Wireless LAN

Jákó András
goya@eik.bme.hu
BME EISzK

Agenda

Bevezető

Fizikai réteg

Közeghozzáférés

Biztonság

Egyéb

Mi is az a wireless LAN?

- vezeték nélküli helyi hálózat
  - 10-200 m (-40 km) kiterjedés
- IEEE 802.11 szabvány – most csak erről lesz szó
  - PHY és MAC specifikáció
    - az OSI rétegmodell alsó 1.5 rétege
    - PHY: rádiófrekvenciás vagy infravörös átvitel
    - MAC: CSMA/CA közeghozzáférési protokoll
- jelenleg 1-54 Mb/s névleges átviteli sebesség
  - ez általában a MAC adatkeret átviteli sebessége
  - a protocol overheadek miatt a hasznos MAC sávszélesség 10-30%-kal kisebb
  - osztott közeg: az állomások osztoznak ezen a sávszélességen
- nem Ethernet
  - legalábbis nem sokkal jobban, mint pl. a Token Ring
  - annak ellenére, hogy itt tényleg az „éter” az átviteli közeg

Az „éter” mint médium jellemzői

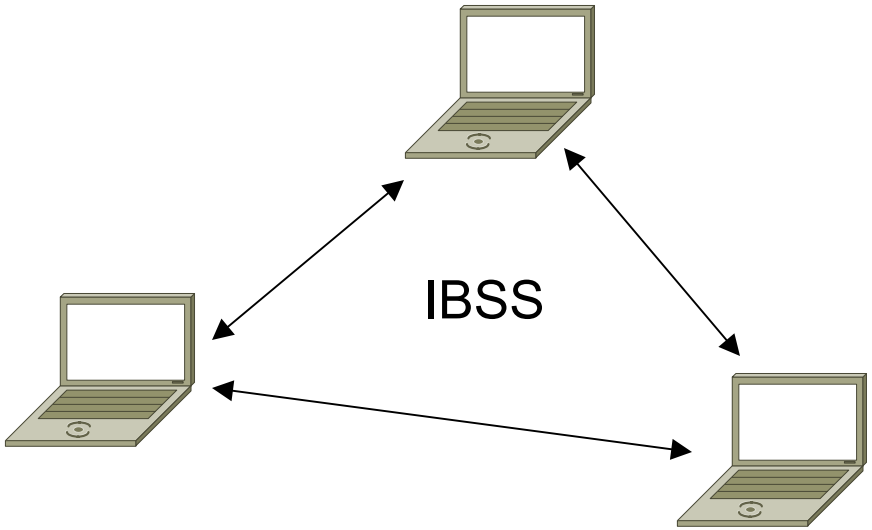
- rendszerint nincsenek jól definiált határai
  - RF esetén szinte egyáltalán nincsenek határok
    - Faraday kalitkát kevesen készítenek
  - IR esetén valamennyire lenne, mégpedig a helyiség
- védtelen a külső zavaró jelektől
- megbízhatatlan
- dinamikus a topológia
- nincs feltétlenül minden állomásnak minden állomással kapcsolata
- időben változó, aszimmetrikus jelterjedési idők

Architektúra

- állomások
  - mobilitás lehetséges
    - működés közben is mozoghat
- BSS – Basic Service Set
  - állomások egy csoportja
  - időben egymás közt osztják meg a vezeték nélküli médiumot
    - azaz együtt használják a CSMA/CA protokollt
- működési módok:
  - ad-hoc mód
  - infrastruktúra mód

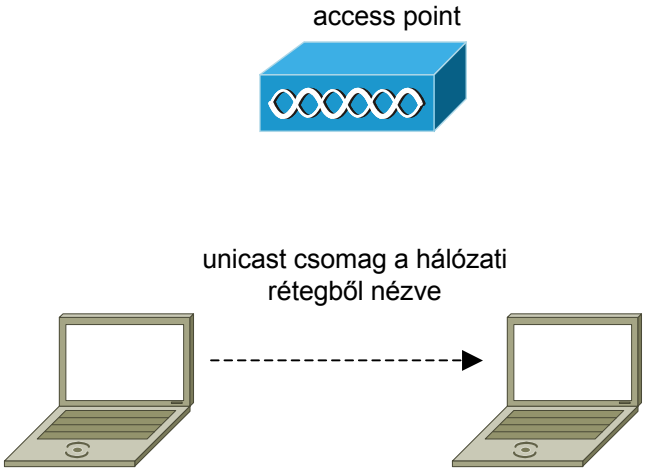
Ad-hoc mód

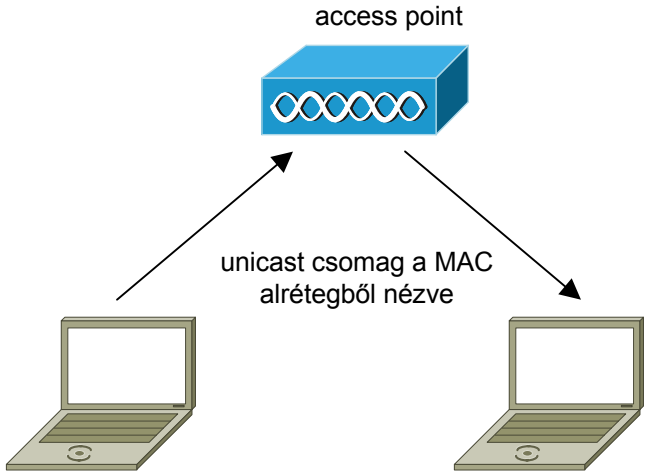
- IBSS – Independent BSS
- az állomások közvetlenül egymással kommunikálnak
- elosztott rendszer
  - nincs központi állomás
- korlátozott térbeli méret



Infrastruktúra mód

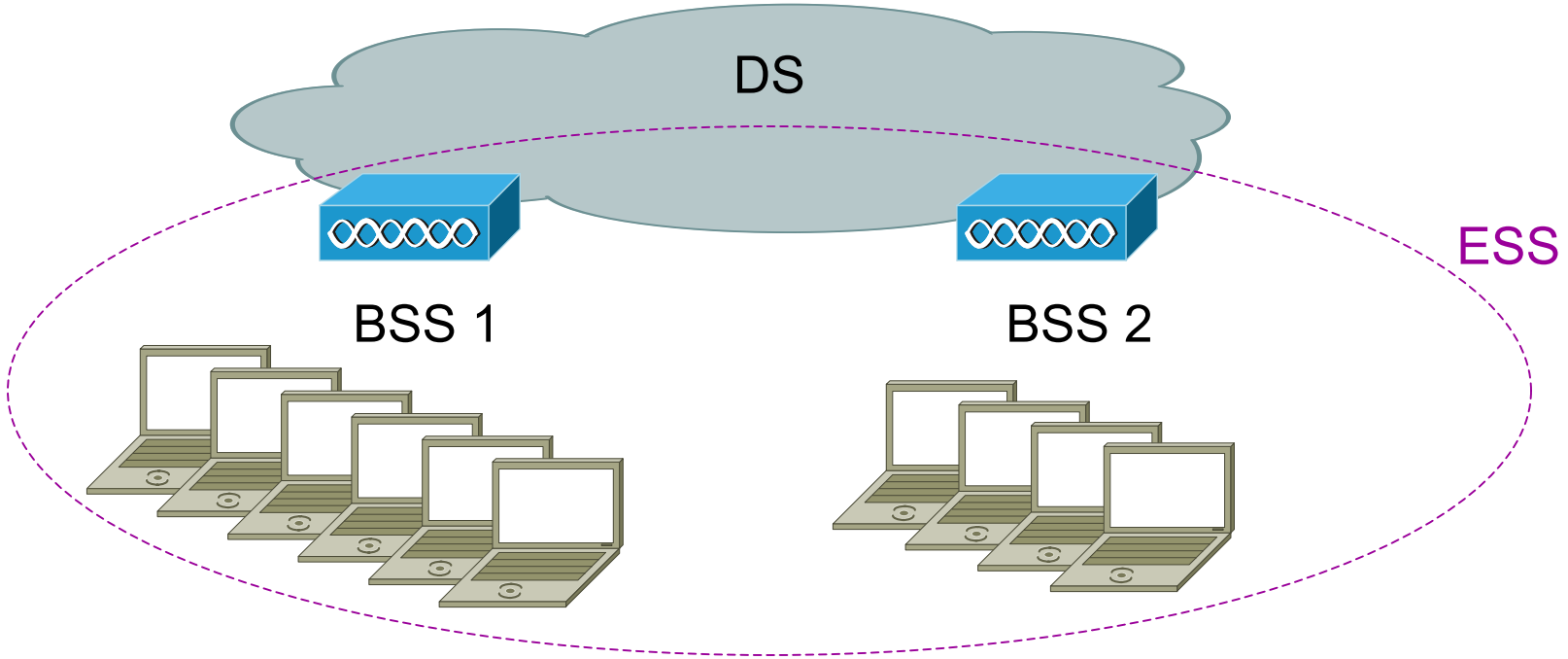
- access point: kitűntetett központi állomás
  - minden BSS-ben pontosan egy AP
- az AP-tal minden állomásnak tudnia kell kommunikálni
  - mivel csak így tudnak csatlakozni az infrastruktúra módú BSS-hez
- a többi állomással nem kritérium a közvetlen kapcsolat
  - a BSS többi tagja egymással az AP-on keresztül kommunikál
  - így nagyobb lehet a BSS térbeli kiterjedése is





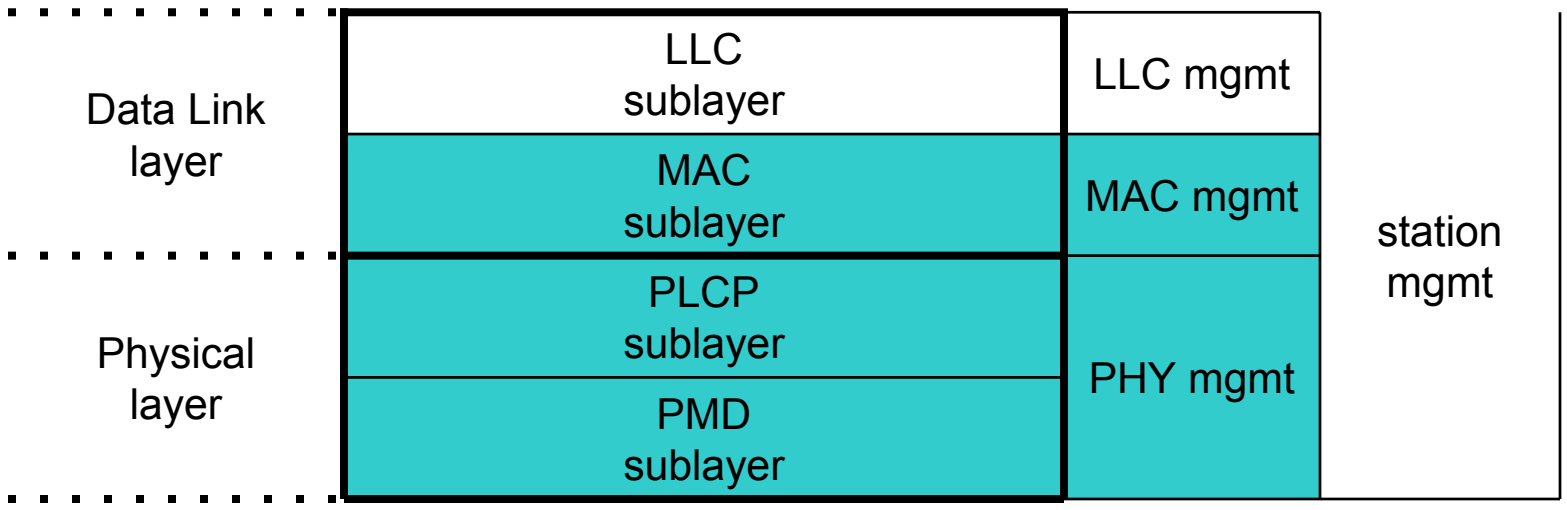
Infrastruktúra mód – ESS

- ESS – Extended Service Set
  - egymással összekapcsolt BSS-ek
- DS – Distribution System
  - összeköti a BSS-eket
  - vezeték nélküli, vezetékes IEEE 802 LAN, IP hálózat, stb.
  - a BSS-t az access point kapcsolja a distribution systemhez



Referenciamodell

- LLC – Logical Link Control
- MAC – Medium Access Control
- PLCP – Physical Layer Convergence Protocol
- PMD – Physical Medium Dependent
- PHY – Physical



Agenda

Bevezető

Fizikai réteg

Közeghozzáférés

Biztonság

Egyéb

802.11 fizikai rétegek

- 1997: IEEE 802.11
  - Infrared (IR)
  - Frequency Hopping Spread Spectrum (FHSS)
  - Direct Sequence Spread Spectrum (DSSS)
- 1999: IEEE 802.11a
  - Orthogonal Frequency Division Multiplexing (OFDM)
- 1999: IEEE 802.11b
  - High-Rate DSSS
- ? 2003: IEEE 802.11g
  - ? OFDM (+ CCK-OFDM, + PBCC)

Agenda

Fizikai réteg

IR PHY

Rádióhullámok

Antennák, deciBelek

FHSS PHY

DSSS PHY

High-Rate DSSS PHY

OFDM PHY

802.11g

Infravörös hullámok

- majdnem látható tartomány
- a látható fényhez nagyon hasonló terjedés
  - pl. tipikusan jól verik vissza a fényes felületek
- falon nem jut át, az ablaküveg nagyon csillapítja
  - nincs IR interferencia két szomszédos helyiség közt
  - kisebb a lehallgatás veszélye
- zavaró IR sugárforrások:
  - Nap
  - bizonyos mesterséges fényforrások
  - egyéb IR eszközök
    - távirányítók
    - IrDA

IR PHY

- nem nagyon használják
- 850-950 nm (f ≈ 320-350 THz)
- diffúz infravörös jel: csak beltéri használatra
  - zavarná a vevőt a közvetlen napsugárzás
  - visszaverő felületek kellenek (rálátás nem szükséges)
- max. 10-20 m távolság
- 1 és 2 Mb/s átviteli sebesség
- PPM – Pulse Position Modulation
  - L-PPM: L-ből 1 slotban „világít” az adó IR LED
  - slot: 250 ns
  - 1 Mb/s: 16-PPM
    - 4 adatbit 16 slotban
  - 2 Mb/s: 4-PPM
    - 2 adatbit 4 slotban

16-PPM, 4-PPM

- adatbitek Grey kód szerint
  - kis pozíciócsúszás kevés bithibát okoz

adat	4-PPM optikai jel
00	___|
01	__|_
11	_|__
10	|___

adat	16-PPM optikai jel
0000	_____|
0001	_____|_
0011	_____|__
0010	_____|___
0110	_____|____
0111	_____|_____
0101	_____|_____
0100	_____|_____
1100	_____|_____
1101	_____|_____
1111	_____|_____
1110	_____|_____
1010	_____|_____
1011	_____|_____
1001	_____|_____
1000	|_____

Agenda

Fizikai réteg

IR PHY

Rádióhullámok

Antennák, deciBelek

FHSS PHY

DSSS PHY

High-Rate DSSS PHY

OFDM PHY

802.11g

Frekvenciasávok

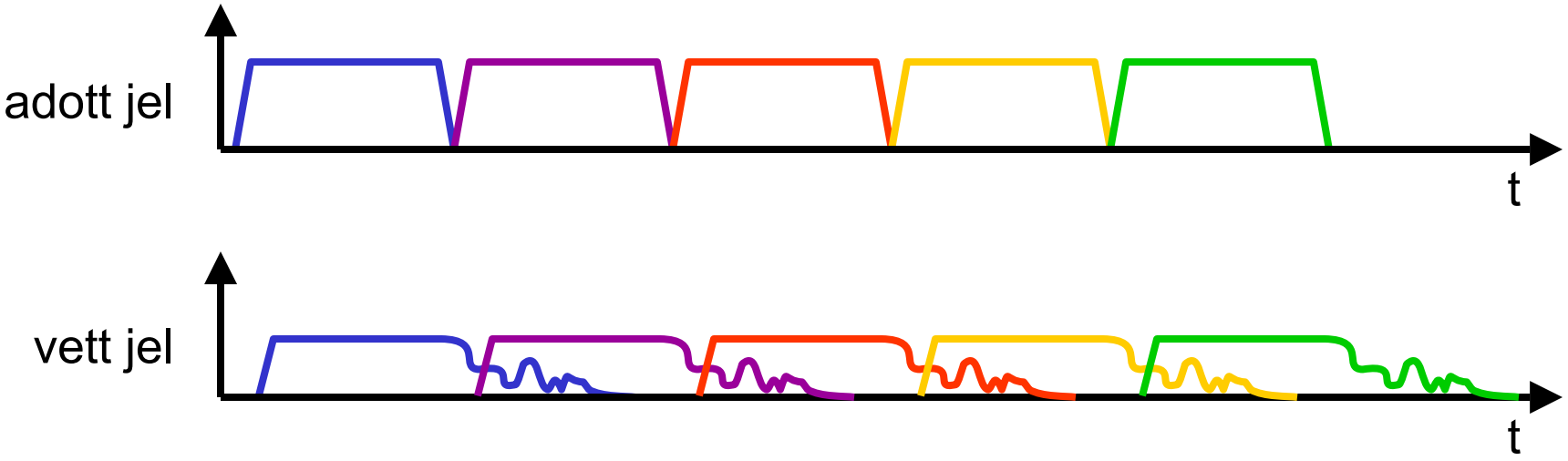
- rendszerint állami és nemzetközi szabályozás
- mikrohullám
- ISM – Industrial, Scientific and Medical
  - 2.4 GHz ($\lambda \approx 12$ cm)
  - engedély általában nem szükséges
  - sok zavaró jel
    - DECT, mikrohullámú sütő, stb.
- U-NII – Unlicensed National Information Infrastructure
  - 5 GHz ($\lambda \approx 6$ cm)
  - kevés zavaró jel
- frekvencia++ = távolság--, adatsebesség++

Rádióhullám terjedés

- a mikrohullámú sugarak levegőben kb. egyenesen haladnak
- a pontszerű sugárzó jele fokozatosan gyengül az adótól távolodva, a távolsággal négyzetes arányban
- iránya megváltozik különböző tereptárgyak miatt
  - visszaverődés (reflexió): λ-nál jóval nagyobb felület visszaverheti a hullámot
  - elhajlás (diffrakció): λ-hoz hasonló nagyságú élek mögé „bekanyarodik” a hullám
  - törés (refrakció): közeghatárokon a terjedés iránya megváltozik, ha a két közegben más a terjedési sebesség
- elnyelődés (abszorpció)
- néhány km adó-vevő távolság felett a Föld görbülete is jelentős

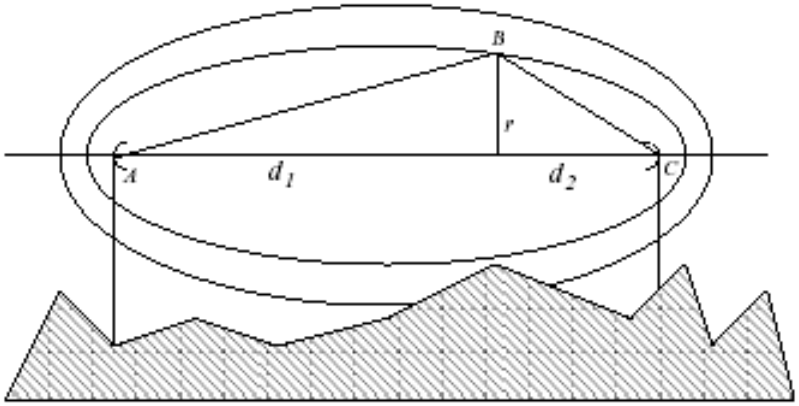
Többutas terjedés

- a reflexiók, diffrakciók, refrakciók következtében a jel több úton jut el az adótól a vevőig
- az útvonalak hossza különböző
- a vett jel időben „szétkenődik”
  - a beltéri differencia tipikusan < 100 ns



Fresnel zóna

- ellipszoid, fókuszai az antennák
  - k-adik Fresnel zóna: AB + BC = AC + k * λ/2
  - első Fresnel zóna: $r_{max} = 0.5 * \sqrt{\lambda * AC}$
- 0.6 * r_{max} maximális sugarú üres ellipszoid szükséges a jó mikrohullámú átvitelhez



2.4 GHz, λ = 12.5 cm

AC	0.6 * r_{max}
100 m	1 m
350 m	2 m
800 m	3 m
4 km	7 m
10 km	11 m
20 km	15 m
40 km	21 m

Agenda

Fizikai réteg

IR PHY

Rádióhullámok

Antennák, deciBelek

FHSS PHY

DSSS PHY

High-Rate DSSS PHY

OFDM PHY

802.11g

dB, dBm

- dB: 10 * log (A / B)
  - A és B arányát fejezi ki
  - könnyebb vele számolni, szorzás és osztás helyett összeadni és kivonni kell
- dBm: 10 * log (P / 1 mW)
  - adó teljesítménye, vevő érzékenysége

dB	arány
30	A = 1000 * B
10	A = 10 * B
6	A = 4 * B
3	A = 2 * B
0	A = B
-10	A = B / 10
-30	A = B / 1000

dBm	teljesítmény
30	1 W
20	100 mW
7	5 mW
0	1 mW
-83	5 pW (0.000 000 005 mW)

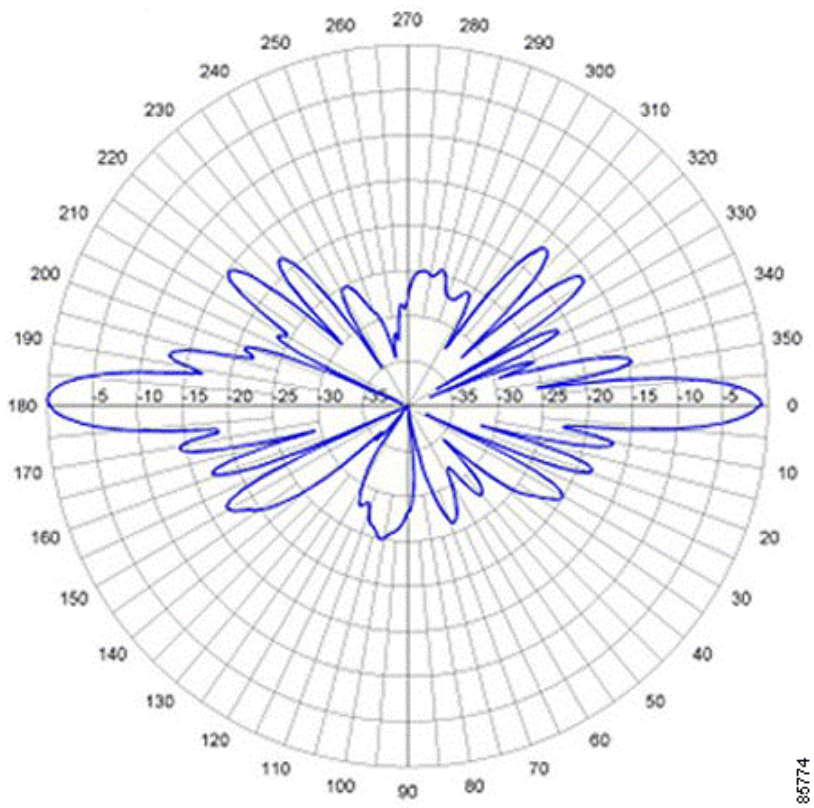
Antennák

- izotropikus antenna: hipotetikus ideális gömbsugárzó
- karakterisztika: sugárzás, érzékenység irányonként más
  - irányított vagy omni
- nyereség: adott irányba sugárzott teljesítmény (vagy vételi érzékenység) aránya az izotropikus antennához képest
  - dBi: nyereség dB-ben az izotropikus antennához képest
  - dBd: nyereség dB-ben a dipólus antennához képest (0 dBd = 2.14 dBi)
- polarizáció: az elektromos tér rezgésének módja
  - lineáris
    - függőleges vagy vízszintes síkban
  - elliptikus, cirkuláris
  - az adó és a vevő polarizációjának egyeznie kell

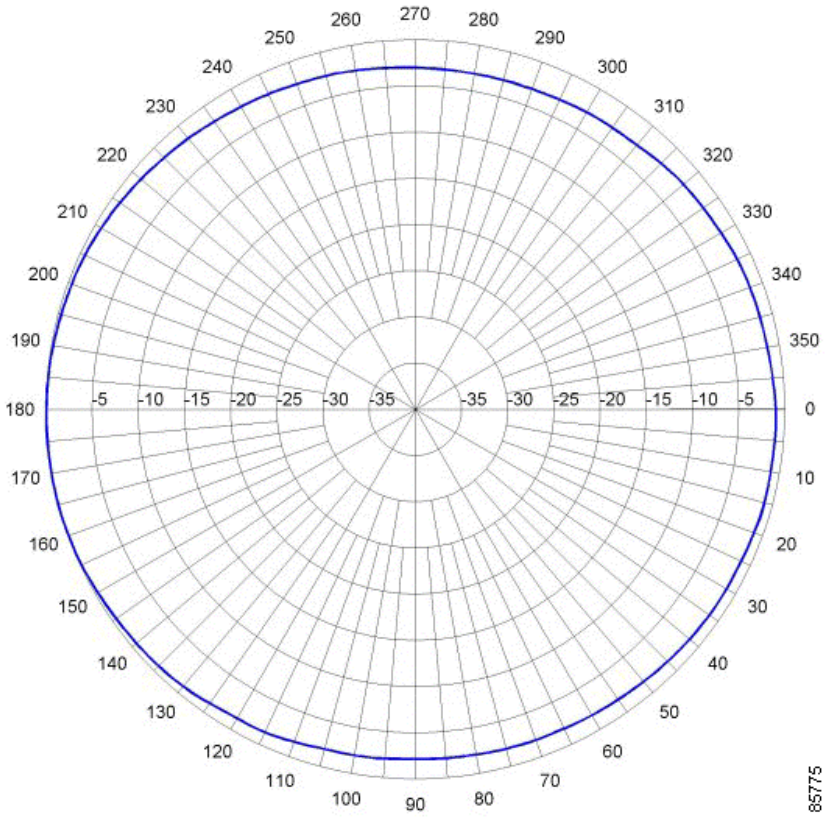
Antenna karakterisztika

- a valós antennák sugárzása/érzékenysége irányonként változik, ezt írja le az antenna karakterisztika

oldalnézet / függőleges minta / elevation-plane

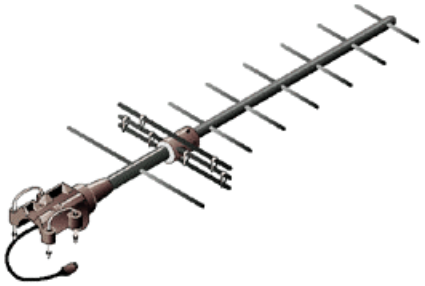


felülnézet / vízszintes minta / azimuth-plane



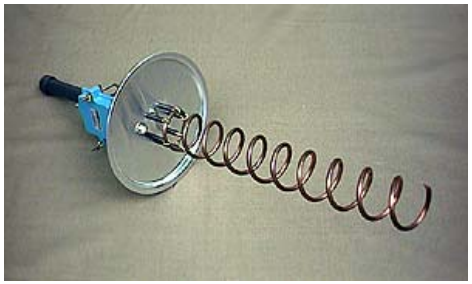
Antenna típusok

- omni
  - dipólus
  - co-linear
- irányított
  - panel, patch
  - helix
  - Yagi
  - parabola
- diversity: két antenna
  - egyszerre csak az egyik vesz
  - zeg-zugos terekben jó







Link power budget

- adó teljesítmény: 1-30 dBm (1-100 mW)
- csatlakozó veszteség: 0.01-0.2 dB
  - TNC, SMA, N, BNC
- antenna kábel veszteség: 0.1-1 dB méterenként
- antenna nyereség: 2-25 dBi
- veszteség szabadtéri terjedés közben: 40-130 dB
  - Friis formula: $92.46 + 20 * \log f_{GHz} + 20 * \log d_{Km}$
  - eső, hó nem probléma
- veszteség tereptárgyakon:
  - fal, ajtó, ablak: 2-30 dB
  - erdő: 0.3-0.4 dB méterenként
- vevő érzékenység: (-90)-(-65) dBm
- általában min. 10 dB rést szokás hagyni

Spektrum etikett – 2.4 GHz

- EIRP – Equivalent Isotropically Radiated Power
  - ekkora teljesítményű izotropikus antennának felel meg a sugárzás az adott irányban
- helyi szabályok
  - ETSI: Európa nagy részén (Magyarországon is)
    - 20 dBm EIRP
  - ART: Franciaország (??? Spanyolország)
    - 2.4-2.446 GHz: 4 dBm (kültéri), 10 dBm (beltéri)
    - 2.4465-2.4835 GHz: 20 dBm (beltéri és kültéri, kültéren csak magánterületen és engedéllyel)
  - FCC, IC: USA, Kanada
    - Point-to-Multipoint: max. 1 W adóteljesítmény és max. 36 dBm EIRP
    - Point-to-Point: max. 30-k dBm adótelj. és max 36+3k dBm EIRP (k>=0)
  - MPHPT: Japán
    - 2.4-2.4835 GHz: 3 mW/MHz FHSS, 10 mW/MHz DSSS
    - 2.471-2.497 GHz: 10 mW/MHz FHSS és DSSS

Spektrum etikett – 5 GHz

- FCC: USA
  - U-NII 1: 5.15-5.25 GHz
    - csak beltéri
    - max. 40 mW adóteljesítmény és max. 22 dBm EIRP
  - U-NII 2: 5.25-5.35 GHz
    - max. 200 mW adóteljesítmény és max. 29 dBm EIRP
  - U-NII 3: 5.725-5,825 GHz
    - csak kültéri
    - max. 800 mW adóteljesítmény és max. 35 dBm EIRP
- ETSI: Európa
  - 5.15-5.35 GHz: 23 dBm EIRP
  - 5.470-5.725 GHz: 30 dBm EIRP

Link power budget: Kültér, 1 km

- 10 mW adóteljesítmény: 10 dBm
- 0.2 dB csatlakozó: -0.2 dB
- 12 m kábel, 0.3 dB/m: -3.6 dB
- 13 dBi Yagi antenna: +13 dB
  - EIRP: P = 10 dBm - 0.2 dB - 3.6 dB + 13 dB =19.2 dBm ✓ (<20 dBm)
- 1 km távolság, levegő: -100.3 dB
- 13 dBi Yagi antenna: +13 dB
- 6 m kábel, 0.3 dB/m: -1.8 dB
- 0.2 dB csatlakozó: -0.2 dB
  - vett jel: P = 19.2 dBm - 100.3 dB + 13 dB - 1.8 dB - 0.2 dB = -70.1 dBm
- -85 dBm érzékenységű vevő
- rés: -70.1 dBm + 85 dBm = 14.9 dB ✓ (>10 dB)

Link power budget: Beltér, 30 m

- 20 mW adóteljesítmény: 13 dBm
- 0.2 dB csatlakozó: -0.2 dB
- 1 m kábel, 0.3 dB/m: -0.3 dB
- 6.5 dBi diversity patch antenna: +6.5 dB
  - EIRP: P = 13 dBm - 0.2 dB - 0.3 dB + 6.5 dB =19 dBm ✓ (<20 dBm)
- 30 m távolság, levegő: -70 dB
- 2 fal: -15 dB
- 2 dBi PCMCIA kártyába épített dipólus antenna: +2 dB
  - vett jel: P = 19 dBm - 70 dB - 15 dB + 2 dB = -64 dBm
- -82 dBm érzékenységű vevő
- rés: -64 dBm + 82 dBm = 18 dB ✓ (>10 dB)

Agenda

Fizikai réteg

IR PHY

Rádióhullámok

Antennák, deciBelek

FHSS PHY

DSSS PHY

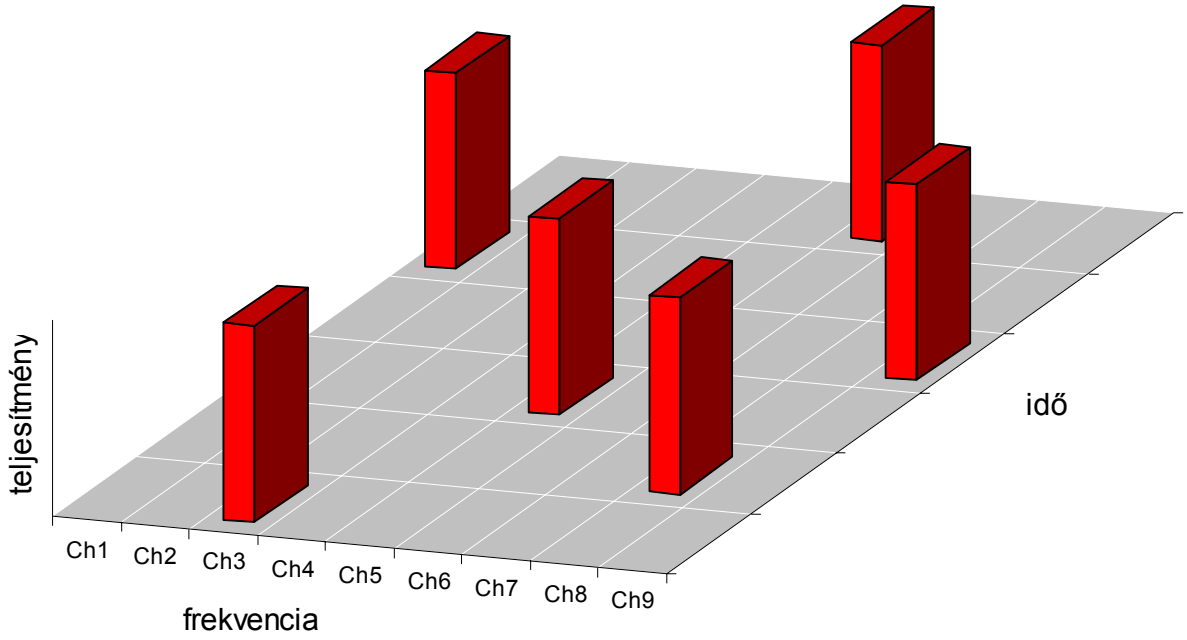
High-Rate DSSS PHY

OFDM PHY

802.11g

Frequency Hopping Spread Spectrum

- (időben) szórt spektrumú átviteli eljárás
- a vivőfrekvencia periodikusan változik
  - ugrási minta: frekvenciák meghatározott sorrendje
  - váltás egyszerre, meghatározott időnként (20-400 ms)
    - a beacon keretek segítenek a szinkronizálásban
  - IEEE 802.11d: ugrási minta automatikus generálása egyéb országokra



Ugrási minták

- vivőfrekvenciák 1 MHz-enként
- minden ugrás legalább 6 MHz (Japánban 5 MHz)
- ugrási mintákból három készlet
  - az egy készleten belüliek nem zavarják egymást

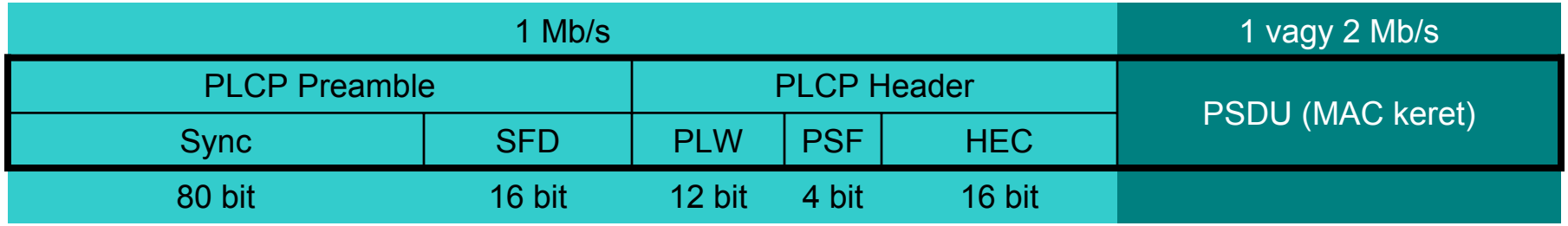
hely	frekvenciatartomány	vivők	ugrási minták	egyszerre használható ugrási minták
Európa	2.4-2.4835 GHz	79	78	26
Franciaország	2.4465-2.4835 GHz	35	33	11
Spanyolország	2.445-2.4475 GHz	27	27	9
USA	2.4-2.4835 GHz	79	78	26
Japán	2.471-2.497 GHz	23	12	4

FHSS PHY moduláció

- GFSK – Gaussian shaped Frequency Shift Keying
  - az adatfolyam négyszögjelének szűrése aluláteresztő Gauss szűrővel
  - a vivő frekvenciájának modulálása a szűrt jellel
  - 1 Mb/s: 2-GFSK
  - 2 Mb/s: 4-GFSK Grey kóddal
    - 10: f_c+225 KHz
    - 11: f_c+75 KHz
    - 01: f_c-75 KHz
    - 00: f_c-225 KHz
- mindig 1 Mbaud jelzési sebesség

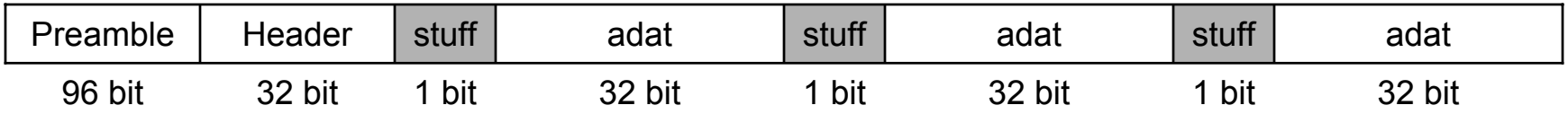
FHSS PLCP keretformátum

- Sync: 0101010101…
  - bitszinkronhoz
  - diversity esetén vevő antenna kiválasztása
- SFD – Start Frame Delimiter: 0000 1100 1011 1101
  - keretszinkronhoz
- PLW – PSDU Length Word: adatrész (PSDU) hossza byte-ban
- PSF – PLCP Signaling Field: adatrész adási sebessége
- HEC – Header Error Check: CCITT CRC-16 a PLCP fejlécre



FHSS PLCP adatrész

- az adatbitek egy 127 bit hosszú pseudo-random bitsorozattal vannak XOR-olva (scrambling)
  - DC komponens csökkentése
- 32/33 kódolás: 1 stuff bit, 32 adatbit
  - a stuff bit jelzi, hogy a 32 adatbit invertálva van-e
  - 0/1 arány hosszú távú kiegyenlítése



FHSS PHY

- legrosszabb vevő érzékenység
  - -80 dBm @ 1 Mb/s
  - -75 dBm @ 2 Mb/s
- maximális keret hibaarány
  - 400 byte-os kereteknél 0.03
- PMD rétegben mért statisztikai paraméter:
  - RSSI – Received Signal Strength Indication

Agenda

Fizikai réteg

IR PHY

Rádióhullámok

Antennák, deciBelek

FHSS PHY

DSSS PHY

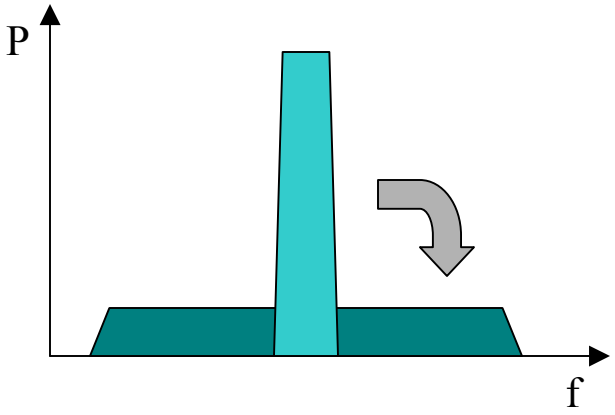
High-Rate DSSS PHY

OFDM PHY

802.11g

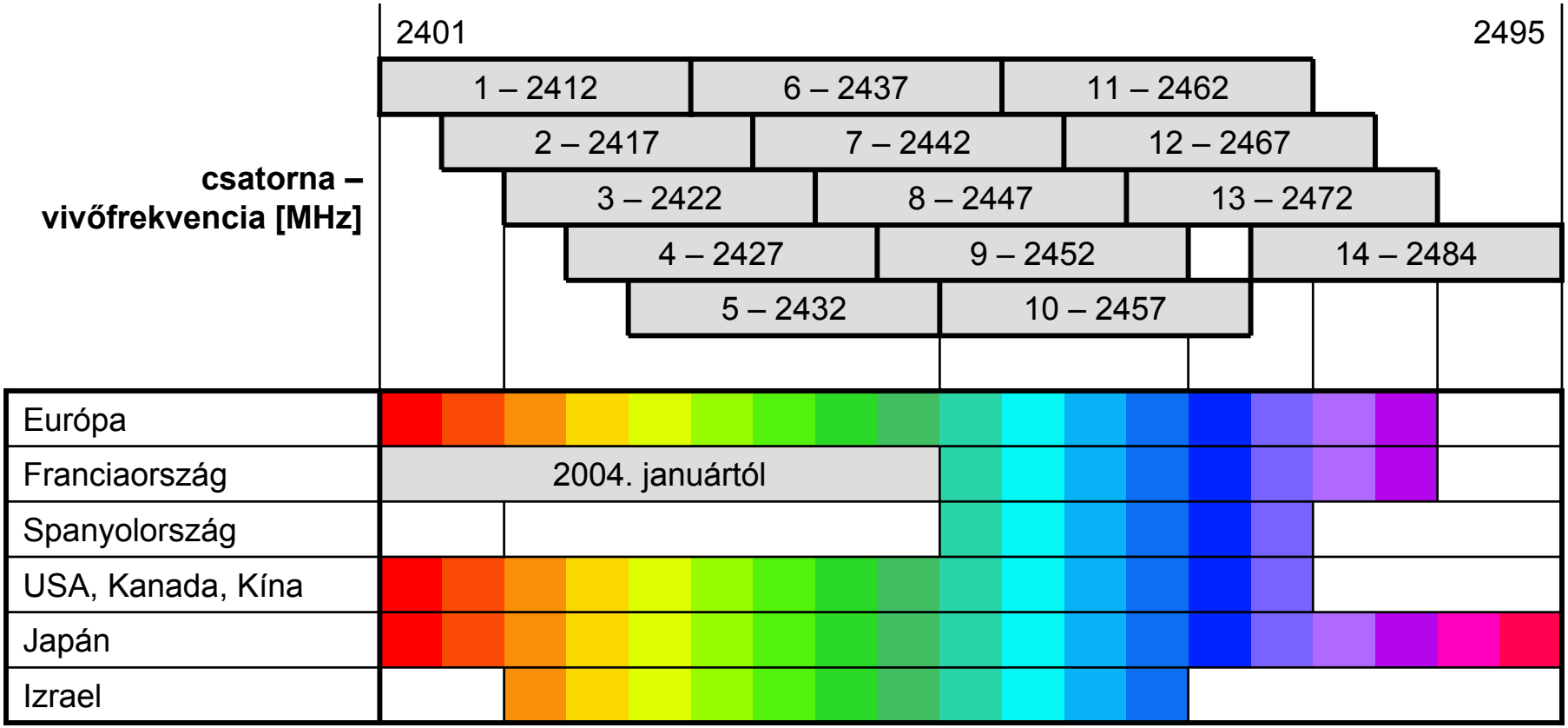
Direct Sequence Spread Spectrum

- szórt spektrumú átviteli eljárás
- 1 adatbit helyett egy 11 bites sorozat (chipping sequence)
  - PSK modulációval ez a spektrum kiszélesedését eredményezi
- chipping sequence: 10110111000
  - 11 bites Barker sorozat
    - jó autokorrelációs tulajdonságai vannak
  - 1 – 10110111000
  - 0 – 01001000111



DSSS PHY frekvenciák

- 22 MHz széles csatornák
- átfedik egymást



DSSS PHY moduláció

- DPSK – Differential Phase Shift Keying
  - az adatnak megfelelő szöggel változik a vivő fázisa
  - DBPSK – Differential Binary PSK
    - 0: +0
    - 1: +π
  - DQPSK – Differential Quadrature PSK, Grey kóddal
    - 00: +0
    - 01: +π/2
    - 11: +π
    - 10: +3π/2

DSSS PLCP keretformátum

- Sync: 1111111111…
- SFD – Start Frame Delimiter: 1111 0011 1010 0000
- Signal: adatrész adási sebessége
- Service: 0, későbbi felhasználásra fenntartott
- Length: az adatrész (MPDU) hossza µs-ban
- CRC: CCITT CRC-16 a PLCP fejlécre
- a teljes PLCP keret (Sync is) XOR-olva van egy scrambler (önszinkronizáló pseudo-random generátor) kimenetével

1 Mb/s						1 vagy 2 Mb/s
PLCP Preamble		PLCP Header				PSDU (MAC keret)
Sync	SFD	Signal	Service	Length	CRC	
128 bit	16 bit	8 bit	8 bit	16 bit	16 bit	

DSSS PHY

- antenna impedancia: 50 Ω
- legrosszabb vevő érzékenység:
  - -80 dBm @ 2 Mb/s
- maximális keret hibaarány:
  - 0.08 @ 2 Mb/s, 1024 byte-os keretekre
- CCA – Clear Channel Assessment
  - vett energia és/vagy vivőérzékelés alapján
- PMD rétegben mért statisztikai paraméterek:
  - RSSI – Received Signal Strength Indication
  - SQ – Signal Quality
    - (bit)szinkronizált állapotban a vett jel és a Barker seqence közötti korreláció

Agenda

Fizikai réteg

IR PHY

Rádióhullámok

Antennák, deciBelek

FHSS PHY

DSSS PHY

High-Rate DSSS PHY

OFDM PHY

802.11g

High-Rate DSSS PHY

- a DSSS PHY kiterjesztése
  - 5.5 és 11 Mb/s sebesség
  - CCK, PBCC
  - short preambe
  - channel agility
- IEEE 802.11b
- felülről kompatibilis a DSSS PHY-vel

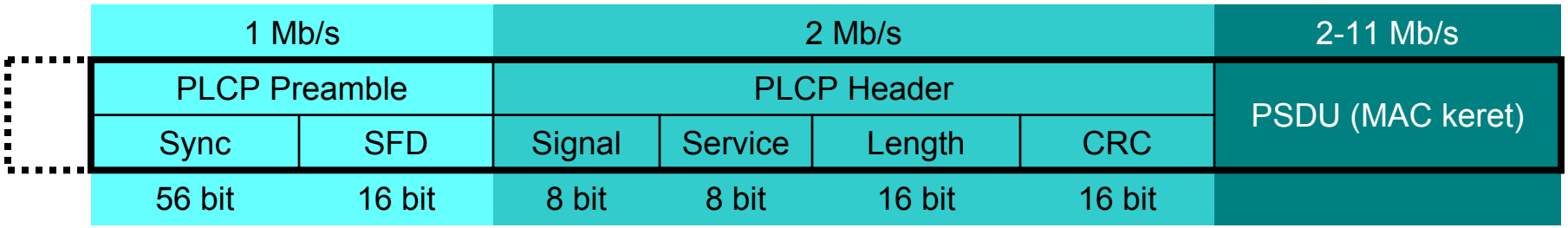
Long PLCP

- mint a 802.11 DSSS PHY PLCP, de
- Signal: 1, 2, 5.5, 11 Mb/s adatrész sebesség
- Service:
  - 1 bit Locked Clocks
    - a vivőfrekvencia és szimbólum időzítés közös oszcillátorról megy
  - 1 bit CCK/PBCC
  - 1 bit a Lengh mező kerekítési hibájának jelzése
    - 8 Mb/s felett az egészekre felfelé kerekített, µs-ban megadott hossz nem egyértelmű

1 Mb/s						1-11 Mb/s
PLCP Preamble		PLCP Header				PSDU (MAC keret)
Sync	SFD	Signal	Service	Length	CRC	
128 bit	16 bit	8 bit	8 bit	16 bit	16 bit	

Short PLCP

- mint a 802.11b long PLCP, de
- Sync: 0000000000…
- SFD: 0000 0101 1100 1111
- Signal: 2, 5.5, 11 Mb/s adatrész sebesség
- a PLCP Header 2 Mb/s sebességgel megy adásba



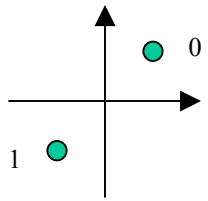
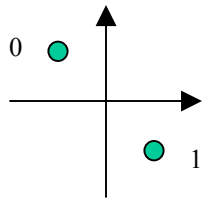
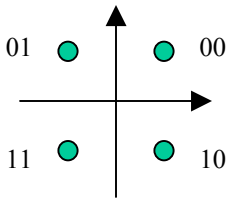
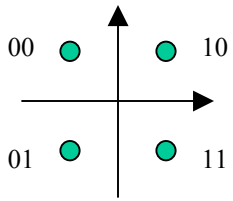
Complementary Code Keying

- 11 Mbaud jelzési sebesség
- DQPSK alapú rendszer
- 8 fázisváltás hosszúságú szimbólumok
  - 4^8 = 65536 lehetséges szimbólum
- egy szimbólumba kódolt adatbitek:
  - 5.5 Mb/s sebességnél 4 bit (16 érvényes szimbólum)
  - 11 Mb/s sebességnél 8 bit (256 érvényes szimbólum)

Packet Binary Convolutional Coding

- opcionális átviteli eljárás 5.5 és 11 Mb/s adatsebességre
- 64 állapotú ½ sebességű bináris konvolúciós kódoló
  - keret elején a 000000 állapotból indul
  - minden PLCP kerethez hozzá van fűzve egy 0x00 byte, hogy a kódoló ismert állapotba kerüljön a keret végén
- S – cover sequence: 256 bites pseudo-random sorozat
  - ez adja meg a pillanatnyi PSK konstellációt

adatsebesség	5.5 Mb/s	11 Mb/s
konvolúciós kód sebessége	11 Mb/s	22 Mb/s
moduláció	BPSK	QPSK
jelzési sebesség	11 Mbaud	

	S = 0	S = 1
BPSK		
QPSK		

High-Rate DSSS PHY

- legrosszabb vevő érzékenység:
  - -76 dBm @ 11 Mb/s
- maximális keret hibaarány:
  - 0.08 @ 11 Mb/s, 1024 byte-os keretekre
- PMD rétegben mért statisztikai paraméterek:
  - RSSI – Received Signal Strength Indication
  - SQ – Signal Quality
    - PLCP preamble és header alatt vett jel és a Barker seqence közötti korreláció
- channel agility
  - opcionális frequency hopping a 22 MHz-es csatornák közt
  - lehetővé teszi az interoperabilitást az IEEE 802.11 FHSS PHY-vel

Agenda

Fizikai réteg

IR PHY

Rádióhullámok

Antennák, deciBelek

FHSS PHY

DSSS PHY

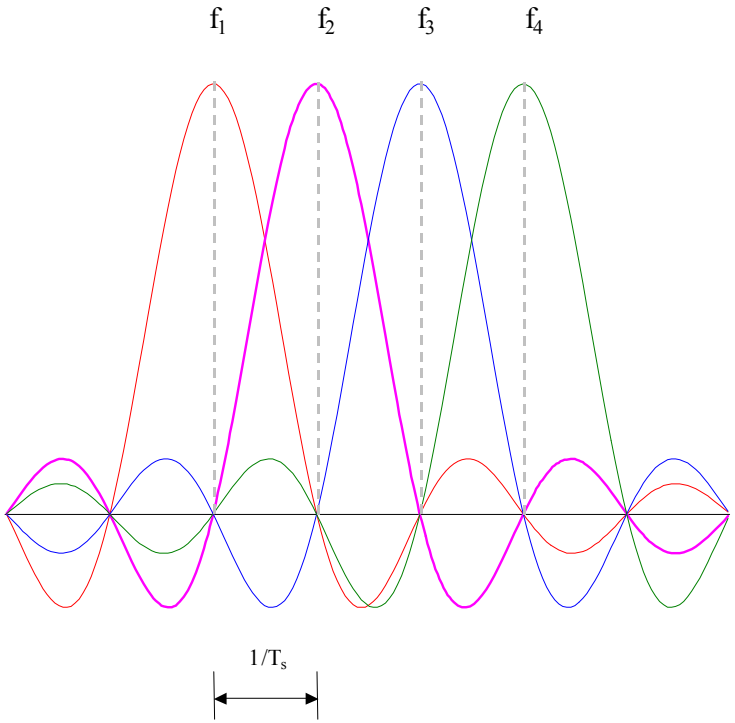
High-Rate DSSS PHY

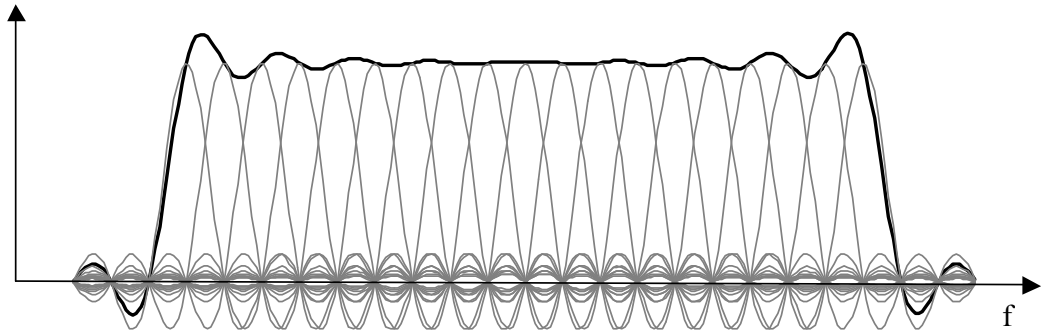
OFDM PHY

802.11g

OFDM

- OFDM – Orthogonal Frequency Division Multiplexing
  - egy csatornában több alcsatorna ortogonális subcarrier frekvenciákkal
  - az ortogonalitás miatt minden subcarrier frekvenciánál nullátmenete van az összes többi alcsatorna spektrumának
  - olyan FDM ez, ahol nagyon közel tehetők egymáshoz az alcsatornák



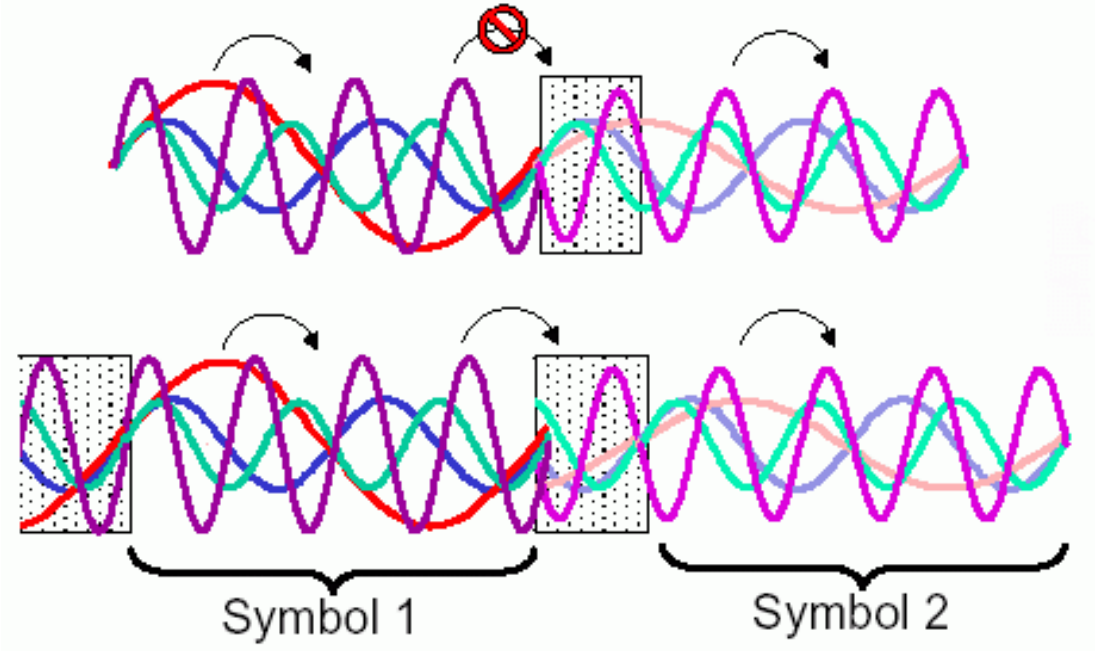


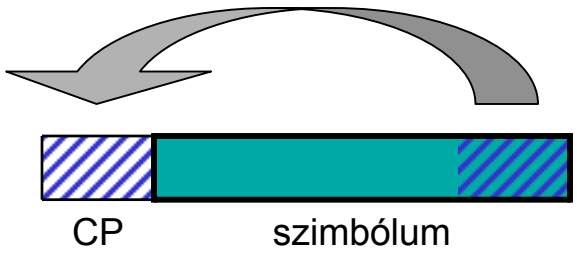
OFDM (folyt.)

- a subcarrierek modulált jeleinek összege megy adásba
  - a moduláció memóriában, számításokkal kezelhető könnyen
  - az összegzés IFFT-vel (Inverse Fast Fourier Transformation) történik
  - a kapott időtartománybeli jelet továbbítja az adó
  - a vevő FFT-vel bontja modulált subcarrierekre a vett jelet
- szimbólum: két „jelszintváltás” közti szakasz
  - ezalatt periodikus jel van a csatornán
    - mert minden alcsatornán egy-egy modulált sinus van
- jól viseli a többutas terjedést
  - sok alcsatorna miatt kisebb jelzési sebesség szükséges
    - hosszabb szimbólumok
  - a többutas terjedésből adódó visszhang hossza (delay spread) kicsi lesz a megnövekedett szimbólumhosszhoz képest
  - a subcarrierek frekvenciája ortogonális marad

Guard interval

- a szimbólumidő közepén nem gond a visszhang
- szimbólumhatáron probléma, amikor a késleltetett jel a következő szimbólumot torzítja
  - rövid „szünet” a szimbólumok közt, hogy a többutas terjedés miatt később érkező jelek lecsenghessenek
  - nem csend, hanem a következő szimbólum kiegészítve ciklikus prefixszel



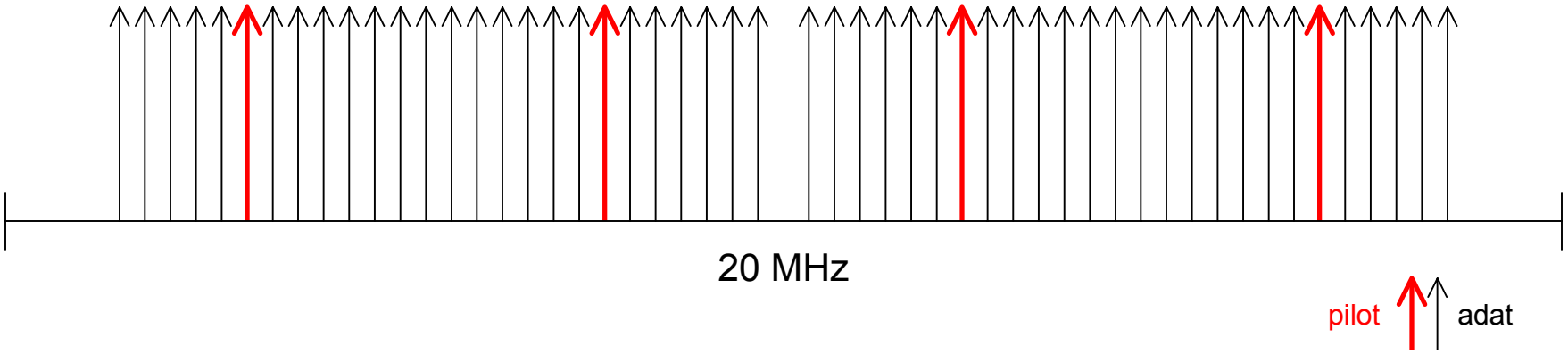


OFDM csatornák

- 20 MHz széles csatornák
  - nem fedik át egymást
    - de -20 dB a csatornán kívüli oldalfrekvenciák maximuma, ami okozhat problémát szomszédos csatornák közt
- USA
  - U-NII 1 és 2: 5.15-5.35 GHz, 8 csatorna 20 MHz-enként a közepén
  - U-NII 3: 5.725-5.825 GHz, 4 csatorna 20 MHz-enként a közepén
- Japán, Tajvan, Szingapúr
  - 4-4 csatorna
- Európa
  - jelenleg nem használható
  - 802.11h: ezekkel a kiegészítésekkel használható lesz Európában is
    - Transmit Power Control
    - Dynamic Frequency Selection

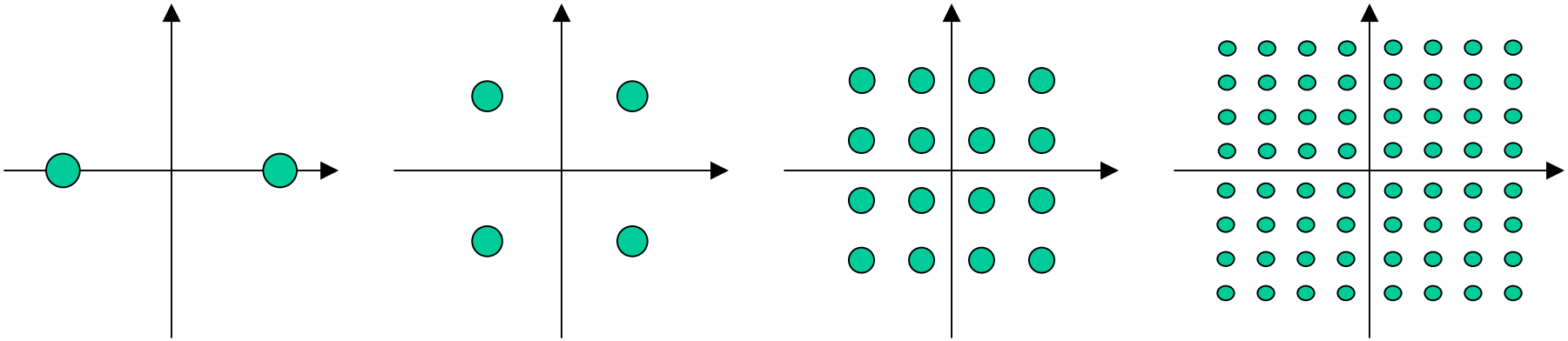
OFDM alcsatornák

- egy 20 MHz széles csatornában 52 alcsatorna
  - 48 alcsatornán adatok
  - 4 alcsatornán pilot jel
  - 0.3125 MHz (20 MHz / 64) távolság a subcarrier frekvenciák közt
  - a csatorna középfrekvenciája ki van hagyva a subcarrierek közül
    - az egyszerűbb implementáció érdekében



OFDM PHY moduláció

- BPSK – Binary Phase Shift Keying
- QPSK – Quadrature Phase Shift Keying
- 16-QAM – Quadrature Amplitude Modulation
- 64-QAM



Interleaving

- két lépcsős interleaving (kódátfűzés)
- 1. alcsatornák között
  - három alcsatornánként szórja szét a szomszédos biteket
  - több alcsatornára kiterjedő spektrumú zavarok ellen is véd
- 2. konstelláció helyiértékei között
  - csak QAM modulációnál érdekes
    - [MSB_{Horiz} … LSB_{Horiz} MSB_{Vert} … LSB_{Vert}] adatbitek adják meg a konstellációs pont helyét
    - LSB különbözik: közel van egymáshoz a konstelláció két pontja
    - MSB különbözik: messze van egymástól a konstelláció két pontja
  - szomszédos bitek ne kerüljenek sorozatban LSB helyre
    - mivel az LSB könnyen sérül
  - ezt az alcsatornák közti interleaving teszi szükségessé
    - az teszi a szomszédos biteket sorozatban LSB helyre

OFDM PHY sebességek

- 48 alcsatorna
- 1/2, 2/3 vagy 3/4 sebességű konvolúciós kódoló
  - 1/2 sebességű, kiszúrással
  - hatékony dekódolás: soft-decision Viterbi
- 250 Mbaud jelzési sebesség
  - 4 μs szimbólumhossz (ebből 0.8 μs a guard interval)

moduláció	kódolt bitek alcsatornánként	kódolt bitek szimbólumonként	kódoló sebessége	adatbitek szimbólumonként	adatsebesség [Mb/s]
BPSK	1	48	1/2	24	6
BPSK	1	48	3/4	36	9
QPSK	2	96	1/2	48	12
QPSK	2	96	3/4	72	18
16-QAM	4	192	1/2	96	24
16-QAM	4	192	3/4	144	36
64-QAM	6	288	2/3	192	48
64-QAM	6	288	3/4	216	54

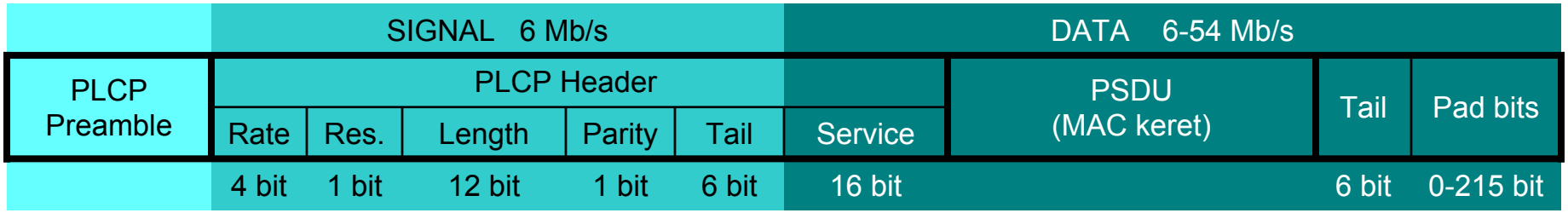
PLCP keret – Preamble

- 16 µs:
  - 10 rövid (0.8 µs) training szimbólum 12 subcarrieren
  - 1.6 µs guard interval
  - 2 hosszú (3.2 µs) training szimbólum 52 subcarrieren
- funkciói:
  - vivőérzékelés
  - AGC (Automatic Gain Control) erősítő beállás
    - mint egy automatikus felvételi szint szabályzós magnó
  - diversity esetén antennaválasztás
  - frekvencia beállítás
  - idő szinkronizálás

	SIGNAL 6 Mb/s					DATA 6-54 Mb/s			
PLCP Preamble	PLCP Header						PSDU (MAC keret)	Tail	Pad bits
	Rate	Res.	Length	Parity	Tail	Service			
	4 bit	1 bit	12 bit	1 bit	6 bit	16 bit		6 bit	0-215 bit

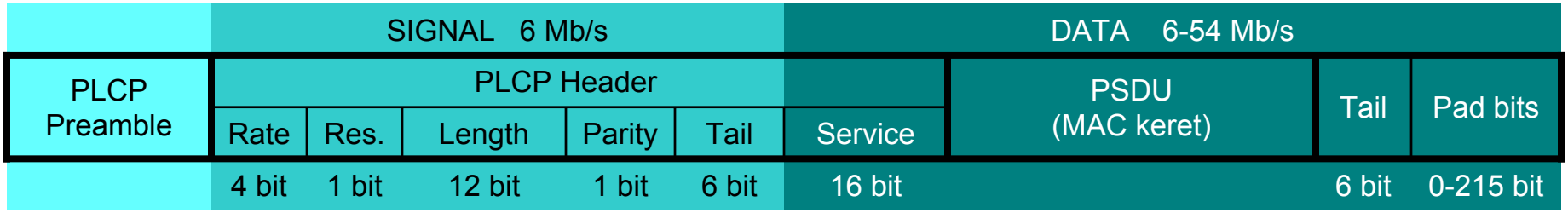
PLCP keret – SIGNAL

- a header első 24 bitje
  - 6 Mb/s sebesség (BPSK, 1/2), 4 µs, 1 szimbólum
- Rate: DATA sebessége
- Res.: reserved
- Length: PSDU mérete byte-ban
- Parity: az előző három mezőhöz páros paritás
- Tail: 000000
  - hogy meglegyen a szimbólum



PLCP keret – DATA

- a szokásos 127 bites scrambler kimenetével XOR-olva
- Service:
  - 7 „0” bit a scrambler szinkronizálásához a vételkor
  - 9 reserved bit
- Tail: 000000 a konvolúciós kódoló alapállapotba vezetéséhez
  - scrambling után újra visszaírva 000000-ra
- Pad bits:kiegészítés egész szimbólumokra



OFDM PHY adás

- Preamble
  - speciális módon
- SIGNAL
  - mindig BPSK, 1/2, 6 Mb/s
  - csak 3-9.
- DATA
  1. padding
  2. scrambling, Tail visszaírása 000000-ra
  3. 1/2 sebességű konvolúciós kódolás, szükség esetén (2/3, 3/4) kiszúrás
  4. interleaving
  5. adat subcarrierek modulációja (BPSK, QPSK, 16-QAM, 64-QAM)
  6. pilot subcarrierek hozzáadása (BPSK)
  7. IFFT
  8. guard interval (ciklikus prefix) hozzáillesztése
  9. D/A konverzió, felkeverés a megfelelő csatornába, adás

OFDM PHY

- antenna impedancia: 50 Ω
- legrosszabb vevő érzékenység:
  - -82 dBm @ 6 Mb/s
  - …
  - -65 dBm @ 54 Mb/s
- maximális keret hibaarány:
  - 0.1, 1000 byte-os keretekre
- PMD rétegben mért statisztikai paraméterek:
  - RSSI – Received Signal Strength Indication

Agenda

Fizikai réteg

IR PHY

Rádióhullámok

Antennák, deciBelek

FHSS PHY

DSSS PHY

High-Rate DSSS PHY

OFDM PHY

802.11g

IEEE 802.11g

- 54 Mb/s a 2.4 GHz ISM sávban
- felülről kompatibilis a 802.11b-vel
- kötelező az OFDM és a 802.11b DSSS-CCK
  - opcionális a CCK-OFDM és a nagysebességű PBCC
- a szabvány várhatóan megjelenik 2003-ban
  - a draft alapján készült termékek már kaphatók

Agenda

Bevezető

Fizikai réteg

Közeghozzáférés

Biztonság

Egyéb

Agenda

Közeghozzáférés

Alapok

Distributed Coordination Function

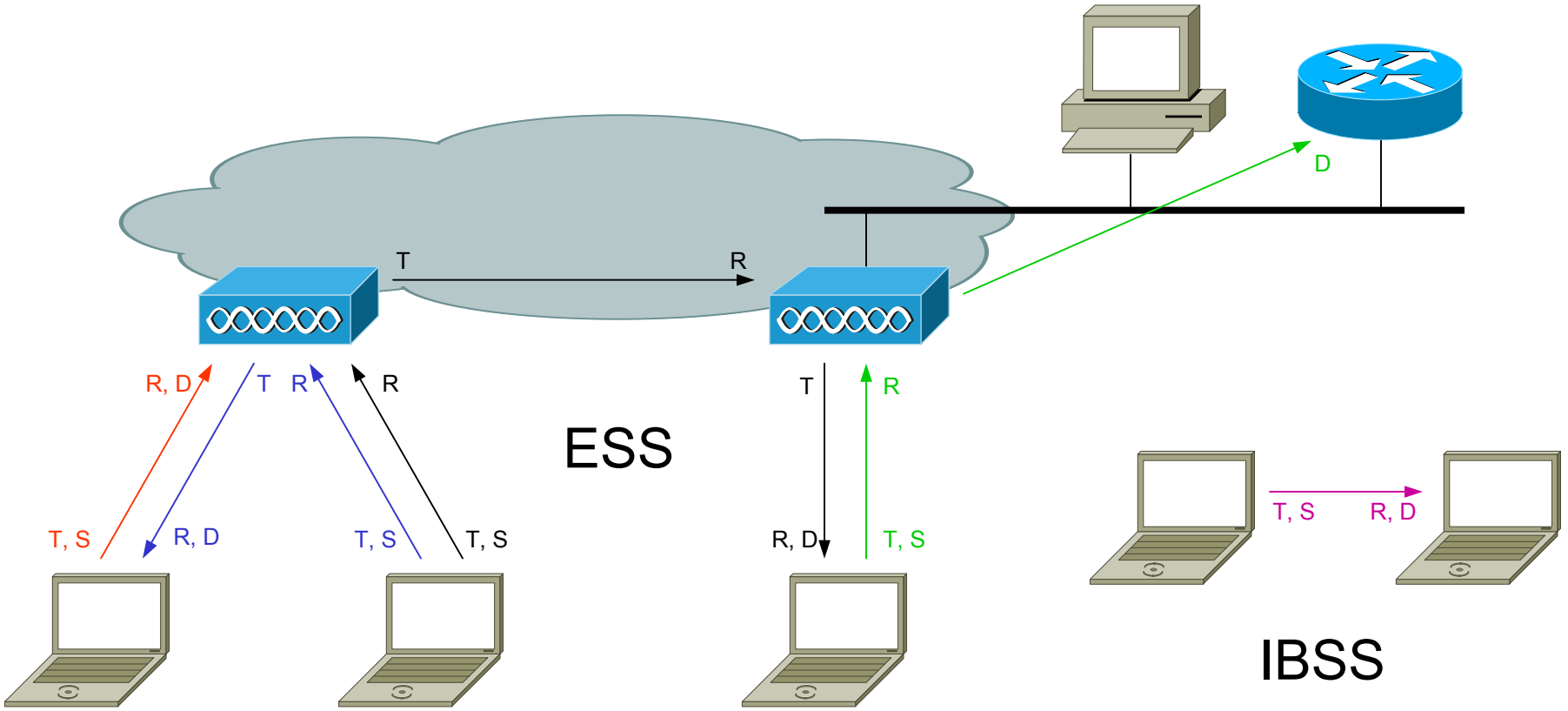
Menedzsment funkciók

Point Coordination Function

Keretformátumok

Adó, vevő, forrás, cél

- Transmitter (adó), Receiver (vevő)
- Source (forrás), Destination (cél)



Címzés

- minden állomásnak 48 bites IEEE 802 címe van
- BSSID – Basic Service Set IDentifier
  - a BSS-t azonosítja
  - 48 bit
  - infrastruktúra módban az AP wireless MAC címe
  - ad-hoc módban az IBSS-t indító állomás generálja véletlenszerűen
  - 0xFFFFFFFFFFFF a broadcast BSSID érték
    - Probe Request keretekben használatos
- SSID – Service Set Identifier
  - ESS-t vagy IBSS-t azonosít
  - max. 32 byte
  - access point konfigurációs paramétere
  - kliens állomás vagy megtanulja vagy konfigurálva van rajta
  - az üres (0 hosszúságú) SSID a broadcast SSID

MAC keretformátum

- Frame Control: keret típus és jelzőbitek
- Duration/AID: lásd később
- Addr 1-4:
  - 1: Receiver Address (vevő)
  - 2: Transmitter Address (adó)
  - 3-4: Source Address (forrás), Destination Address (cél), vagy BSSID
- Sequence Control: sorszám a duplikáció detektálásához
- FCS: 32 bites CRC
- Addr 2-4, Seqence Control és Payload nincs minden típusú keretben

MAC Header							Payload	FCS
Frame Control	Duration / AID	Addr 1 (RA)	Addr 2 (TA)	Addr 3	Seq Control	Addr 4		
2	2	6	6	6	2	6	0-2312	4

Keret típusok

- kontroll
  - a közeghozzáférési protokoll működéséhez szükségesek
- menedzsment
  - a BSS működéséhez szükségesek
- adat
  - felsőbb rétegek adatainak továbbítására
- az adat és menedzsment keretek viselkedése, kezelése a közeghozzáférésnél nagyon hasonló

DCF, PCF

- két közeghozzáférés működési mód
- DCF – Distributed Coordination Function
  - CSMA/CA
    - a közeghez való hozzáférés elosztott vezérlése
- PCF – Point Coordination Function
  - polling
    - a közeghez való hozzáférést az access point vezérli
  - csak infrastruktúra módban használható
- tipikusan csak DCF
  - vagy DCF és PCF váltakozik periodikusan

Agenda

Közeghozzáférés

Alapok

Distributed Coordination Function

Menedzsment funkciók

Point Coordination Function

Keretformátumok

CSMA/CA

- Carrier Sense Multiple Access with Collision Avoidance
  - közeghozzáférési protokoll a BSS-ben
  - hasonlít a CSMA/CD-re (Ethernet)
  - Collision Detection nem lehetséges WLAN-on
    - nem biztos, hogy minden állomás mindenkit hall
    - nem lehet egyszerre adni és venni
- CSMA/CA
  - több állomás használ egy kommunikációs csatornát
  - csak akkor sikeres az átvitel, ha egyszerre csak egy állomás beszél
- CSMA/CA
  - adás előtt az állomás belehallgat a csatornába
  - ha valaki éppen ad, akkor kivárja a keret végét, különben egyből ad
- CSMA/CA
  - amikor csend lesz, véletlen késleltetés után kezd adni
    - (a CSMA/CD egyből adni kezdene a megüresedett csatornán)

Collision Avoidance

- minden keret vége után versenyezni kell a médiumért
  - diszkrét egyenletes eloszlású véletlen várakozás
    - SlotTime valahányszorosa (vö. réselt Aloha protokoll)
  - exponential backoff – a várható értéke exponenciálisan növekszik
    - felső korlát
- aki a legkisebb véletlent generálta, az ad
  - a többiek megvárják a keret végét, majd újra versenyeznek
    - megnövelt várható értékű véletlenekkel
  - ha többen generáltak azonos értéket, ami nyer, akkor ütközés van
- saját keret adása után is versenyezni kell
  - akkor is el kell indítani a véletlen késleltetést, ha nincs következő adásra váró kerete az állomásnak, mert lehet, hogy hamarosan lesz
- egy keret átvitele alatt gyakran két verseny is van
  - küldő állomás → access point
  - access point → vevő(k)

CSMA/CA

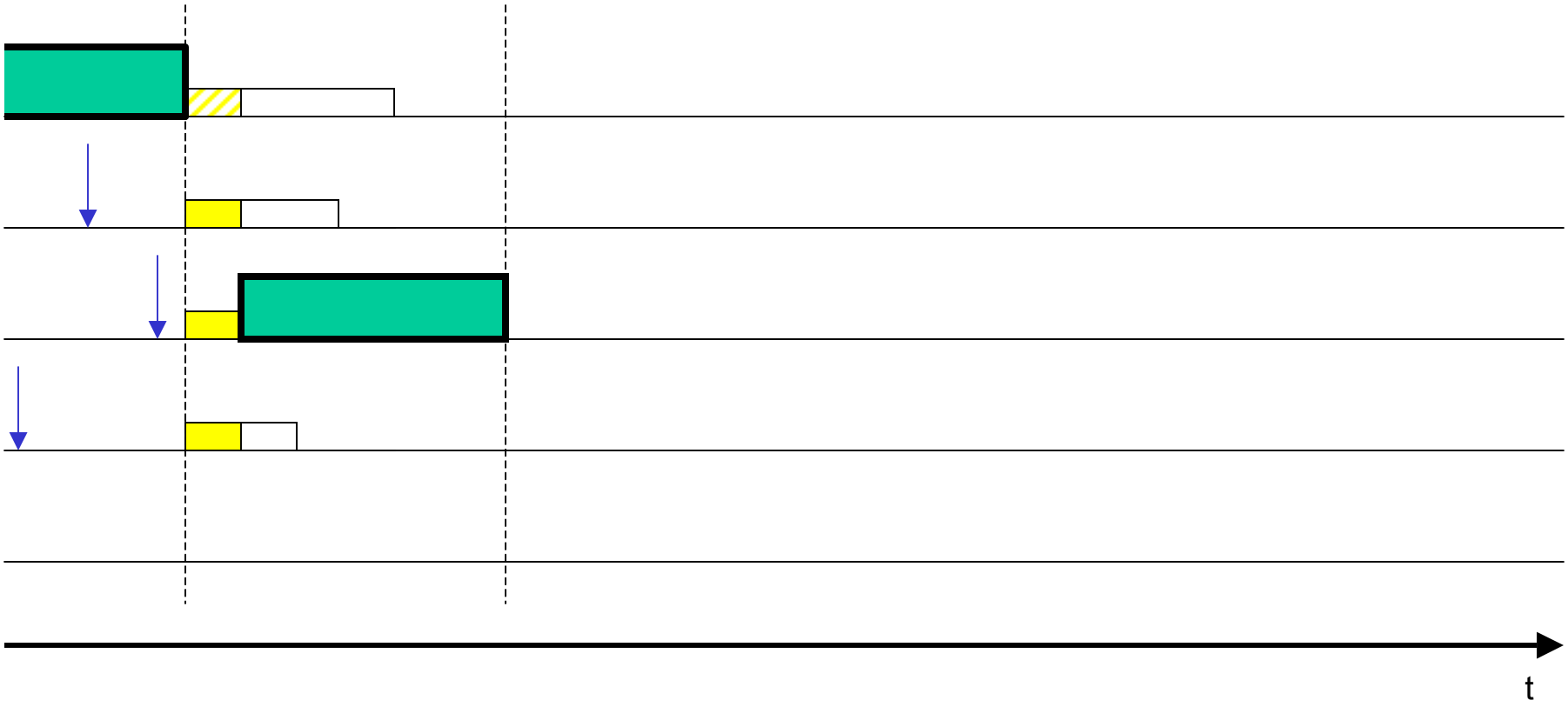
CSMA/CA

CSMA/CA

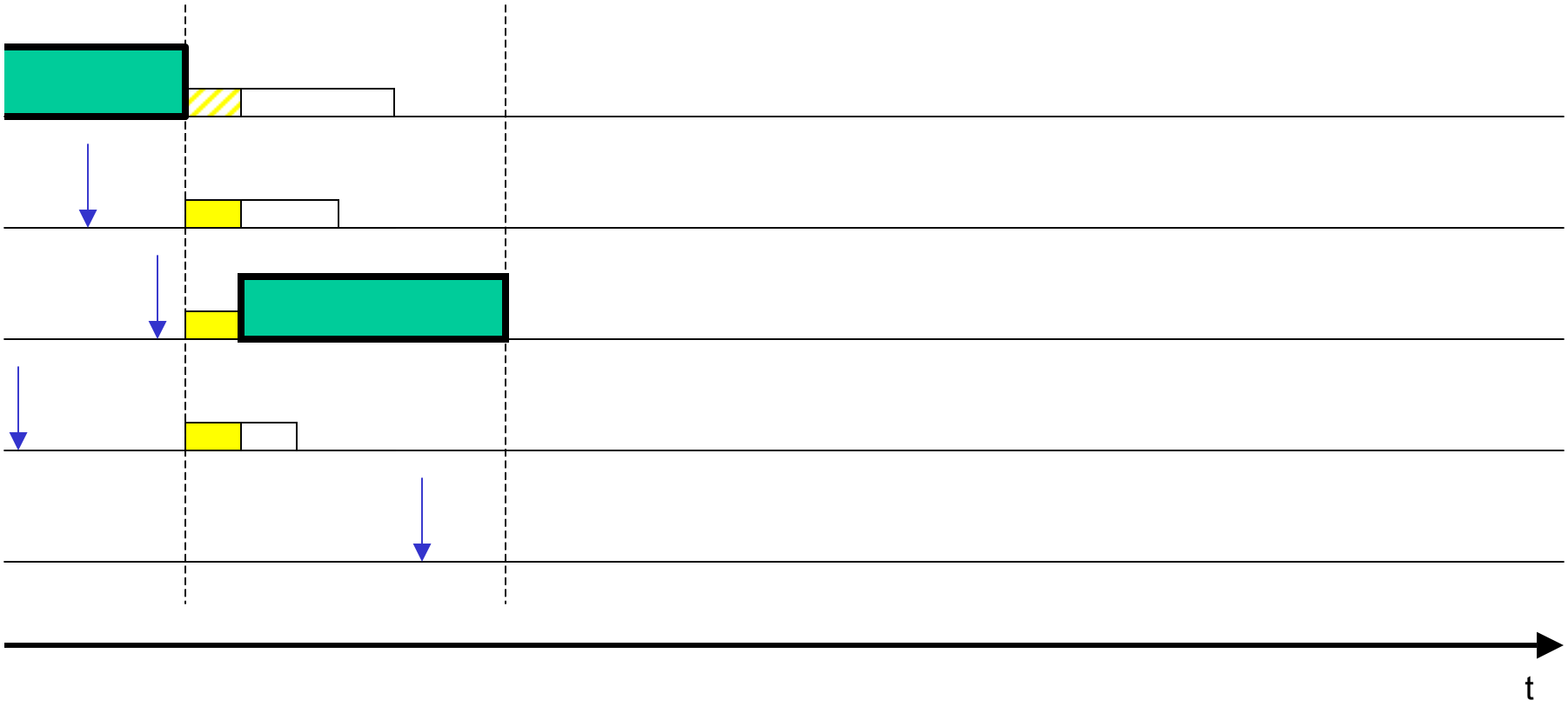
CSMA/CA

CSMA/CA

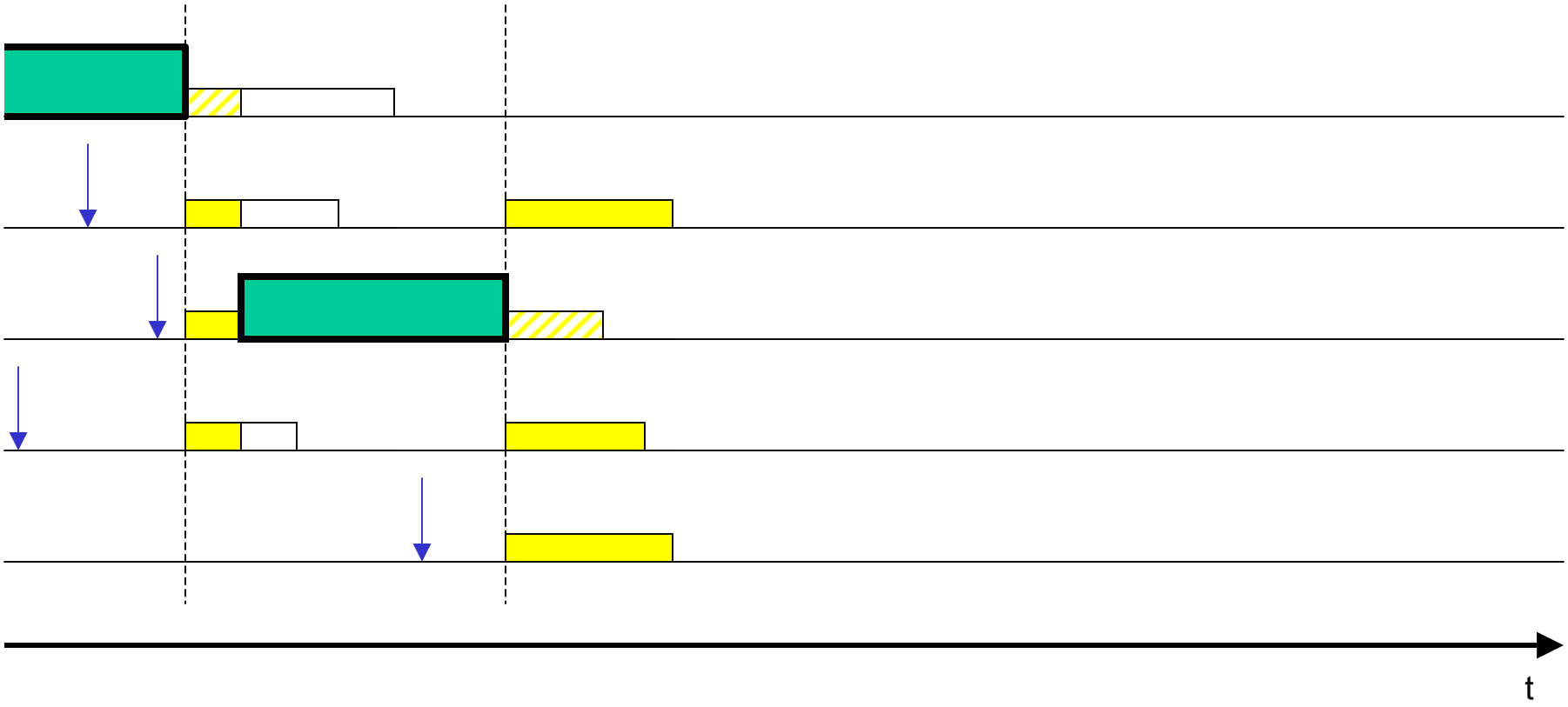
CSMA/CA



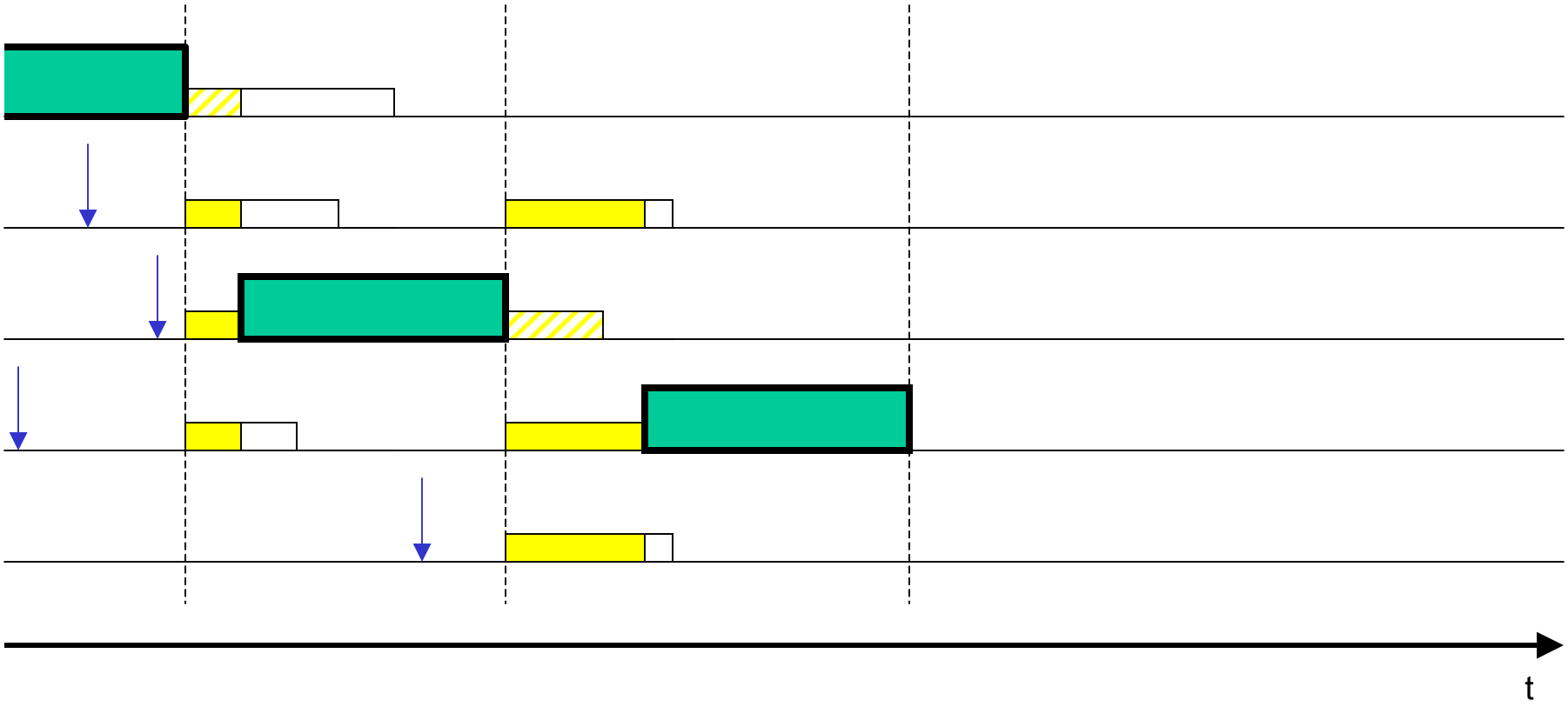
CSMA/CA



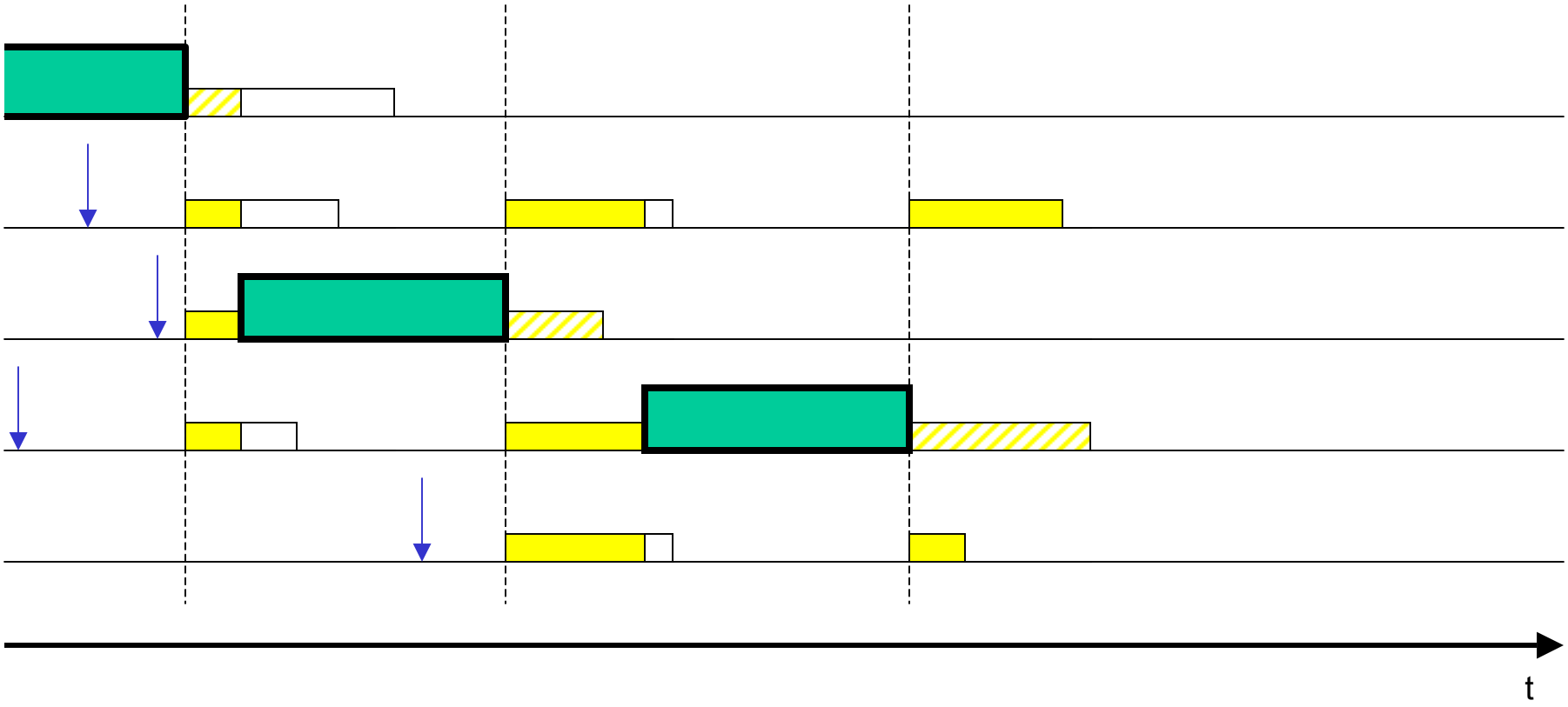
CSMA/CA



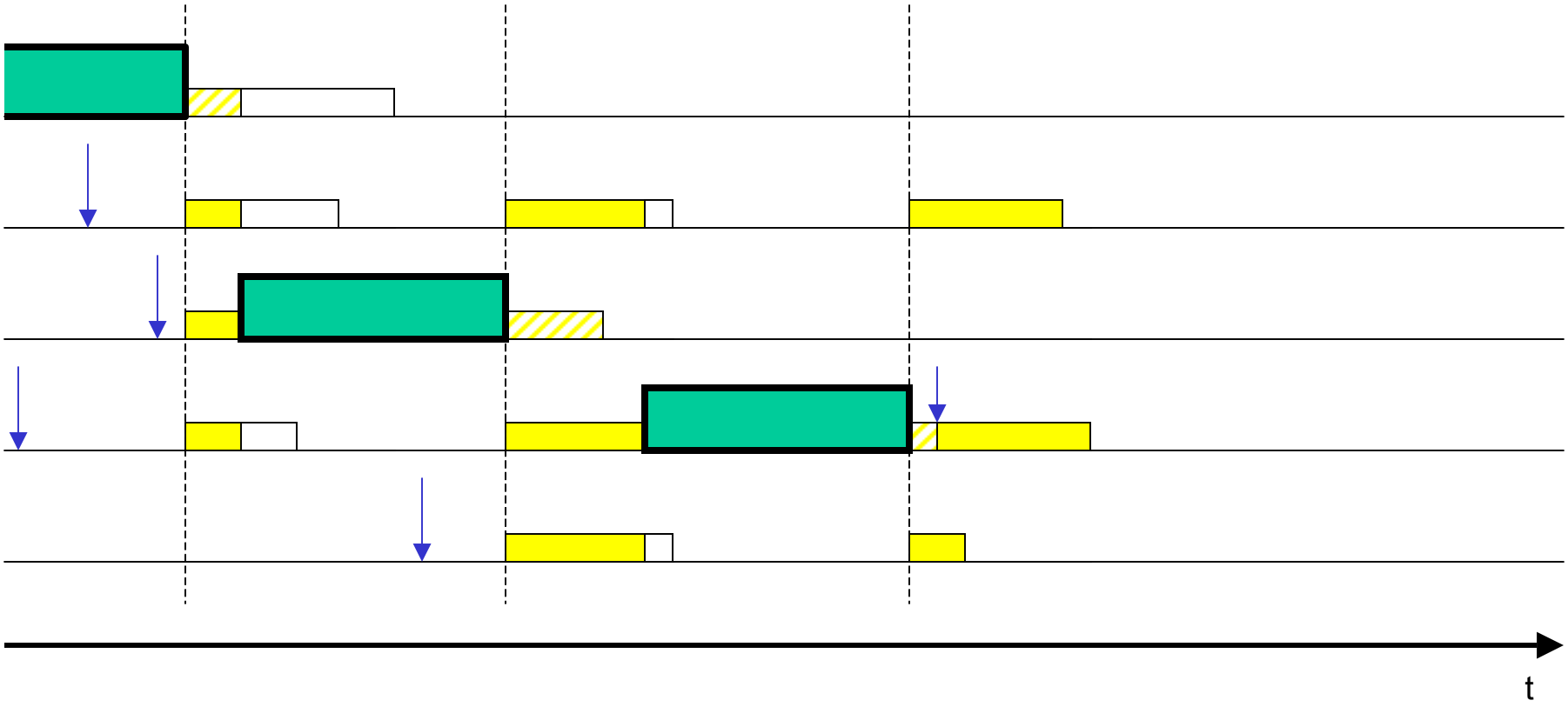
CSMA/CA



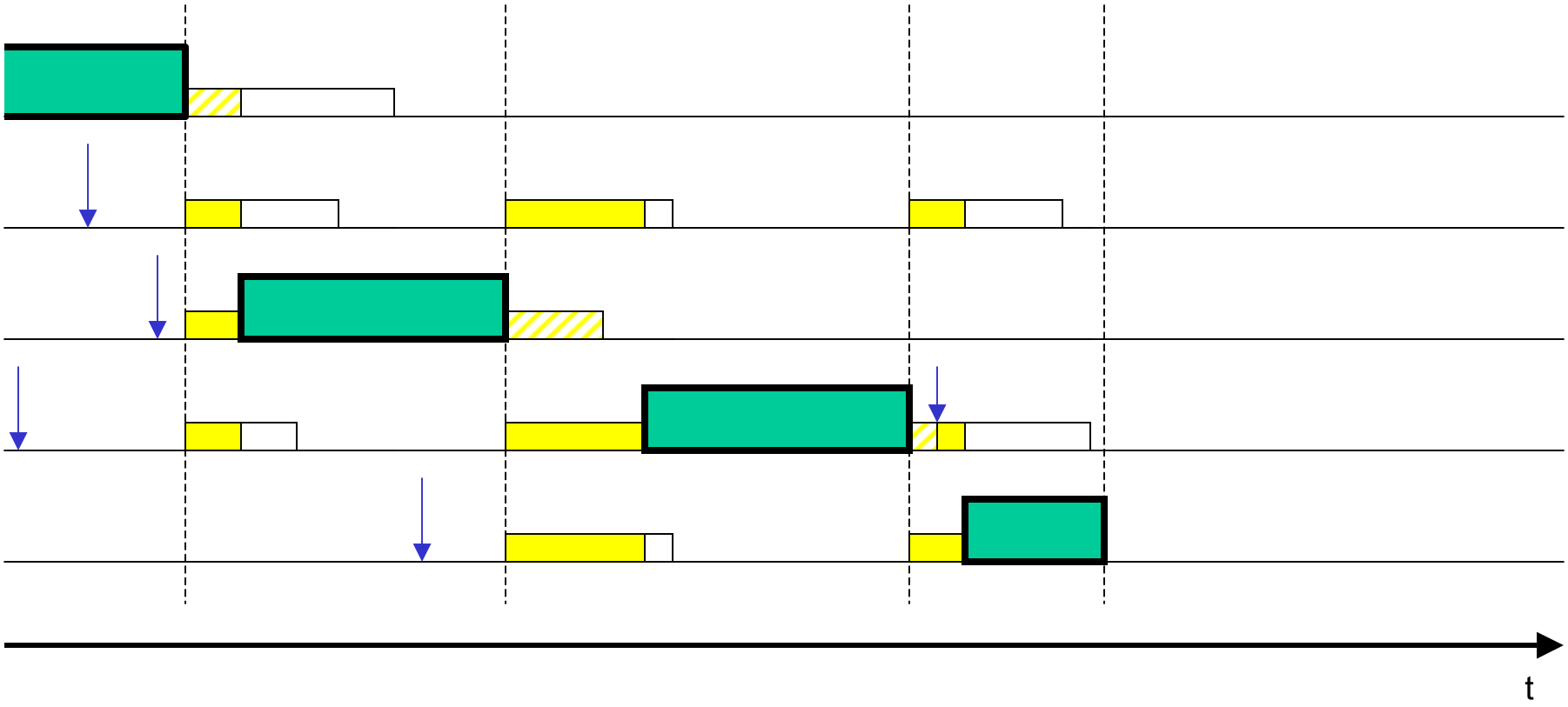
CSMA/CA



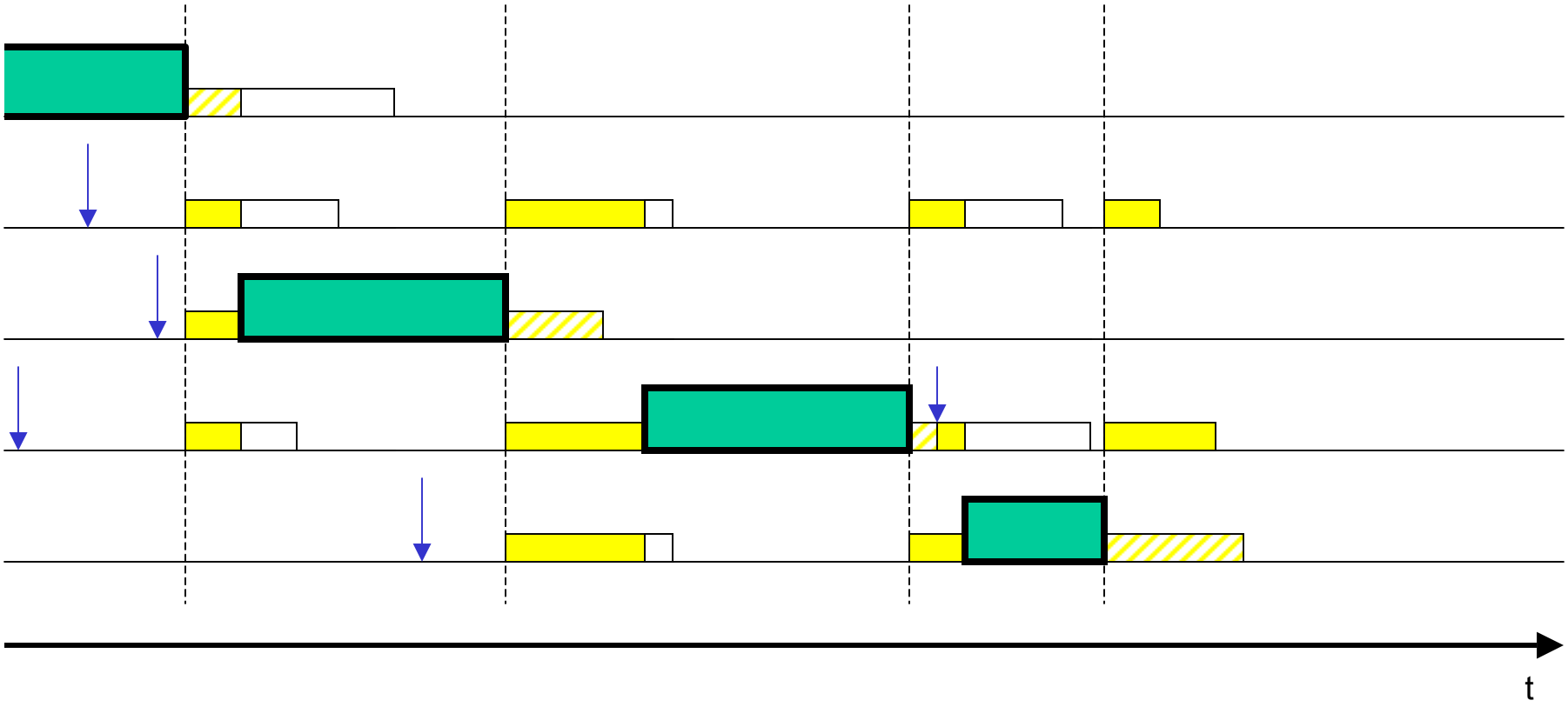
CSMA/CA



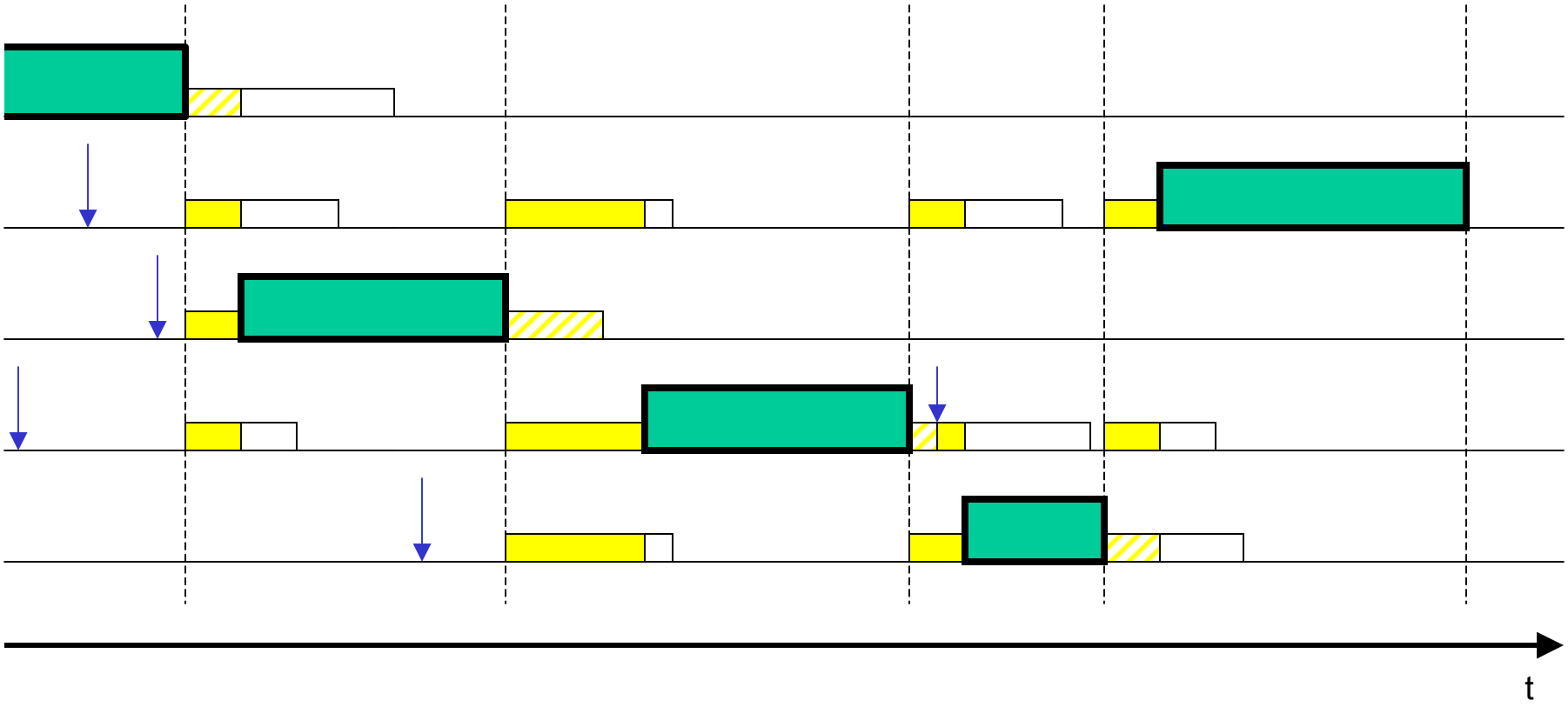
CSMA/CA



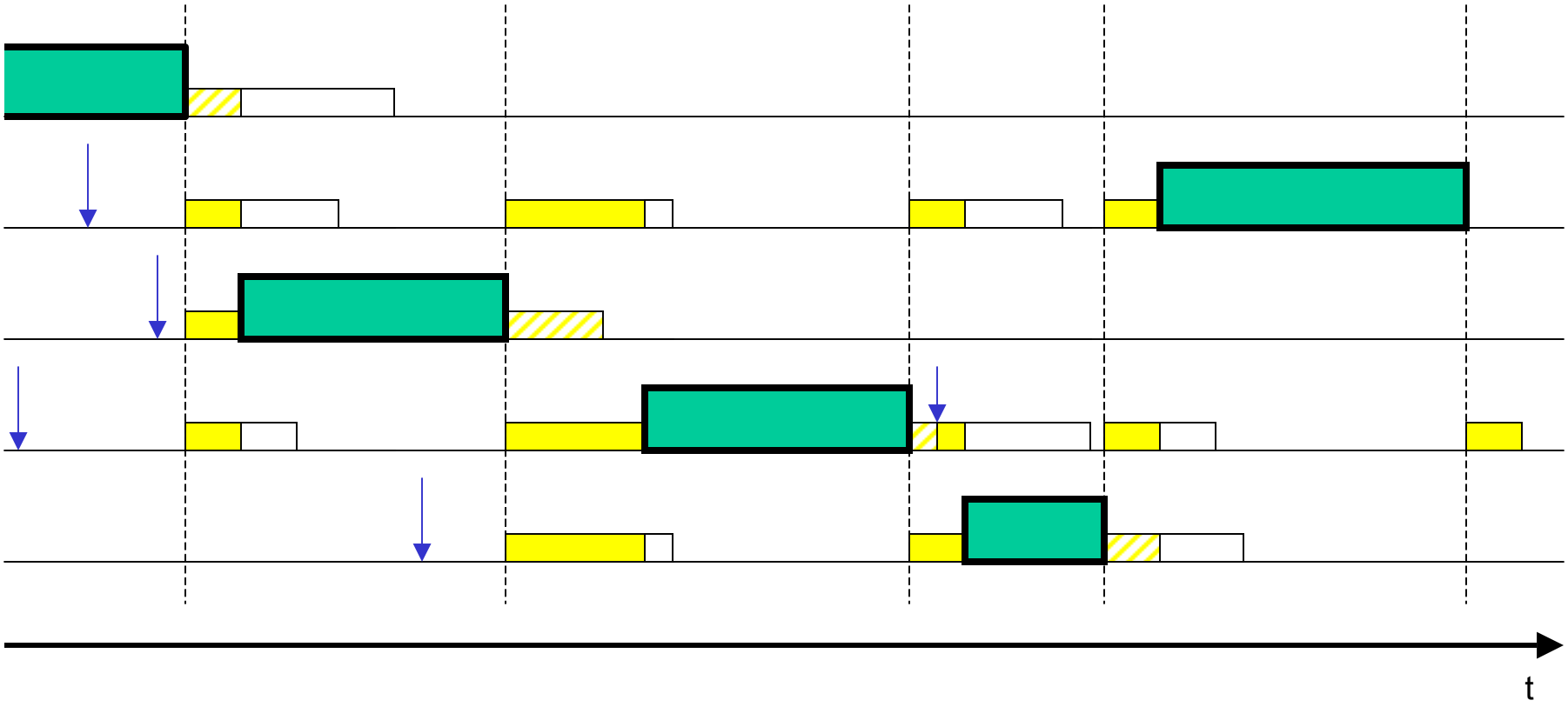
CSMA/CA



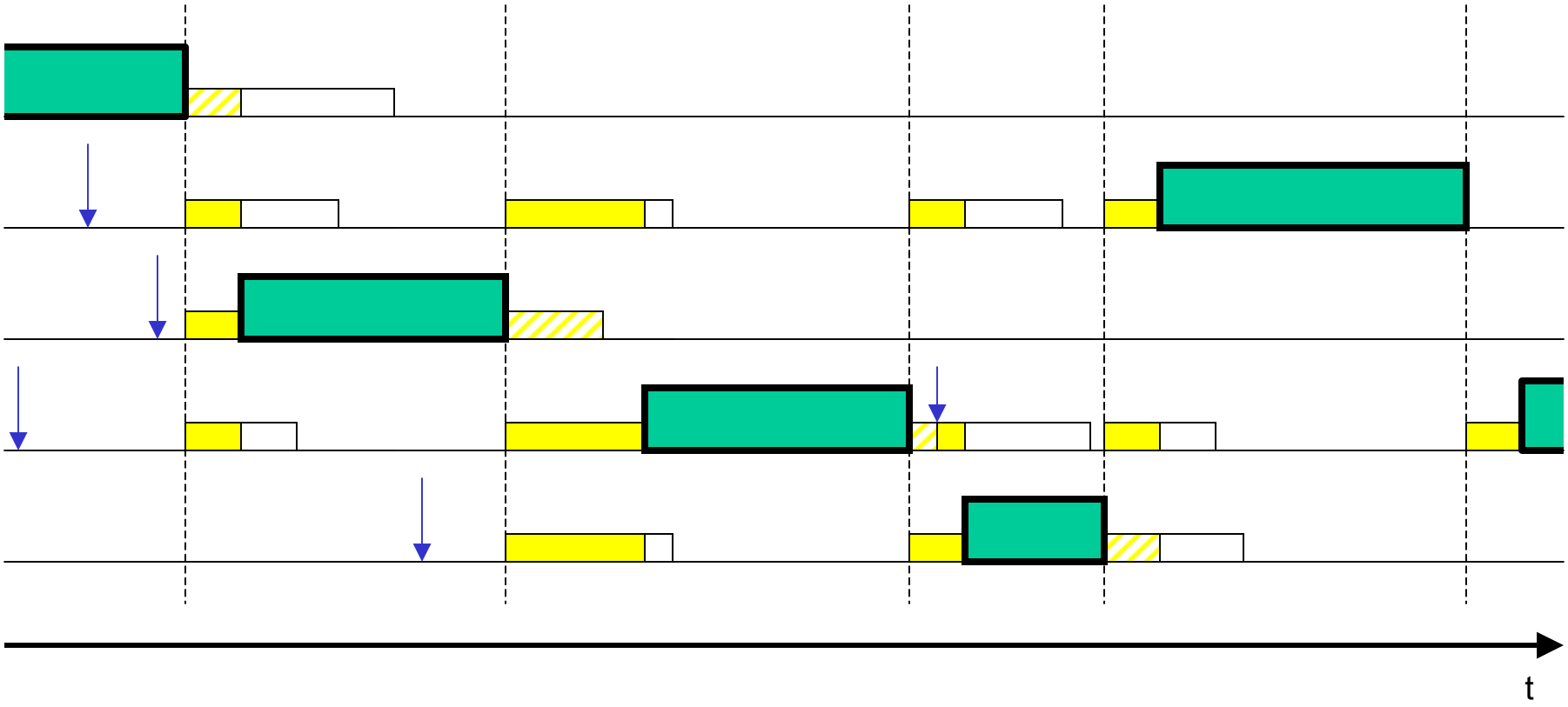
CSMA/CA



CSMA/CA

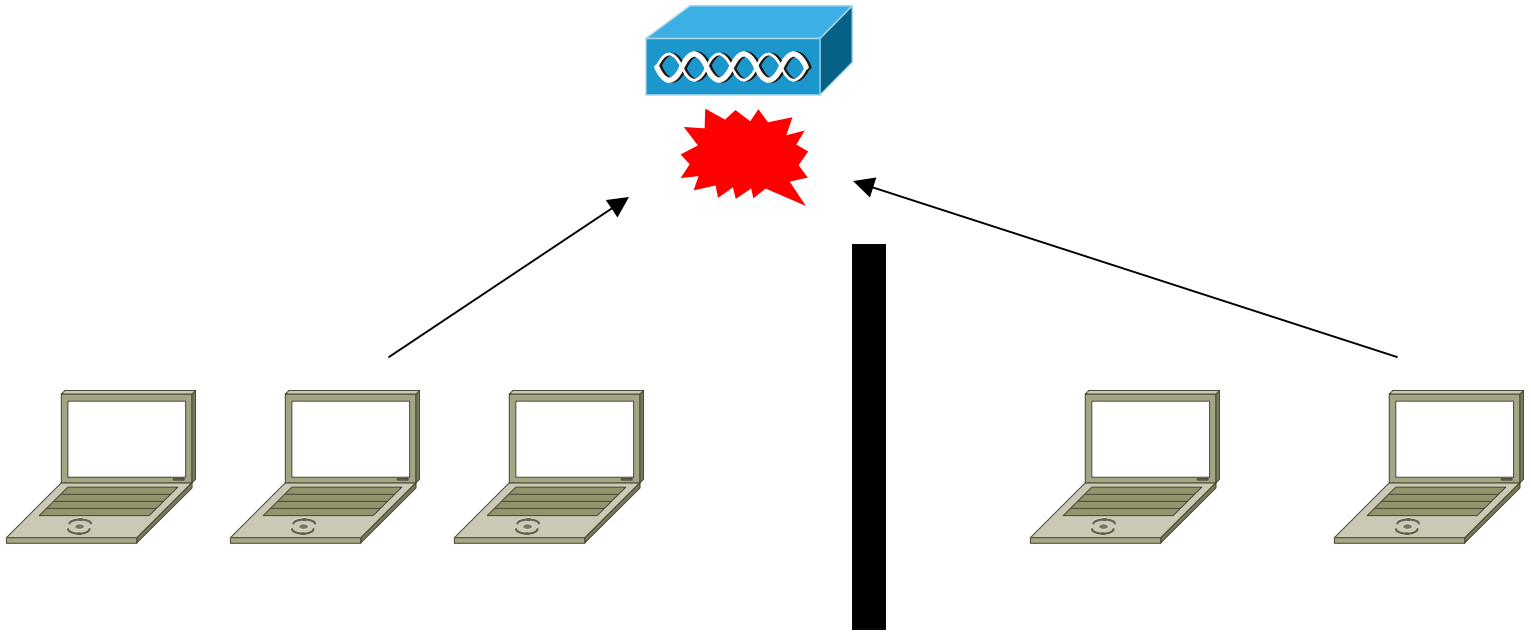


CSMA/CA



Rejtett állomások

- infrastruktúra módban nem biztos, hogy minden állomás mindenkit hall a BSS-ben
  - az access point mindenkit hall, őt is mindenki hallja
- nagyon könnyen adhat egyszerre két állomás
  - ha nem hallják egymást, és mindkettő csendesnek hiszi a csatornát

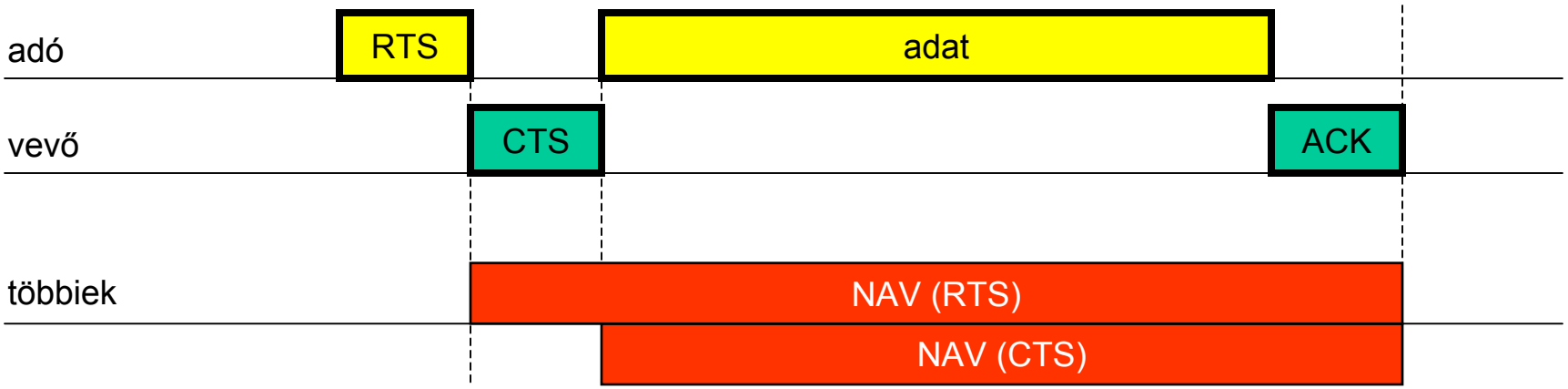


Carrier Sense

- a rejtett állomások miatt a fizikai vivőérzékelés nem elegendő
  - fizikai és virtuális vivőérzékelés szükséges
- fizikai vivőérzékelés: CCA – Clear Channel Assessment
  - a fizikai rétegben
  - rádiófrekvenciás vivőjel vétele
  - energia detektálás
- virtuális vivőérzékelés
  - a MAC alrétegben
  - RTS/CTS üzenetek segítségével

RTS/CTS

- Request To Send, Clear To Send
  - rövid kontrollüzenetek
- az adó az adatkeret előtt RTS-t küld, a vevő CTS-szel válaszol
  - mindenki biztosan hallja legalább az egyiket az RTS és a CTS közül
    - vagy az adó vagy a vevő az access point (infrastruktúra mód, DCF)
  - NAV – Network Allocation Vector
    - mindkét üzenetben szerepel a küldendő adatkeret hossza (Duration)
    - ez alapján minden állomás foglaltnak tekinti a csatornát a jelzett ideig



RTS/CTS (folyt.)

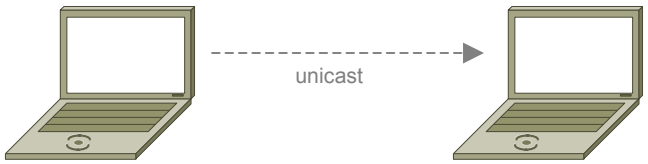
- ezek is ütközhetnek, de rövidek, ezért
  - kisebb az ütközés esélye
  - nem probléma az ütközés, hiszen csak rövid idő válik haszontalanná
- az RTS állomásonként konfigurálható
  - konfigurálható minimális adatkeret méret: RTS csak nagy keretek előtt
    - rövid kereteknél túl nagy lenne az RTS/CTS overhead
- kapott RTS-re CTS válasz mindig kötelező
- mellékhatásként a vevő elérhetőségét is ellenőrzi
  - hosszú adatkeret és el nem érhető vevő esetén nyereség

Pozitív nyugtázás

- a sikeres vételről az adó semmit sem tud
  - még az ütközést sem tudja detektálni
- az irányított adat- vagy menedszment keret sikeres vételét ACK keret küldésével nyugtázza a vevő állomás
- irányított keret (directed frame)
  - unicast
  - broadcast és multicast, ami az access pointnak megy

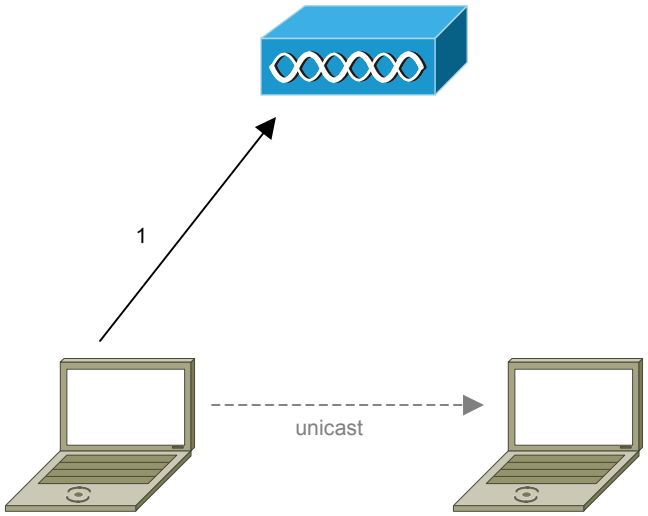
Pozitív nyugtázás

- a sikeres vételről az adó semmit sem tud
  - még az ütközést sem tudja detektálni
- az irányított adat- vagy menedszment keret sikeres vételét ACK keret küldésével nyugtázza a vevő állomás
- irányított keret (directed frame)
  - unicast
  - broadcast és multicast, ami az access pointnak megy



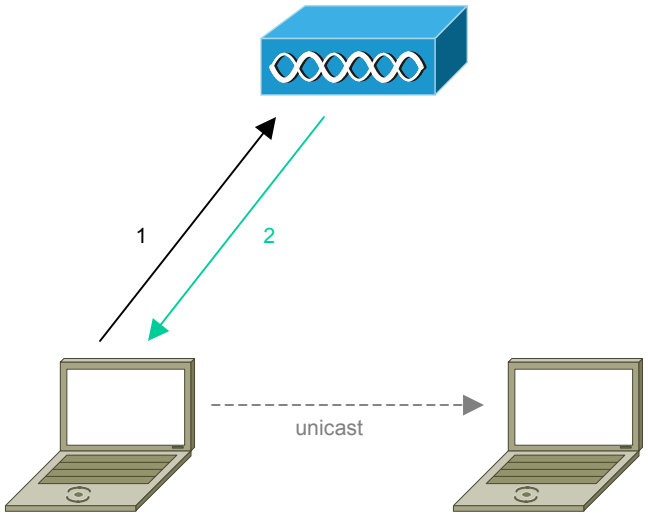
Pozitív nyugtázás

- a sikeres vételről az adó semmit sem tud
  - még az ütközést sem tudja detektálni
- az irányított adat- vagy menedszment keret sikeres vételét ACK keret küldésével nyugtázza a vevő állomás
- irányított keret (directed frame)
  - unicast
  - broadcast és multicast, ami az access pointnak megy



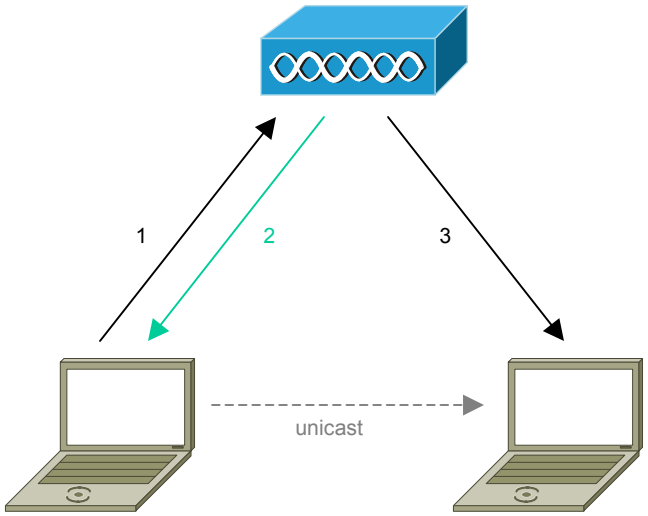
Pozitív nyugtázás

- a sikeres vételről az adó semmit sem tud
  - még az ütközést sem tudja detektálni
- az irányított adat- vagy menedszment keret sikeres vételét ACK keret küldésével nyugtázza a vevő állomás
- irányított keret (directed frame)
  - unicast
  - broadcast és multicast, ami az access pointnak megy



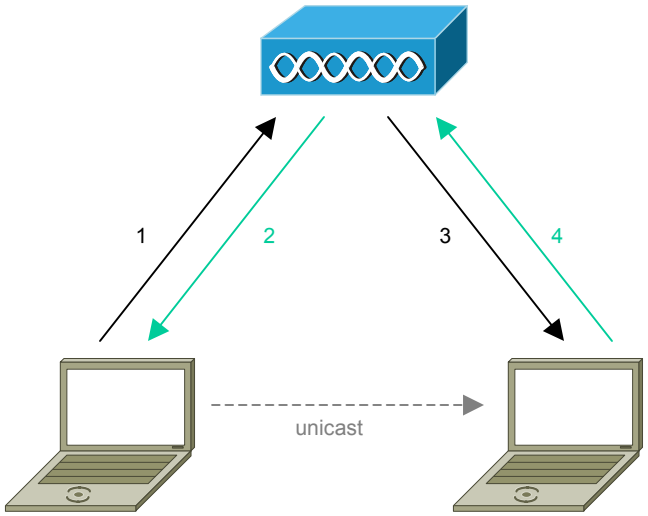
Pozitív nyugtázás

- a sikeres vételről az adó semmit sem tud
  - még az ütközést sem tudja detektálni
- az irányított adat- vagy menedszment keret sikeres vételét ACK keret küldésével nyugtázza a vevő állomás
- irányított keret (directed frame)
  - unicast
  - broadcast és multicast, ami az access pointnak megy



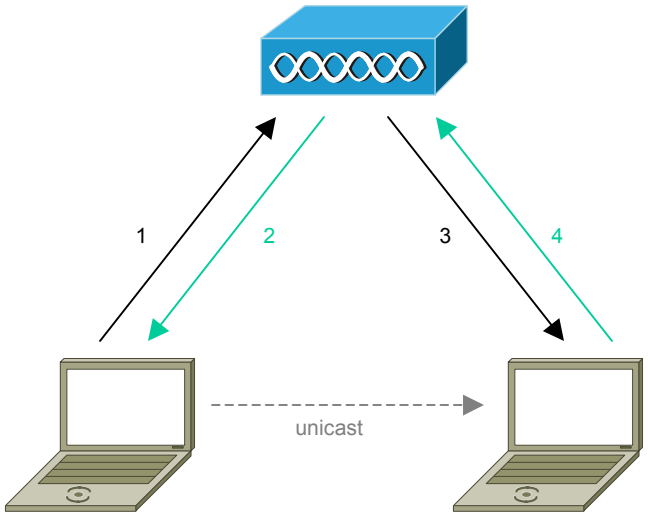
Pozitív nyugtázás

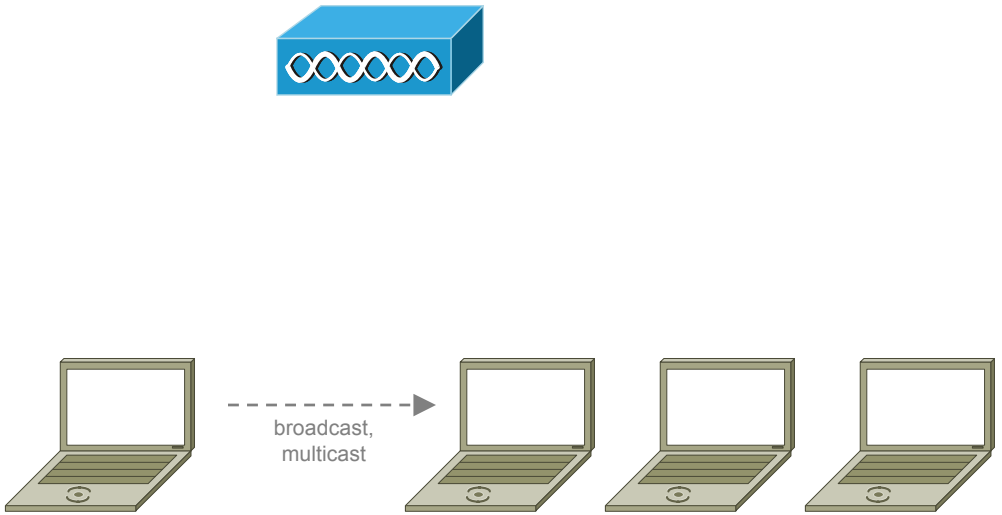
- a sikeres vételről az adó semmit sem tud
  - még az ütközést sem tudja detektálni
- az irányított adat- vagy menedszment keret sikeres vételét ACK keret küldésével nyugtázza a vevő állomás
- irányított keret (directed frame)
  - unicast
  - broadcast és multicast, ami az access pointnak megy



Pozitív nyugtázás

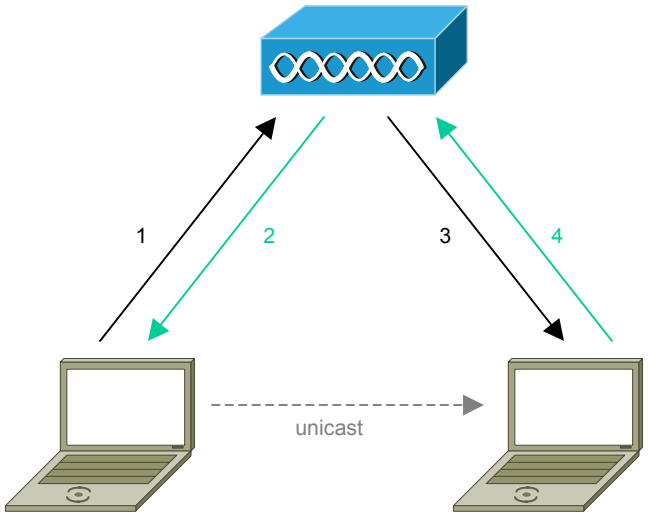
- a sikeres vételről az adó semmit sem tud
  - még az ütközést sem tudja detektálni
- az irányított adat- vagy menedszment keret sikeres vételét ACK keret küldésével nyugtázza a vevő állomás
- irányított keret (directed frame)
  - unicast
  - broadcast és multicast, ami az access pointnak megy

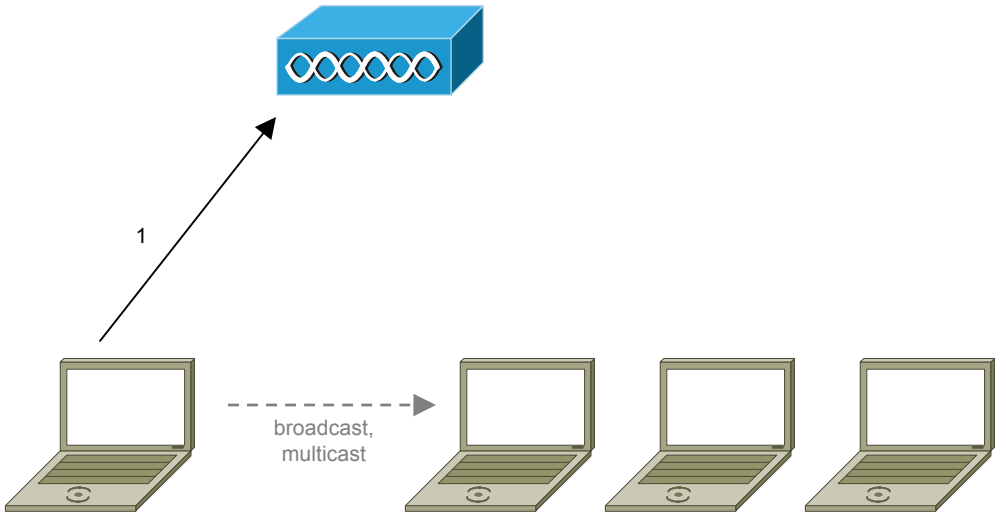




Pozitív nyugtázás

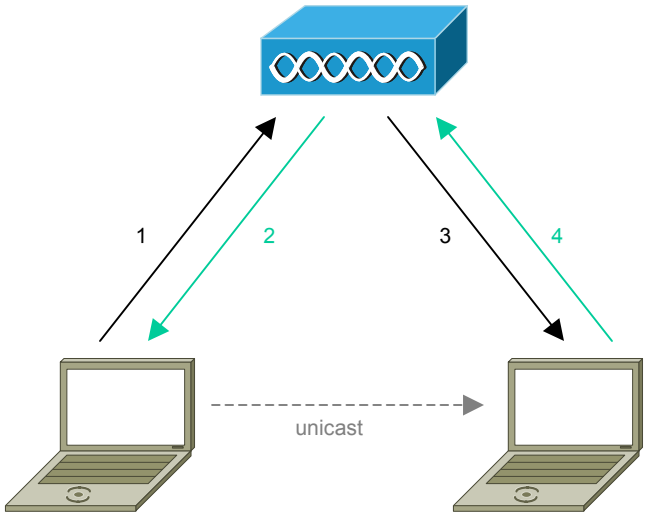
- a sikeres vételről az adó semmit sem tud
  - még az ütközést sem tudja detektálni
- az irányított adat- vagy menedszment keret sikeres vételét ACK keret küldésével nyugtázza a vevő állomás
- irányított keret (directed frame)
  - unicast
  - broadcast és multicast, ami az access pointnak megy

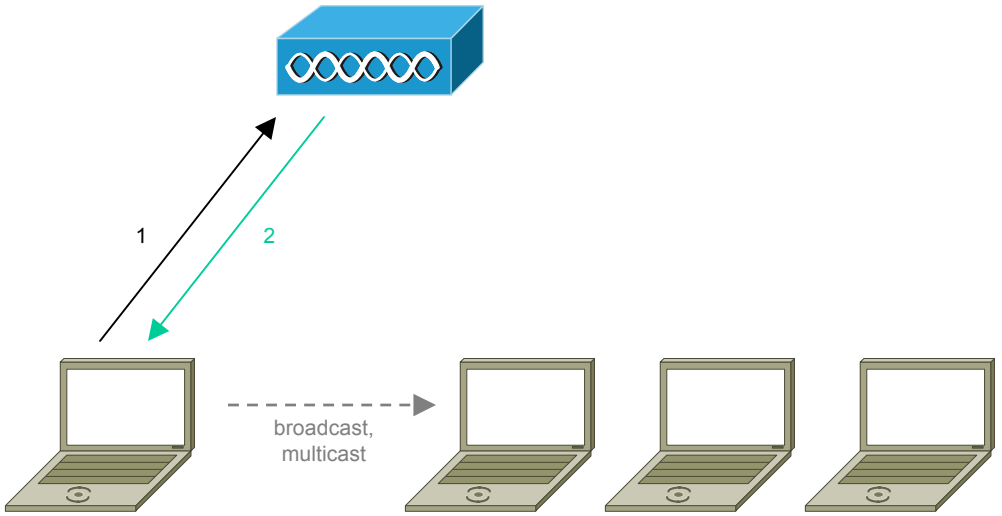




Pozitív nyugtázás

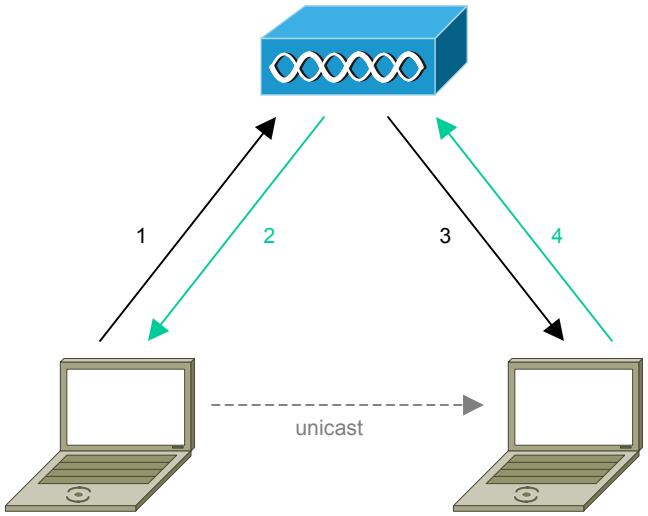
- a sikeres vételről az adó semmit sem tud
  - még az ütközést sem tudja detektálni
- az irányított adat- vagy menedszment keret sikeres vételét ACK keret küldésével nyugtázza a vevő állomás
- irányított keret (directed frame)
  - unicast
  - broadcast és multicast, ami az access pointnak megy

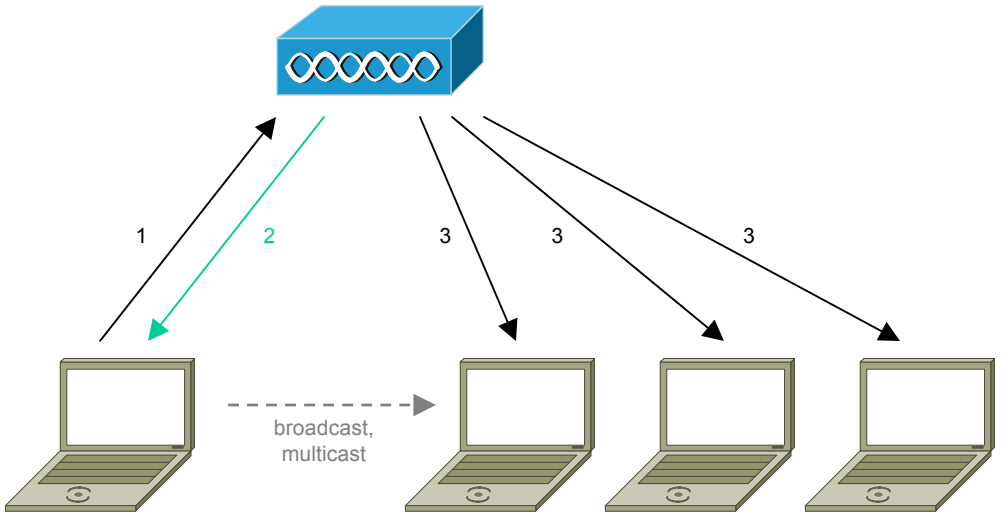




Pozitív nyugtázás

- a sikeres vételről az adó semmit sem tud
  - még az ütközést sem tudja detektálni
- az irányított adat- vagy menedszment keret sikeres vételét ACK keret küldésével nyugtázza a vevő állomás
- irányított keret (directed frame)
  - unicast
  - broadcast és multicast, ami az access pointnak megy



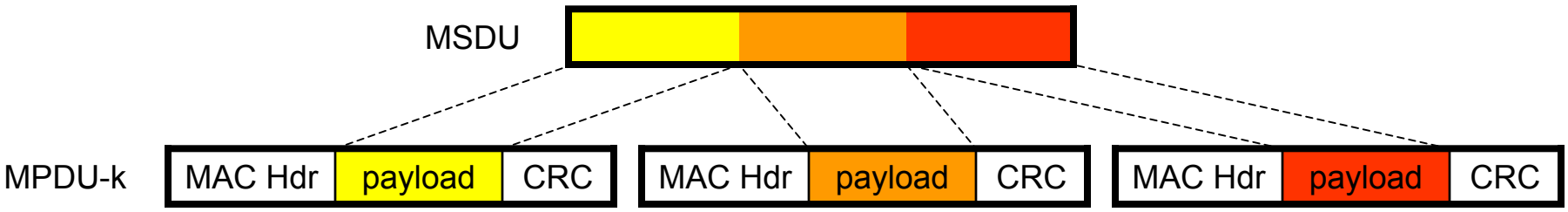


Újraküldés

- a MAC alréteg újraküldi a keretet, ha
  - irányított adat- vagy menedzsment keretre nem érkezik ACK
  - RTS-re nem érkezik CTS
- újraküldéskor versenyezni kell a csatornáért
- az adatkereteknek sorszáma van
  - ha nem az adatkeret sérül, hanem az ACK, akkor duplikált keret keletkezik, de ezt a vevő felismeri az azonos sorszámból

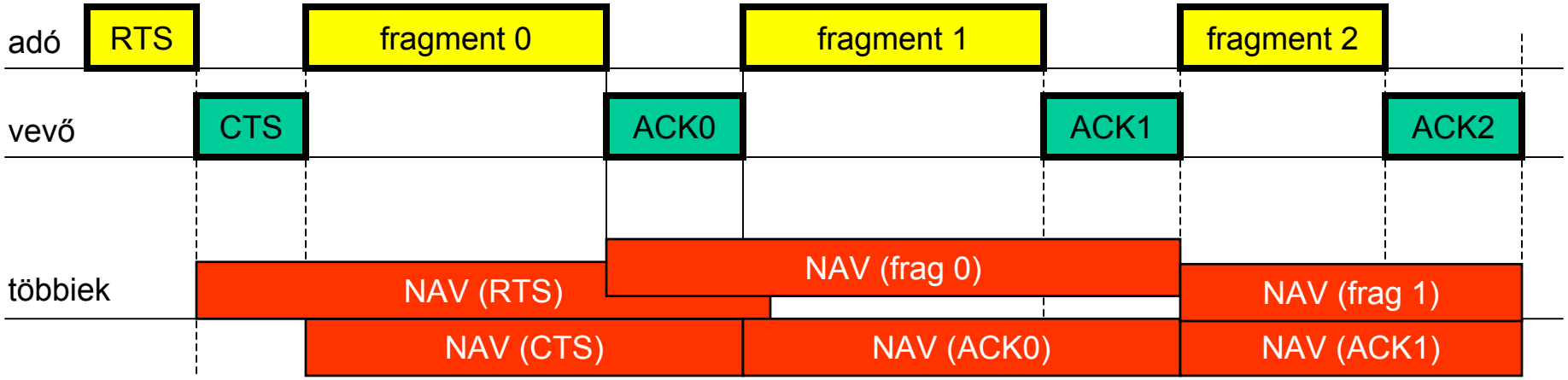
Tördelés

- a MAC alréteg kisebb részekre tördelheti az MSDU-t
  - csak unicastnál
  - minden töredék külön MAC keret (MPDU)
  - minden töredékre külön ACK
    - szükség esetén az újraküldés töredékenként lehetséges
  - a maximális töredékméret állomásonként konfigurálható
    - az ennél kisebb kereteket nem tördeli az állomás
- a töredékek összeállítása a vevőnél történik
  - a töredékek csak az „éterben” élnek külön életet; ahogy beérnek egy állomásra, az összerakja őket, akkor is, ha ő csak vevő, de nem a címzett



Tördelés (folyt.)

- fragment burst: egy MSDU összes töredéke átküldhető egymás után
  - közben nem kell a csatornáért versenyezni
  - ha van RTS/CTS, akkor csak a burst elején
    - NAV frissítése a töredék és ACK fejlécek Duration mezője alapján
  - megszakadhat a burst
    - nem érkezik ACK
    - FH PHY használatakor elérkezik a frekvenciaváltás ideje
  - ha megszakad, akkor folytatáskor versenyezni kell a csatornáért

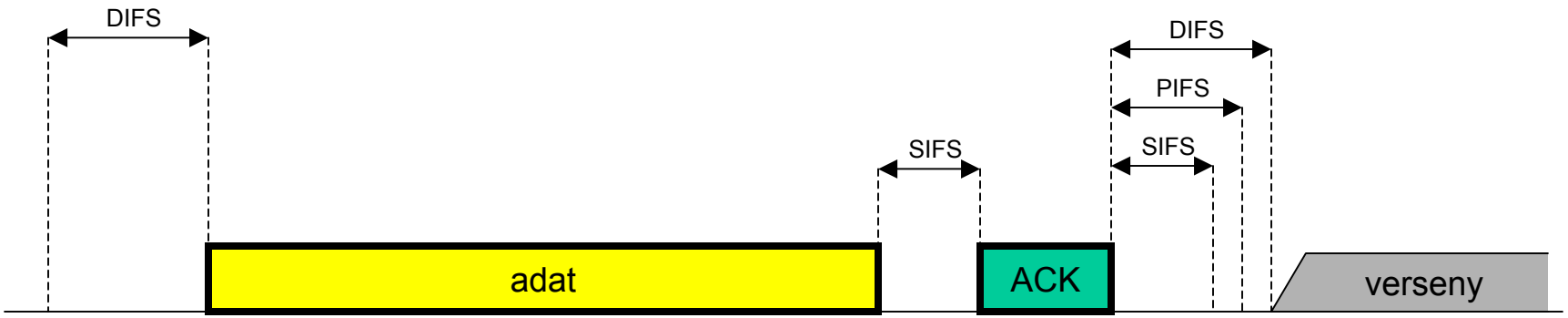


IFS – interframe space

- keretek közti szünet
- SIFS < PIFS < DIFS << EIFS
- gyakorlatilag közeghozzáférési prioritásokat határoz meg
  - különböző szituációk között
- SIFS – Short InterFrame Space
  - összetartozó szomszédos keretek közt, ahol nem kell versenyezni a médiumért
    - adat-ACK, RTS-CTS-adat-ACK, töredék-ACK-töredék-ACK, stb.
  - ennyi idő alatt a rádió átkapcsolható vételről adásra ill. fordítva
- PIFS – PCF InterFrame Space
  - lásd később

IFS – interframe space (folyt.)

- DIFS – DCF InterFrame Space
  - keret vége és a következő keretet előtti véletlen késleltetés kezdete közt
  - a csatornába való belehallgatáskor ennyi idő után tekinthető üresnek a csatorna
- EIFS – Extended InterFrame Space
  - másnak szóló, hibásnak érzékelt keret után
  - ennyi idő alatt odaér az ACK
    - lehet, hogy a keretet a megjelölt vevő jól vette, csak ez az állomás hitte hibásnak



Agenda

Közeghozzáférés

Alapok

Distributed Coordination Function

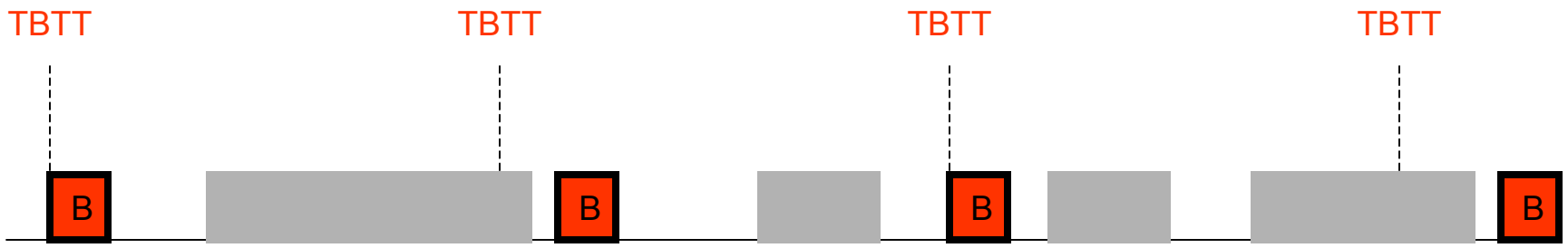
Menedzsment funkciók

Point Coordination Function

Keretformátumok

Beacon (irányfény)

- periodikusan küldött menedzsment keret
  - TBTT – Target Beacon Transmission Time
    - fix periódus szerinti időpontok
    - ehhez képest a Beacon késhet, ha foglalt a csatorna
  - a periódus általában néhányszáz ms
- infrastruktúra módban az AP küldi
- ad-hoc módban bárki küldheti
  - TBTT-kor az állomások versenyezni kezdenek, a nyerő küldi a Beacont



A Beacon tartalma

- idő az állomások óráinak szinkronizálásához
  - ad-hoc módban az elosztott időszinkron miatt csak előre szabad igazítani az órát
- SSID
- BSS paraméterek
  - ESS/IBSS
  - van-e PCF
  - a fizikai réteg paraméterei (pl. FH PHY esetén ugrási minta)
  - használt adatsebességek
- PCF paraméterek
  - PCF időszak max. hossza, periódusideje, legközelebbi kezdése
  - éppen tartó PCF időszakból hátralevő max. idő (NAV beállításához)
- TIM
  - lásd később

Power management

- az állomások gyakran akkumulátorról működnek
  - szükség lehet az energiatakarékosságra
- AM – Active mode
  - „normál” működés
    - az állomás folyamatosan ébren van
  - az access point mindig így működik
- PS – Power Save mode
  - az állomás ébrenlét (awake) és szundikálás (doze) között váltogat
  - doze állapotban nem működik a rádió (vagy az IR adó/vevő)

PwrMgmt – infrastruktúra mód

- az access point nyilvántartja, hogy melyik állomás alszik
  - az elalvásról az utolsó elküldött keret fejlécében a Power Management bit bebillentésével tájékoztatja a küldő az access pointot
- az access point puffereli az alvó állomásoknak szóló kereteket
  - és a broadcast vagy multicast kereteket, ha bárki alszik
- TIM – Traffic Indication Map
  - bittérkép
    - megadja, hogy melyik állomás számára van pufferelt keret
  - minden Beacon keretben szerepel
- DTIM – Delivery TIM
  - minden N-edik Beacon keret DTIM Beacon
    - a TIM-ben szerepel, hogy hányadik Beacon lesz legközelebb DTIM Beacon
  - a DTIM Beacon keret után az AP adja a pufferelt broadcast és multicast kereteket

PwrMgmt – infrastruktúra mód (folyt.)

- az alvó állomás időnkét TBTT előtt felébred
  - veszi a Beacont, megnézi a TIM-et
  - ha van számára pufferelt unicast keret a TIM szerint, akkor PS-Poll kontroll keretet küld az AP-nak, mire az elküldi a pufferelt keretet
  - DTIM Beacon után megvárja az AP által adott broadcast/multicast kereteket
  - ha a TIM PCF elején jelez számára pufferelt keretet, akkor megvárja, amíg megszólítja őt az AP a pufferelt kerettel

PwrMgmt – ad-hoc mód

- minden állomás önállóan
  - nyilvántartja (amennyire tudja), hogy melyik állomás alszik
  - puffereli az alvó állomásoknak szánt kereteit
- ATIM – Announcement Traffic Indication Message
  - menedzsment keret, adatrésze nincs
  - ATIM window: minden TBTT-vel kezdődő fix hosszúságú időszak
    - ekkor csak Beacon és ATIM (és arra válaszoló ACK) kereteket szabad küldeni
    - ezalatt minden állomás ébren van
  - akinek pufferelt kerete van (unicast vagy broadcast/multicast), a megfelelő címzettnek ATIM keretet küld az ATIM window alatt
- aki ATIM keretet kap, ébren marad a következő TBTT-ig
  - az ATIM window után, a következő TBTT előtt lehet a pufferelt kereteket elküldeni
- a Beacon küldője ébren marad a következő Beaconig
  - hogy legalább egyvalaki mindig ébren legyen

Csatlakozás BSS-hez

- passzív keresés:
  - a csatlakozni kívánó állomás Beacon keretet vár
- aktív keresés:
  - Probe Request/Response menedzsment keretek
  - a csatlakozni kívánó állomás Probe Request keretet küld
  - Probe Response
    - minden benne van, ami a Beaconben, kivéve a TIM
    - infrastruktúra módú BSS-ben az AP válaszol
    - IBSS-ben az, aki az utolsó Beacont küldte
  - a PHY-től és a beállításoktól függően több csatornát végig kell próbálni
- új BSS indítása: Beacon keretek adásának megkezdése
  - az állomáson konfigurált paraméterek használatával
  - ad-hoc módú BSS-t bárki indíthat
    - BSSID-t kell generálni
  - infrastruktúra módút csak access point indíthat

Csatlakozás ESS-hez

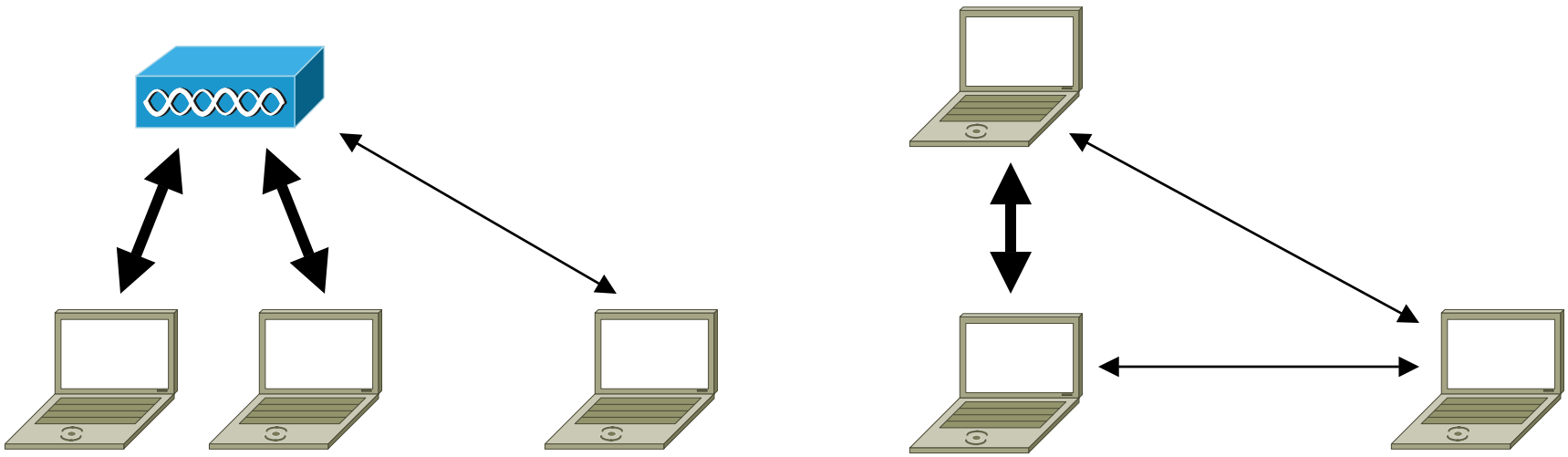
- csatlakozás az egyik BSS-hez
- autentikáció
- association kialakítása az access pointtal

Association

- ESS-ben a keretek célbajuttatásához a Distribution Systemnek tudnia kell, hogy melyik állomás melyik AP-on keresztül érhető el
- association: állomás → AP összerendelés
  - Association Request/Response ill. Reassociation Request/Response menedzsment keretek használatával jön létre
  - Association ID (AID): 1-2007 közti érték, az AP adja
    - pl. a TIM bittérképben ezt használják indexnek
- reassociation: roaming (ESS-en belül)
  - csatlakozás ugyanannak az ESS-nek egy másik access pointjához
  - az access pointok között szükséges adminisztratív protokoll még nem része a szabványnak
    - jelenleg gyártóspecifikus megoldások
    - később IEEE 802.11f – Inter Access Point Protocol

Multirate

- a BSS állomásai használhatnak több adatsebességet
- néhány menedzsment üzenetben szerepelnek a használt adatsebességek
  - Beacon
  - Probe Request/Response
  - Association Request/Response
  - Reassociation Request/Response



Multirate (folyt.)

- BSS basic rate set:
  - a használható sebességek egy részhalmaza
  - a BSS minden tagjának támogatnia kell ezeket a sebességeket
  - ilyen sebességekkel mehetnek:
    - kontroll keretek
    - irányítatlan broadcast és multicast keretek
  - a Beacon és Response üzenetekben külön jelölve vannak a többi sebesség közt

IEEE 802.11d – world mode

- az állomás a BSS-hez való csatlakozáskor megtanulja a helyi beállításokat
  - spektrum etikett
    - használható csatornák
    - max. adóteljesítmény
  - FH PHY esetén ugrási minták
- a BSS-t indító állomáson konfigurálva vannak a helyi paraméterek
- csak passzív keresés BSS-hez való csatlakozáskor
  - a spektrum etikett tökéletes betartása érdekében

Agenda

Közeghozzáférés

Alapok

Distributed Coordination Function

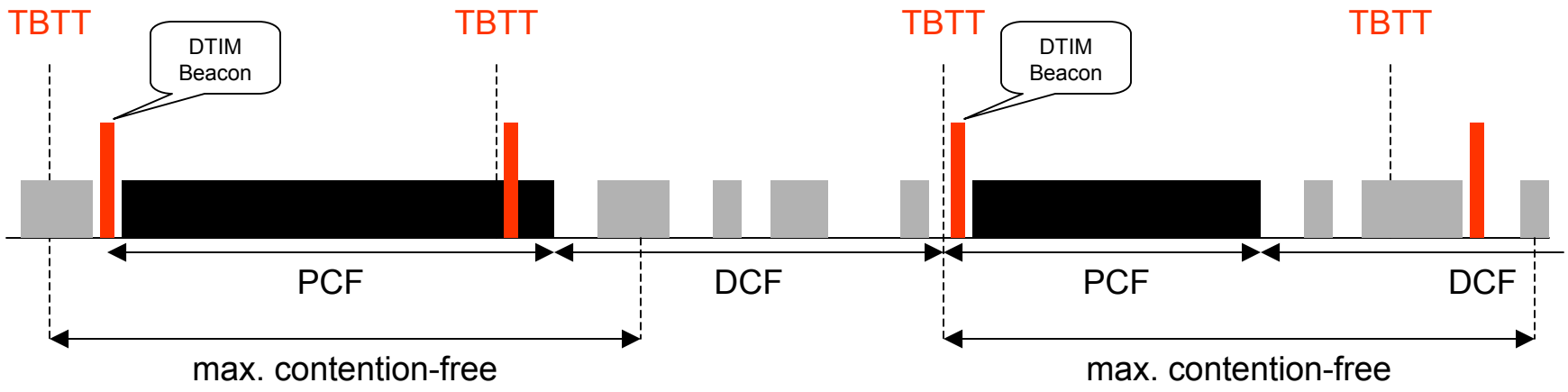
Menedzsment funkciók

Point Coordination Function

Keretformátumok

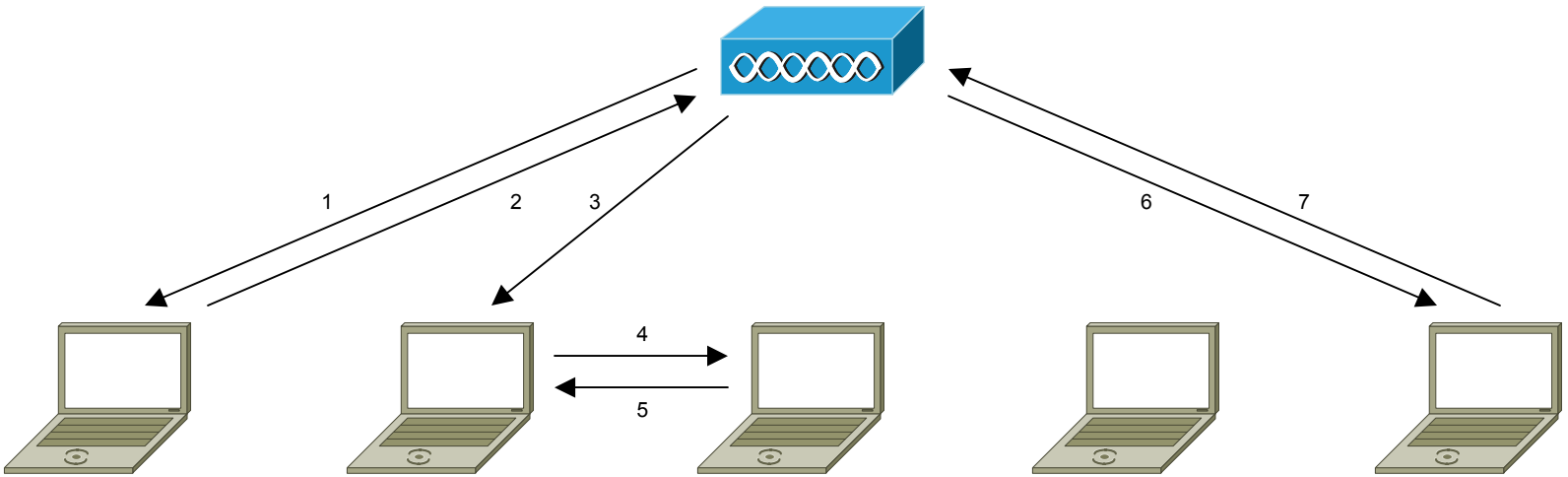
Point Coordination Function

- CSMA/CA „megáll” egy kis időre, helyette polling
  - a NAV és a PIFS biztosítja a prioritást a DCF felett
  - az access point a polling master (point coordinator)
- DCF és PCF időben váltogatja egymást
  - DTIM Beacon után kezdődik a PCF időszak (contention-free period)
  - megadott számú DTIM-enként periodikusan ismétlődik
  - megadott maximális PCF időtartam
  - a PCF időszak végét a CF-End (Contention-Free-End) kontroll üzenettel jelzi az access point



Polling

- az állomások a BSS-hez való csatlakozáskor kérhetik a pollingot
  - az access point nyilvántartja a pollingot kérő állomások listáját
- az access point szólítja meg az állomásokat
  - a megszólított állomás egy keretet küldhet (és kell is küldenie)
    - közvetlenül bármelyik állomás lehet a vevő, nem csak az access point



PCF prioritás

- SIFS a keretek között
  - kivéve ha az access point nem kap választ, ilyenkor PIFS
- a Beacon keretekben szerepel a PCF időszak végéig hátralevő idő
  - ezt használják az állomások a NAV beállítására
  - CF-End törli a NAV esetlegesen hátralevő részét

Polling és ACK

- piggybacked polling és ACK
  - az access point a pollingot az állomásnak küldött keret típusában jelzi
  - minden állomás a kerettípusban jelzi az ACK-et az előző keretre
- 8 adatkeret altípus létezik
  - DCF időszakban csak a 0000 (Data) használatos

keret altípus				funkció
Res.	No data	Poll	Ack	
0	0	0	0	Data
0	0	0	1	Data + CF-Ack
0	0	1	0	Data + CF-Poll
0	0	1	1	Data + CF-Ack + CF-Poll
0	1	0	0	Null
0	1	0	1	CF-Ack
0	1	1	0	CF-Poll
0	1	1	1	CF-Ack + CF-Poll

PCF adatkeret altípusok

- CF-Poll-os kereteket csak az access point küldhet
- CF-Ack bit: ACK az előző keretre
  - az access point által küldött CF-Ack-es keret címzettje tipikusan más, mint akinek az ACK szól
    - ez nem baj, hiszen az AP adását mindenki hallja
- Null keret
  - a megszólított állomásnak nincs adnivalója
  - FH PHY esetén az adnivaló keret nem fér el frekvenciaváltás előtt

Agenda

Közeghozzáférés

Alapok

Distributed Coordination Function

Menedzsment funkciók

Point Coordination Function

Keretformátumok

Frame control

- Type: kontroll, menedzsment, vagy adatkeret
- Subtype: keret altípus
- From/To DS: adó/vevő az access point
- More Frag: tördelt keret és nem ez az utolsó töredék
- Retry: újraküldött keret
- Pwr Mgmt: a keret után el fog aludni az adó állomás
- More Data: van még küldeni való keret (pl. pufferelt keret PS állomás részére)
- WEP: a payload titkosítva van

Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgmt	More Data	WEP	Order
2	2	4	1	1	1	1	1	1	1	1

MAC Header							Payload	FCS
Frame Control	Duration / AID	Addr 1 (RA)	Addr 2 (TA)	Addr 3	Seq Control	Addr 4		

Cím mezők a fejlécben

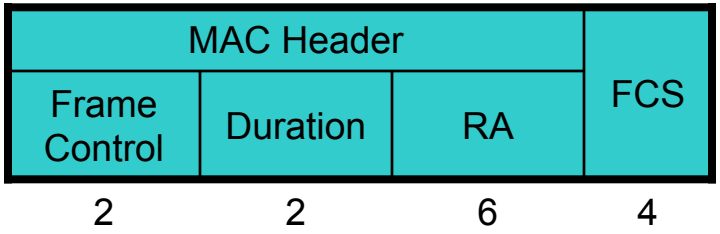
- ToDS/FromDS bitektől függően

To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4
0	0	DA (=RA)	SA (=TA)	BSSID	-
0	1	DA (=RA)	BSSID (=TA)	SA	-
1	0	BSSID (=RA)	SA (=TA)	DA	-
1	1	RA	TA	DA	SA

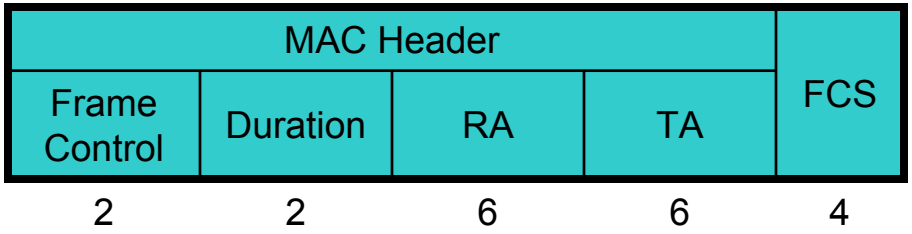
MAC Header							Payload	FCS
Frame Control	Duration / AID	Addr 1 (RA)	Addr 2 (TA)	Addr 3	Seq Control	Addr 4		
2	2	6	6	6	2	6	0-2312	4

Néhány kontroll keret szerkezete

ACK, CTS



RTS



Agenda

Bevezető

Fizikai réteg

Közeghozzáférés

Biztonság

Egyéb

Biztonsági feladatok

- vezeték nélküli médium
  - nincsenek jól definiált határai az átviteli közegnek
  - illetéktelen hozzáférés, lehallgatás triviális
- titkosítás
  - a hálózati forgalom lehallgatásának, módosításának megelőzésére
- autentikáció
  - a hálózathoz való illetéktelen hozzáférés (csatlakozás) megelőzésére
  - BSS-en belül, 2 állomás között
  - infrastruktúra módban
    - csak az AP és más állomás között
    - kötelező
  - ad-hoc módban
    - nem kötelező

Agenda

Biztonság

802.11 titkosítás

WEP problémák

Megoldás a WEP problémáira

802.11 autentikáció

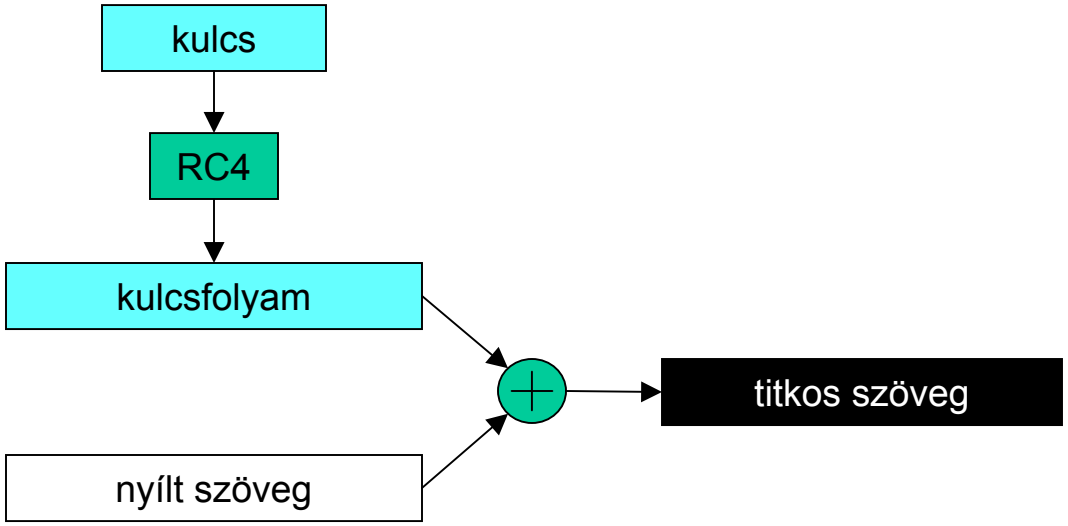
Autentikációs problémák

Autentikációs megoldások

802.11i

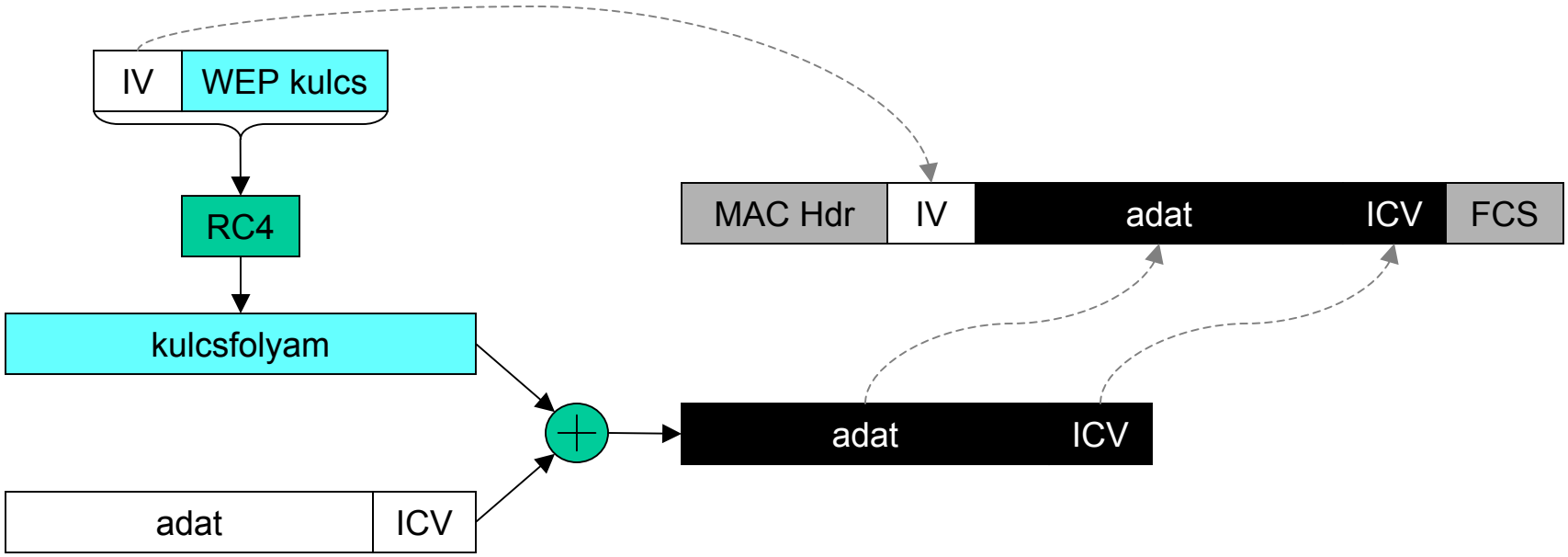
Wired Equivalent Privacy

- adat keretek titkosítása
  - adótól vevőig
  - keretenként
- RC4 szimmetrikus kulcsú folyamkódoló
  - a bemenetére adott rövid kulcsból hosszú véletlenszerű kulcsfolyamot generál determinisztikusan
  - a nyílt szöveget a kulcsfolyammal XOR-olva kapjuk a titkosított szöveget



Wired Equivalent Privacy (folyt.)

- IV – Initialization Vector
  - egy kulcsfolyam többszöri felhasználása veszélyes
  - (kulcs, IV) az RC4 bemenete, így a kulcsfolyam más, ha az IV más
- ICV – Integrity Check Value
  - 32 bites CRC hozzáadása titkosítás előtt
  - titkosított keret észrevétlen módosítása ellen



WEP tulajdonságok

- 24 bites IV
- 40 vagy 104 bites kulcs
  - a szabványban csak a 40 bites kulcs szerepel
  - a 104 bites kulcsot rendszerint 128-nak írják a marketing anyagokban
- lehet a BSS-ben közös kulcsot használni
  - egyszerre négy közös kulcs adható meg
    - adáskor az adó választ egyet
    - a sorszámát beleírja a keret feljécébe
- a közös kulcsok felülbírálhatók adó-vevő párhoz tartozó kulccsal
  - broadcast és multicast forgalom mindig közös kulcsokkal
- a kulcsmenedzsmentről nem szól a szabvány

Agenda

Biztonság

802.11 titkosítás

WEP problémák

Megoldás a WEP problémáira

802.11 autentikáció

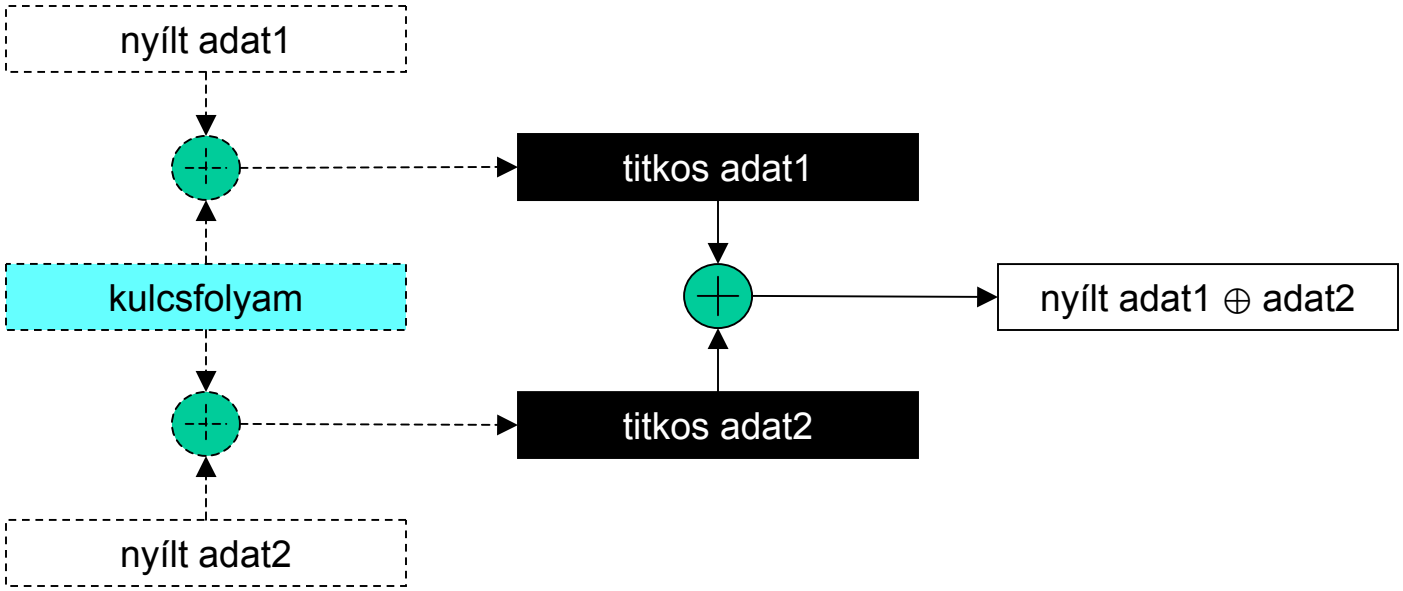
Autentikációs problémák

Autentikációs megoldások

802.11i

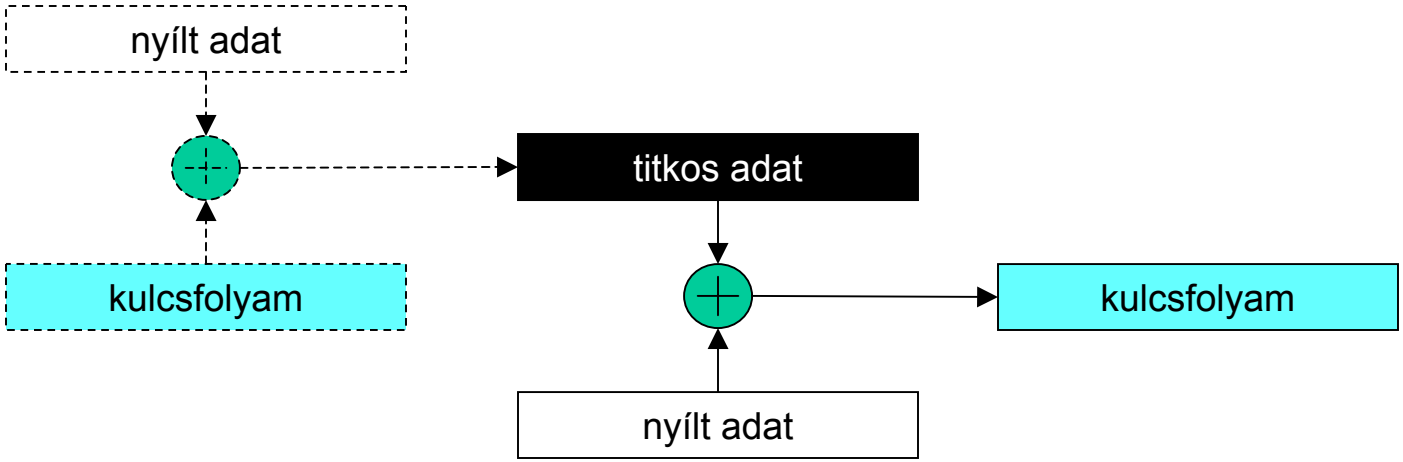
IV ütközés

- azonos IV-k azonos kulcsfolyamot eredményeznek
  - feltéve, hogy a kulcs sem változott
  - 2^{24} lehetséges IV-vel ez könnyen előfordul
- nyílt szövegek egymással XOR-olt összege megkapható azonos IV-vel titkosított keretek XOR-olásával
  - ez egyszerűvé teszi statisztikai jellemzőkre épülő támadásokat



IV ütközés (folyt.)

- a nyílt és a hozzá tartozó titkosított keretpár
  - XOR-olásuk megadja az adott IV-hez tartozó kulcsfolyamot
  - egy ilyen pár ismerete alapján minden ezzel az IV-vel kódolt keret visszafejthető

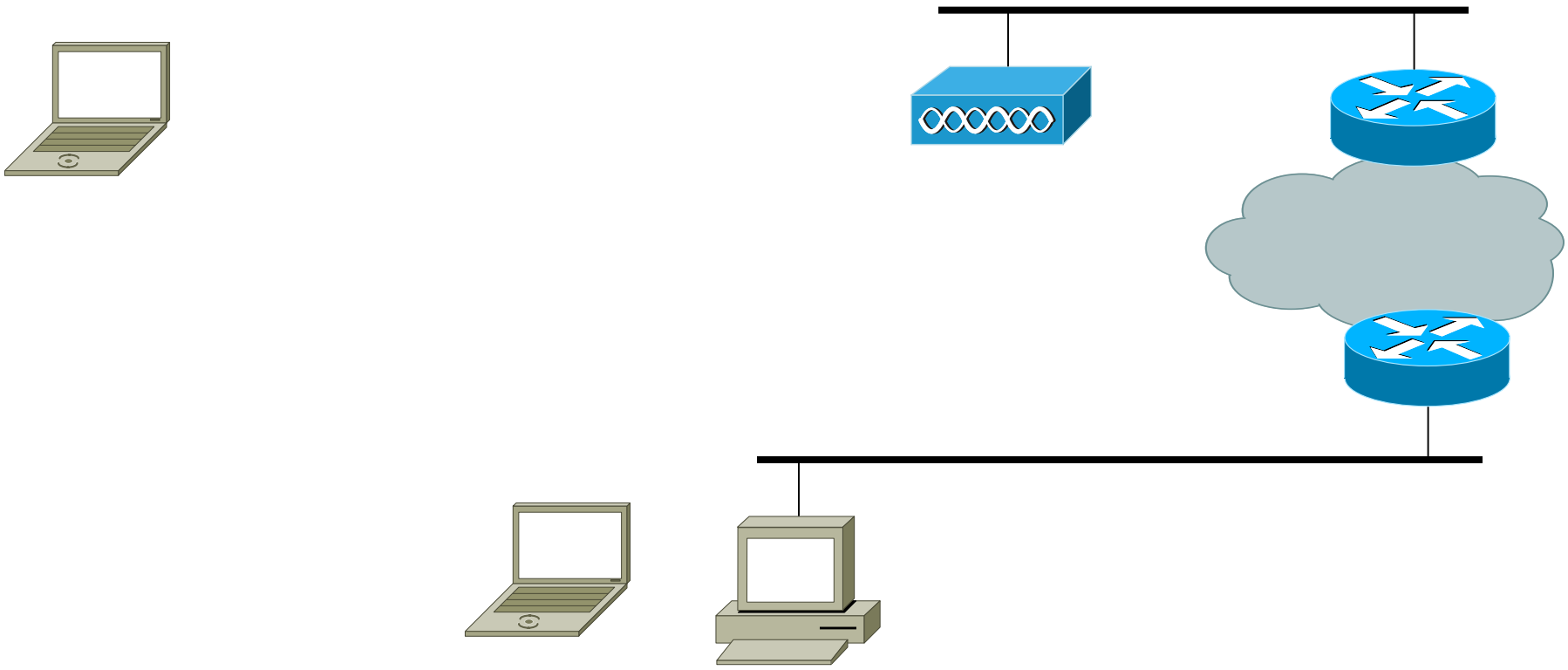


Nyílt+titkos keretpár támadás 1.

- az access point kódolóként való használata
  - a támadó keretet küld a vezetékes hálózatból a vezeték nélkülibe
  - majd ott lehallgatja azt

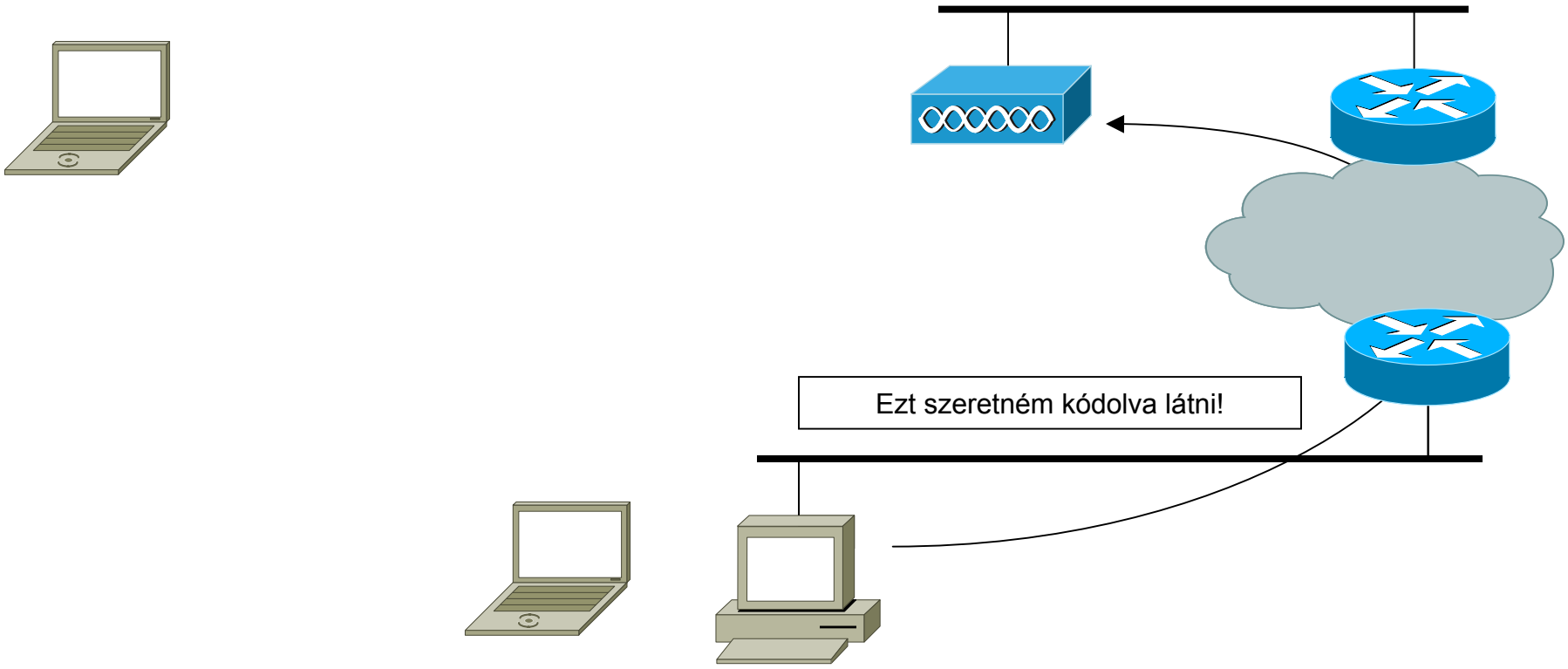
Nyílt+titkos keretpár támadás 1.

- az access point kódolóként való használata
  - a támadó keretet küld a vezetékes hálózatból a vezeték nélkülibe
  - majd ott lehallgatja azt



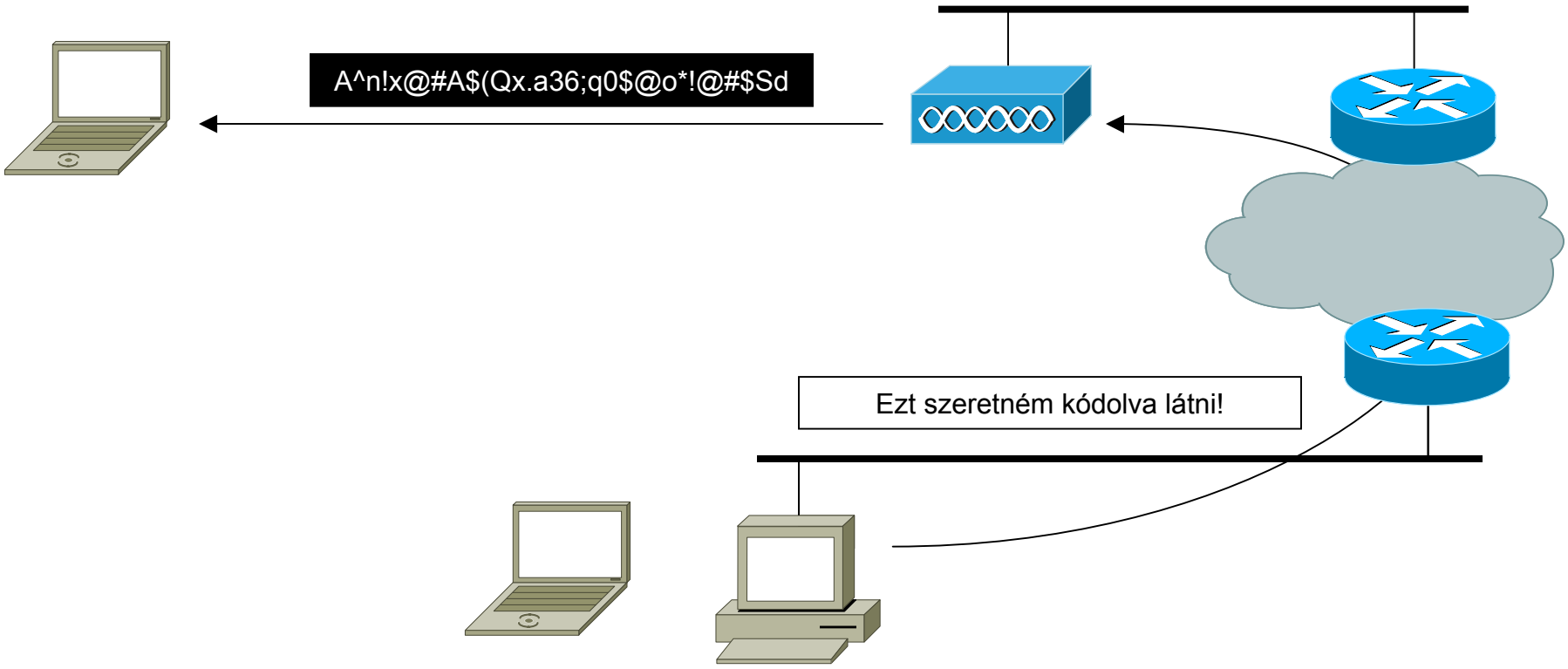
Nyílt+titkos keretpár támadás 1.

- az access point kódolóként való használata
  - a támadó keretet küld a vezetékes hálózatból a vezeték nélkülibe
  - majd ott lehallgatja azt



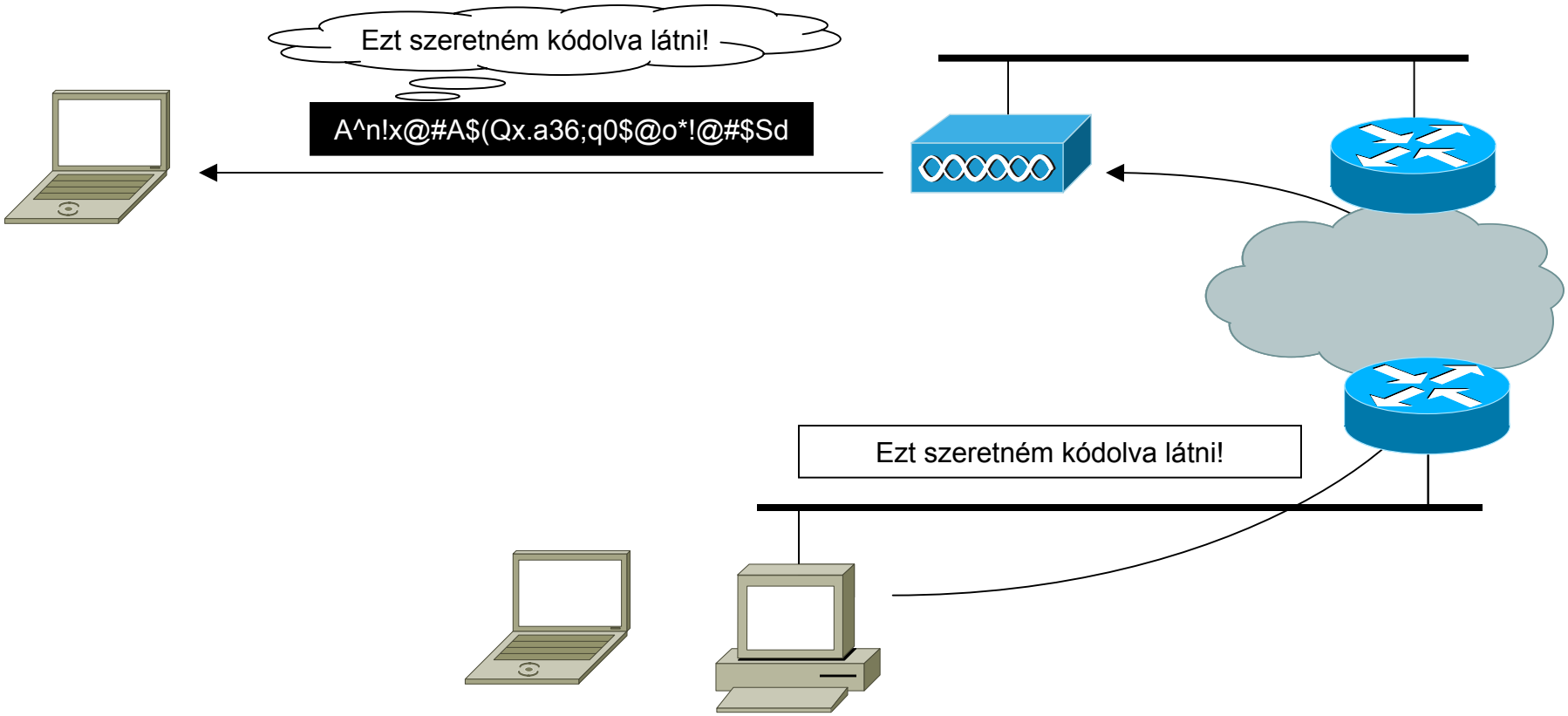
Nyílt+titkos keretpár támadás 1.

- az access point kódolóként való használata
  - a támadó keretet küld a vezetékes hálózatból a vezeték nélkülibe
  - majd ott lehallgatja azt



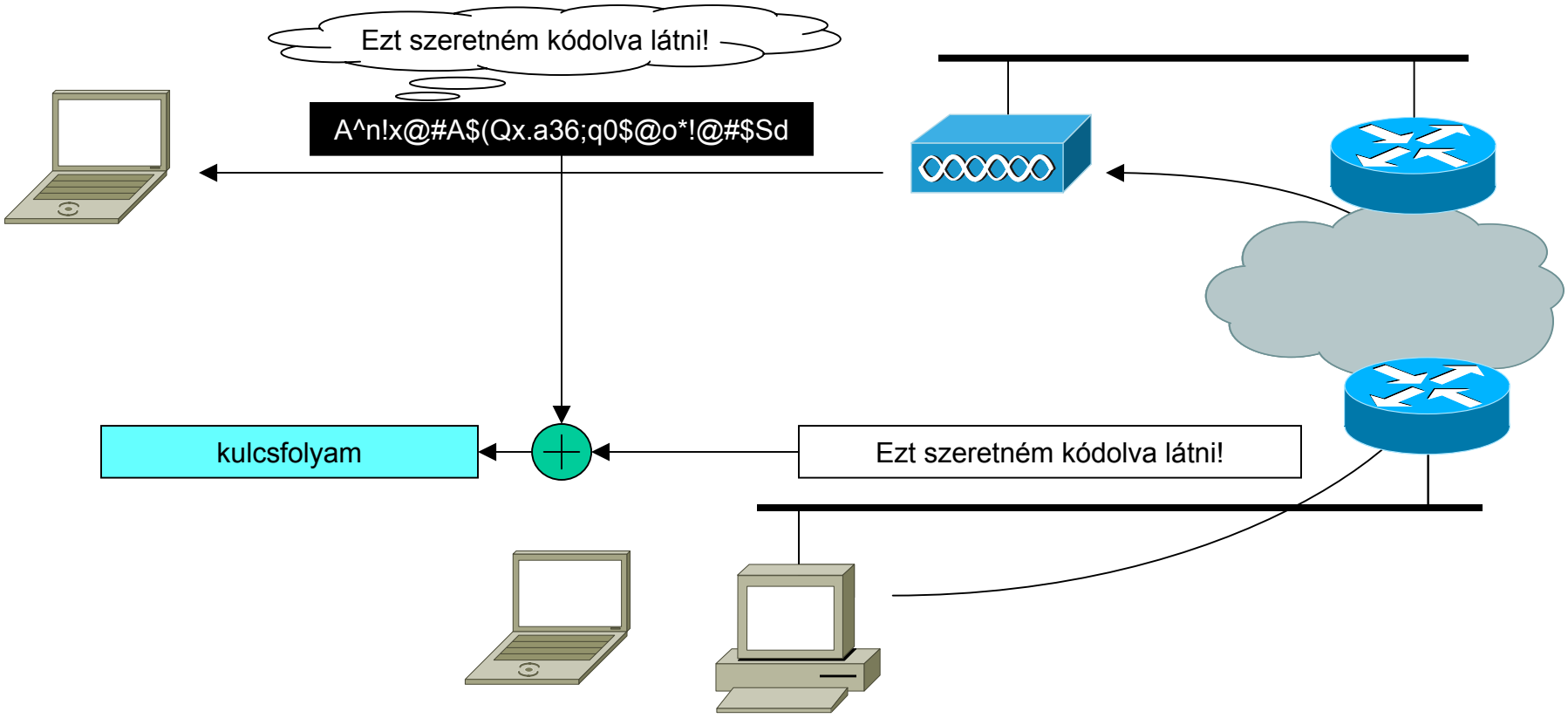
Nyílt+titkos keretpár támadás 1.

- az access point kódolóként való használata
  - a támadó keretet küld a vezetékes hálózatból a vezeték nélkülibe
  - majd ott lehallgatja azt



Nyílt+titkos keretpár támadás 1.

- az access point kódolóként való használata
  - a támadó keretet küld a vezetékes hálózatból a vezeték nélkülibe
  - majd ott lehallgatja azt

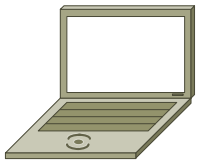


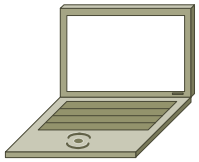
Nyílt+titkos keretpár támadás 2.

- titkos üzenet tartalmának megtippelése
  - titkos üzenet lehallgatása
  - tartalom megtippelése
    - a TCP/IP protokollcsalád fejléceit jól meg lehet tippelni
    - protokoll parancsokat meg lehet tippelni
    - stb.

Nyílt+titkos keretpár támadás 2.

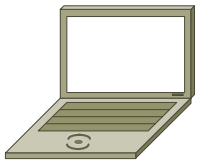
- titkos üzenet tartalmának megtippelése
  - titkos üzenet lehallgatása
  - tartalom megtippelése
    - a TCP/IP protokollcsalád fejléceit jól meg lehet tippelni
    - protokoll parancsokat meg lehet tippelni
    - stb.





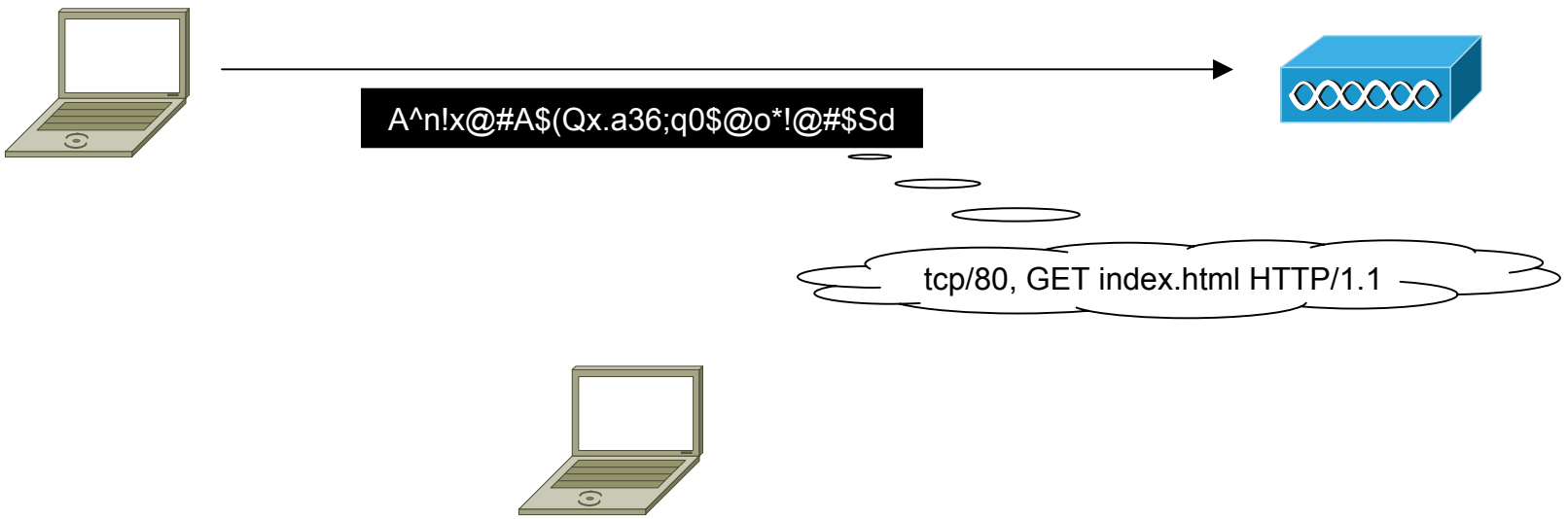
Nyílt+titkos keretpár támadás 2.

- titkos üzenet tartalmának megtippelése
  - titkos üzenet lehallgatása
  - tartalom megtippelése
    - a TCP/IP protokollcsalád fejléceit jól meg lehet tippelni
    - protokoll parancsokat meg lehet tippelni
    - stb.



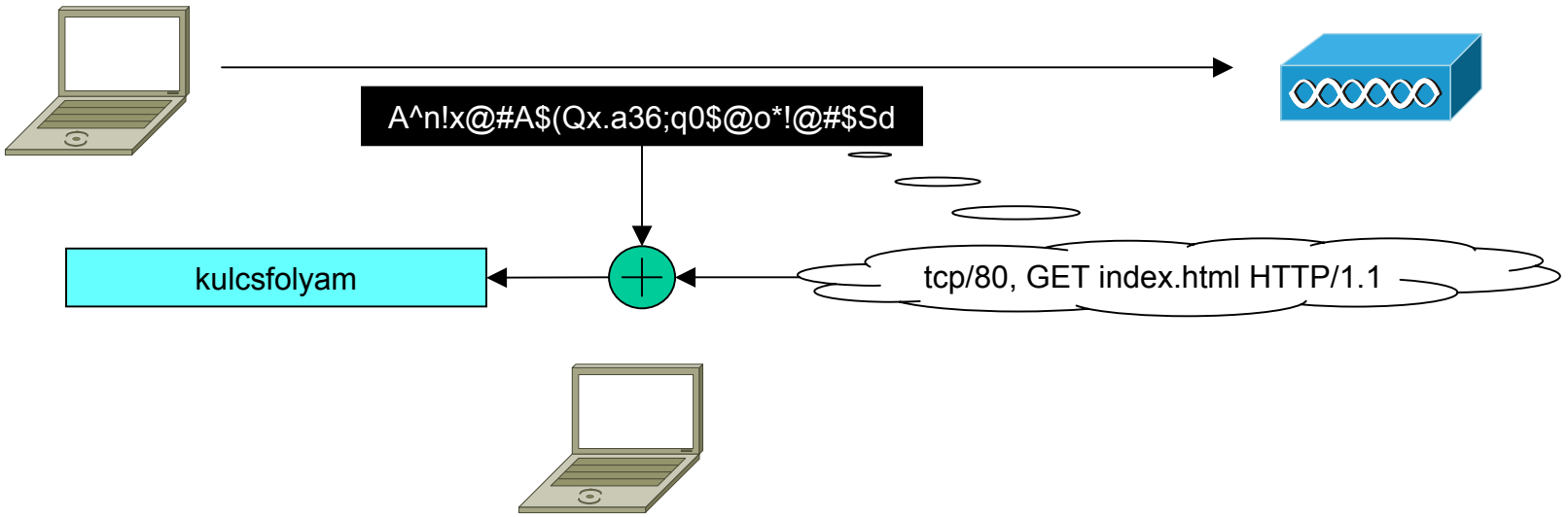
Nyílt+titkos keretpár támadás 2.

- titkos üzenet tartalmának megtippelése
  - titkos üzenet lehallgatása
  - tartalom megtippelése
    - a TCP/IP protokollcsalád fejléceit jól meg lehet tippelni
    - protokoll parancsokat meg lehet tippelni
    - stb.



Nyílt+titkos keretpár támadás 2.

- titkos üzenet tartalmának megtippelése
  - titkos üzenet lehallgatása
  - tartalom megtippelése
    - a TCP/IP protokollcsalád fejléceit jól meg lehet tippelni
    - protokoll parancsokat meg lehet tippelni
    - stb.



Bit flipping

- az ICV-nek használt CRC lineáris
  - CRC(a $\oplus$ b) = CRC(a) $\oplus$ CRC(b)
- a titkosított üzenet bitjei a nyílt üzenet ismerete nélkül észrevétlenül módosíthatók
  - hiszen utána lehet igazítani a titkosított ICV-t

Bit flipping

- az ICV-nek használt CRC lineáris
  - CRC(a $\oplus$ b) = CRC(a) $\oplus$ CRC(b)
- a titkosított üzenet bitjei a nyílt üzenet ismerete nélkül észrevétlenül módosíthatók
  - hiszen utána lehet igazítani a titkosított ICV-t

00*111*00000000001

módosítandó bitek

Bit flipping

- az ICV-nek használt CRC lineáris
  - CRC(a ⊕ b) = CRC(a) ⊕ CRC(b)
- a titkosított üzenet bitjei a nyílt üzenet ismerete nélkül észrevétlenül módosíthatók
  - hiszen utána lehet igazítani a titkosított ICV-t

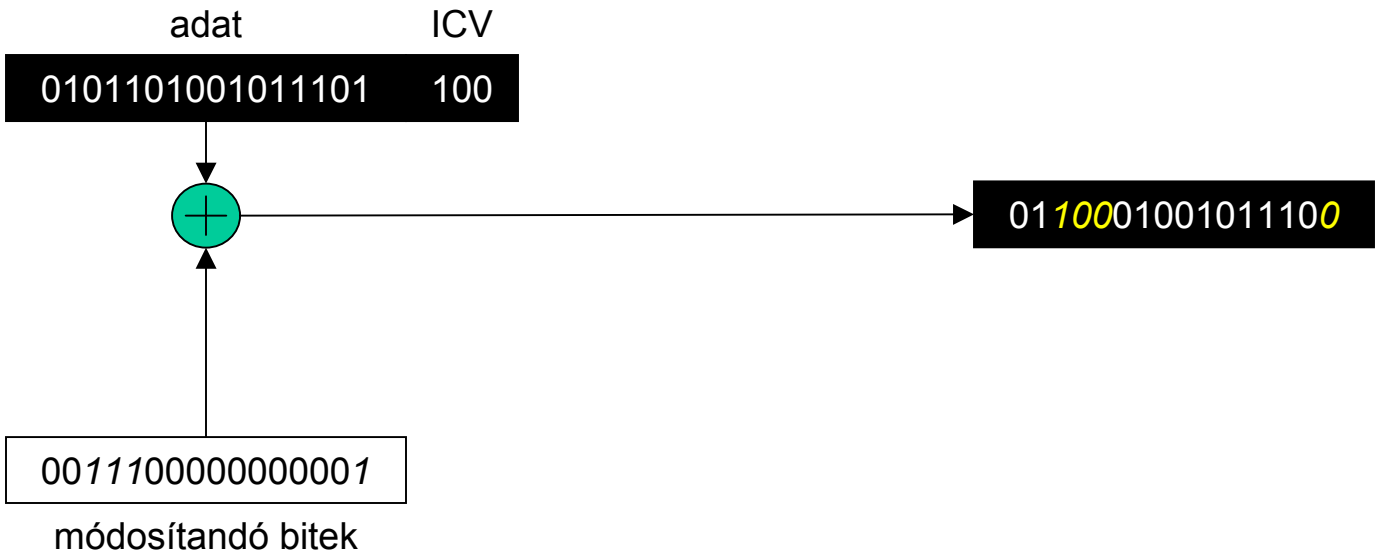
adat	ICV
0101101001011101	100

00*111*00000000001

módosítandó bitek

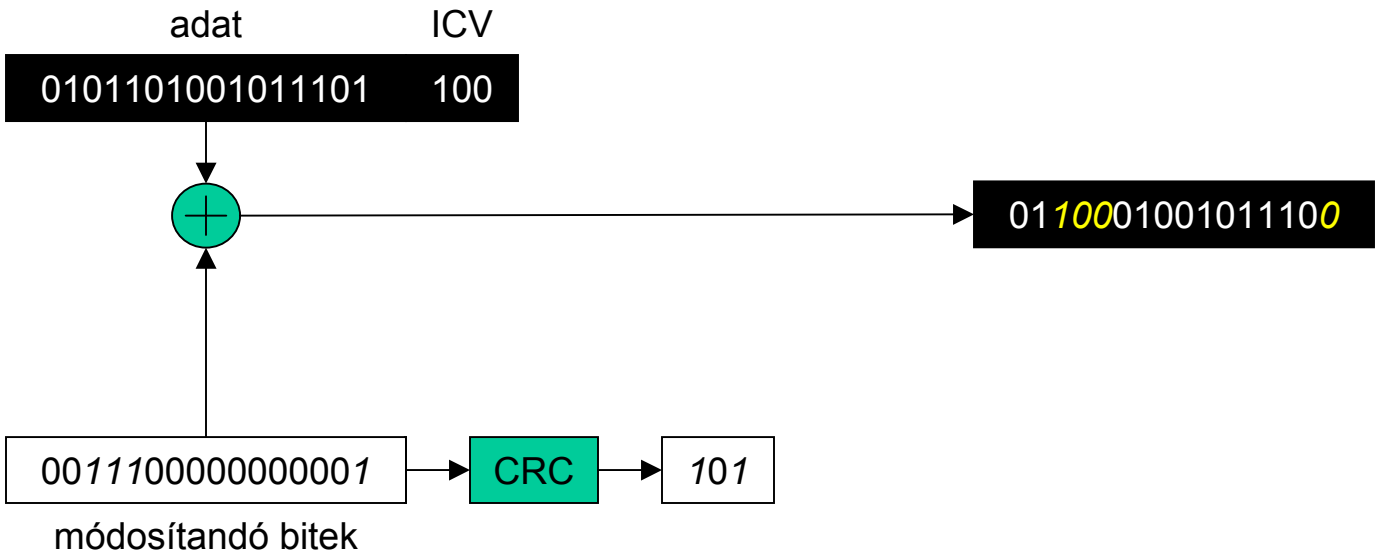
Bit flipping

- az ICV-nek használt CRC lineáris
  - CRC(a ⊕ b) = CRC(a) ⊕ CRC(b)
- a titkosított üzenet bitjei a nyílt üzenet ismerete nélkül észrevétlenül módosíthatók
  - hiszen utána lehet igazítani a titkosított ICV-t



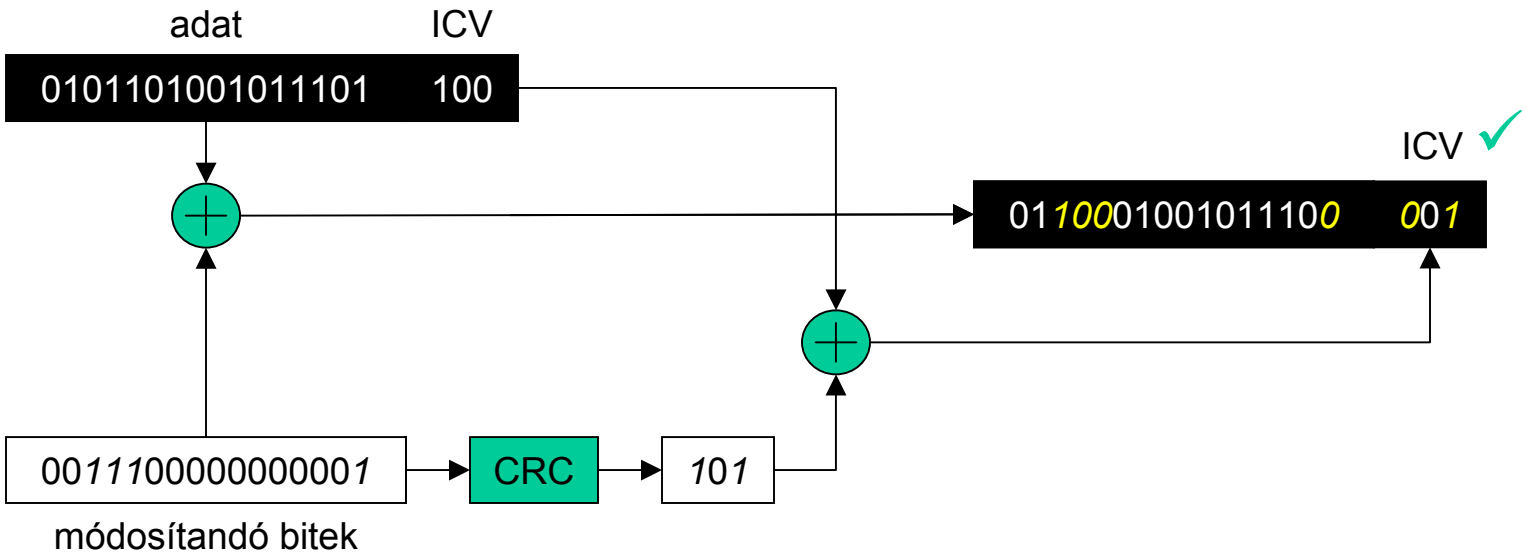
Bit flipping

- az ICV-nek használt CRC lineáris
  - CRC(a ⊕ b) = CRC(a) ⊕ CRC(b)
- a titkosított üzenet bitjei a nyílt üzenet ismerete nélkül észrevétlenül módosíthatók
  - hiszen utána lehet igazítani a titkosított ICV-t



Bit flipping

- az ICV-nek használt CRC lineáris
  - CRC(a ⊕ b) = CRC(a) ⊕ CRC(b)
- a titkosított üzenet bitjei a nyílt üzenet ismerete nélkül észrevétlenül módosíthatók
  - hiszen utána lehet igazítani a titkosított ICV-t

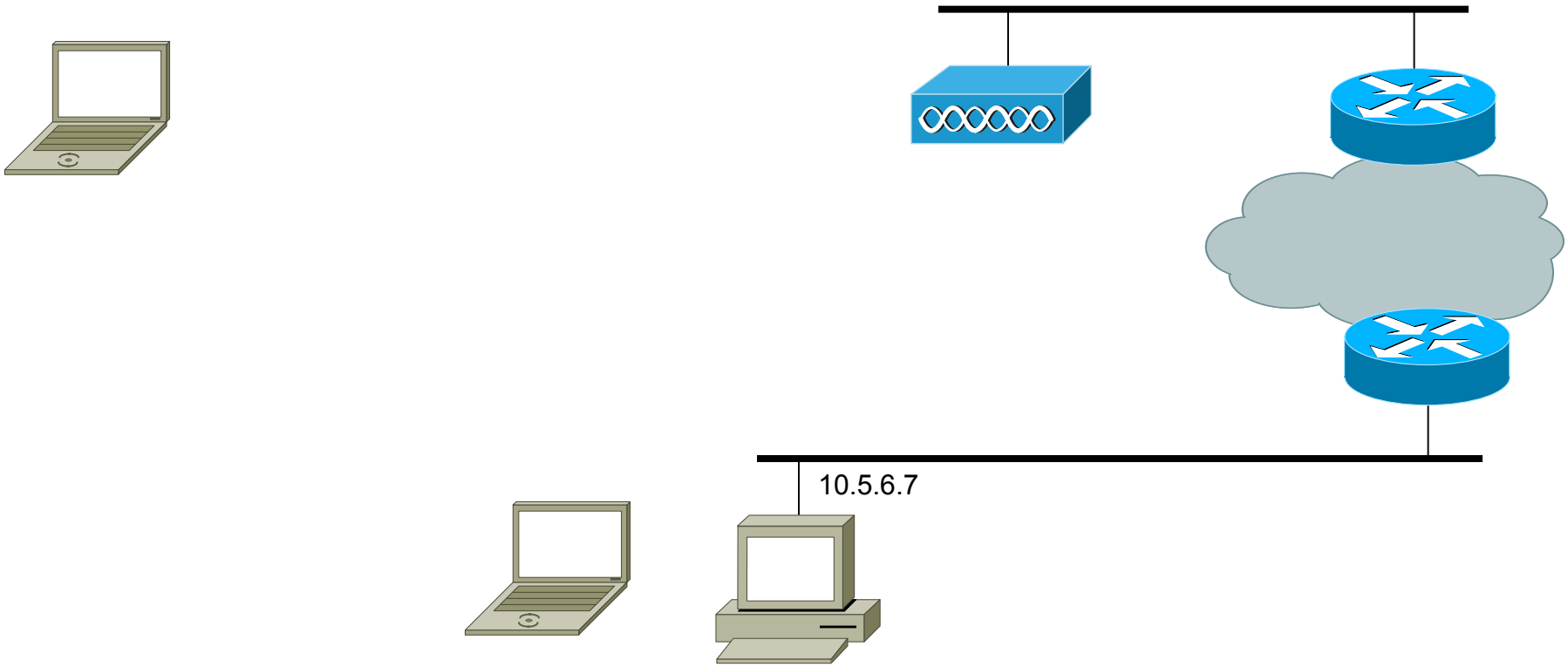


Bit flipping támadás 1.

- eltérítés
  - IP cél cím megváltoztatása saját vezetékes hálózati gép címére
  - az access point dekódolja a visszajátszott keretet
  - majd továbbküldi a vezetékes hálózatba a támadó gépére

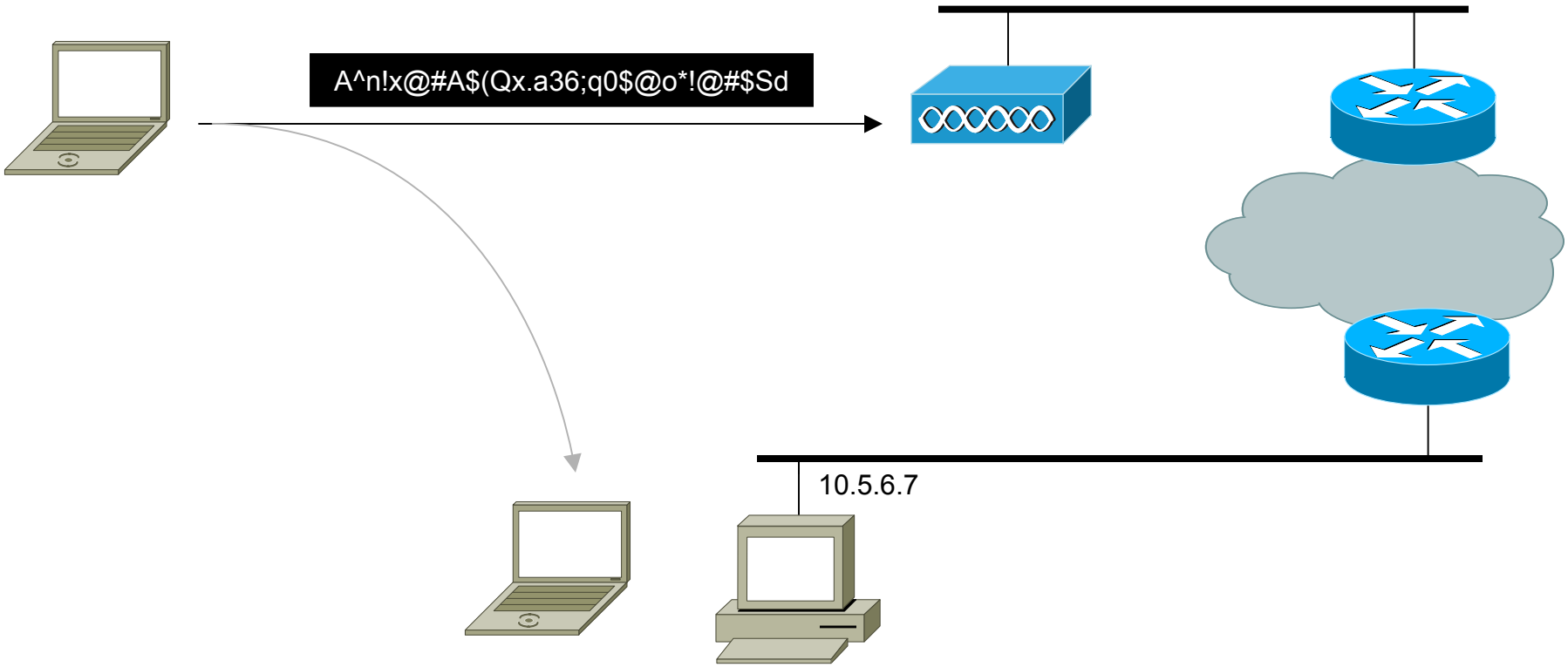
Bit flipping támadás 1.

- eltérítés
  - IP cél cím megváltoztatása saját vezetékes hálózati gép címére
  - az access point dekódolja a visszajátszott keretet
  - majd továbbküldi a vezetékes hálózatba a támadó gépére



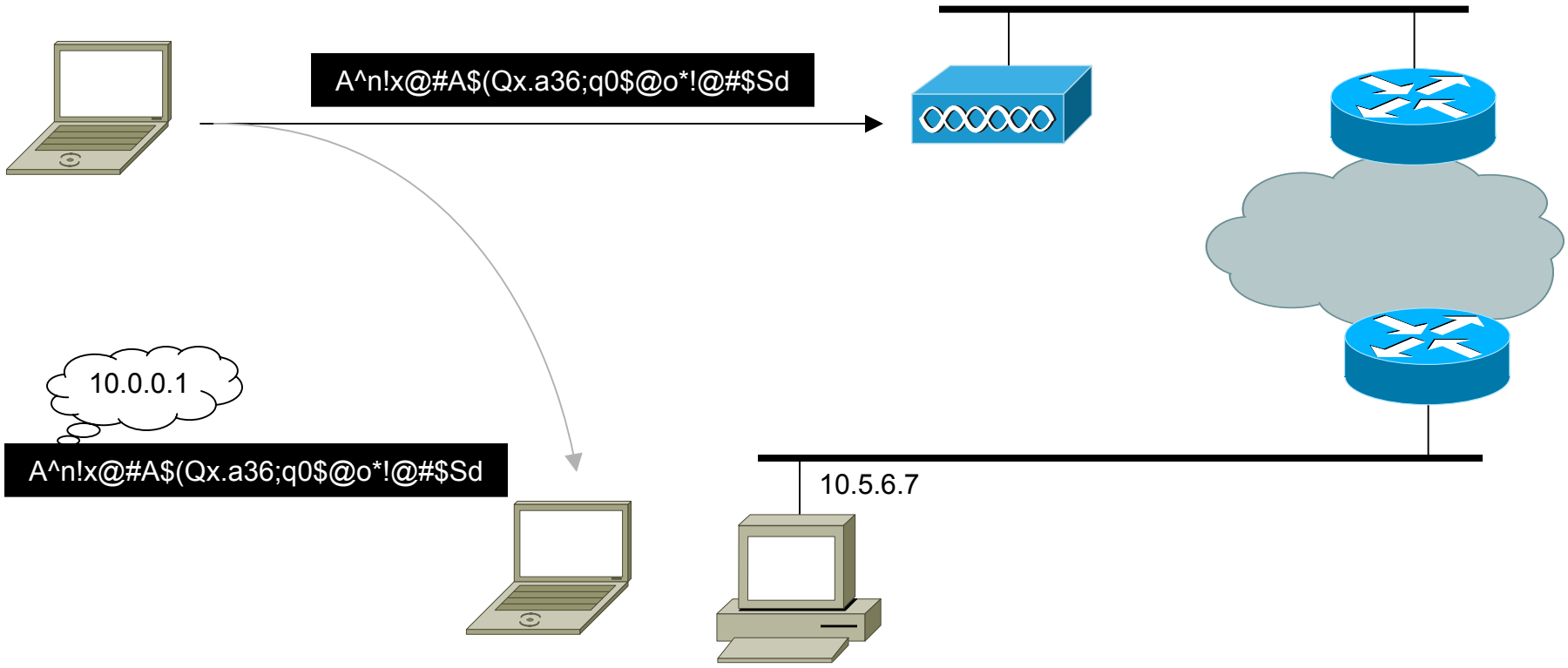
Bit flipping támadás 1.

- eltérítés
  - IP cél cím megváltoztatása saját vezetékes hálózati gép címére
  - az access point dekódolja a visszajátszott keretet
  - majd továbbküldi a vezetékes hálózatba a támadó gépére



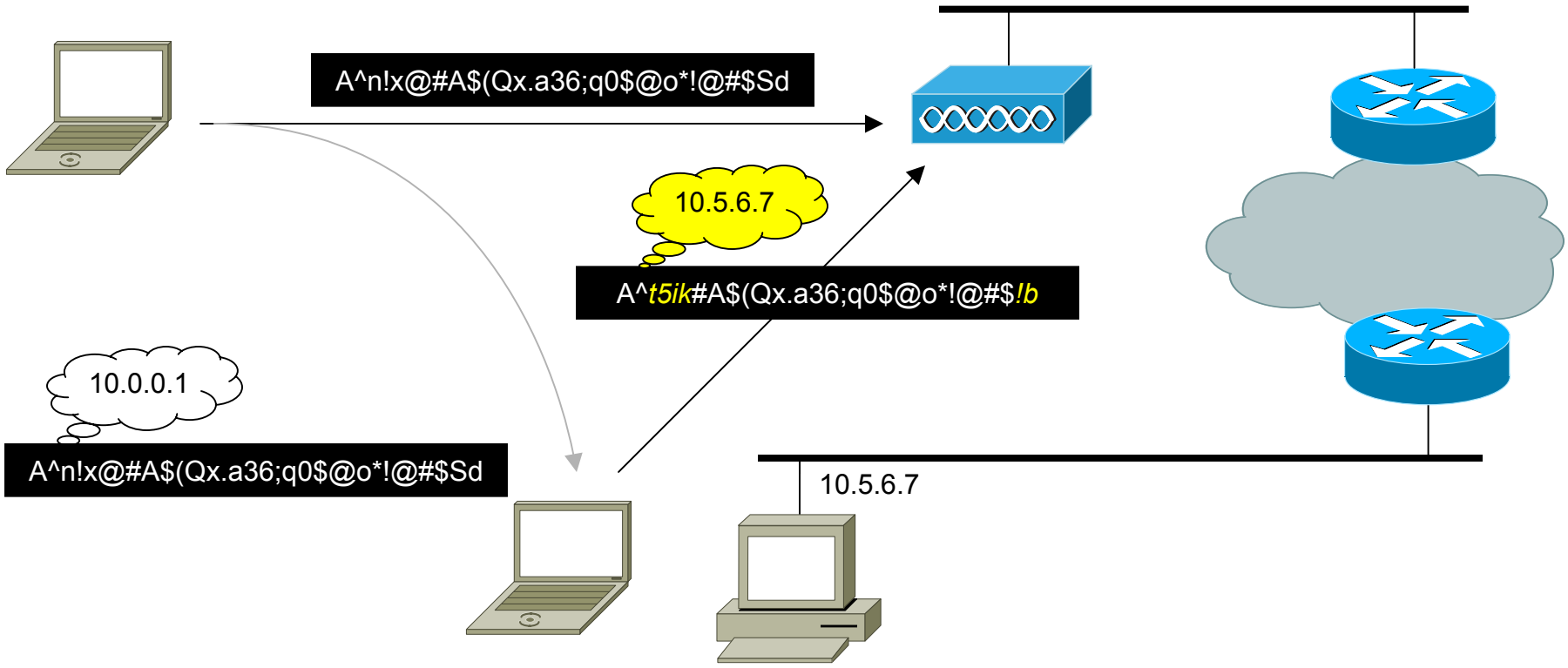
Bit flipping támadás 1.

- eltérítés
  - IP cél cím megváltoztatása saját vezetékes hálózati gép címére
  - az access point dekódolja a visszajátszott keretet
  - majd továbbküldi a vezetékes hálózatba a támadó gépére



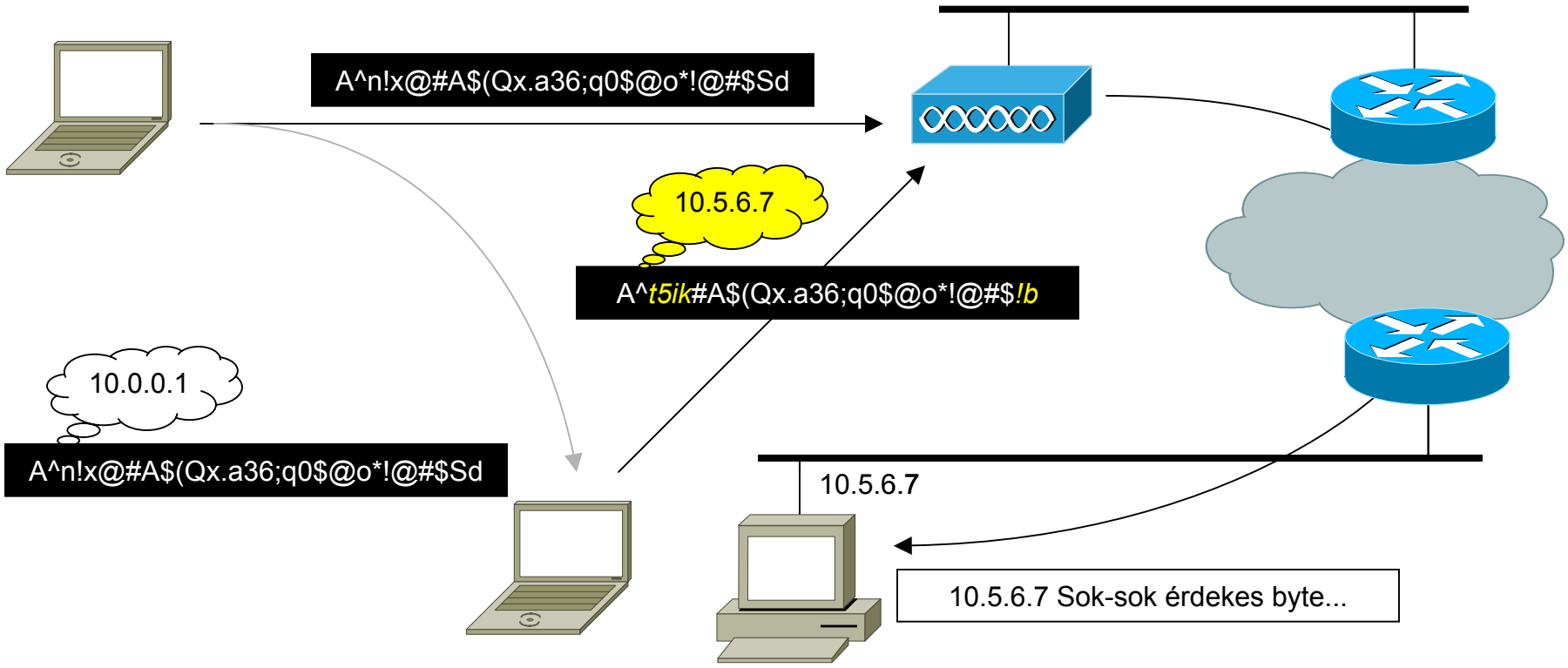
Bit flipping támadás 1.

- eltérítés
  - IP cél cím megváltoztatása saját vezetékes hálózati gép címére
  - az access point dekódolja a visszajátszott keretet
  - majd továbbküldi a vezetékes hálózatba a támadó gépére



Bit flipping támadás 1.

- eltérítés
  - IP cél cím megváltoztatása saját vezetékes hálózati gép címére
  - az access point dekódolja a visszajátszott keretet
  - majd továbbküldi a vezetékes hálózatba a támadó gépére

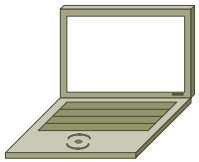


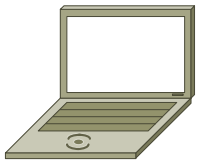
Bit flipping támadás 2.

- layer 3 hiba generálása
  - lehallgatott IP csomag elrontás utáni visszajátszása
  - a vezetékes hálózatból jól megbecsülhető hibaüzenet jön vissza
  - titkosított hibaüzenet lehallgatása, majd XOR-olása a megtippelt nyílt hibaüzenettel

Bit flipping támadás 2.

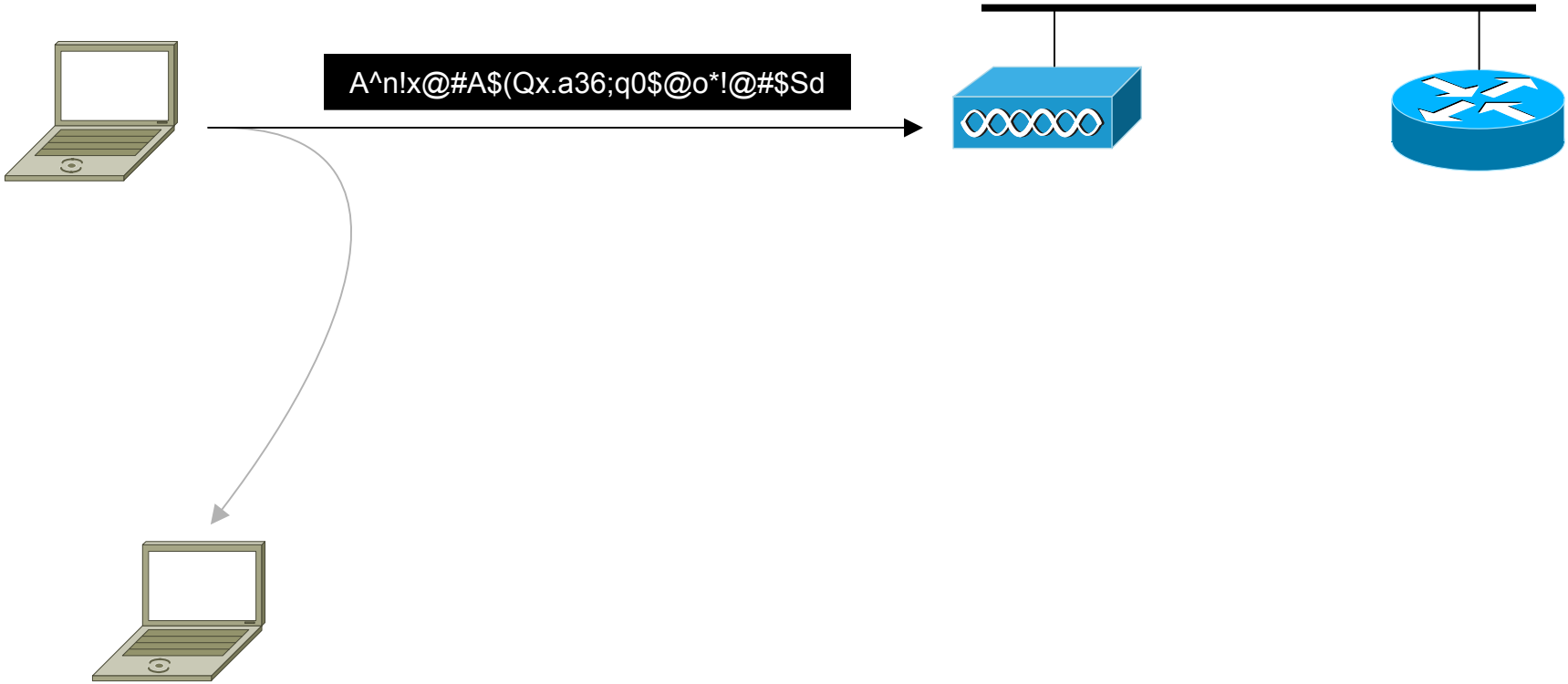
- layer 3 hiba generálása
  - lehallgatott IP csomag elrontás utáni visszajátszása
  - a vezetékes hálózatból jól megbecsülhető hibaüzenet jön vissza
  - titkosított hibaüzenet lehallgatása, majd XOR-olása a megtippelt nyílt hibaüzenettel





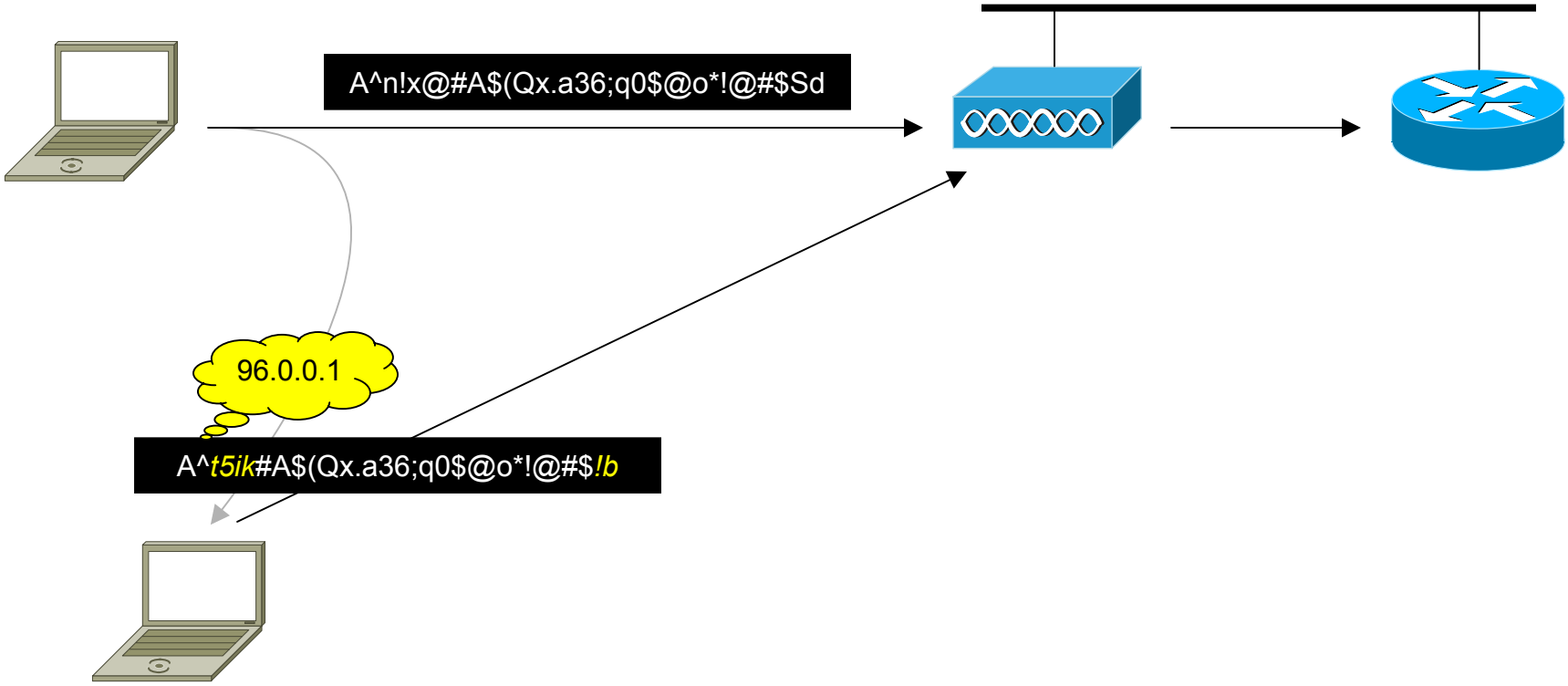
Bit flipping támadás 2.

- layer 3 hiba generálása
  - lehallgatott IP csomag elrontás utáni visszajátszása
  - a vezetékes hálózatból jól megbecsülhető hibaüzenet jön vissza
  - titkosított hibaüzenet lehallgatása, majd XOR-olása a megtippelt nyílt hibaüzenettel



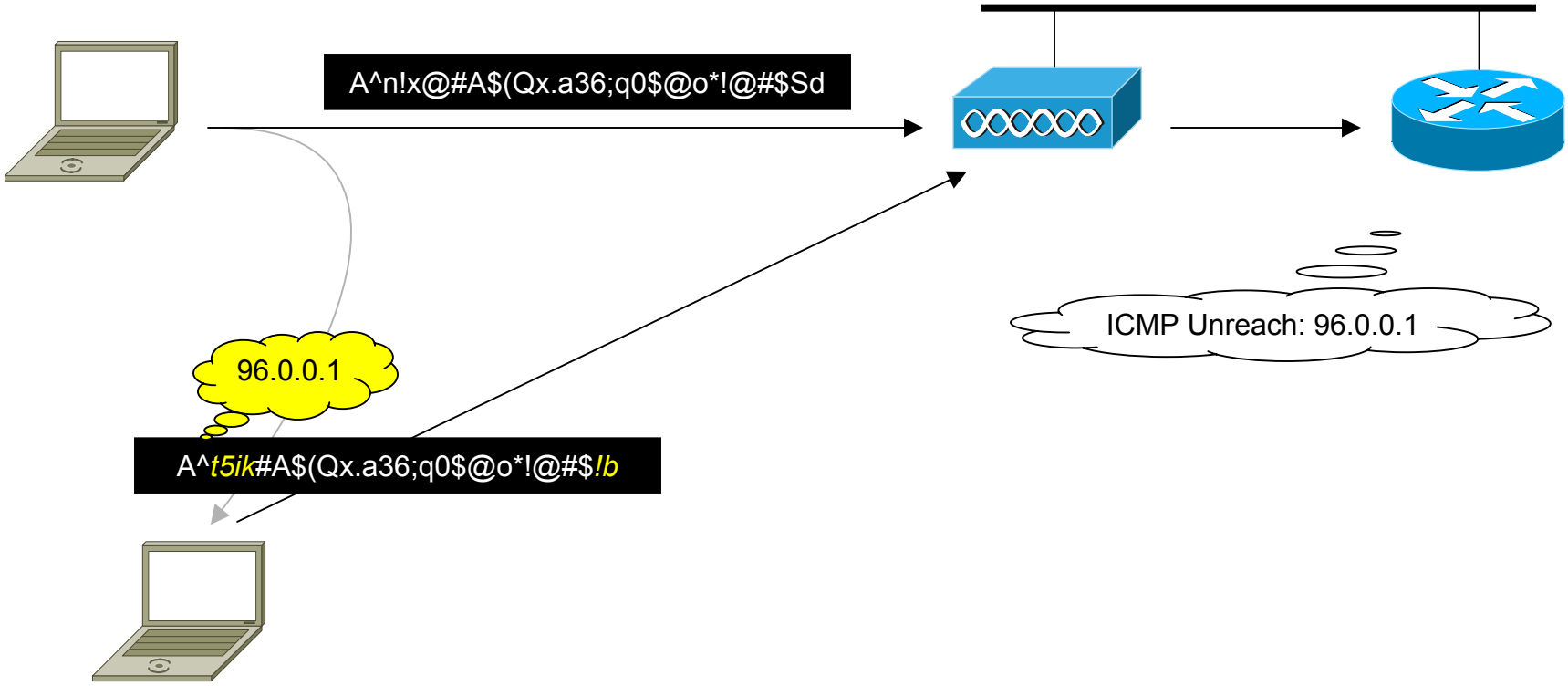
Bit flipping támadás 2.

- layer 3 hiba generálása
  - lehallgatott IP csomag elrontás utáni visszajátszása
  - a vezetékes hálózatból jól megbecsülhető hibaüzenet jön vissza
  - titkosított hibaüzenet lehallgatása, majd XOR-olása a megtippelt nyílt hibaüzenettel



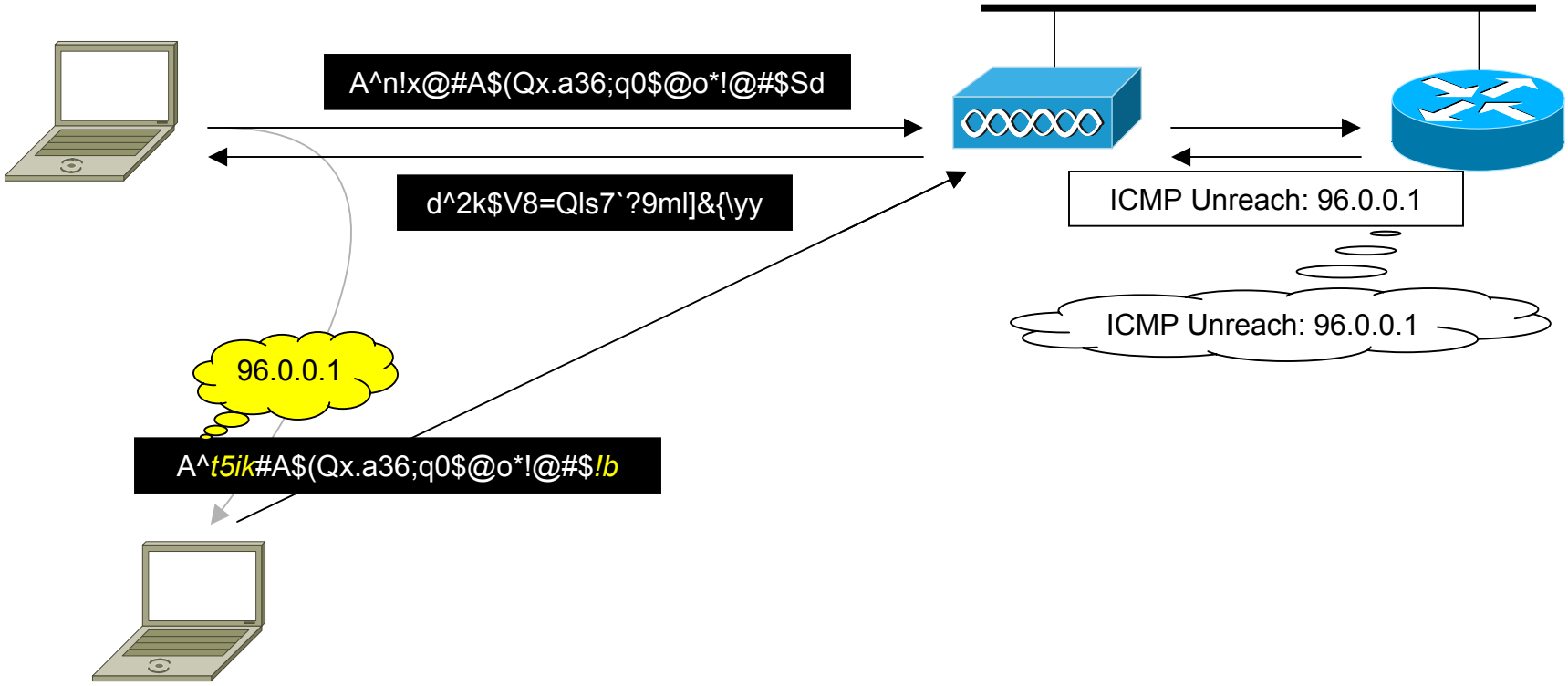
Bit flipping támadás 2.

- layer 3 hiba generálása
  - lehallgatott IP csomag elrontás utáni visszajátszása
  - a vezetékes hálózatból jól megbecsülhető hibaüzenet jön vissza
  - titkosított hibaüzenet lehallgatása, majd XOR-olása a megtippelt nyílt hibaüzenettel



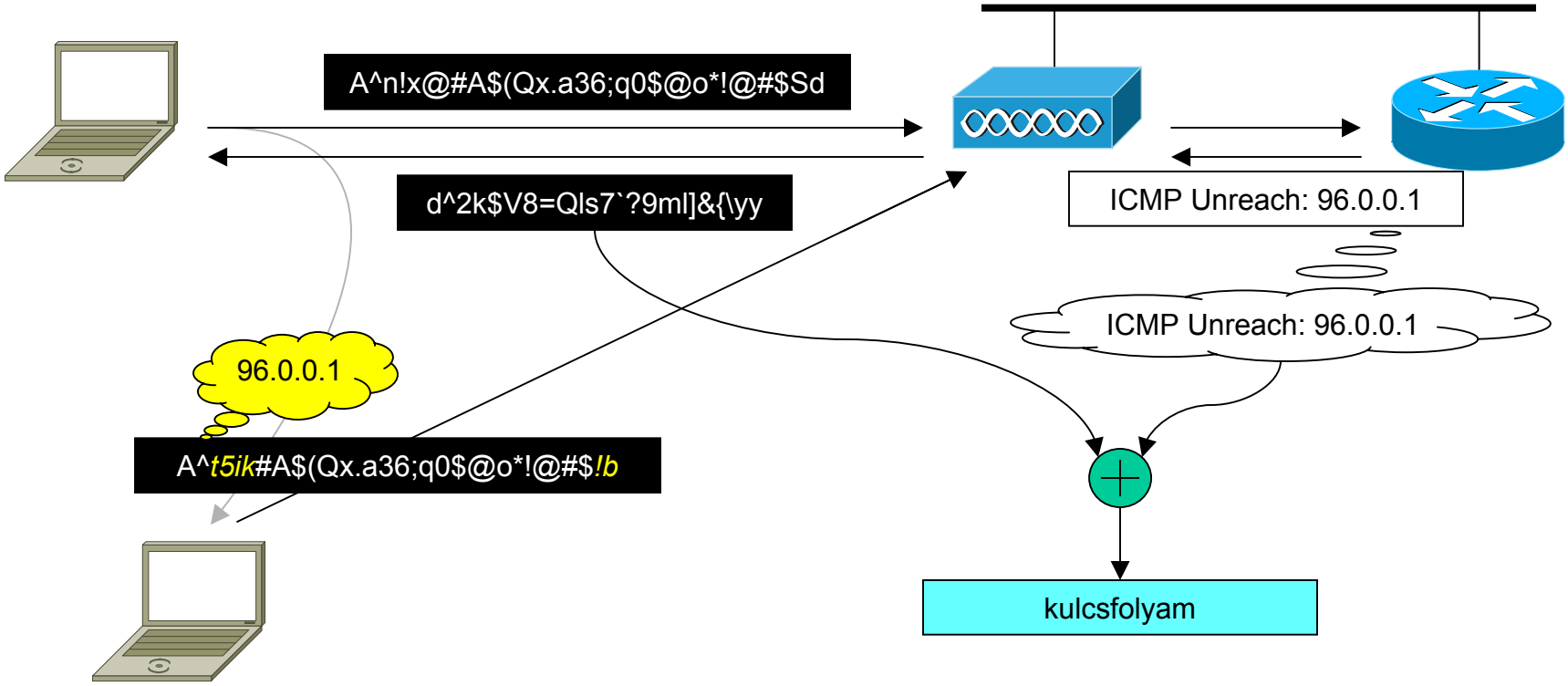
Bit flipping támadás 2.

- layer 3 hiba generálása
  - lehallgatott IP csomag elrontás utáni visszajátszása
  - a vezetékes hálózatból jól megbecsülhető hibaüzenet jön vissza
  - titkosított hibaüzenet lehallgatása, majd XOR-olása a megtippelt nyílt hibaüzenettel



Bit flipping támadás 2.

- layer 3 hiba generálása
  - lehallgatott IP csomag elrontás utáni visszajátszása
  - a vezetékes hálózatból jól megbecsülhető hibaüzenet jön vissza
  - titkosított hibaüzenet lehallgatása, majd XOR-olása a megtippelt nyílt hibaüzenettel



Gyenge RC4 IV-k

- 2001. aug.: Scott Fluhrer, Itsik Mantin és Adi Shamir
- bizonyos gyenge IV-k esetén a kulcsfolyam elejéből következtetni lehet kulcsbitekre
  - a kulcsfolyam eleje általában ismert, hiszen a nyílt keret elejét könnyű megtippelni
- titkosított keretek lehallgatásával kitalálható a WEP kulcs
- általában 4-10 millió keret szükséges
  - néhány óra egy közepesen kihasznált 802.11b hálózaton
- WEPCrack, AirSnort

Agenda

Biztonság

802.11 titkosítás

WEP problémák

Megoldás a WEP problémáira

802.11 autentikáció

Autentikációs problémák

Autentikációs megoldások

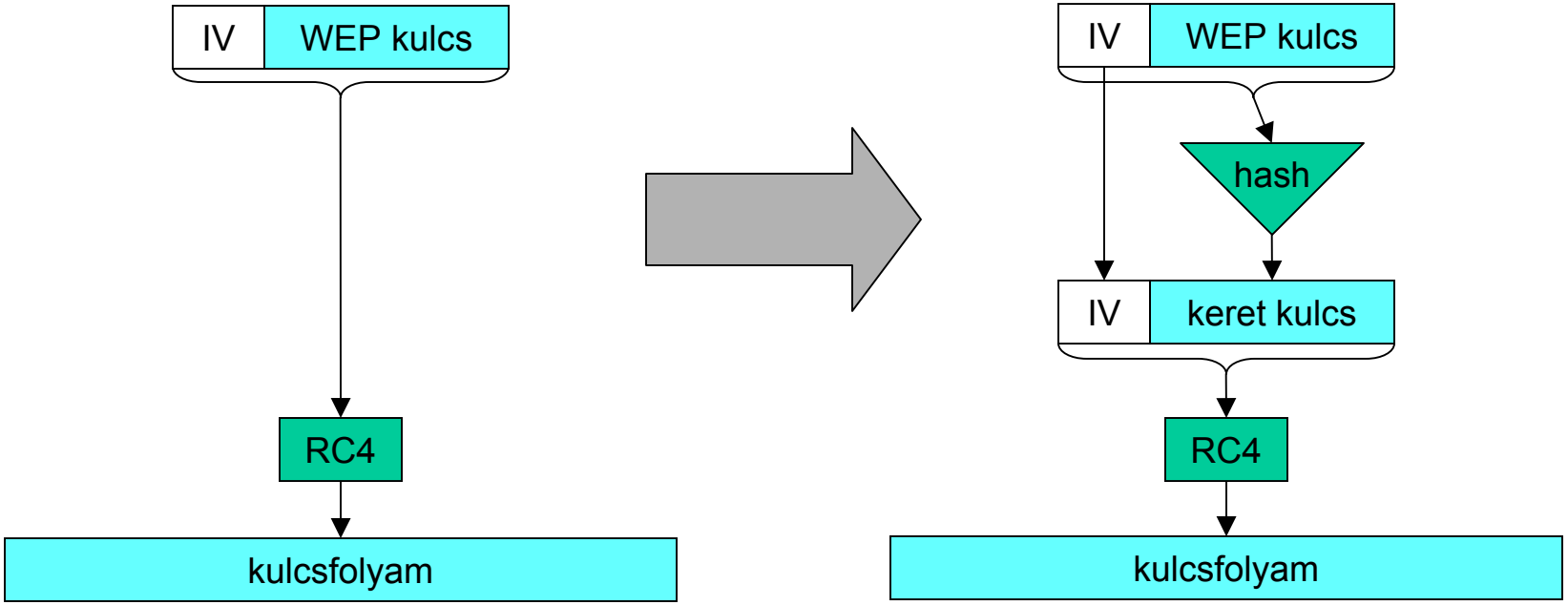
802.11i

Megoldás a WEP problémáira

- állomásonként különböző WEP kulcs használata
- WEP kulcs gyakori cseréje
  - 802.1x + RADIUS session timeout + reauthentication
- IV nem közvetlenül része az RC4 bemenetnek
  - TKIP per-packet keying
- kriptográfiailag erős integritásellenőrző kód CRC helyett
  - TKIP MIC

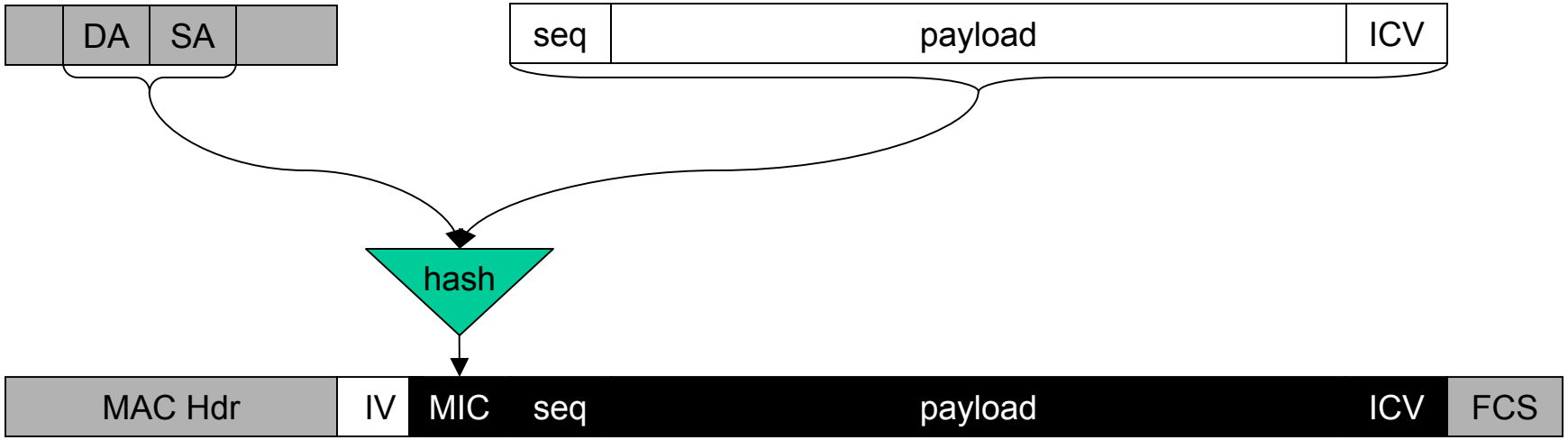
Temporal Key Integrity Protocol

- per-packet keying
  - hash függvény segítségével keretenként különböző RC4 bemenet
    - az RC4 teljes bemenete változik, nem csak az IV 24 bitje
  - így is csak 2^{24} különböző kulcsfolyam létezik egy WEP kulcshoz
    - a WEP kulcsot TKIP használatakor is cserélni kell rendszeresen
  - a Fluhrer-Mantin-Shamir támadás így hatástalan



TKIP (folyt.)

- 48 bites IV (24 helyett)
- MIC – Message Integrity Check
  - keretek sorszámozása visszajátszás ellen
  - integritásellenőrző összeg kriptográfiailag erős hash függvénnyel
    - 32 bites MMH
    - DA, SA, seq, payload



Agenda

Biztonság

802.11 titkosítás

WEP problémák

Megoldás a WEP problémáira

802.11 autentikáció

Autentikációs problémák

Autentikációs megoldások

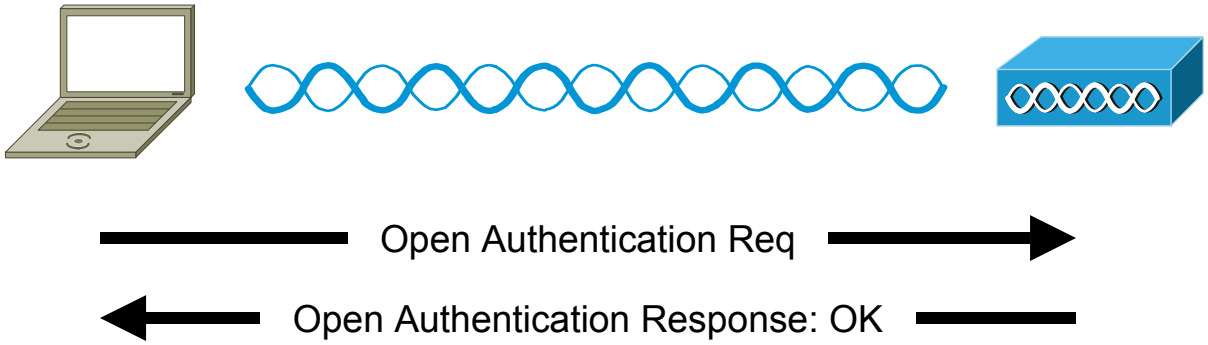
802.11i

SSID

- csak kitöltött SSID mezőjű Association Request
  - broadcast (üres) SSID nem elég
- Beacon keretekből az SSID kihagyása
  - nem szabványos
  - úgyis le lehet hallgatni az SSID-t más menedzsment keretekből
- az SSID nem autentikációra való

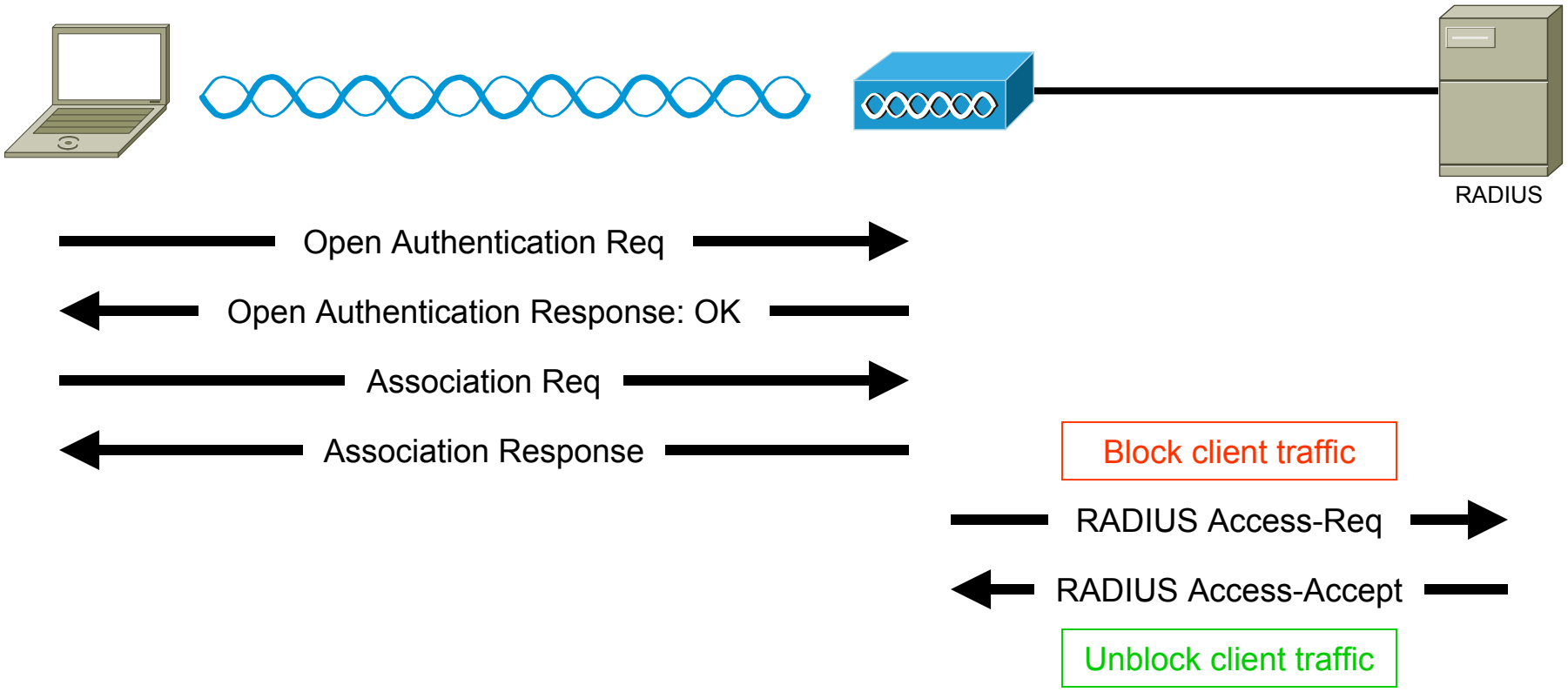
Nyílt autentikáció

- Open Authentication
- gyakorlatilag nincs autentikáció, csak formálisan



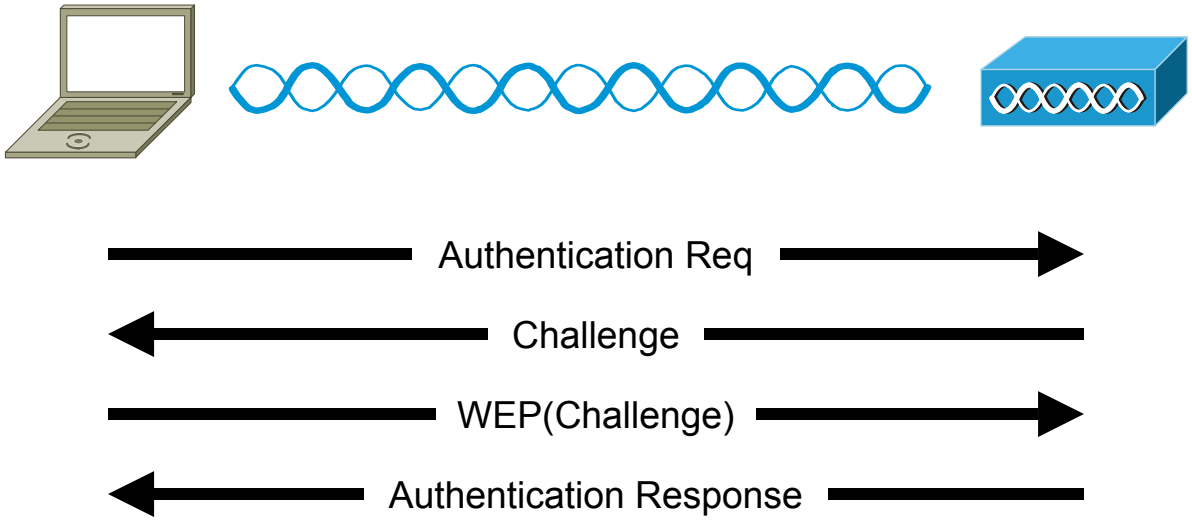
MAC cím autentikáció

- nyílt autentikáció kiegészítve a MAC cím ellenőrzéssel
- megengedett MAC addressek listája
  - lokálisan az access pointban
  - RADIUS/TACACS+ serveren



Közös kulcsos autentikáció

- Shared Key authentication
- véletlen Challenge kódolása mindkét fél által ismert titkos kulccsal
- kétirányú autentikáció újabb 4 üzenettel, a szerepek felcserélésével lehetséges



Agenda

Biztonság

802.11 titkosítás

WEP problémák

Megoldás a WEP problémáira

802.11 autentikáció

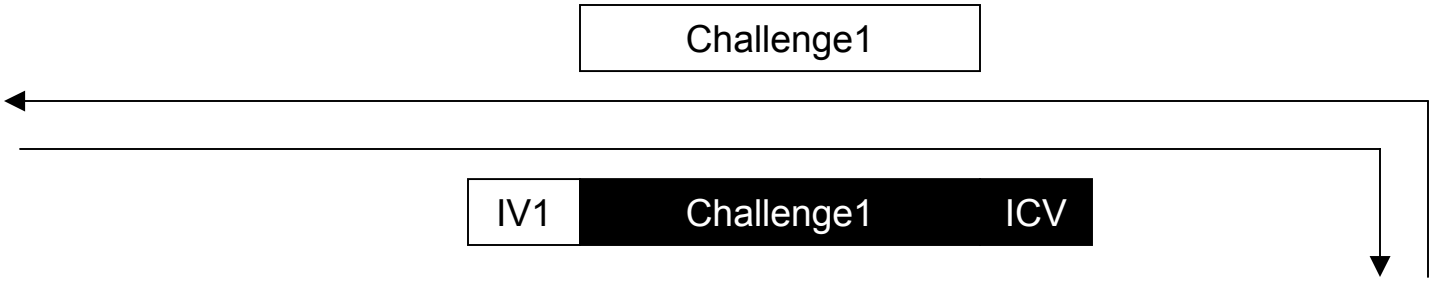
Autentikációs problémák

Autentikációs megoldások

802.11i

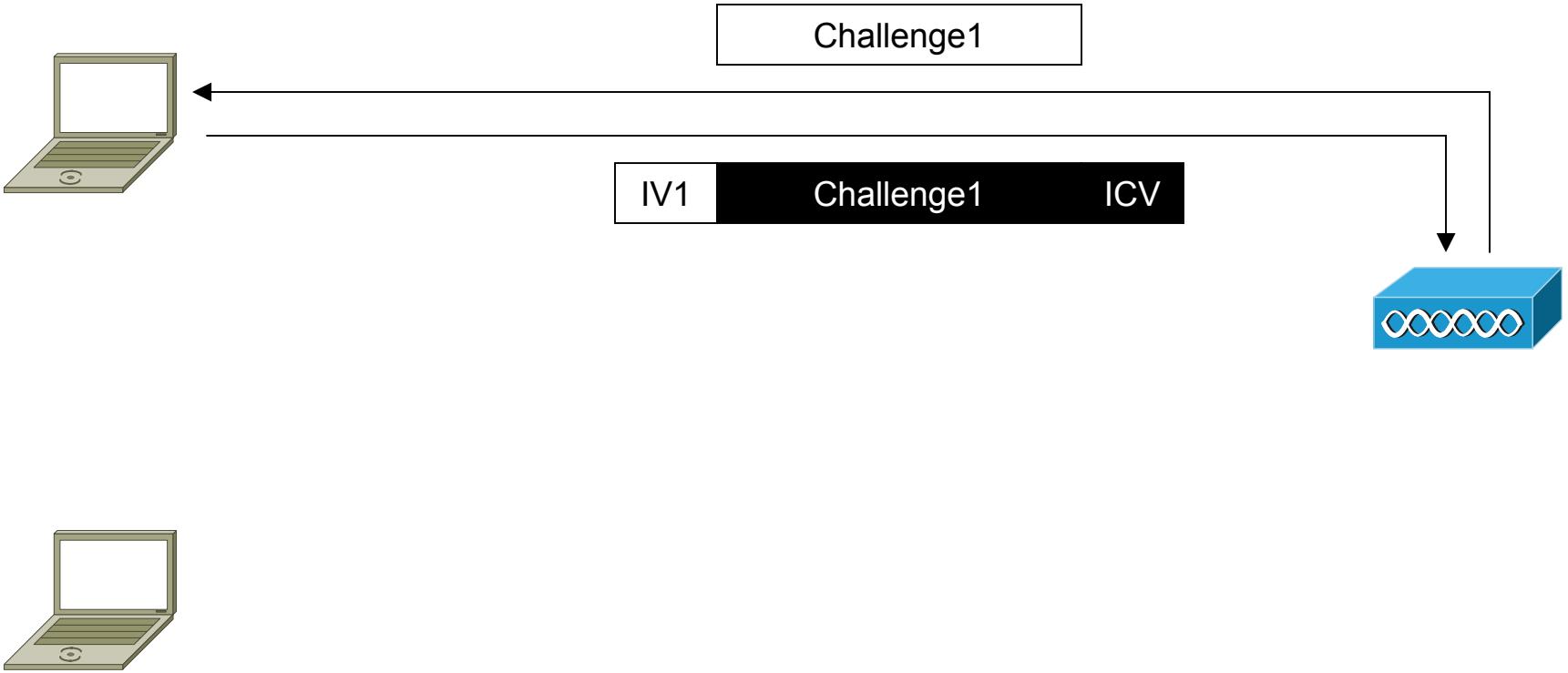
Problémák az autentikációval

- MAC cím alapú: MAC cím megváltoztatható, hamisítható
- közös kulcsos: lehallgatás után könnyen átverhető



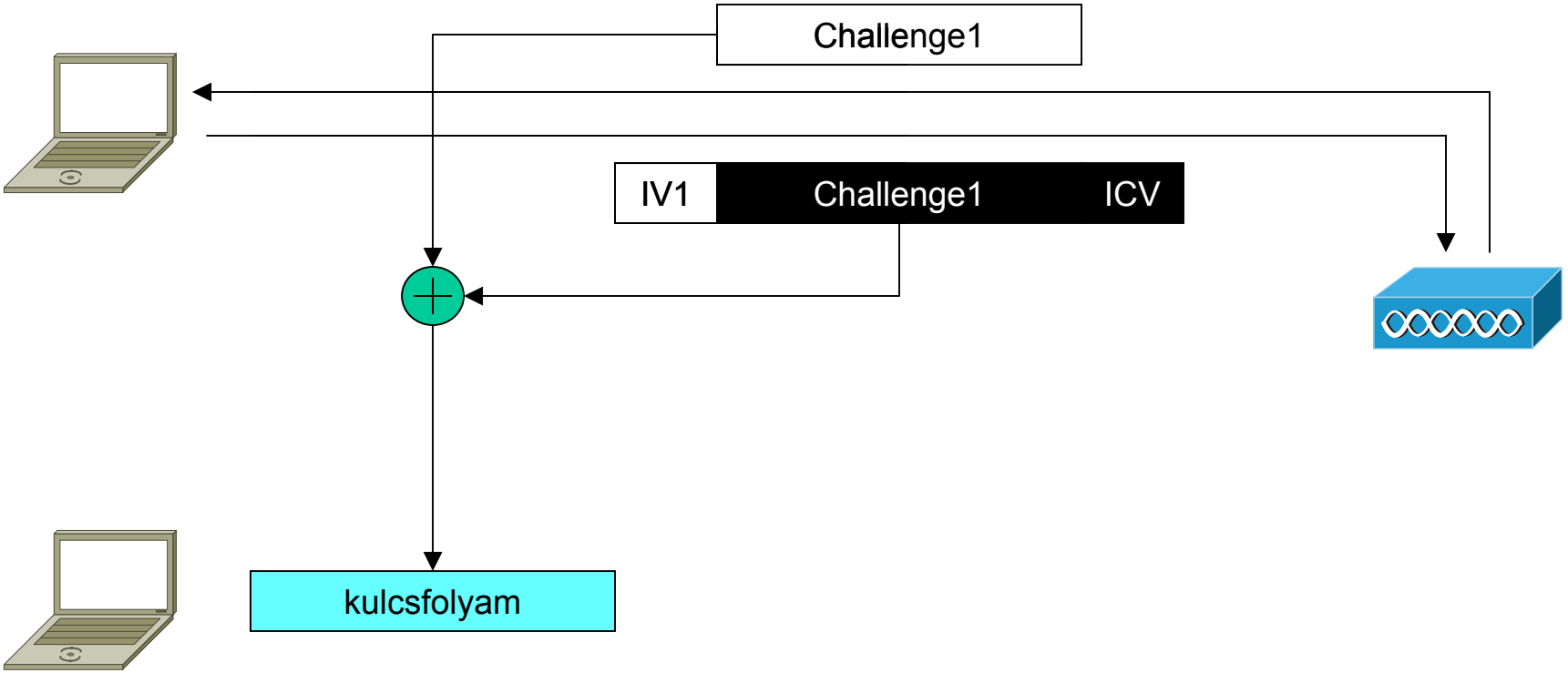
Problémák az autentikációval

- MAC cím alapú: MAC cím megváltoztatható, hamisítható
- közös kulcsos: lehallgatás után könnyen átverhető



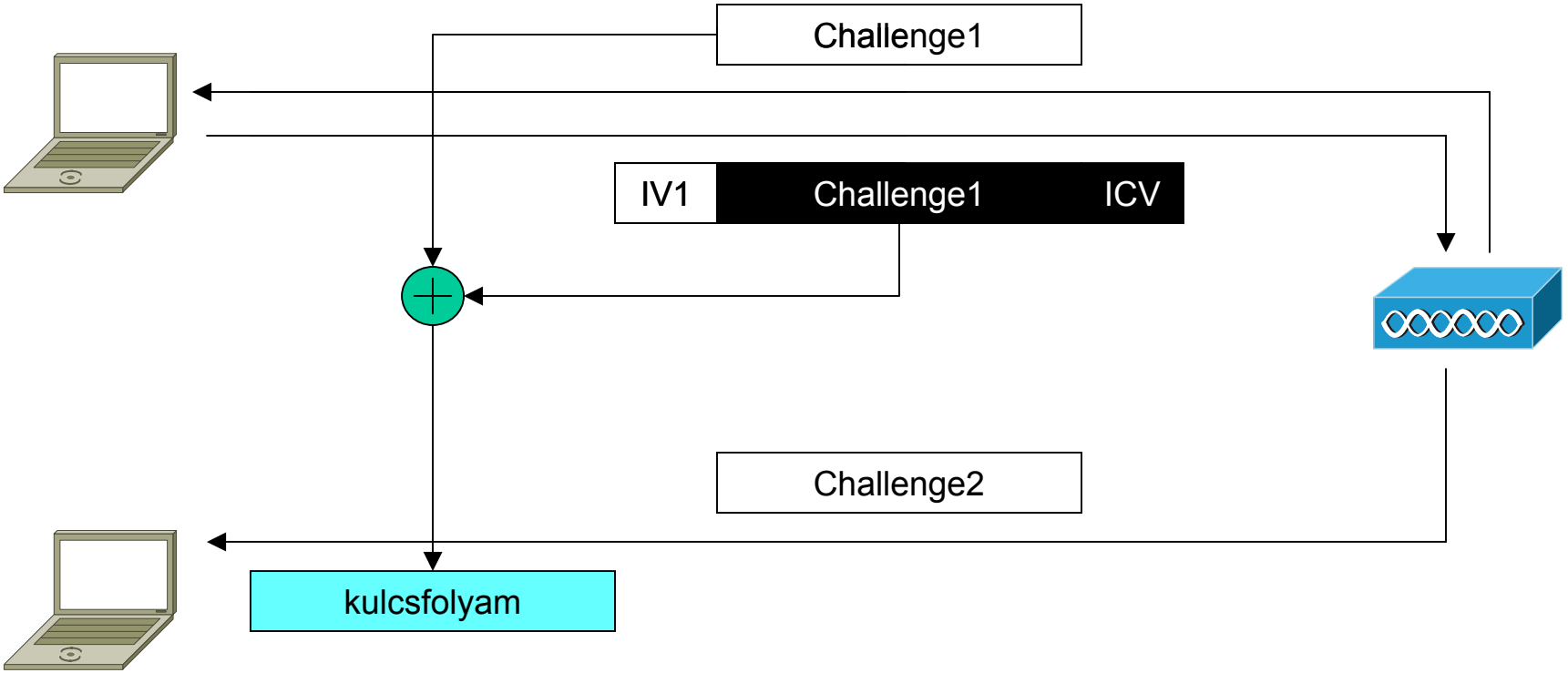
Problémák az autentikációval

- MAC cím alapú: MAC cím megváltoztatható, hamisítható
- közös kulcsos: lehallgatás után könnyen átverhető



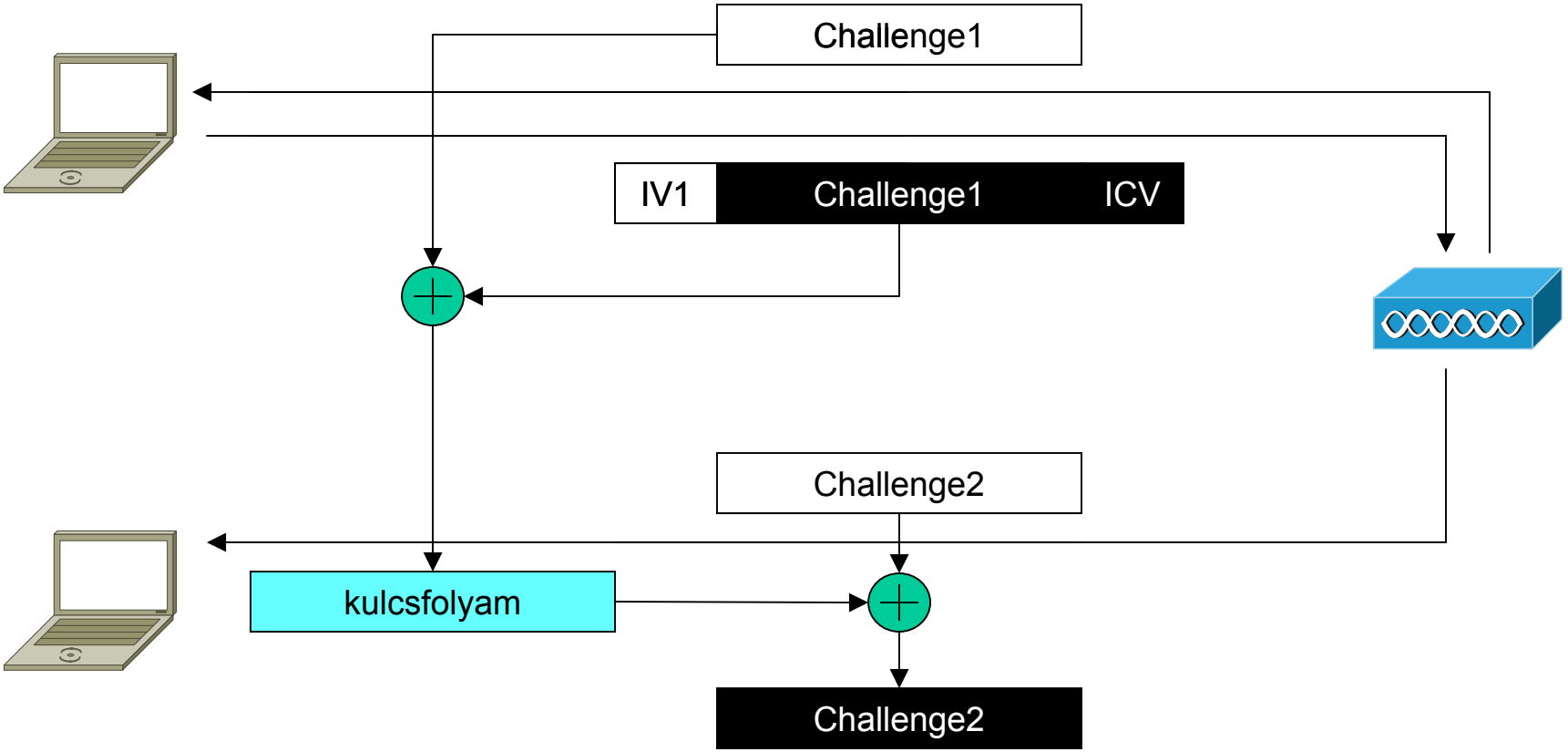
Problémák az autentikációval

- MAC cím alapú: MAC cím megváltoztatható, hamisítható
- közös kulcsos: lehallgatás után könnyen átverhető



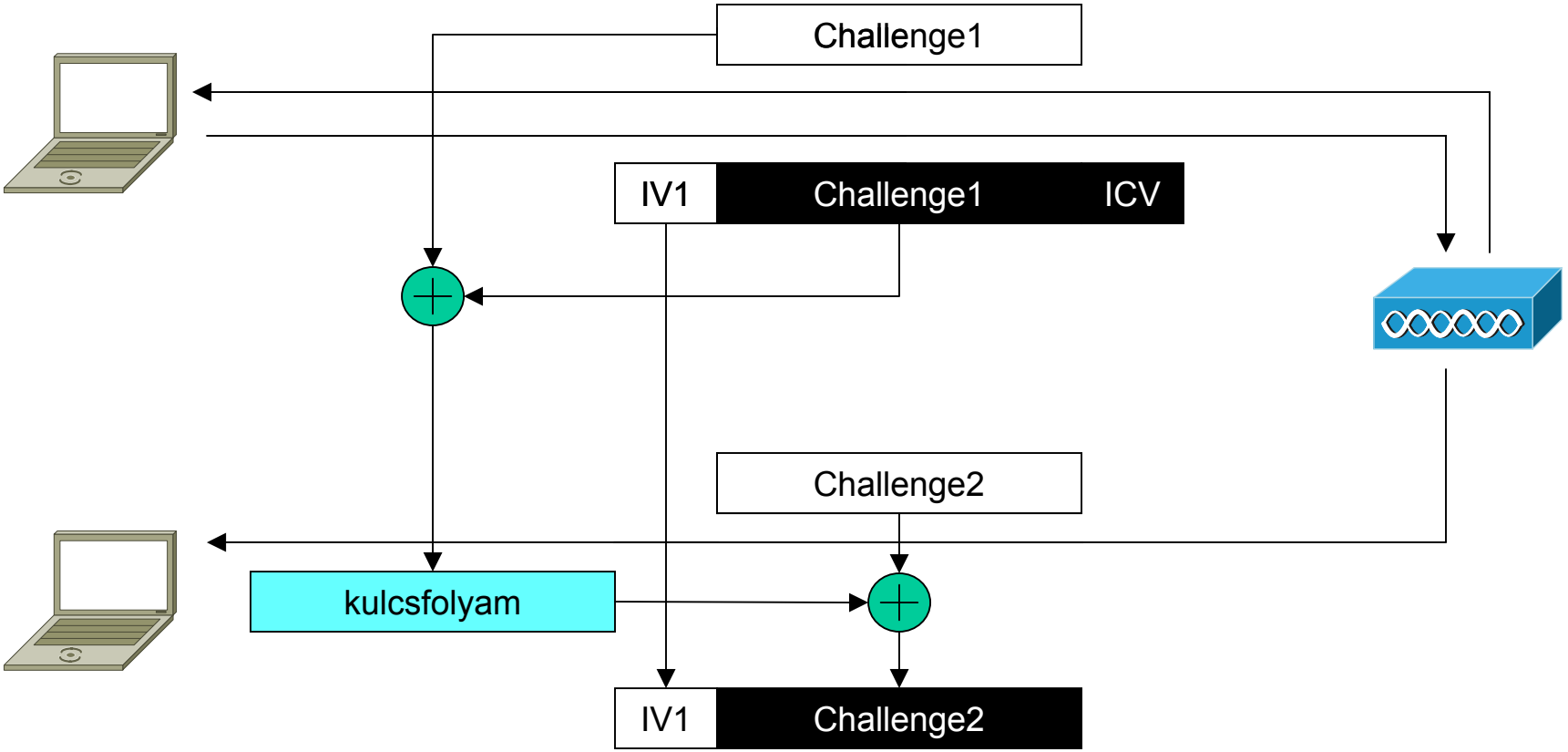
Problémák az autentikációval

- MAC cím alapú: MAC cím megváltoztatható, hamisítható
- közös kulcsos: lehallgatás után könnyen átverhető



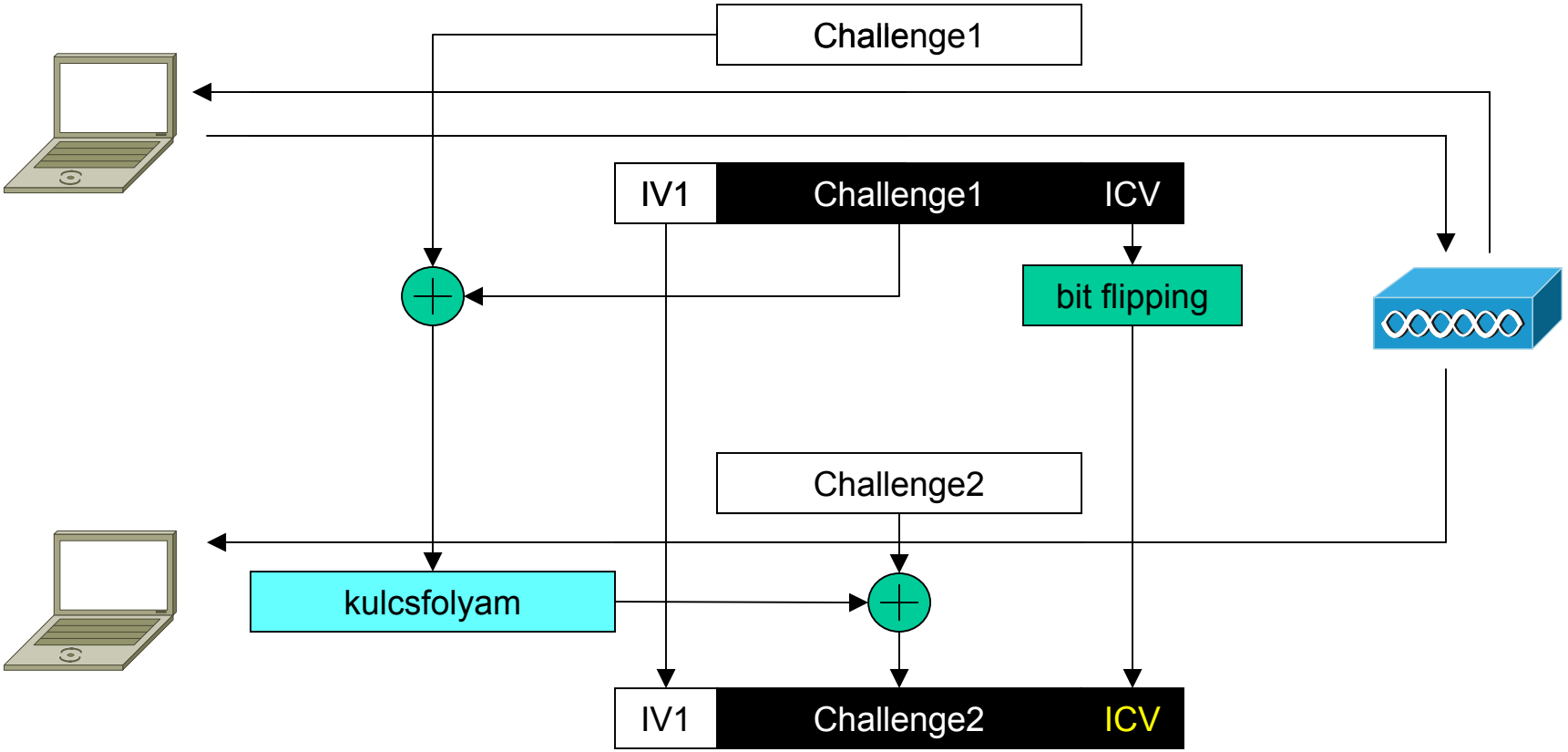
Problémák az autentikációval

- MAC cím alapú: MAC cím megváltoztatható, hamisítható
- közös kulcsos: lehallgatás után könnyen átverhető



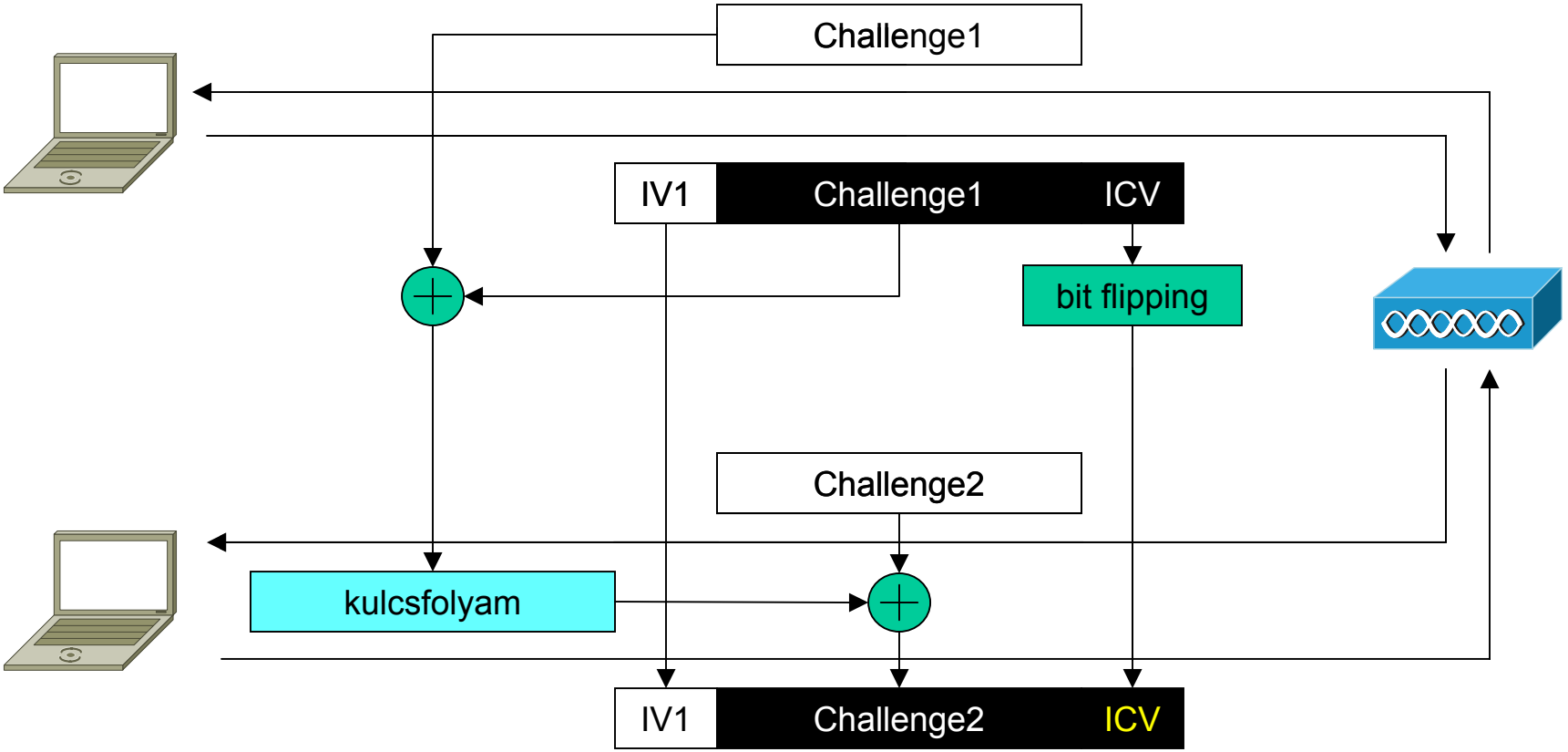
Problémák az autentikációval

- MAC cím alapú: MAC cím megváltoztatható, hamisítható
- közös kulcsos: lehallgatás után könnyen átverhető



Problémák az autentikációval

- MAC cím alapú: MAC cím megváltoztatható, hamisítható
- közös kulcsos: lehallgatás után könnyen átverhető



Agenda

Biztonság

802.11 titkosítás

WEP problémák

Megoldás a WEP problémáira

802.11 autentikáció

Autentikációs problémák

Autentikációs megoldások

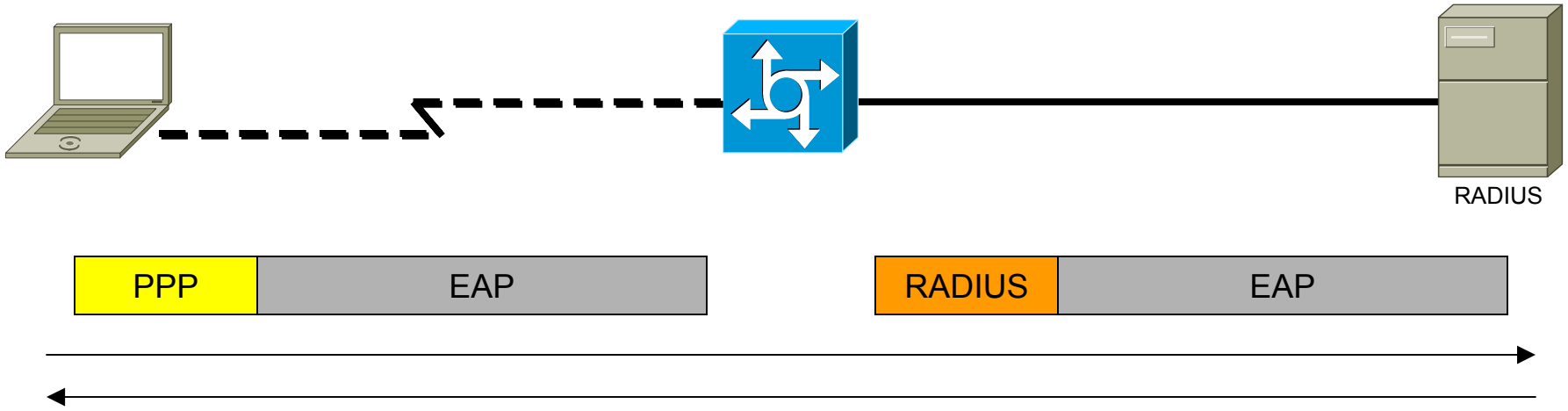
802.11i

Extensible Authentication Protocol

- eredetileg PPP autentikációs protokoll
  - PAP, CHAP, MS-CHAP, EAP…
- sokféle autentikációs metódust tesz lehetővé
  - MD5
  - OTP – One Time Password
  - GTC – Generic Token Card
  - TLS – Transport Layer Security
  - SIM – Subscriber Identity Module
  - stb.
- EAP RADIUS protokoll felett:
  - EAP-Message RADIUS attribútumban lehet átvinni

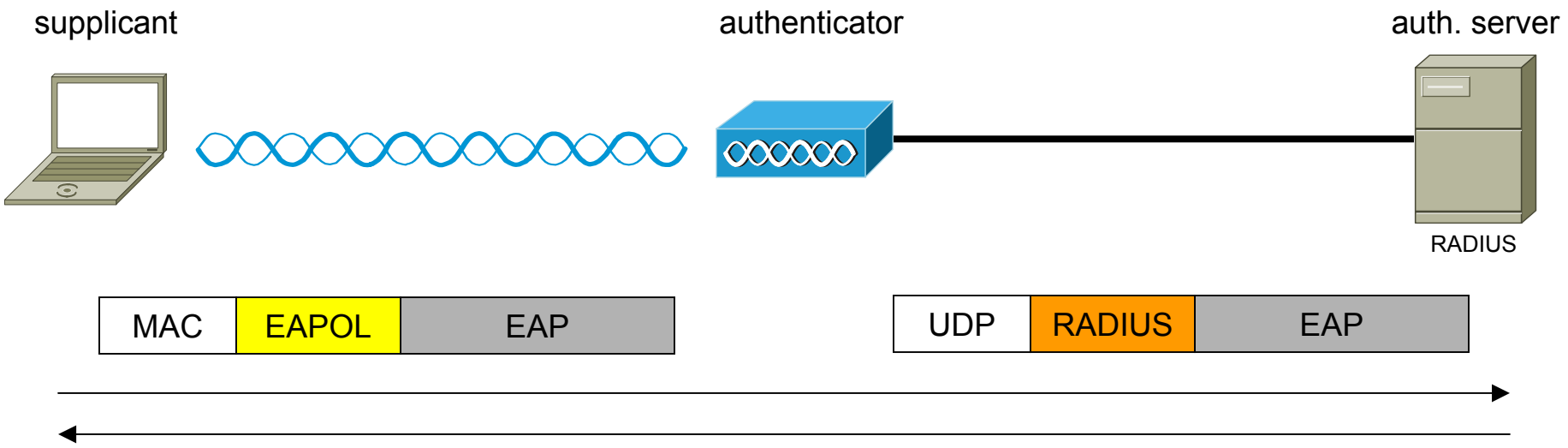
EAP (folyt.)

- az access server nem tudja, hogy mi van az EAP üzenetekben
  - csak után átrakja a PPP keretekből a RADIUS csomagokba és fordítva
- ettől rugalmas az EAP
  - a hordozó protokollhoz (PPP, RADIUS, stb.) csak egyszer kell hozzányúlni
  - új autentikációs mechanizmus később könnyen hozzáadható a rendszerhez



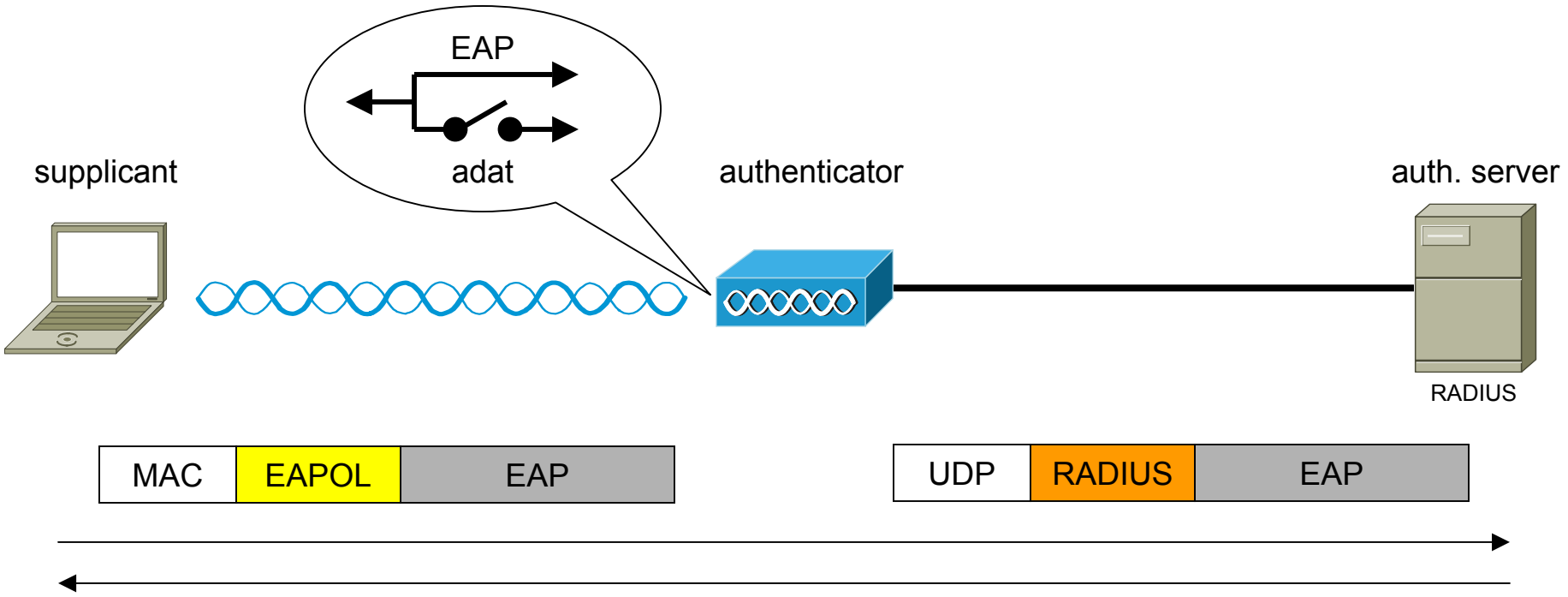
IEEE 802.1x

- EAPOL – EAP over LANs
  - EAP csomagok átvitele 802.3 LAN-ok adatkapcsolati rétege felett
- szereplők:
  - supplicant – hozzá akar férni a hálózathoz
  - authenticator – ellenőrizni akarja a supplicant jogosultságát
  - authentication server – az authenticator számára ellenőrzi a supplicant jogosultságát

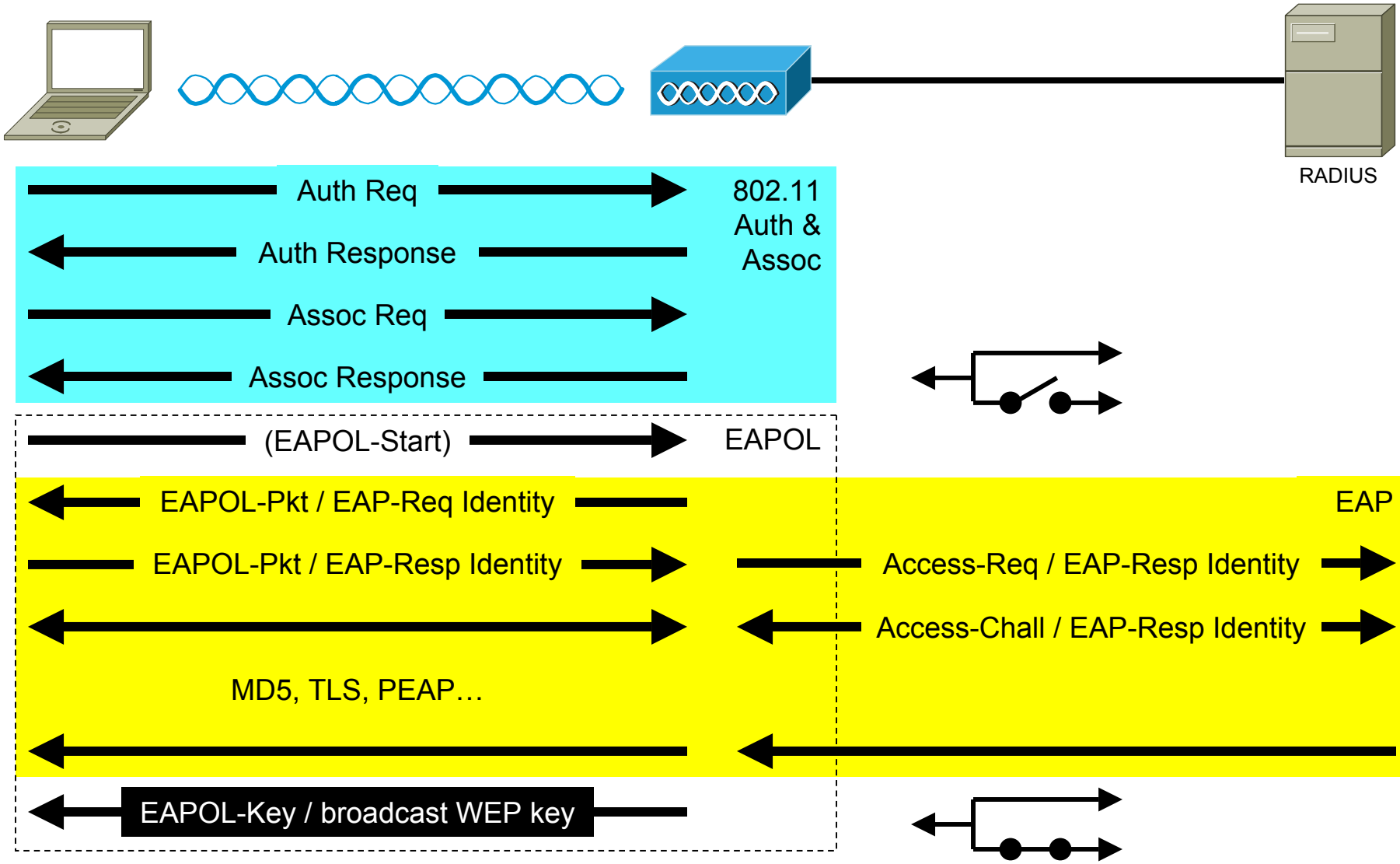


IEEE 802.1x (folyt.)

- amíg a supplicant azonossága nincs igazolva, addig az authenticator csak EAP forgalmat enged át a supplicant portján
  - WLAN esetén ez az Association ID-hez rendelt virtuális port

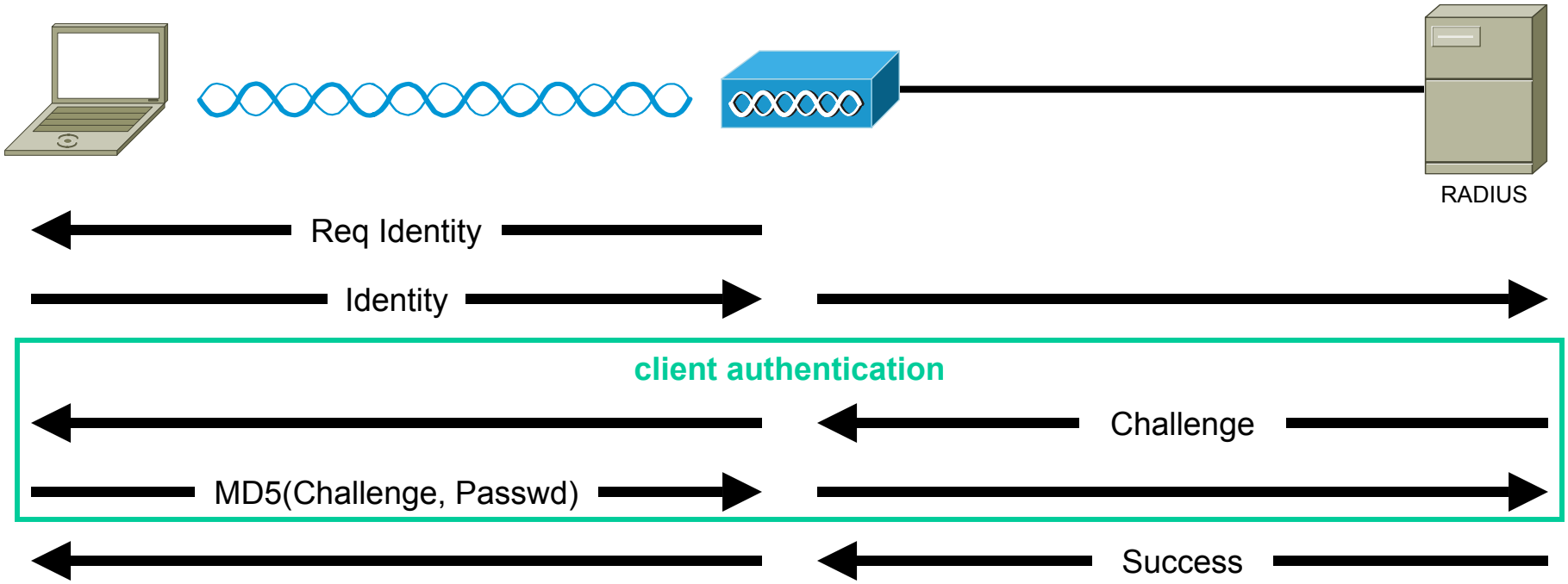


WLAN + EAP


RADIUS
Auth Req
Auth Response
Assoc Req
Assoc Response
802.11
Auth &
Assoc
(EAPOL-Start)
EAPOL
EAPOL-Pkt / EAP-Req Identity
EAPOL-Pkt / EAP-Resp Identity
Access-Req / EAP-Resp Identity
Access-Chall / EAP-Resp Identity
EAP
MD5, TLS, PEAP…
EAPOL-Key / broadcast WEP key

EAP-MD5

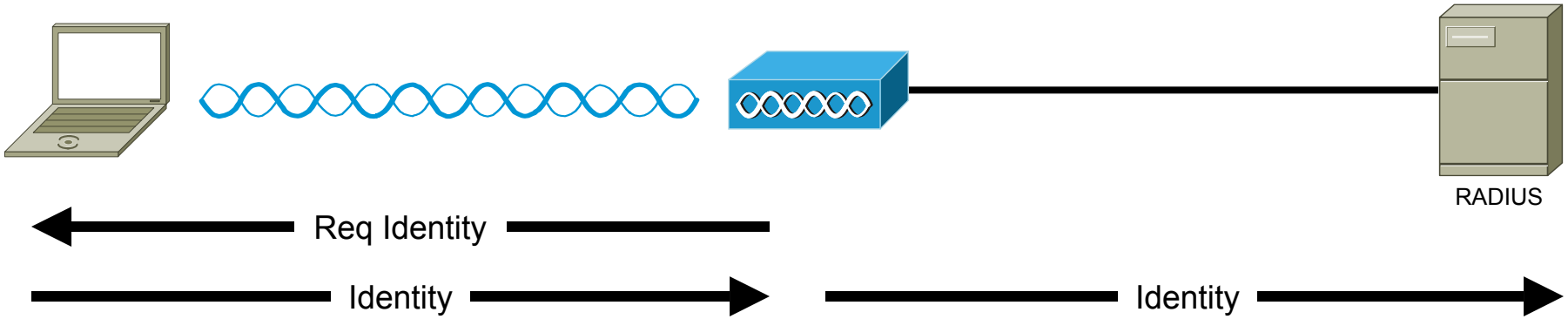
- csak a klienst autentikálja
- nem teszi lehetővé a dinamikus WEP kulcs használatát



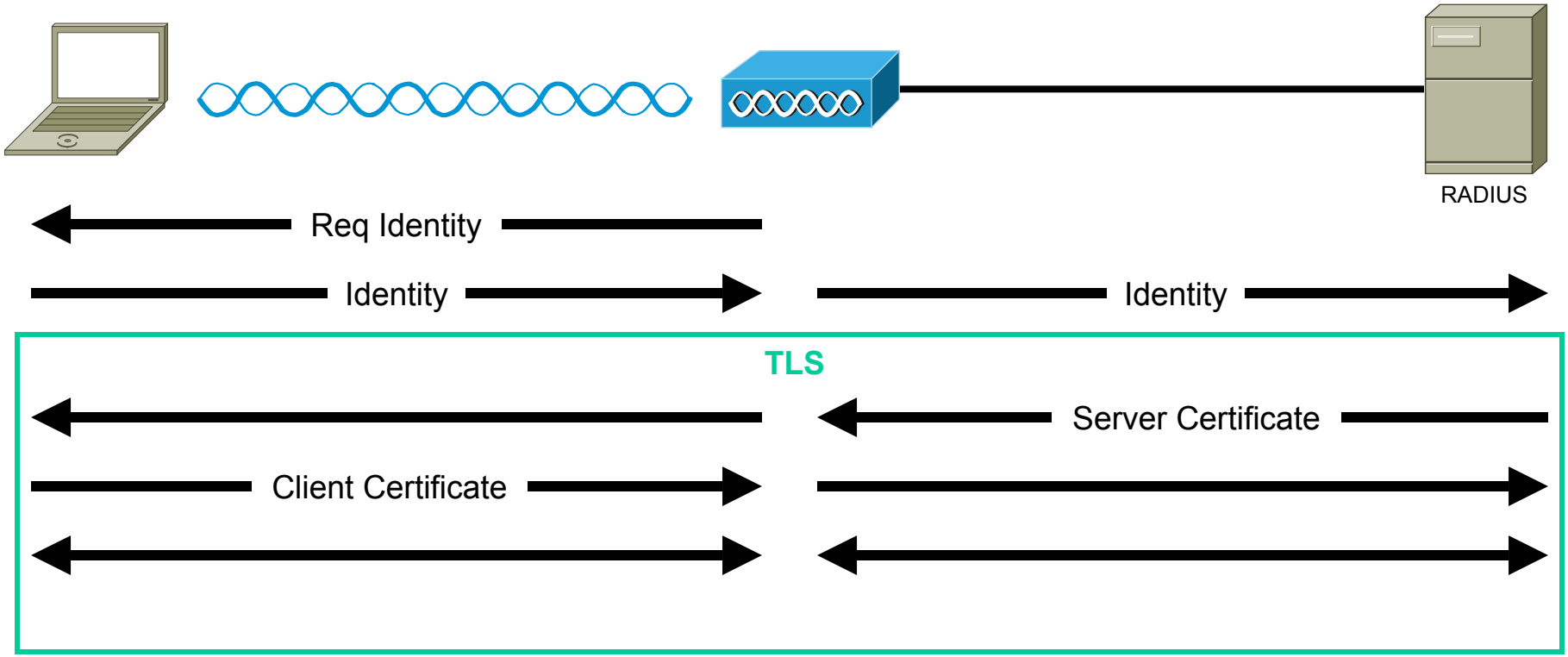
EAP-TLS

- TLS – Transport Layer Security
  - az SSL utódja, HTTP+TLS = https://
- kölcsönös autentikáció
  - digitális tanúsítványok segítségével
  - az összes kliensnek saját digitális tanúsítványra van szüksége
    - nehézkes lehet az adminisztrációja

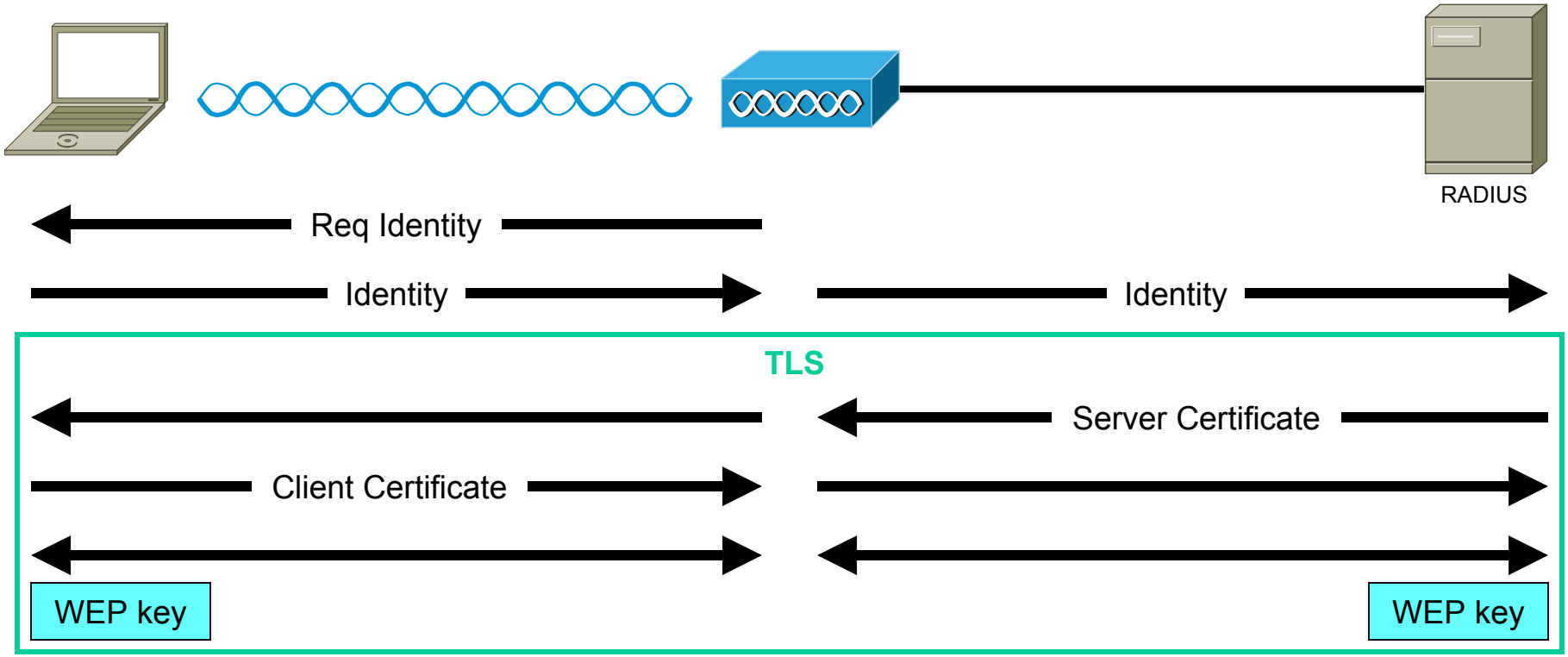
EAP-TLS (folyt.)



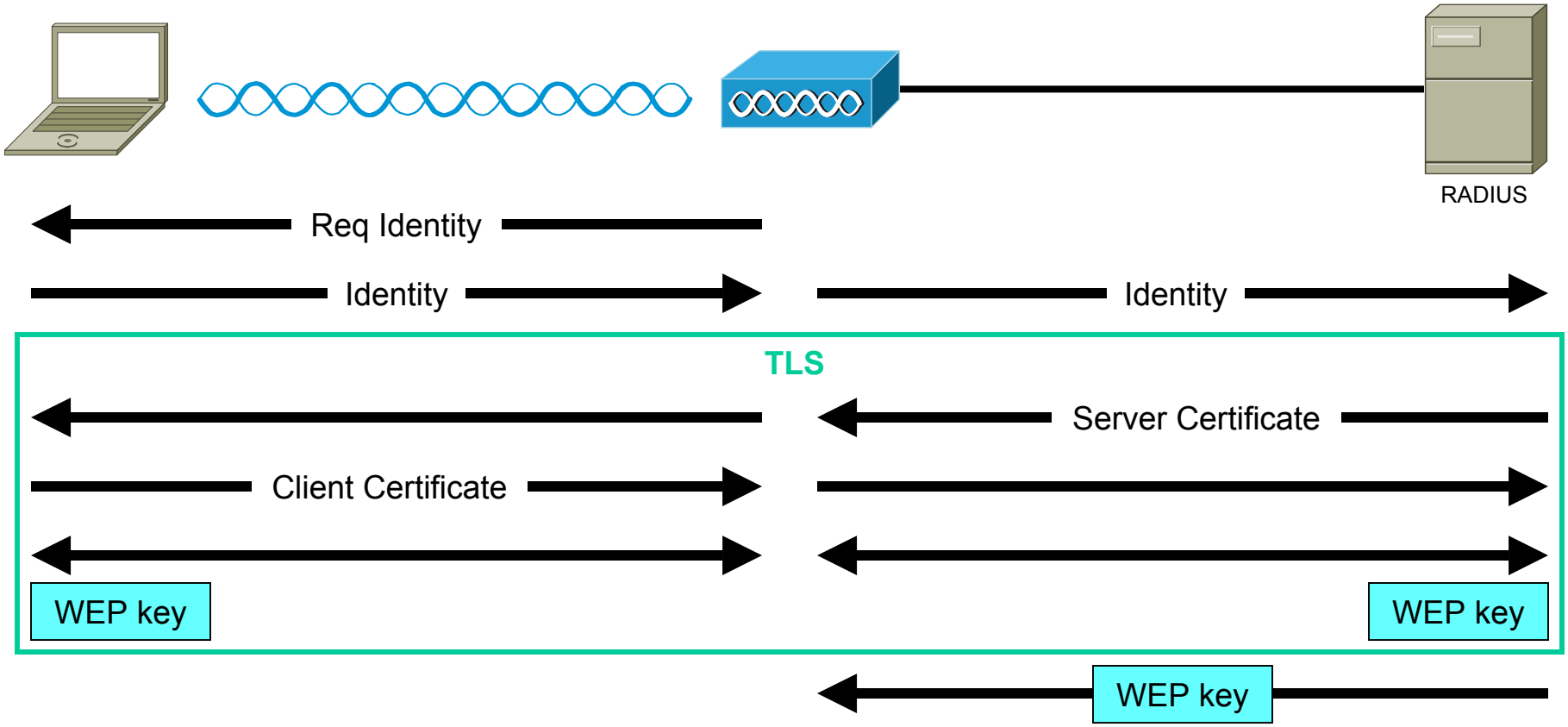
EAP-TLS (folyt.)



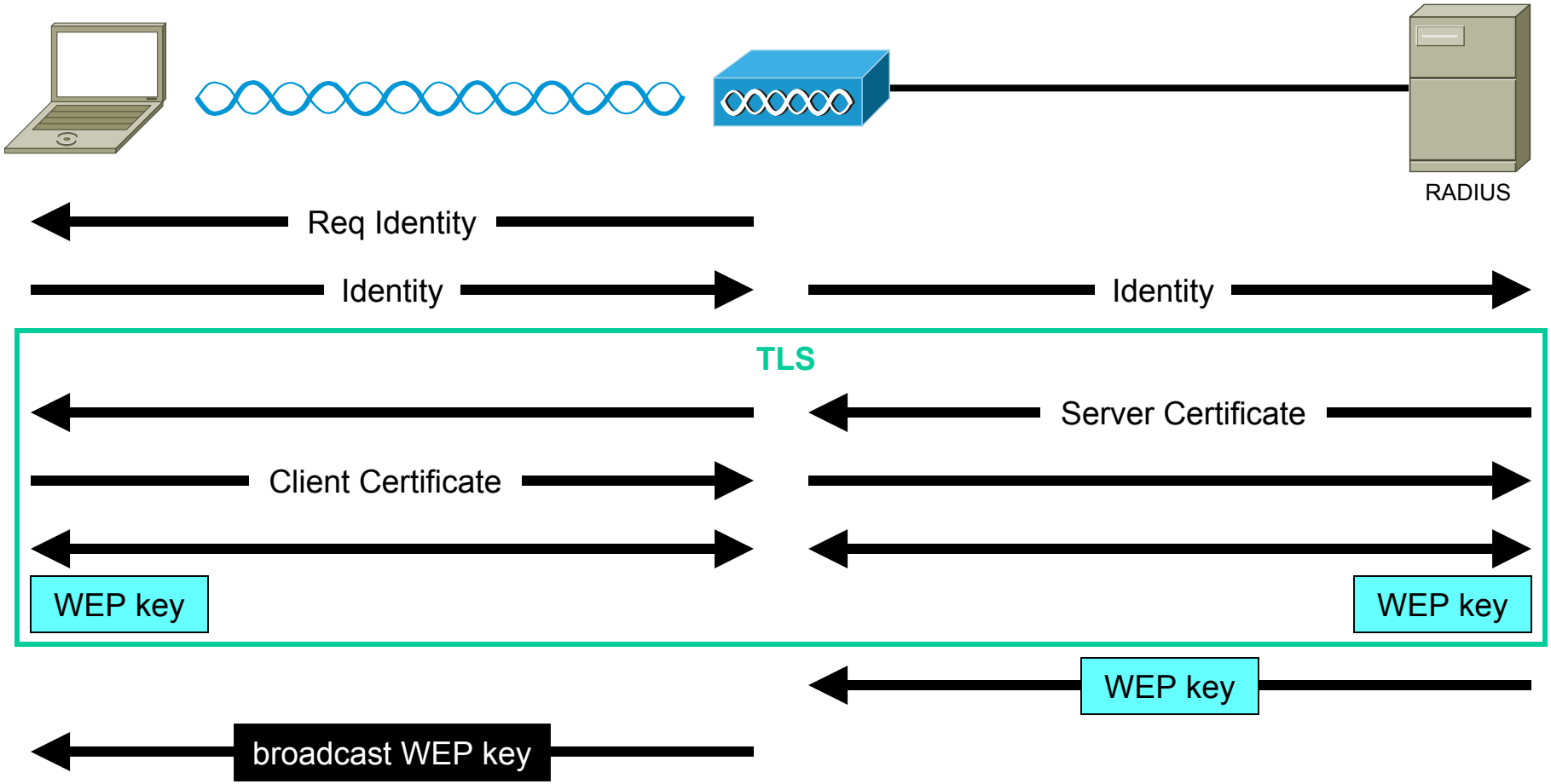
EAP-TLS (folyt.)



EAP-TLS (folyt.)



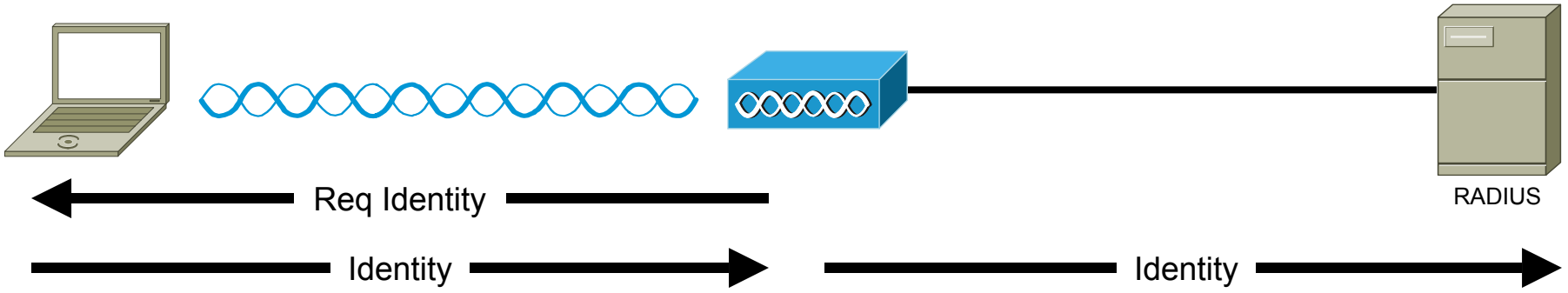
EAP-TLS (folyt.)



EAP-PEAP, EAP-TTLS

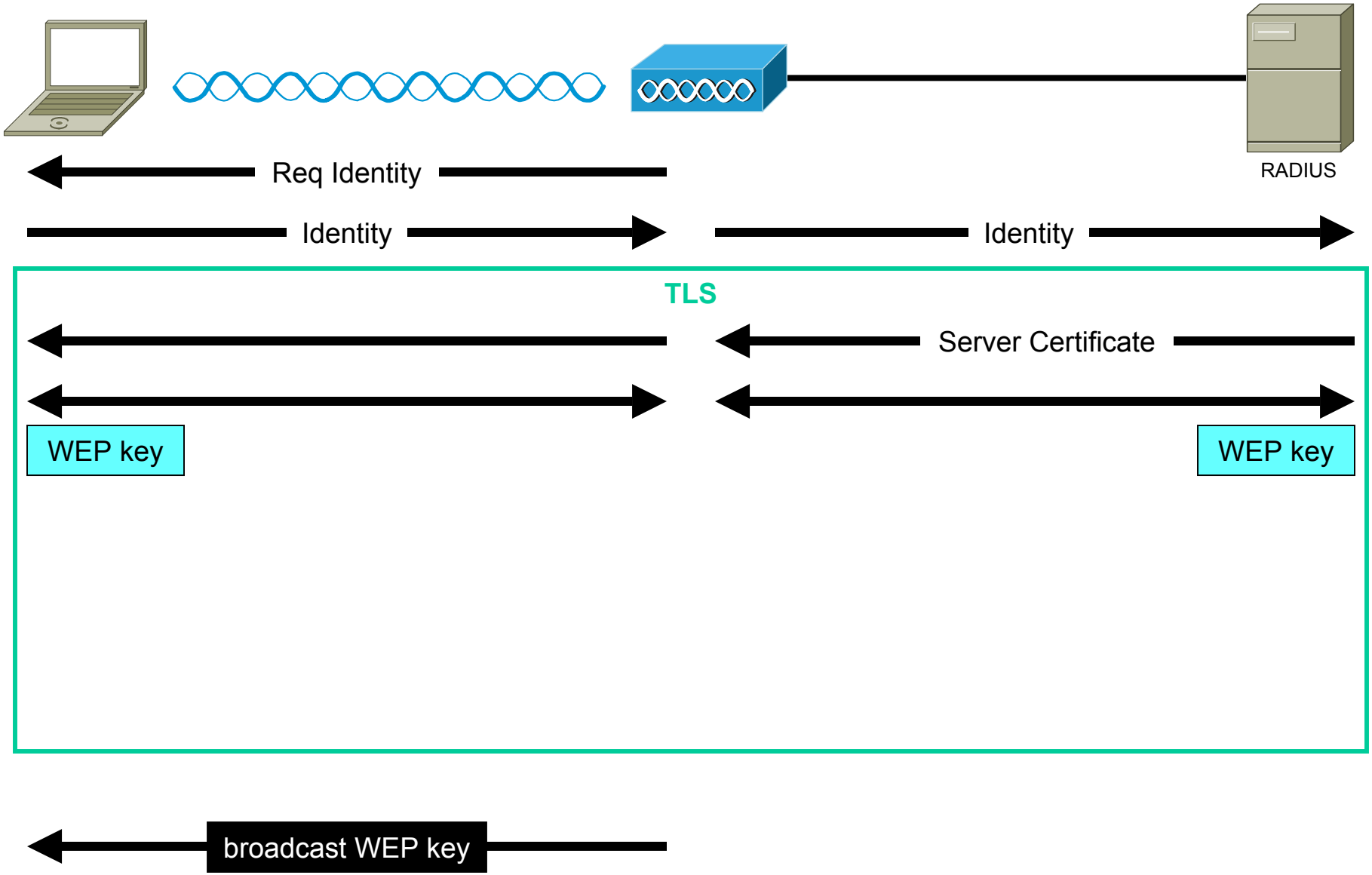
- TLS
  - server autentikációja digitális tanúsítvány alapján
  - titkosított TLS csatorna a supplicant és az authentication server között
  - a klienseknek nincs szükségük saját tanúsítványokra
- kliens autentikációja a biztonságos titkosított TLS csatornán
  - önmagában gyenge autentikációs módszer is megfelelő lehet
    - kódolatlan jelszó
    - MD5-challenge
    - stb.
- EAP-PEAP – Protected EAP
  - kliens autentikációja: EAP-*
- EAP-TTLS – Tunneled TLS
  - kliens autentikációja: PAP, CHAP, MS-CHAP, EAP-*

EAP-PEAP

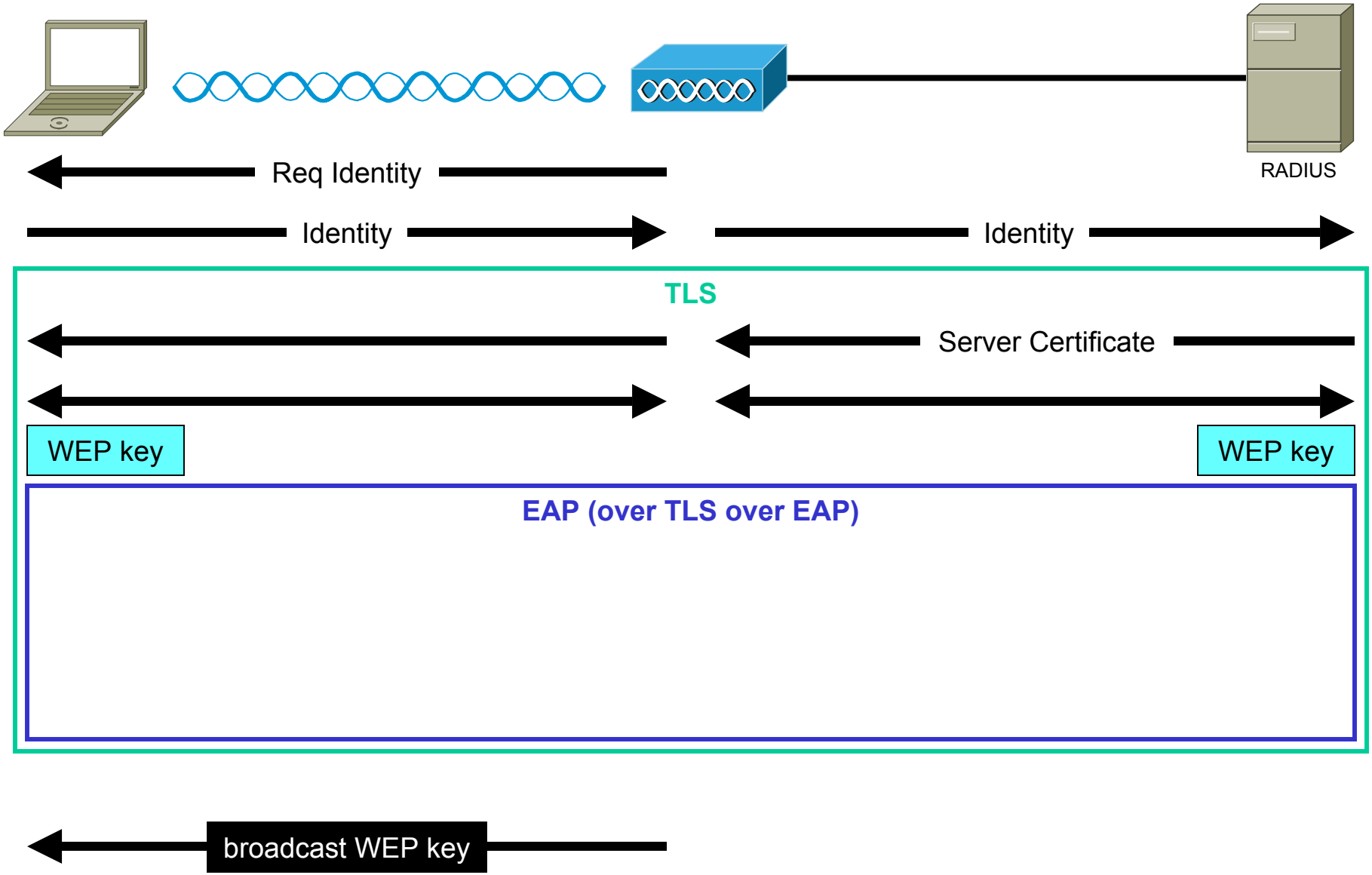


broadcast WEP key

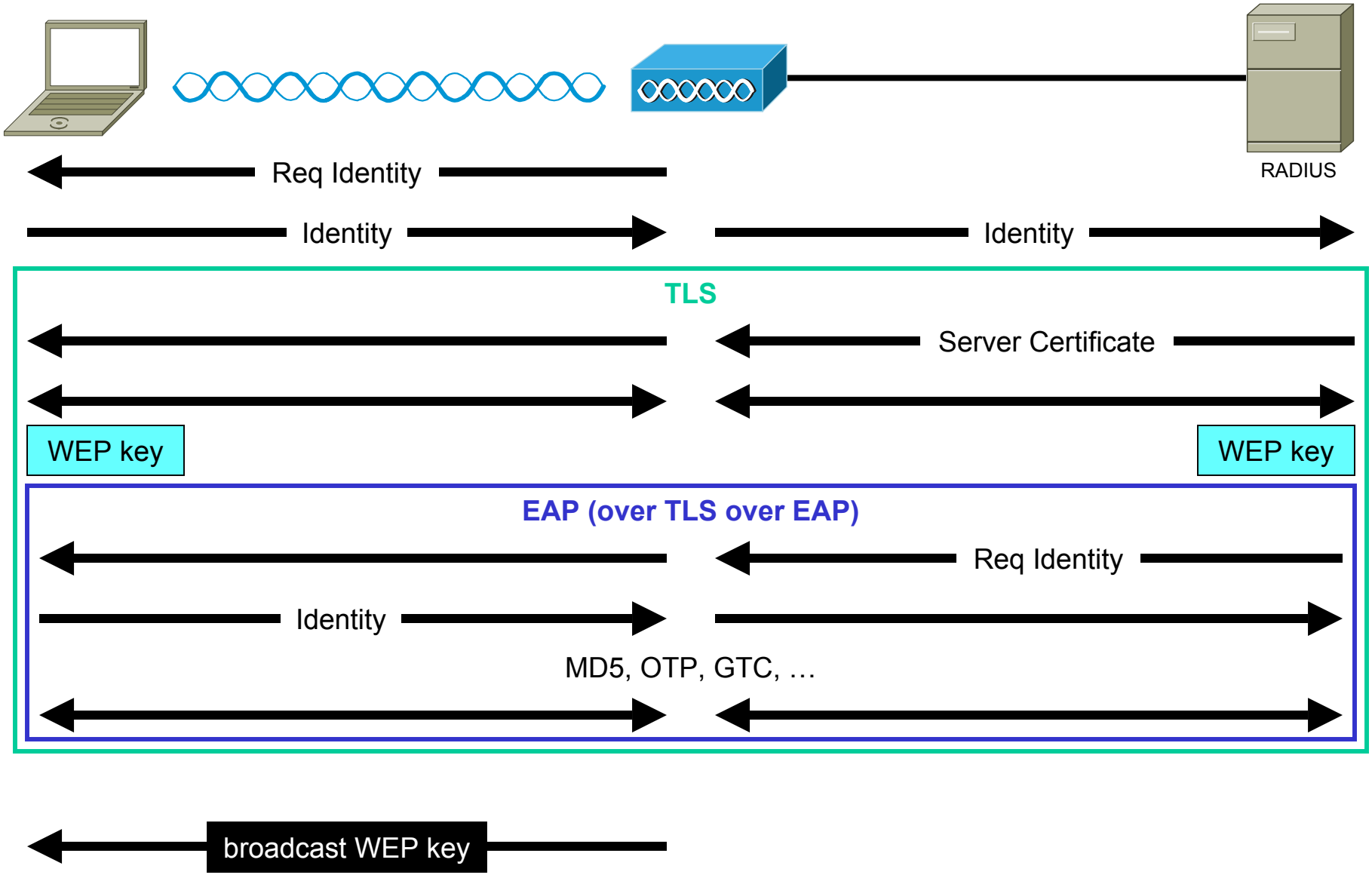
EAP-PEAP


RADIUS
Req Identity
Identity
Identity
TLS
Server Certificate
WEP key
WEP key
broadcast WEP key

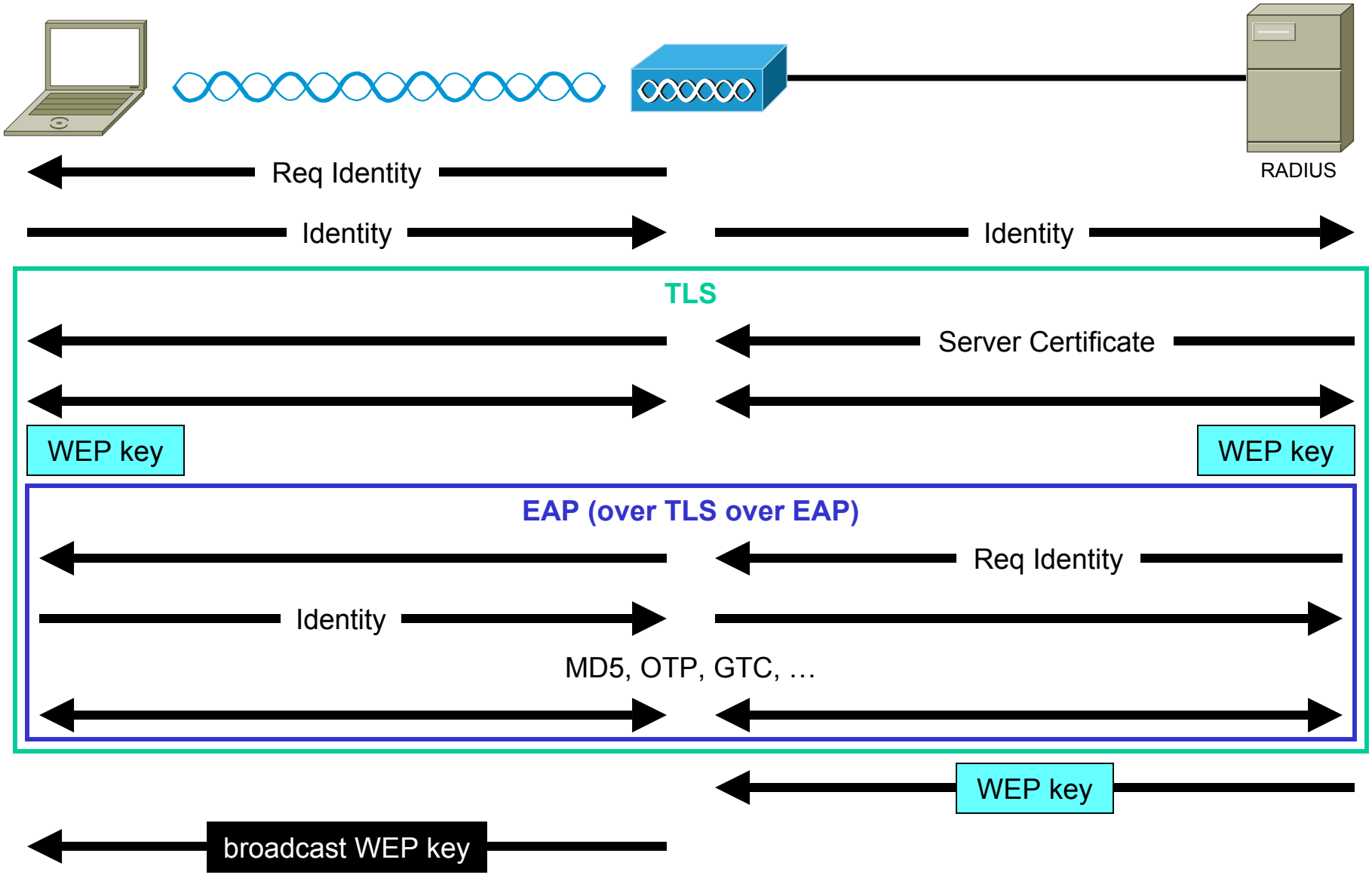
EAP-PEAP


RADIUS
Req Identity
Identity
Identity
TLS
Server Certificate
WEP key
WEP key
EAP (over TLS over EAP)
broadcast WEP key

EAP-PEAP


RADIUS
Req Identity
Identity
Identity
TLS
Server Certificate
WEP key
WEP key
EAP (over TLS over EAP)
Req Identity
Identity
MD5, OTP, GTC, …
broadcast WEP key

EAP-PEAP


RADIUS
Req Identity
Identity
Identity
TLS
Server Certificate
WEP key
WEP key
EAP (over TLS over EAP)
Req Identity
Identity
MD5, OTP, GTC, …
WEP key
broadcast WEP key

Agenda

Biztonság

802.11 titkosítás

WEP problémák

Megoldás a WEP problémáira

802.11 autentikáció

Autentikációs problémák

Autentikációs megoldások

802.11i

IEEE 802.11i

- biztonsági kiegészítések a 802.11 szabványhoz
  - 802.1x autentikáció
  - TKIP
  - AES – Advanced Encription Standard
    - RC4 helyett
    - hardware változtatást tesz szükségessé
  - IBSS biztonság
  - kulcs menedzsment
  - preautentikáció
    - gyors, biztonságos roaminghoz
  - biztonságos deautentikáció és disassociation
    - AP megszemélyesítéses támadás ellen
- várhatóan 2003. végén jelenik meg

Agenda

Bevezető

Fizikai réteg

Közeghozzáférés

Biztonság

Egyéb

Új IEEE 802.11 szabványok

- 802.11e – Quality of Service
- 802.11f – Inter Access Point Protocol
  - roaming access pointok között
- 802.11g – 54 Mb/s a 2.4 GHz ISM sávban
- 802.11h – 54 Mb/s 5 GHz-en (802.11a) Európában is
  - Dynamic Frequency Selection
  - Transmit Power Control
- 802.11i – Security

Wi-Fi

- Wireless Fidelity
- a Wi-Fi Alliance tanusítványokat ad ki
  - IEEE 802.11a és 802.11b termékekre
  - interoperabilitási tesztek alapján
- WPA – Wi-Fi Protected Access
  - biztonsági minősítés 802.11 termékekre
    - Wi-Fi pecsétes eszközökön software módosítással elérhető követelmények
  - az IEEE 802.11i draft részhalmaza
    - 802.1x autentikáció
    - TKIP
    - kulcs menedzsment
  - a később megjelenő 802.11i szabványnak megfelelő Wi-Fi minősítés a WPA2 lesz

Cyber-sátor az Everesten

- Tsering Gyaltsen
  - az 1953-as Hillary expedíciót kísérő serpák közül az egyetlen túlélő unokája
- Mt. Everest alaptábor
  - 5200 m, gleccseren
  - cyber-sátor: néhány gép internetkapcsolattal
- V-SAT link az ISP-hez
  - nem telepíthető gleccsrre, mert az elmozdul
  - szilárd szikla talajon
  - az alaptábortól 1.5 km, 5650 m magasan
- 802.11b a cyber-sátor és a V-SAT antenna között
  - Cisco Aironet 350, a Cisco Systems ajándéka