmernej funkcie
  - Vylepšená kontrola integrity
  - Vylepšené šifrovanie

Štandard IEEE 802.11i

- Špecifikuje koncept RSN (Robust Security Network)
  - Šifrovanie a kontrola integrity sú postavené na AES
  - Nekompatibilné so starými zariadeniami
  - Známy ako WPA2 (WiFi Protected Access 2)
- Definuje aj protokol TKIP (Temporal Key Integrity Protokol)
  - Šifrovanie využíva RC4, ale problémy WEP boli odstránené
  - Beží na starých zariadeniach (po aktualizovaní softvéru)
  - Známy ako WPA (WiFi Protected Access)

802.11 - Bezpečnostné riešenia

porovnanie

	WEP	WPA	WPA2
Kontrola prístupu	pre-shared key	802.1X / pre-shared key	802.1X / pre-shared key
Autentizácia	-	EAP / pre-shared key	EAP / pre-shared key
Šifrovanie	RC4	TKIP (RC4)	AES / TKIP

802.11 - Bezpečnostné riešenia

porovnanie

	WEP	WPA	WPA2
Šifra	RC4	RC4	AES
Veľkosť kľúča	40 (104) bitov	128 bitov šifrovanie 64 bitov autentizácia	128 bitov
Veľkosť IV	24 bitov	48 bitov	48 bitov
Kontrola integrity	CRC-32	Michael	CBC-MAC
Integrita hlavičky	žiadna	Michael	CBC-MAC
Odolnosť voči opakovaniu	žiadna	Sekvenčný IV	Sekvenčný IV
Manažment kľúčov	žiadny	EAP (802.1x)	EAP (802.1x)

IEEE 802.11i
Kontrola prístupu

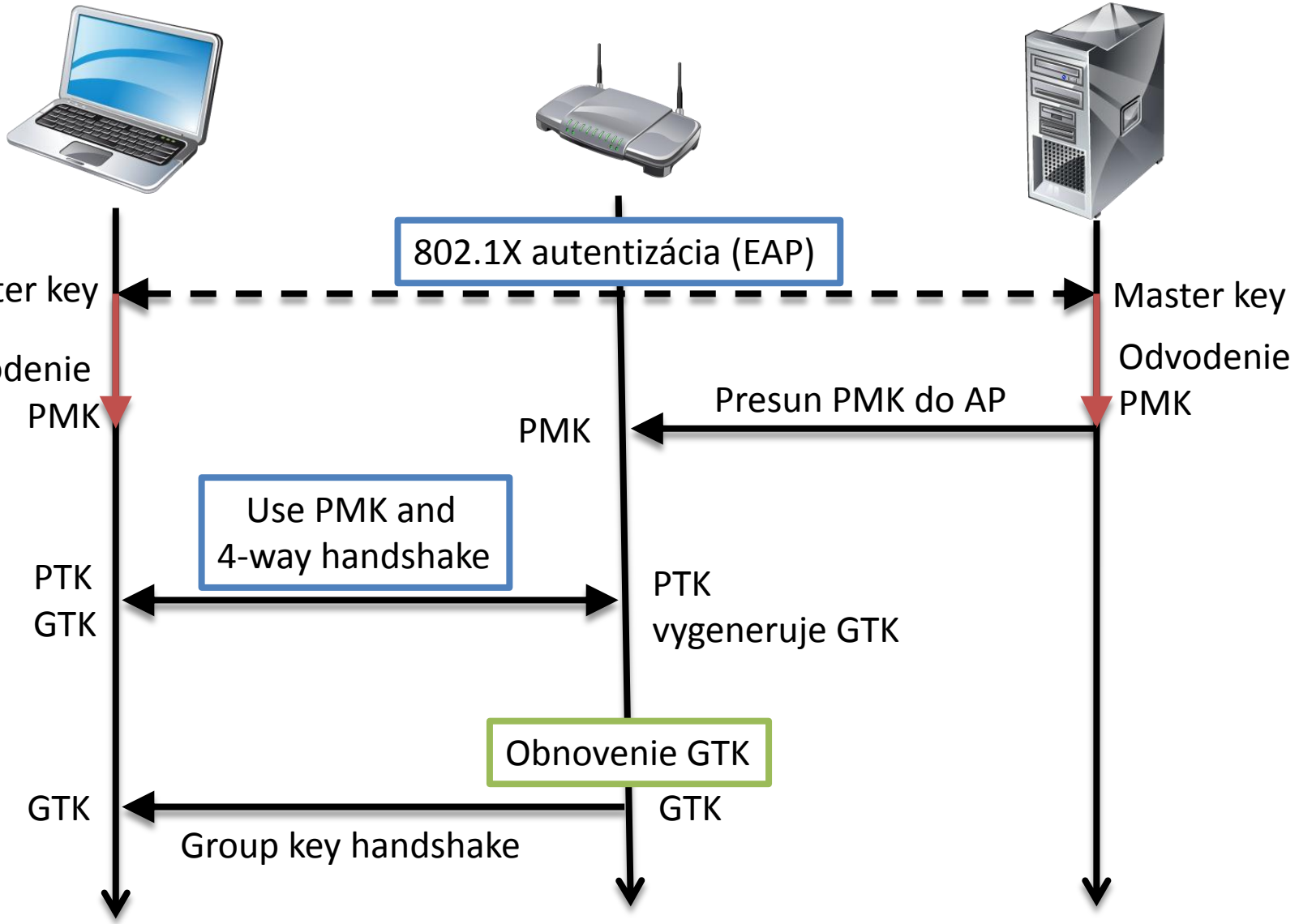
- Domáce použitie
  - Zdieľaný kľúč ako v prípade WEP
  - WPA-Personal, WPA2-Personal
- Korporátne použitie
  - 802.1X (EAP, Radius)
  - WPA-Enterprise, WPA2-Eterprise
  - Výstupom autentizačného procesu je „Master key“ (MK) medzi stanicou a autentizačným serverom.
    - Master key je platný len pre danú reláciu

IEEE 802.11i
Inicializácia kľúčov

- Automatická: využíva 802.1X
  - Po skončení autentizácie 802.1X, stanica aj autentizačný server vypočítajú na základe Master Key tzv. Pairwise Master Key (PMK)
  - Autentizačný server pošle PMK do AP
  - Stanica a AP použijú PMK na vygenerovanie **PTK** (Pairwise transient key)
    - Na šifrovanie správ medzi AP a jednou STA
    - Vypočíta sa pomocou tzv. 4-way handshake protokolu
  - Následne AP vygeneruje GTK (na šifrovanie
    - Na šifrovanie „broadcast“ správ od AP ku všetkým STA
- Manuálna
  - WPA/WPA2-Personal
  - PMK je odvodené z pre-shared key, ďalej sa postupuje rovnako ako v predošlom bode

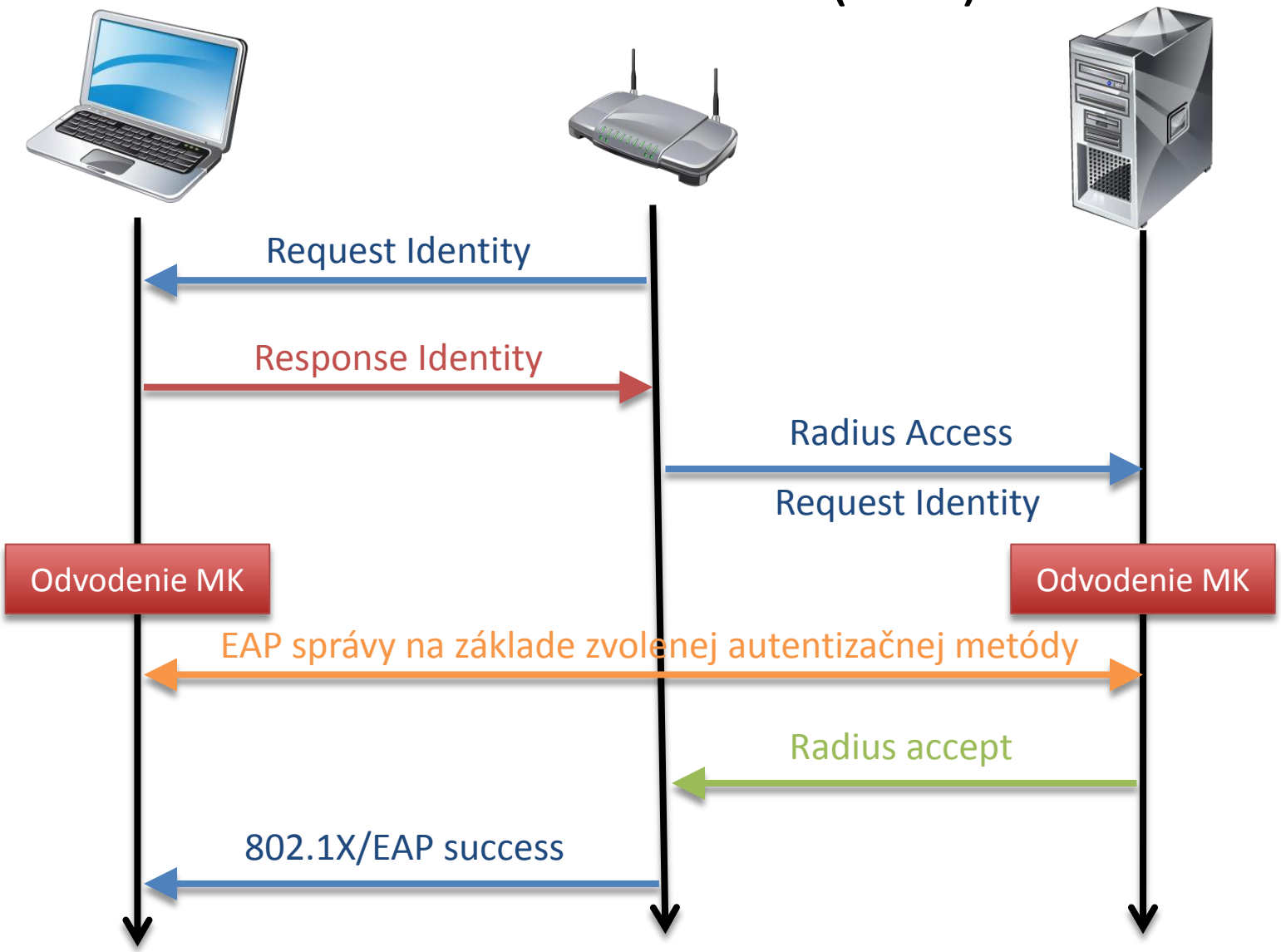
WPA / WPA2

Inicializácia kľúčov



WPA / WPA2 Enterprise

802.1X autentizácia (EAP)



4-way handshake protokol

Spúšťa ho AP a slúži na

- Overenie, že jednotlivé strany poznajú PMK
- Výmenu náhodných správ z ktorých je vygenerované PTK
- Zaslanie GTK

MIC_{KIK} – Message Integrity Code (vypočítaný na základe key-integrity key)

KeyReplayCtr – použitý kvôli ochrane voči útokom opakovaním

AP: vygeneruj náhodné A_r

AP → STA: A_r | KeyReplayCtr

STA: Vygeneruj náhodné S_r
Vypočítaj PTK z A_r , S_r , PMK

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

AP: Vypočítaj PTK a over MIC
Vygeneruj GTK

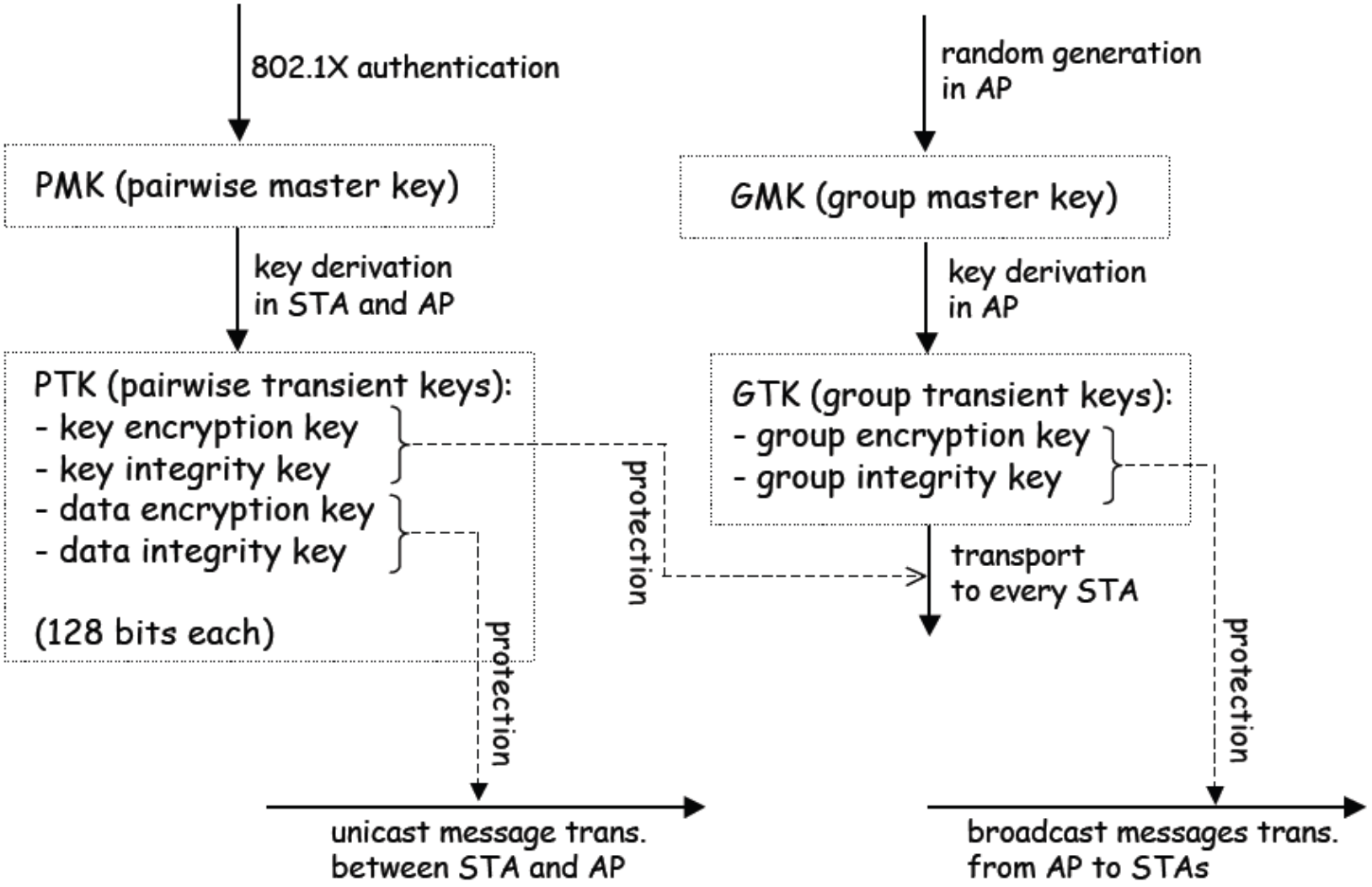
AP → STA: A_r | KeyReplayCtr+1
| $\{GTK\}_{KEK}$ | MIC_{KIK}

STA: Over MIC a nainštaluj kľúče

STA → AP: KeyReplayCtr+1 | MIC_{KIK}

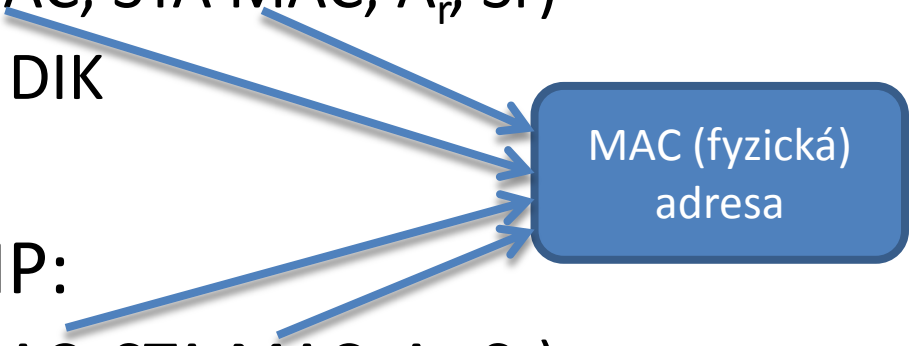
AP: Over MIC a nainštaluj kľúče

IEEE 802.11i
hierarchia kľúčov



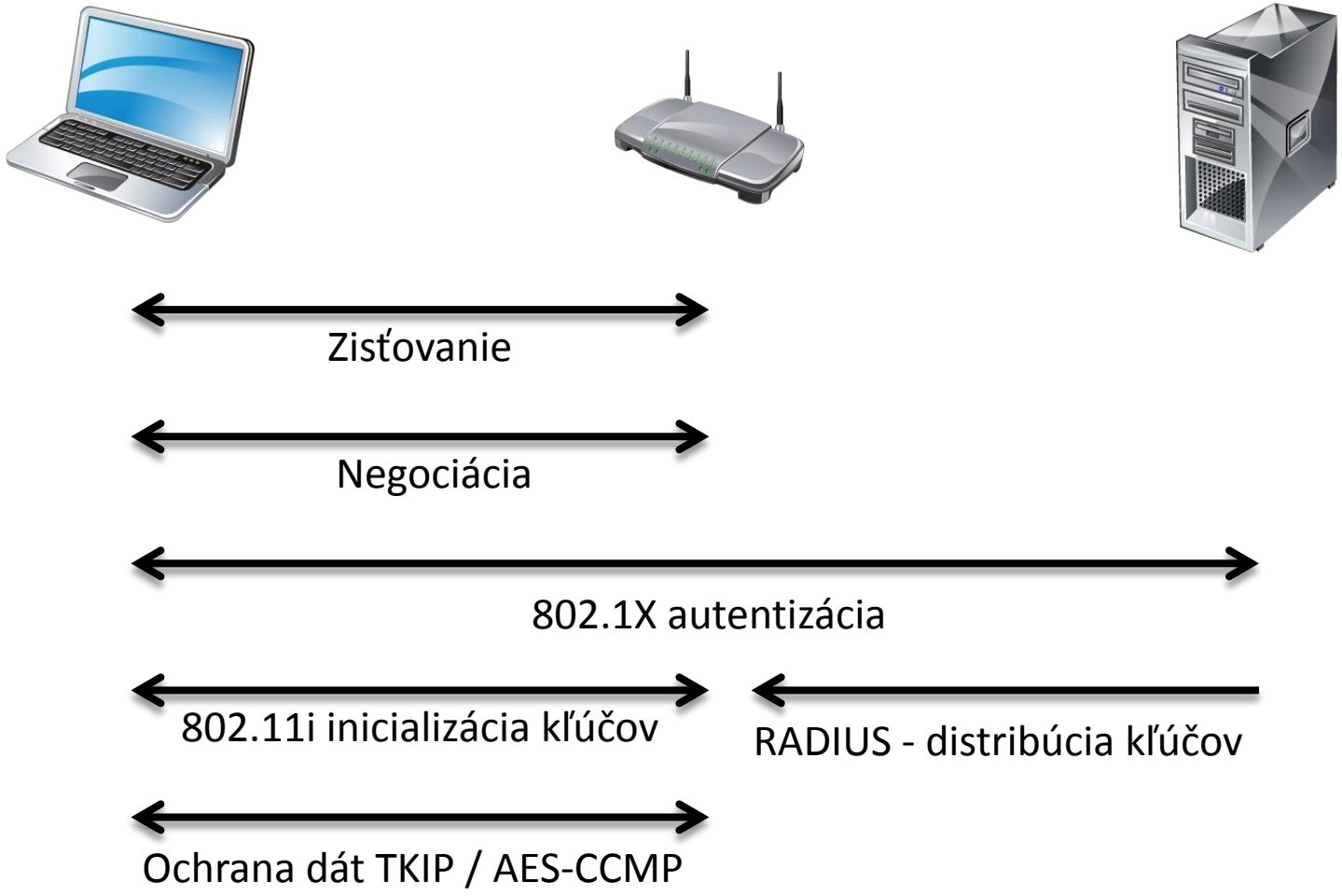
4-way handshake protokol
výpočet PTK

- V prípade TKIP:
  - Prf-512(PMK, AP MAC, STA MAC, A_r, Sr) =
    = KEK | KIK | DEK | DIK
- V prípade AES-CCMP:
  - Prf-384(PMK, AP MAC, STA MAC, A_r, Sr) =
    = KEK | KIK | DE&IK



Prf-512 / Prf-384 – Pseudo-náhodná funkcia s dĺžkou výstupu 512 / 384 bitov.

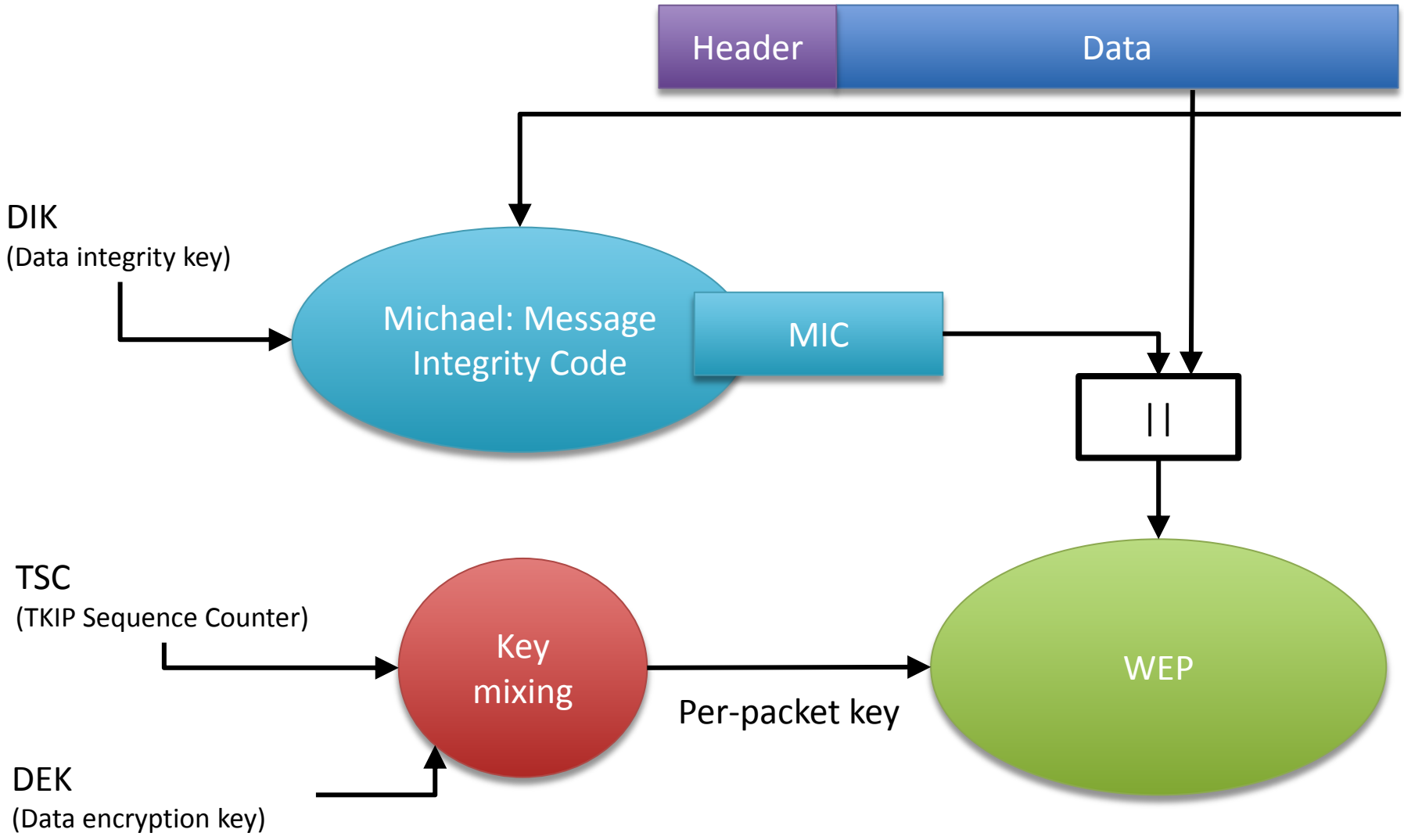
IEEE 802.11i - Sumarizácia



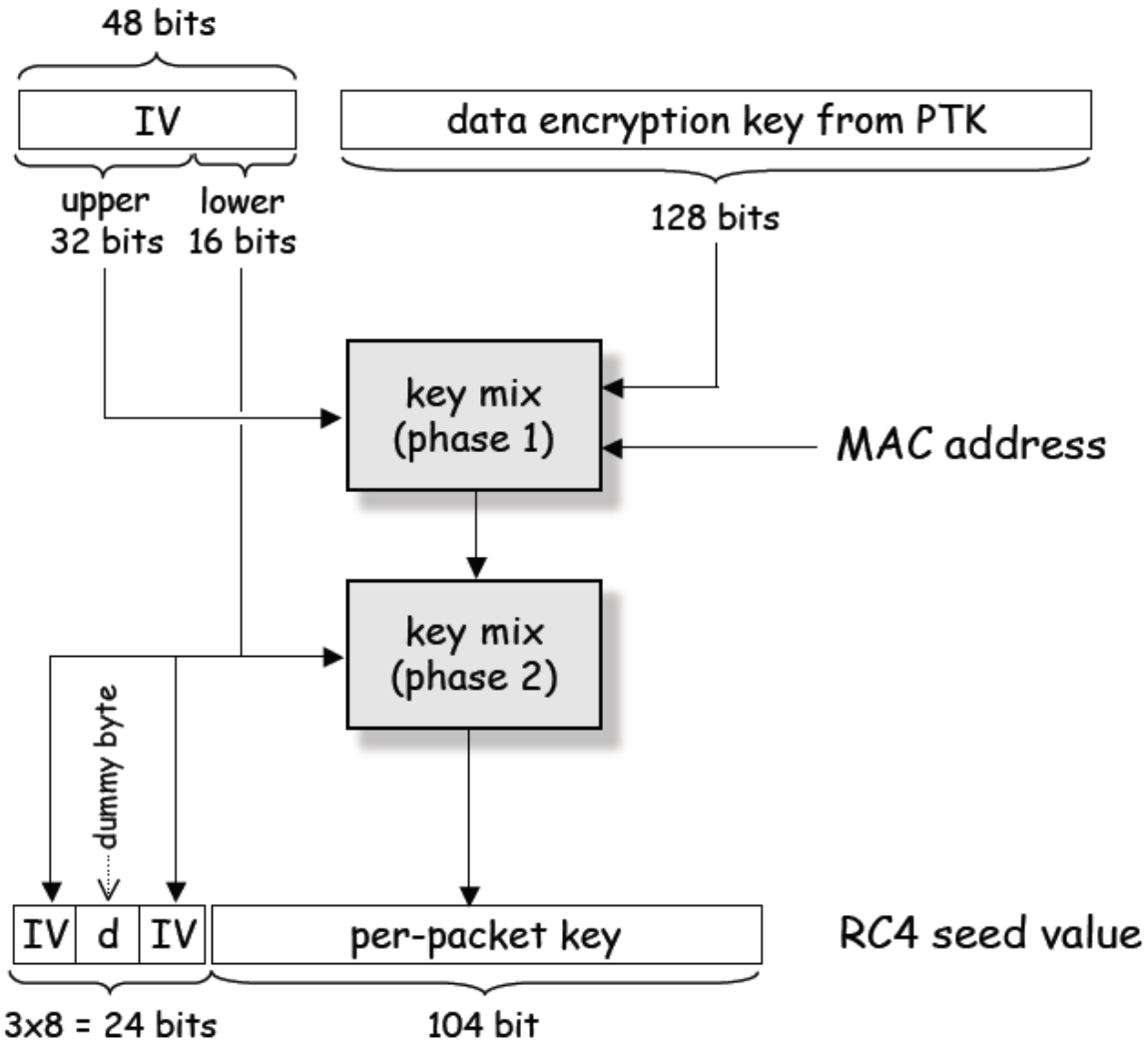
WPA – Šifrovanie
TKIP

- Beží na starších zariadeniach, ktoré podporujú RC4
- 128 bitový tajný kľúč
- Slabiny WEP sú odstránené
  - Nová ochrana integrity správ – Michael
    - Generuje nelineárny 8 bajtový MIC (Message Integrity Code) spolu s 32 bitmi CRC
  - IV je 48-bitový TKIP sequence counter (TSC)
    - Ochrana voči opakovacím útokom, pri novom zdieľanom kľúči sa TSC nastaví na 0 a zakaždým sa inkrementuje

TKIP - šifrovanie



TKIP – generovanie kľúčov pre RC4

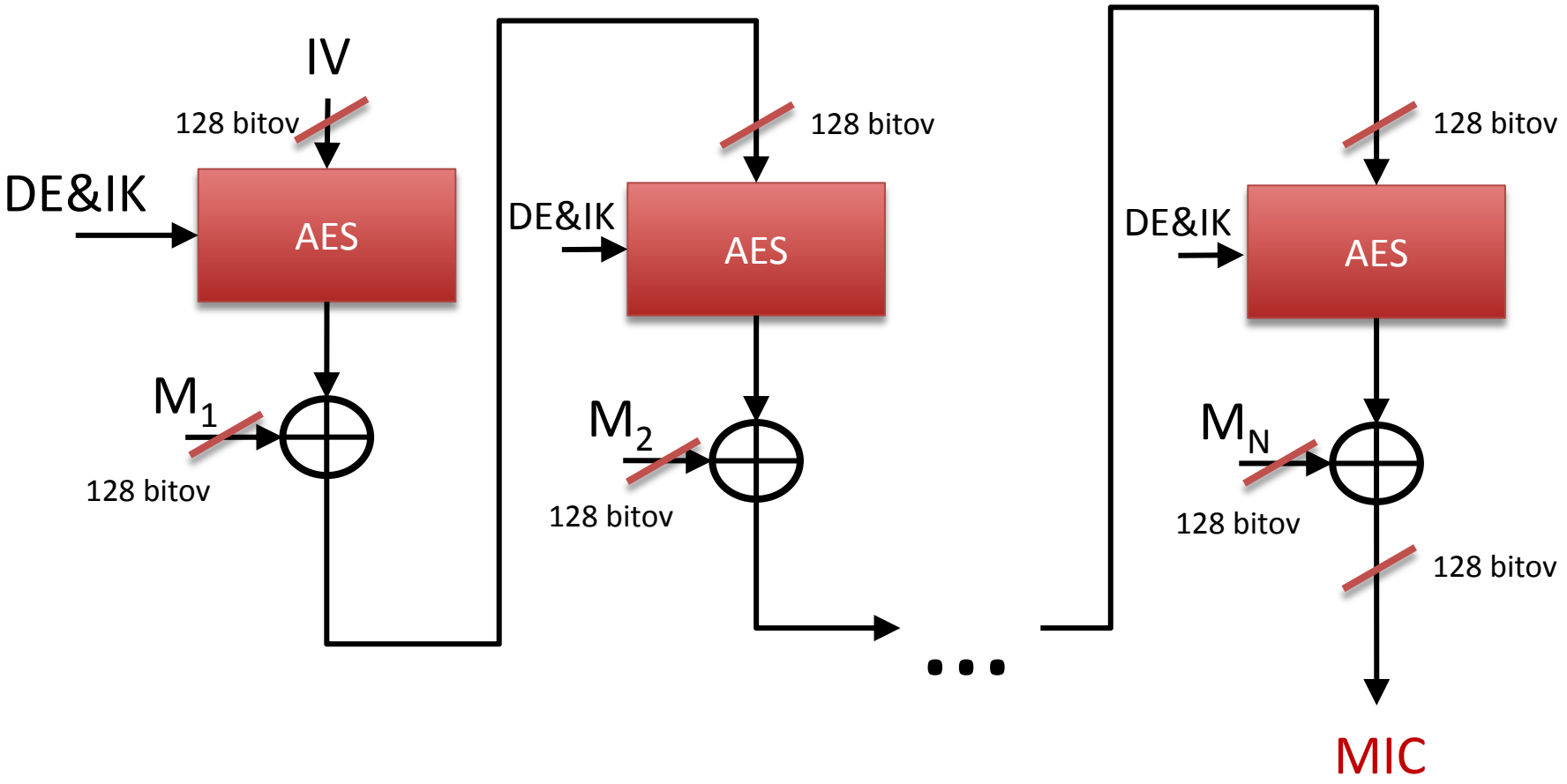


WPA2
AES-CCMP

- WPA2 využíva AES s dĺžkou kľúča 128 bitov
- CCMP znamená CTR mód a CBC-MAC
  - Kontrola integrity postavená na CBC-MAC (využitím AES ako blokovej šifry)
  - Šifrovanie beží v CTR móde (využívajúc AES)
- Rovnaký kľúč pre šifrovanie a autentifikáciu avšak s iným IV
- Nie je spätne kompatibilný s WEP, potreba nového hardware.

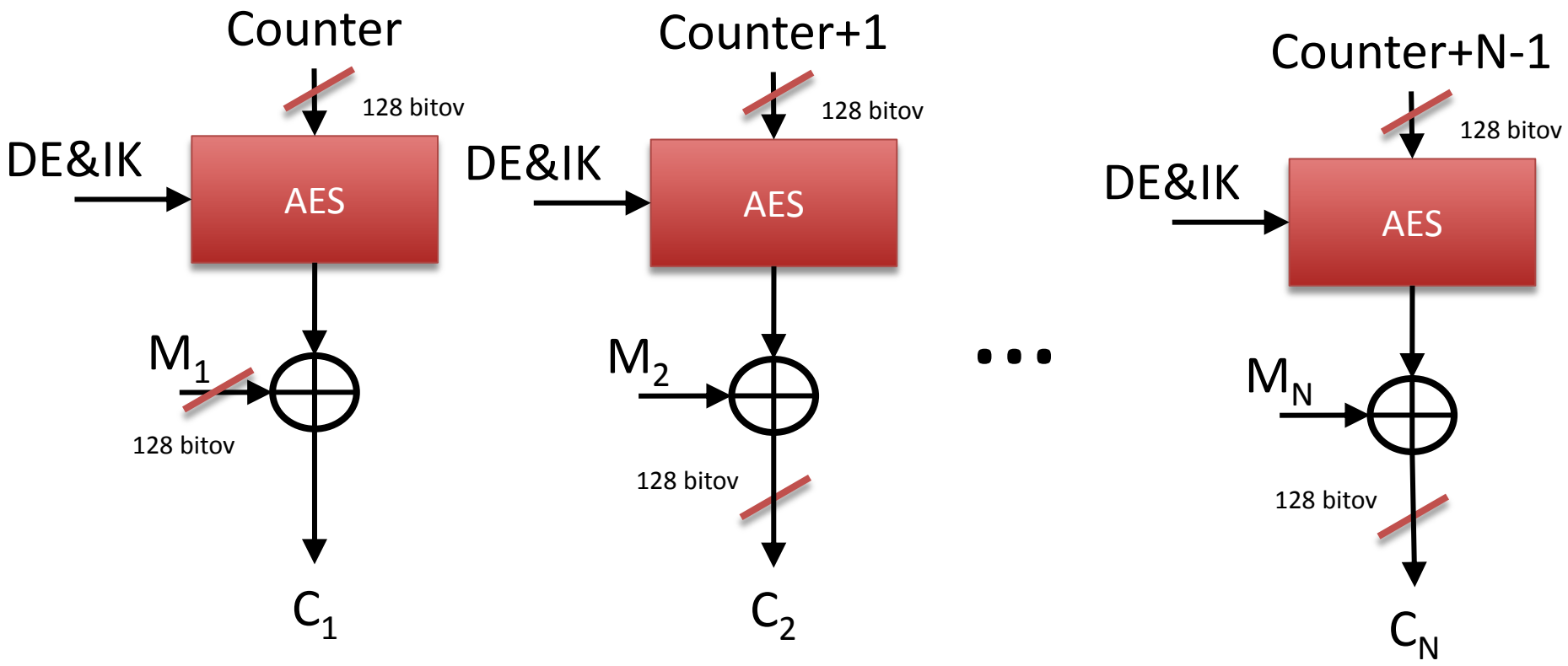
WPA2 šifrovanie

CBC-MAC



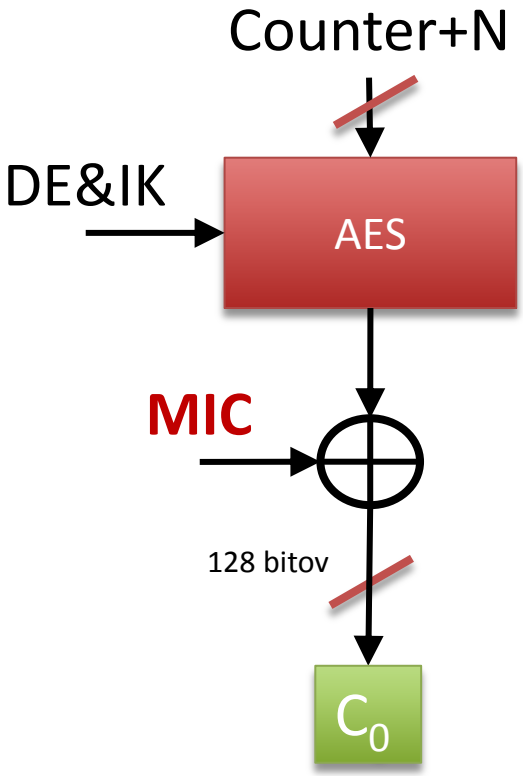
WPA2 šifrovanie

Counter mód



WPA2 šifrovanie

Counter mód (2)



Požiadavky na bezpečnosť bezdrôtových sietí a WPA / WPA2

- ✓ Dôvernosť
  - Vysielané správy musia byť šifrované
- ✓ Autenticita
  - Overenie identity druhej strany
  - Overovanie pôvodu prijatých správ
- ✓ Nemožnosť opakovať odpočuté správy
  - Kontrola čerstvosti prijatých správ
- ✓ Integrita správ
  - Kontrola integrity prijatých správ
- ✓ Riadenie prístupu
  - Prístup k sieti by mal byť povolený iba oprávneným účastníkom
  - Permanentná kontrola prístupu, nie iba pri nadväzovaní spojenia.
- ✗ Ochrana proti rušeniu

Záver

- Bezdrôtové siete sú vo všeobecnosti ľahšie napadnuteľné ako drôtové
  - Útočník nepotrebuje fyzický prístup k sieťovej infraštruktúre
- Pôvodné zabezpečenie WiFi sietí – WEP
  - Veľké bezpečnostné nedostatky, nepoužívať
- Bezpečnostný štandard 802.11i
  - Kontrola prístupu postavená na 802.1X
  - Lepšia správa kľúčov
  - TKIP
    - Beží na starom harware
    - Využíva šifru RC4
    - Oprava slabín vo WEP
  - AES-CCMP
    - CTR mód a CBC-MAC
    - Vyžaduje nový hardware