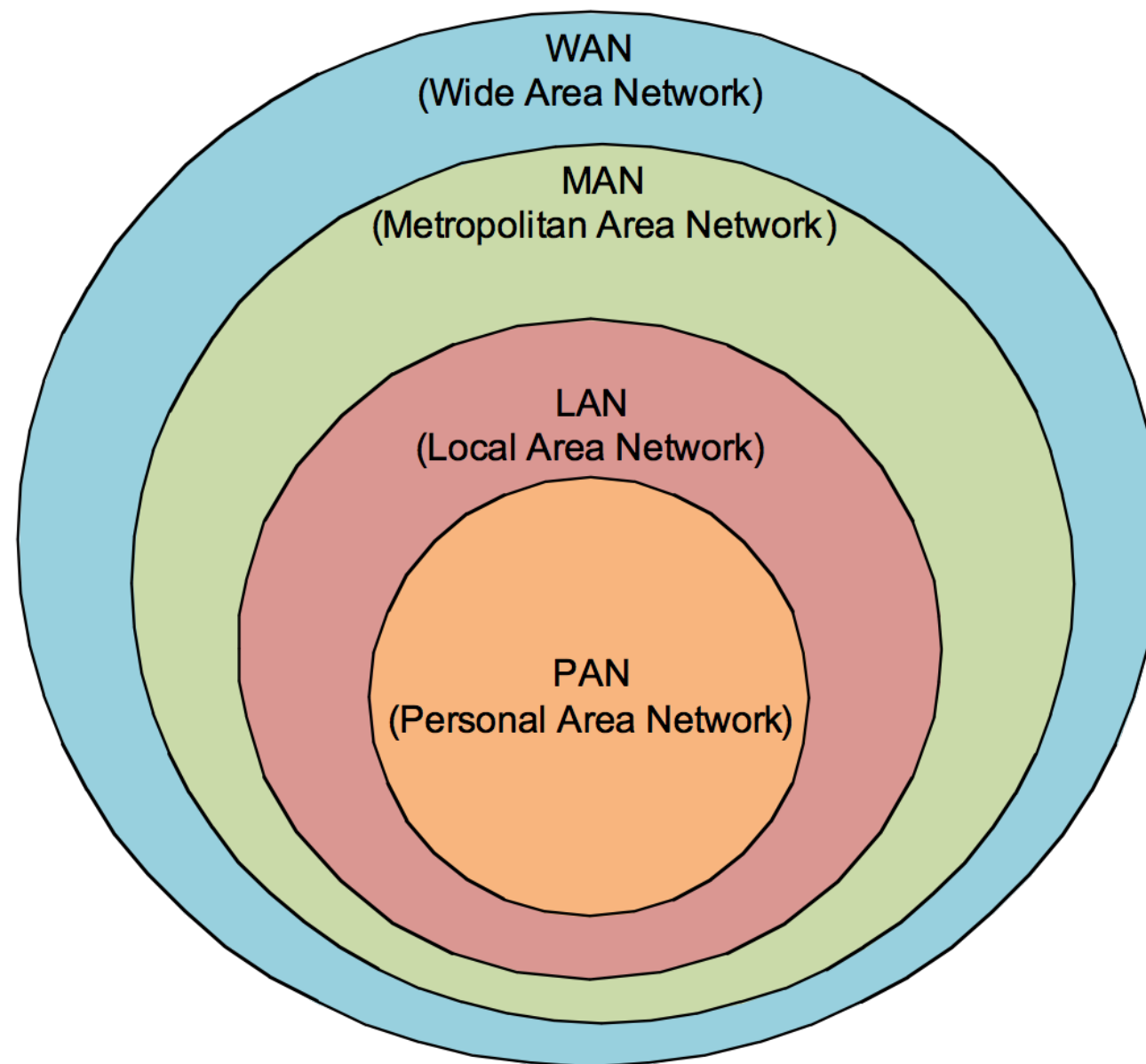


Bezdrôtové siete

WiFi a BT



Delenie bezdrôtových sietí

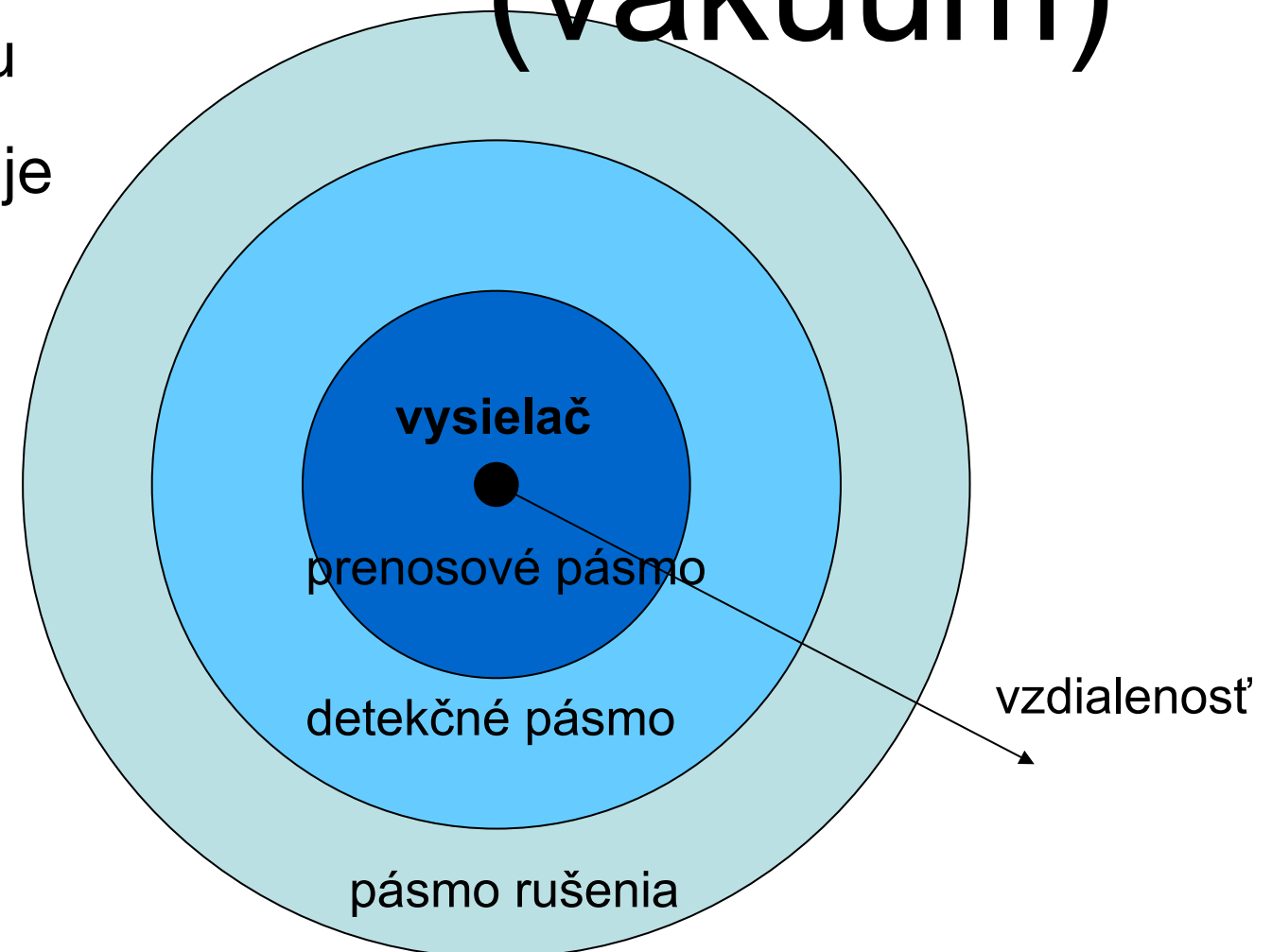
Delenie bezdrôtových sietí

	PAN	LAN	MAN	WAN
Štandard	Bluetooth, ZigBee, IrDA	WiFi HyperLAN	802.11, MMDS, LMDS	GSM, GPRS, CDMA, UMTS LTE, 5G
Rýchlosť	< 24 Mbps	1 – 600 Mbps	22 Mbps+	10 kbps – 1Gbits
Dosah	Krátky (cca 10 m)	Stredný (cca 100 m)	Stredne-dlhý	Dlhý
Aplikácie	Bod-bod Zariadenie-zariadenie	Podnikové siete	Fixný prístup, prístup „poslednej míle“	Mobilné telefóny

Šírenie signálu

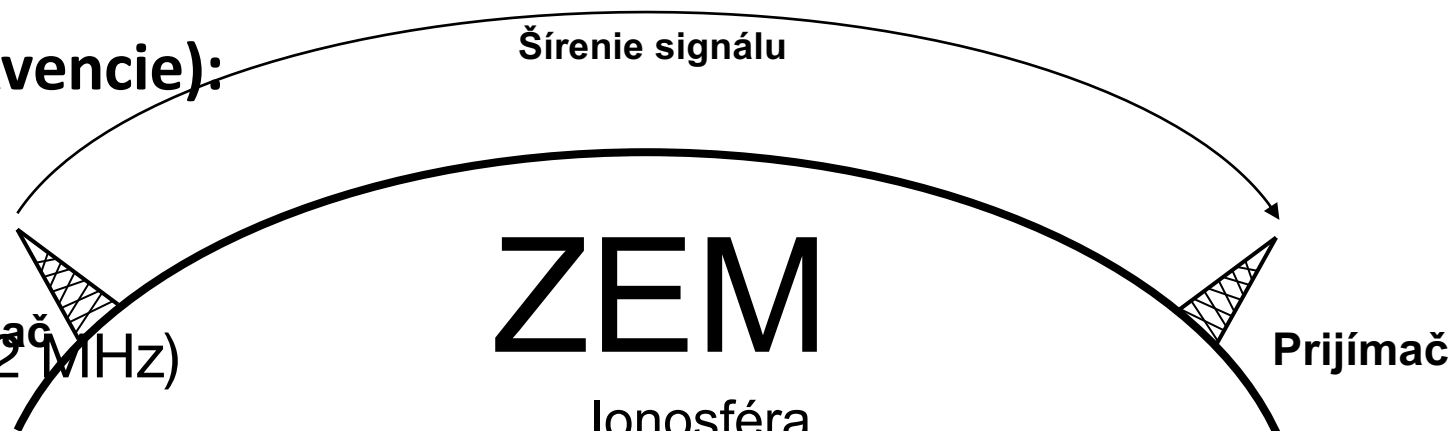
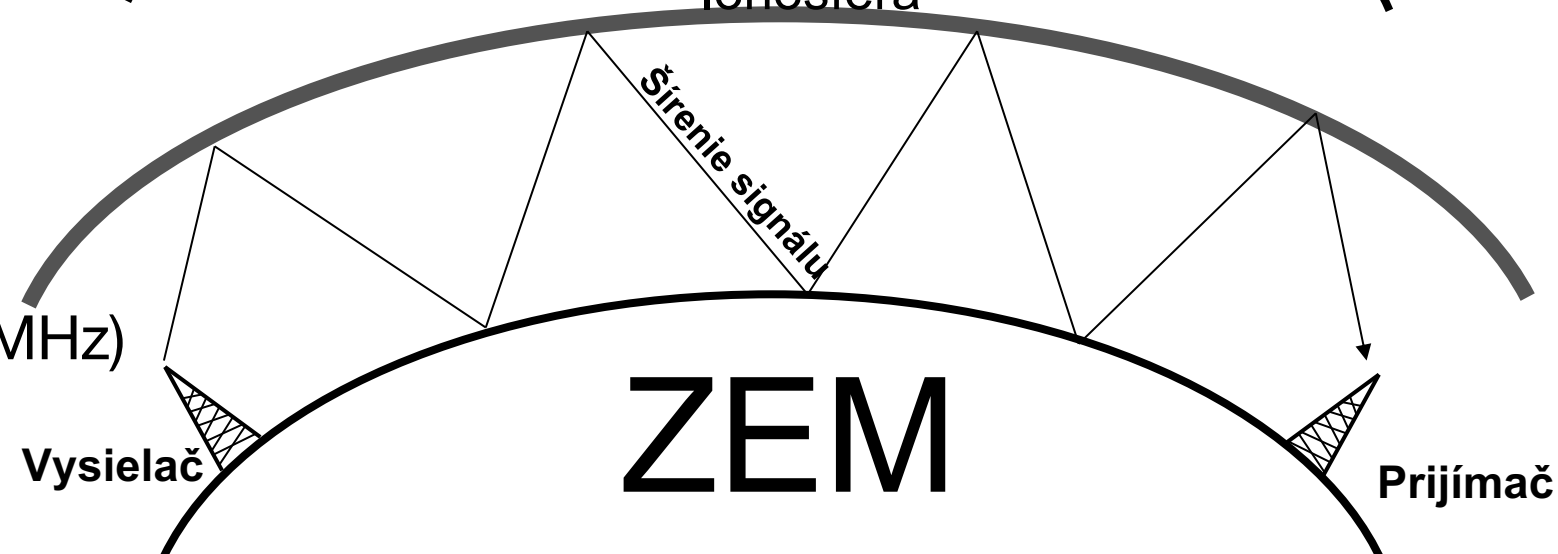

- Prenosové pásmo
 - možnosť komunikácie
 - nízka chybovosť
- Detekčné pásmo
 - možnosť detekcie signálu
 - komunikácia však už nie je možná
- Pásmo rušenia
 - signál sa už nedá detegovať
 - signál sa pridáva do okolitého šumu

Ideálna
situácia
(vákuum)



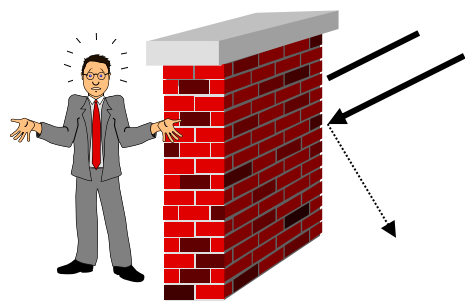
Šírenie signálu

Rozlišujeme nasledovné vlny (podľa frekvencie):

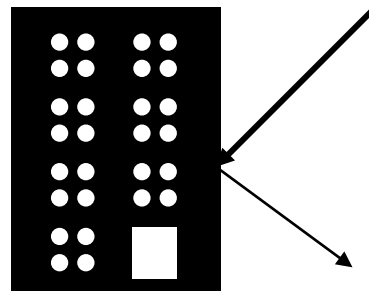
- pozemné (prízemné) vlny (< 2 MHz)

- priestorové vlny (2 – 30 MHz)

- LOS (line-of-sight) vlny (> 30 MHz)


Šírenie signálu

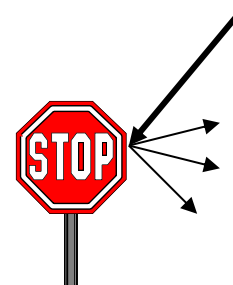
- Prijatý výkon je ešte ovplyvnený
 - útlmom (závislé od frekvencie, vzdialenosti)
 - tienením
 - odrazmi na veľkých prekážkach
 - rozptylom na malých prekážkach
 - difrakciou na okrajoch



tienie



odraz



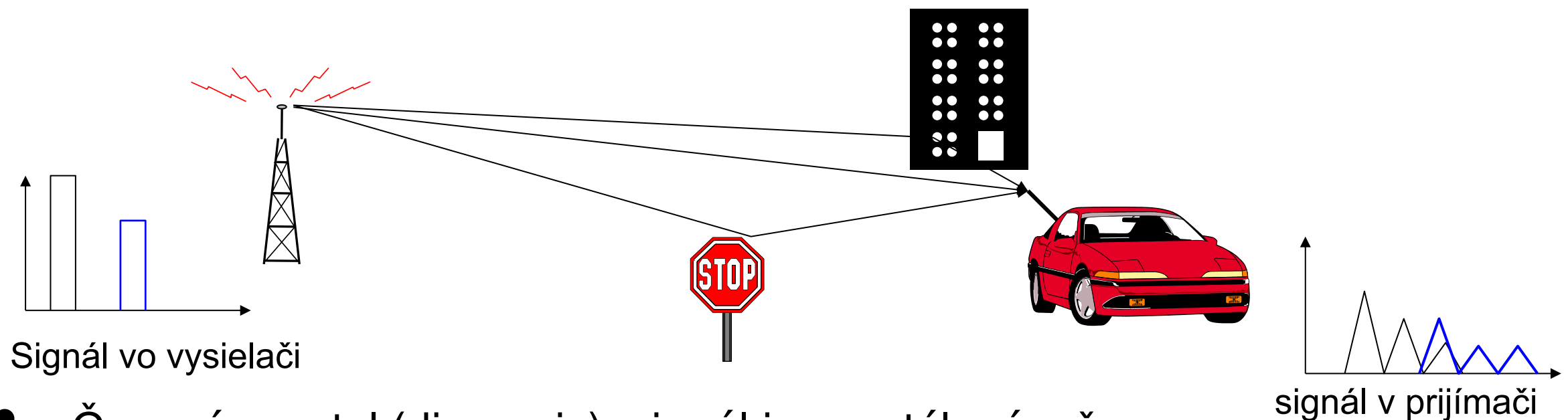
rozptyl



difrakcia

Viaccestné šírenie signálu

- Signál môže prísť od vysielacej k prijímaču rôznymi cestami v závislosti od odrazov, rozptylov a difrakcie na ceste



- Časový rozptyl (disperzia): signál je rozptýlený v čase
 - rušenie susednými symbolmi, medzisymbolová interferencia (ISI)
- Signál príde k prijímaču priamo a fázovo posunutý
 - skreslený signál v závislosti od fáz jednotlivých častí
- Potreba informácie o aktuálnom stave kanála – testovacia postupnosť

Dôsledky mobility

- Charakteristiky kanála sa menia v čase a polohe

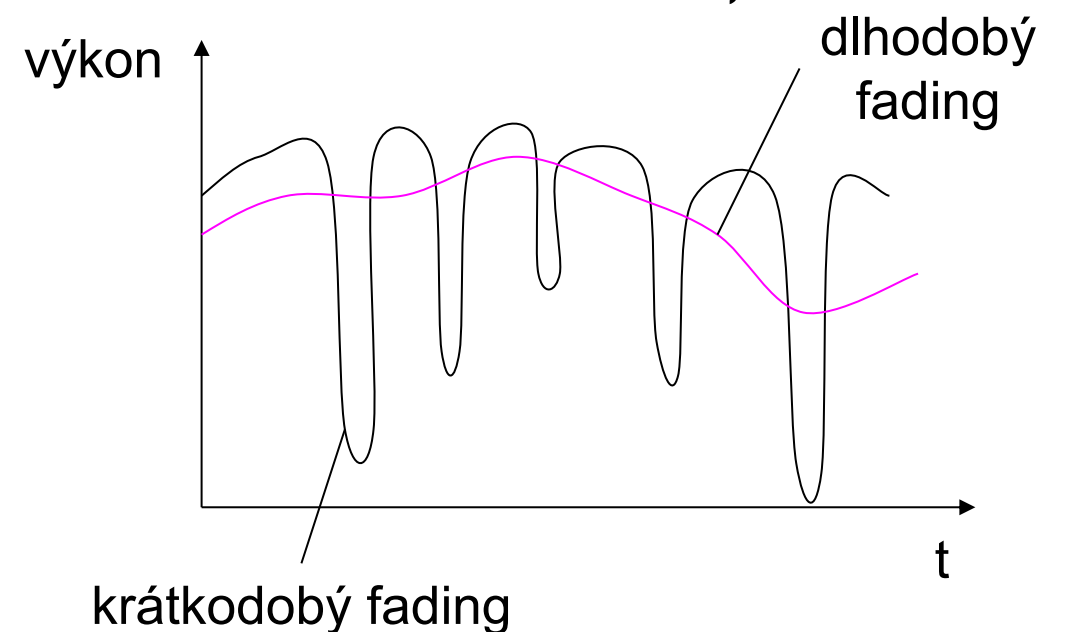
- mení sa cesta signálu
- rôzne oneskorenia jednotlivých častí signálu
- rôzne fázy častí signálu

→ rýchle zmeny v prijatom výkone (krátkodobé slabnutie, únik – short-term fading)

- Okrem toho sa mení

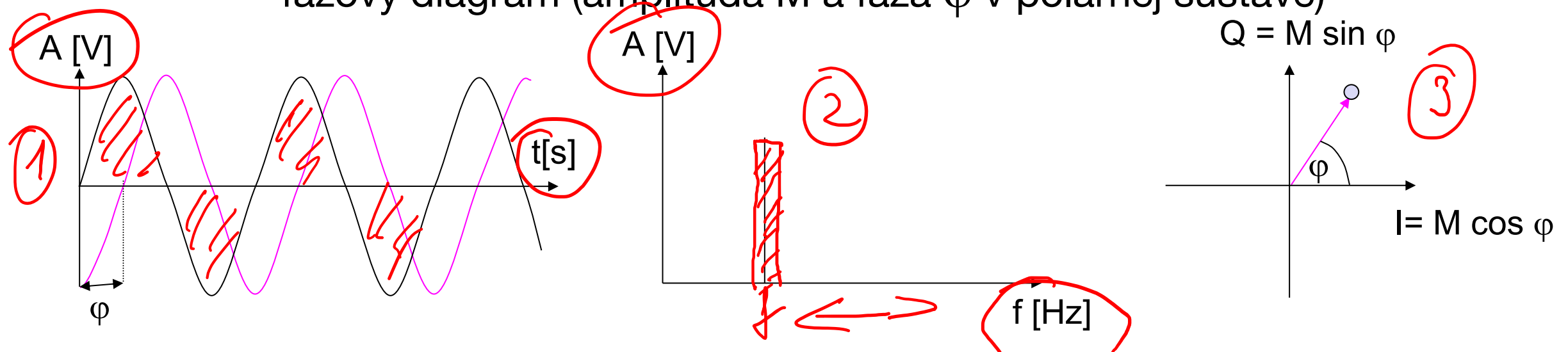
- vzdialenosť vysieláča
- vzdialené prekážky na ceste

→ pomalé zmeny priemerného prijímaného výkonu (dlhodobé slabnutie, únik)



Signály

- fyzická reprezentácia dát,
- rozdelenie
 - spojitý v hodnote, diskretný v čase
 - spojitý v čase, diskretný v hodnote
 - analógový signál = spojitý v čase aj v hodnote
 - digitálny signál = diskretný v čase aj v hodnote
- rôzne zobrazenia signálov
 - časová oblasť (amplitúdové)
 - frekvenčná oblasť (spektrum)
 - fázový diagram (amplitúda M a fáza φ v polárnej sústave)



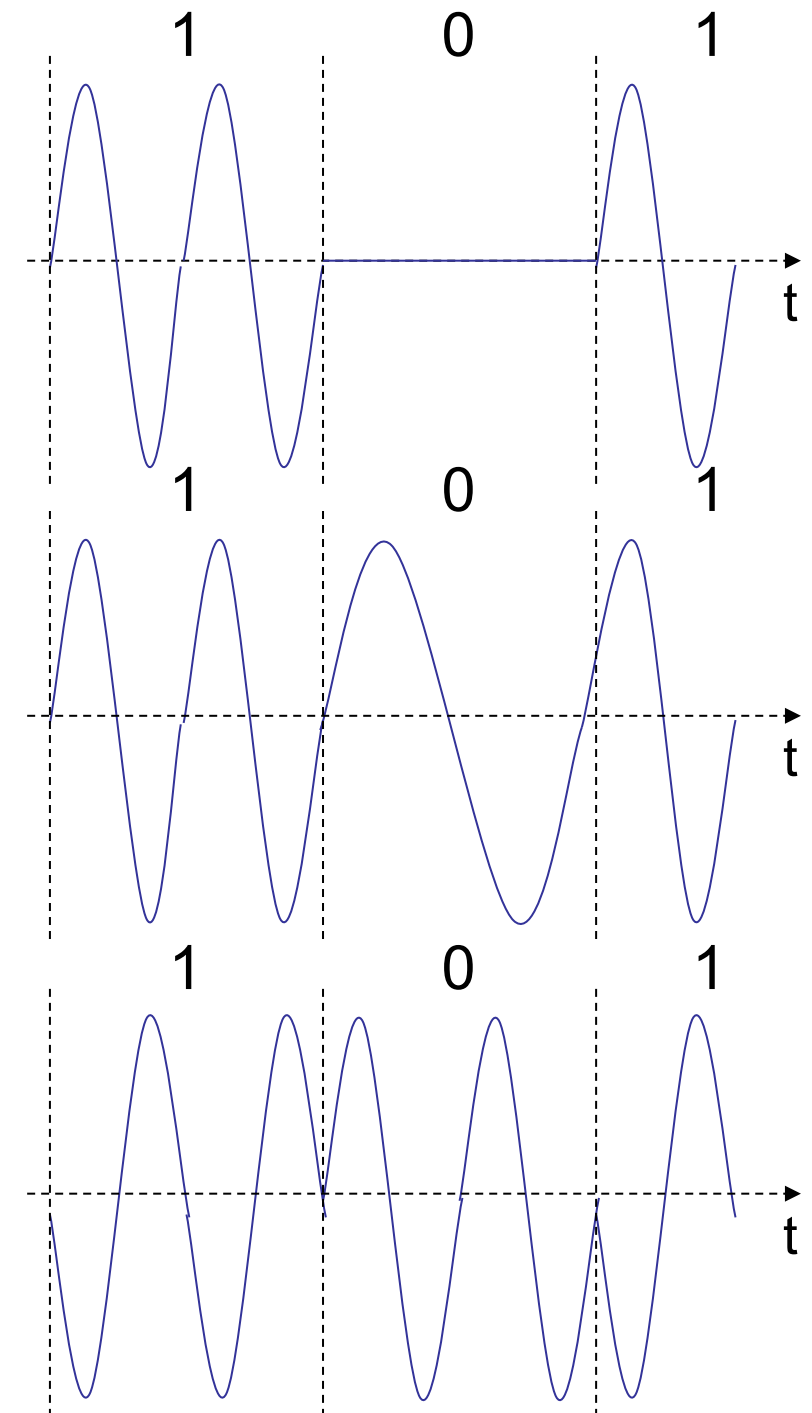
Modulácie

- **Analógová modulácia**
 - posúva spektrum signálu na nosnú frekvenciu
 - Motivácia
 - menšie antény (napr. $\lambda/4$)
 - frekvenčne delené multiplexovanie
 - vlastnosti média
 - Základné schémy $s(t) = A \cdot \sin(2 \cdot \pi \cdot f \cdot t + \phi)$
 - Amplitúdová modulácia (AM)
 - Frekvenčná modulácia (FM)
 - Fázová modulácia (PM)
- **Digitálna modulácia**
 - digitálne dáta sú pretransformované na analógový signál (baseband)
 - ASK, FSK, PSK – pozri ďalej v tejto kapitole
 - rozdiely v spektrálnej efektivite, výkonovej efektivite, robustnosti

Digitálne modulácie

Modulácie digitálneho signálu

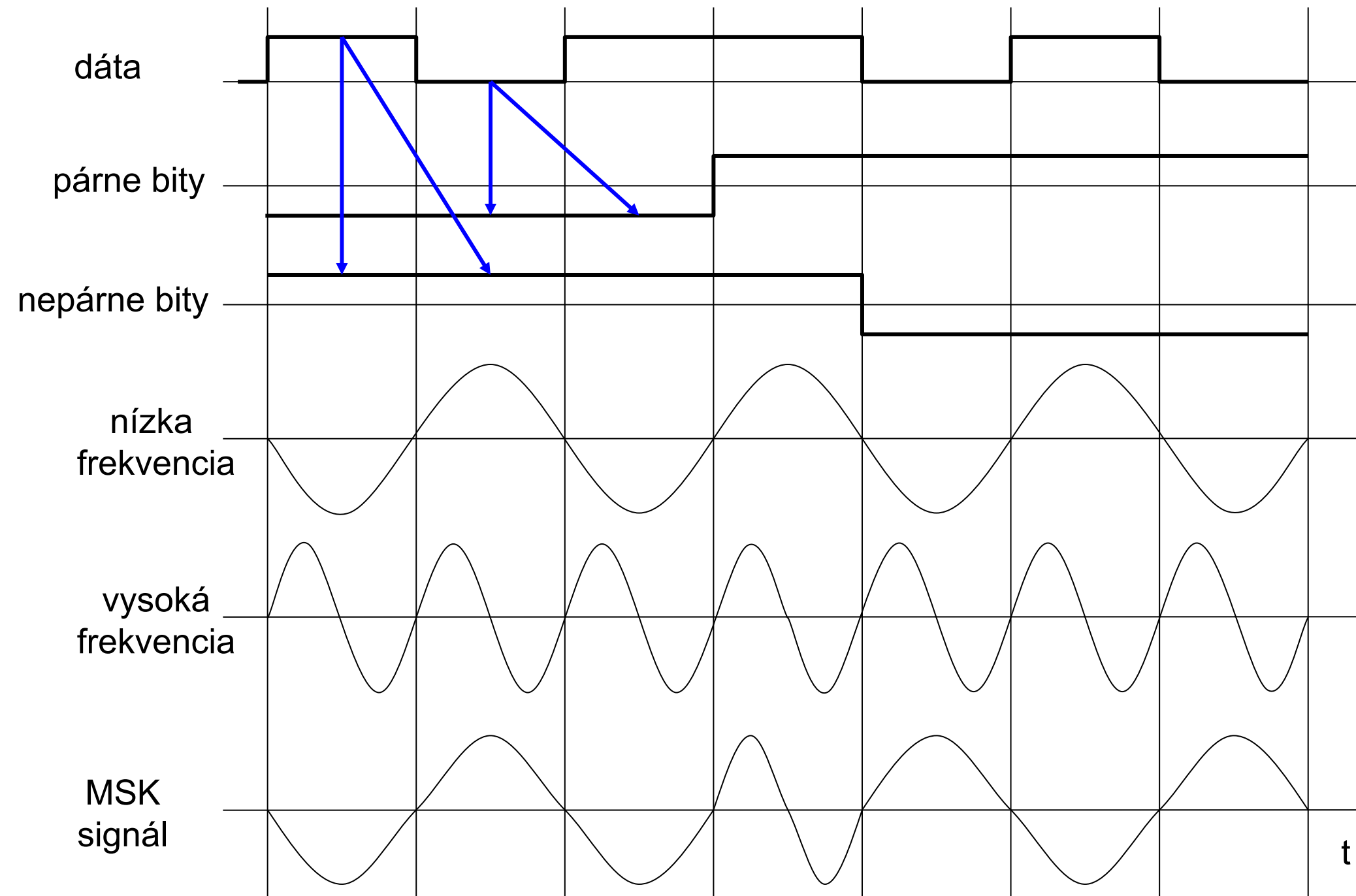
- Amplitude Shift Keying (ASK):
(kľúčovanie posuvom amplitúdy)
 - jednoduchá
 - vyžaduje malú šírku pásma
 - veľmi citlivá na rušenie
- Frequency Shift Keying (FSK):
(kľúčovanie posuvom frekvencie)
 - potrebuje širšie pásmo voči ASK
- Phase Shift Keying (PSK):
(kľúčovanie posuvom fázy)
 - zložitejšia
 - odolná voči rušeniu (interferenciám)



Rozšírenia FSK

- šírka pásma potrebná pre FSK závisí od vzdialenosti medzi nosnými frekvenciami
- špeciálne predvýpočty môžu zabrániť náhlym posunom fázy
- → MSK (Minimum Shift Keying)
 - bity sú rozdelené na párne a nepárne, trvanie bitu je dvojnásobné
 - závisí od hodnôt bitov (párne, nepárne) je vybraná vyššia alebo nižšia frekvencia, pôvodný alebo invertovaný signál
 - frekvencia jednej nosnej je dvojnásobná ďalšej
 - rovnaká ako offsetová QPSK
- možnosť dosiahnuť ešte väčšiu úsporu pásma použitím Gaussovho dolnopriepustného filtra
- → GMSK (Gaussian MSK), použité v GSM

MSK

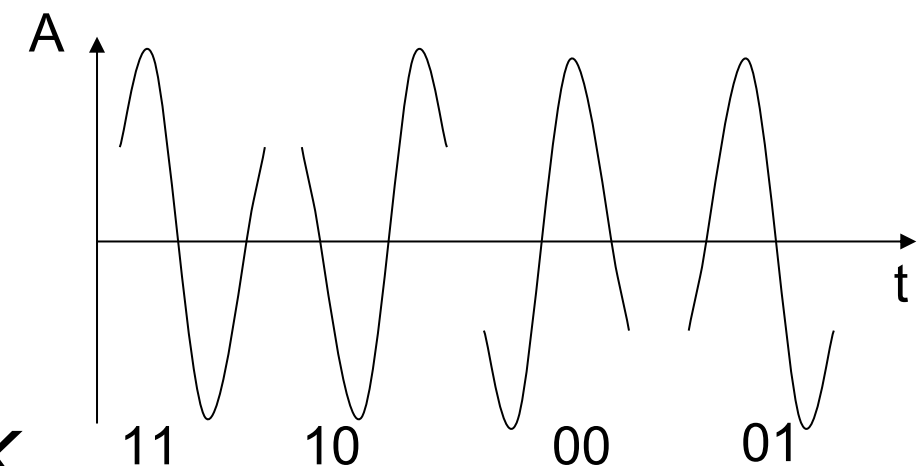
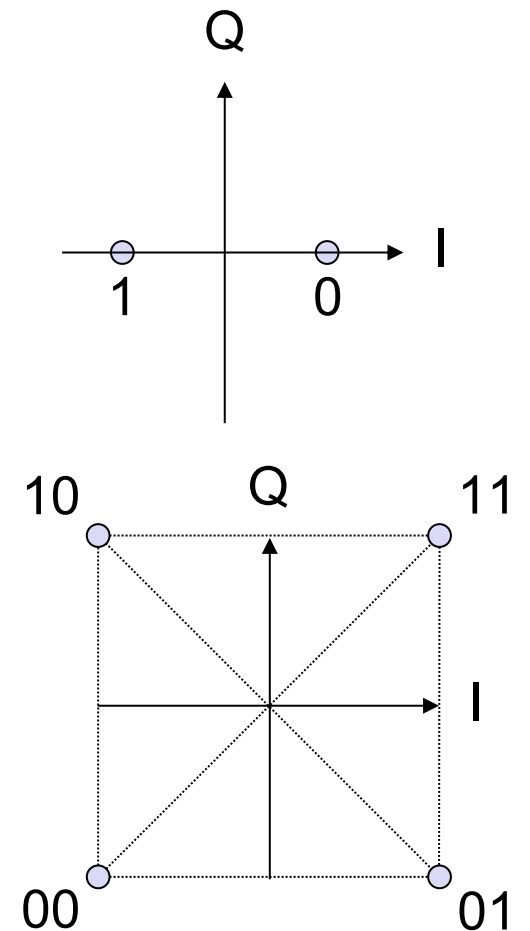


bit	
Párny.	0 1 0 1
Nepárny	0 0 1 1
<hr/>	
Hodnota signálu	v n n v
	- - + +

Bez fázového posunu!

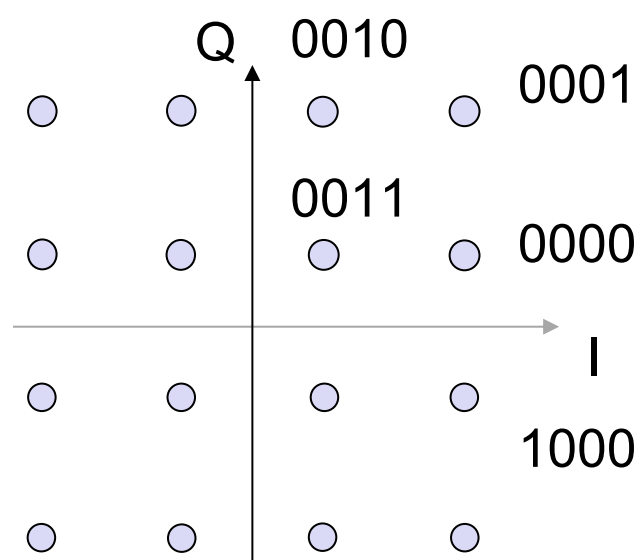
Rozšířená PSK

- BPSK (Binary Phase Shift Keying):
 - bit 0: sínus
 - bit 1: invertovaný sínus
 - jednoduchá PSK
 - nízká spektrálna účinnosť
 - robustná, používa sa napr. v satelitných systémoch
- QPSK (Quadrature Phase Shift Keying):
 - 2 bity kódované ako jeden symbol
 - symbol určuje posunutie sínusu
 - menšia šírka pásma ako BPSK
 - zložitejšia
- Často sa používa aj relatívne fázové posunutie: DQPSK - Diferenčná QPSK (IS-136, PHS)



Kvadrátúrna amplitúdová modulácia

- Quadrature Amplitude Modulation (QAM): spája amplitúdovú a fázovú moduláciu
- umožňuje zakódovanie n bitov do jedného symbolu
- 2^n diskretných úrovní, pri $n=2$ identické ako QPSK
- chybovosť sa zvyšuje s n , avšak menšia chybovosť v porovnaní s PSK



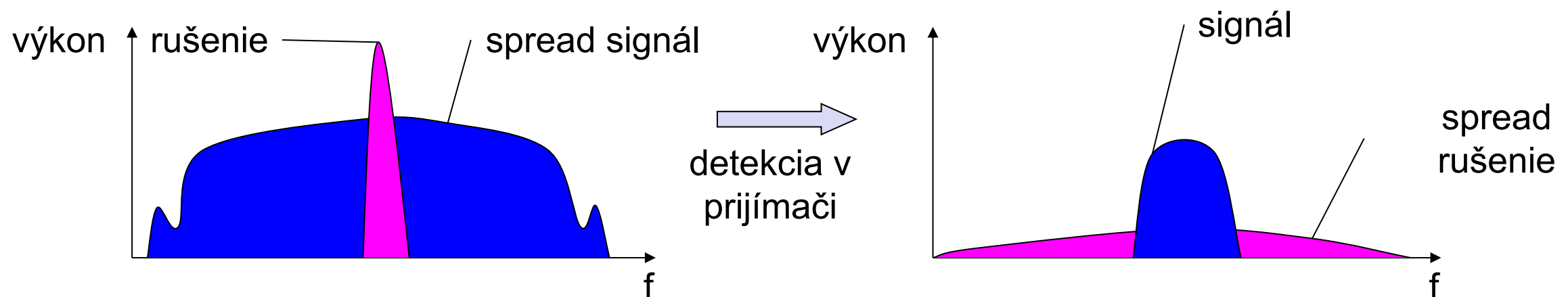
Príklad: 16-QAM (4 bity = 1 symbol)

- Symboly 0011 a 0001 majú rovnakú fázu, avšak odlišnú amplitúdu. 0000 a 1000 majú odlišnú fázu, ale rovnakú amplitúdu.

➔ používa sa v 9600 bit/s modemoch

Spread spektrum

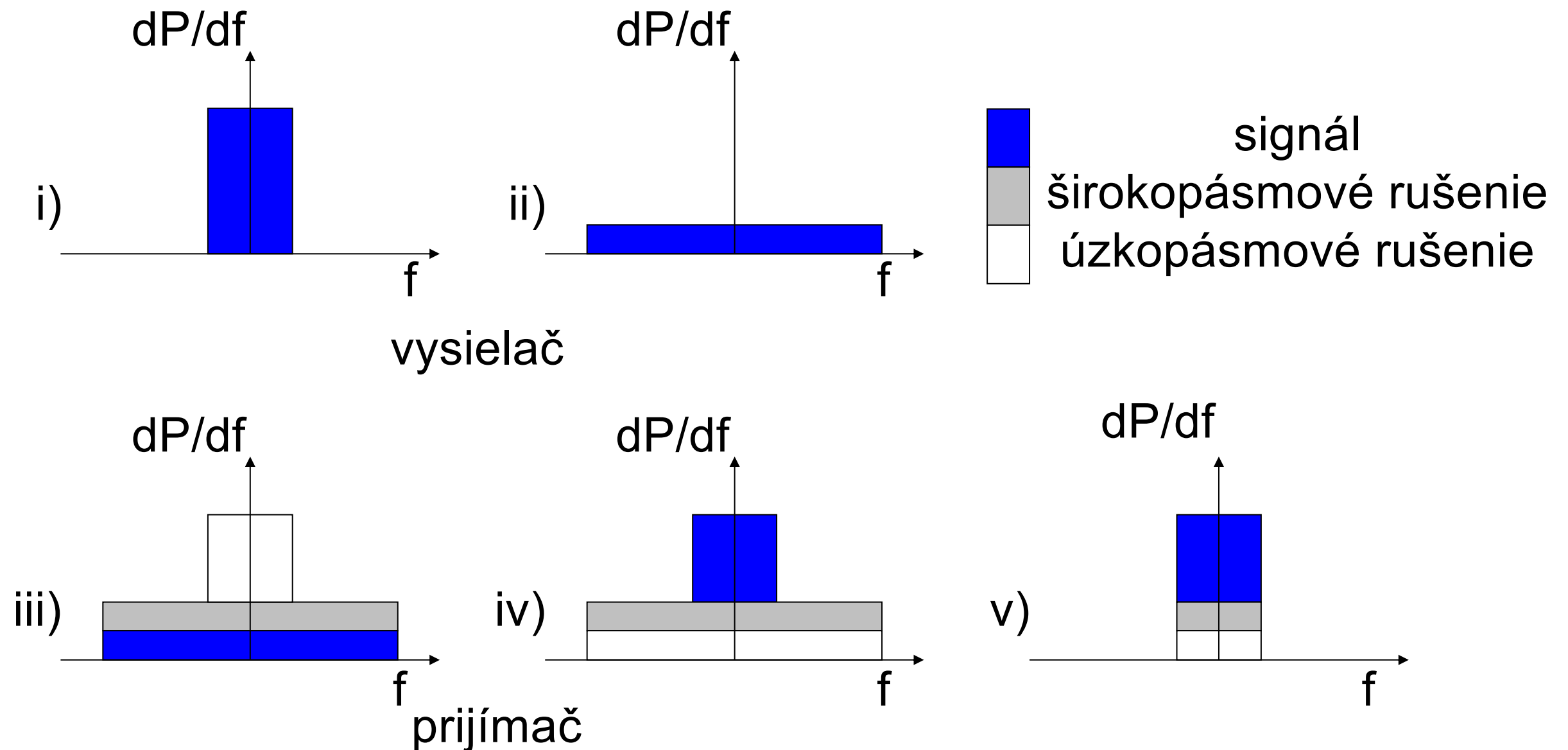
- Problém rádiového prenosu; frekvenčne závislý fading môže zrušiť úzkopásmové signály počas trvania rušenia.
- Riešenie: rozostrieť úzkopásmový signál do širokopásmového signálu použitím špeciálneho kódu
 - ochrana proti úzkopásmovému rušeniu



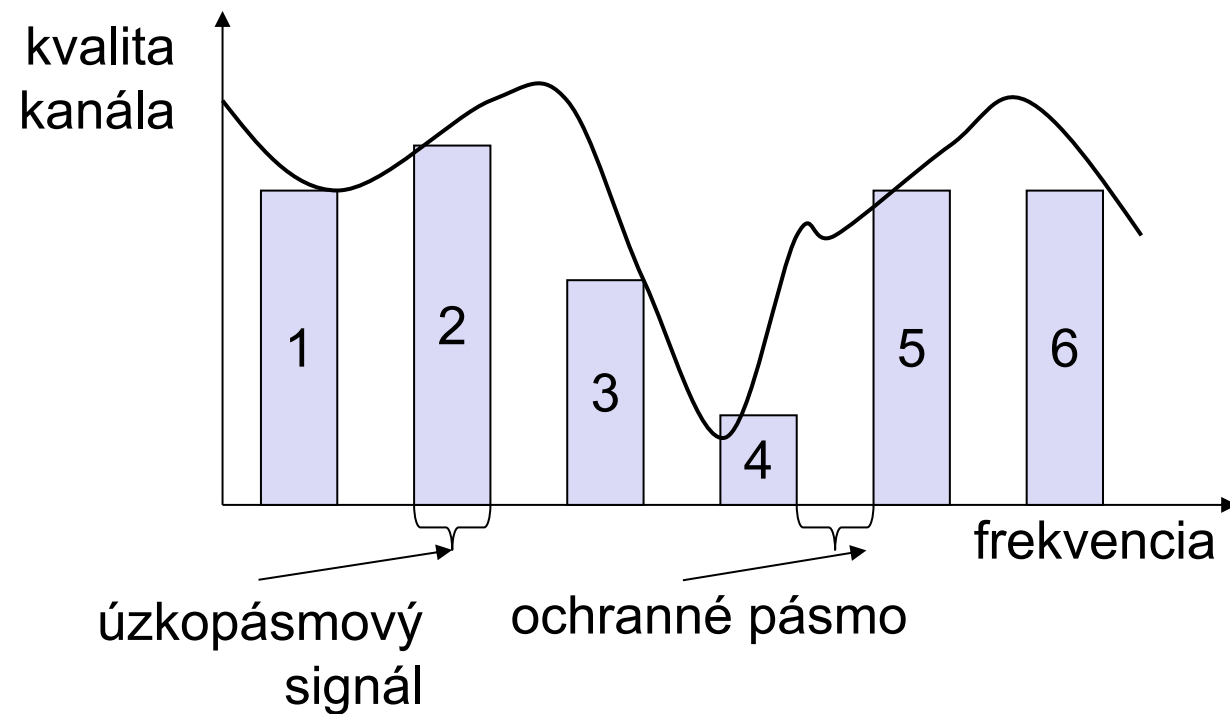
ochrana proti úzkopásmovému rušeniu

- Vedľajšie efekty:
 - existencia niekoľkých signálov bez dynamickej koordinácie
 - odolné voči odposluchu
- Alternatívne riešenia: Direct Sequence, Frequency Hopping

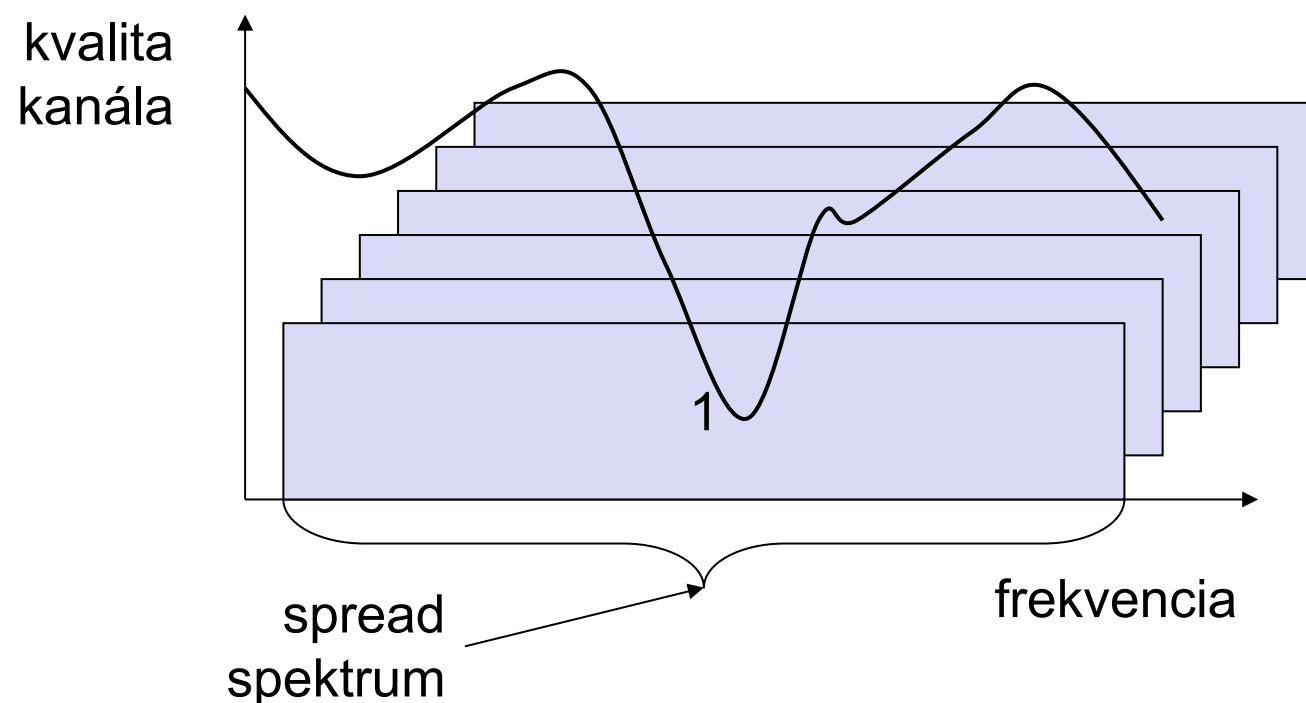
Následky rozprestretia a rušenia



Rozprestretie a frekvenčný fading



úzkopásmové kanály



spread spektrum kanály

DSSS (Direct Sequence Spread Spectrum)

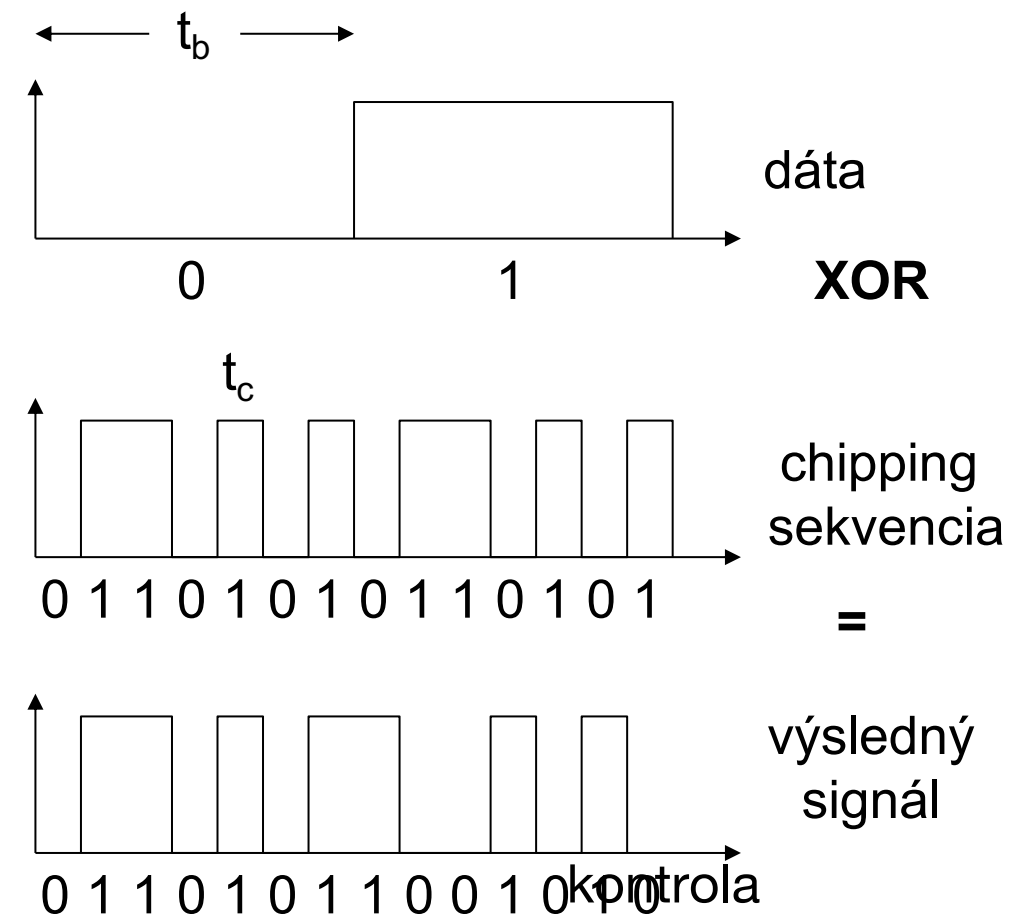
- “XORovanie” signálu so pseudonáhodným číslom (chipping sekvencia)
 - veľa “chipov” na bit (napr. 128) má za výsledok väčšiu šírku pásma signálu

- **Výhody**

- znižuje frekvenčný fading
- v celulárnych sieťach
 - základňové stanice môžu využívať rovnaké frekvenčné pásmo
 - niekoľko základňových staníc môže detekovať a obnoviť signál
 - soft handover

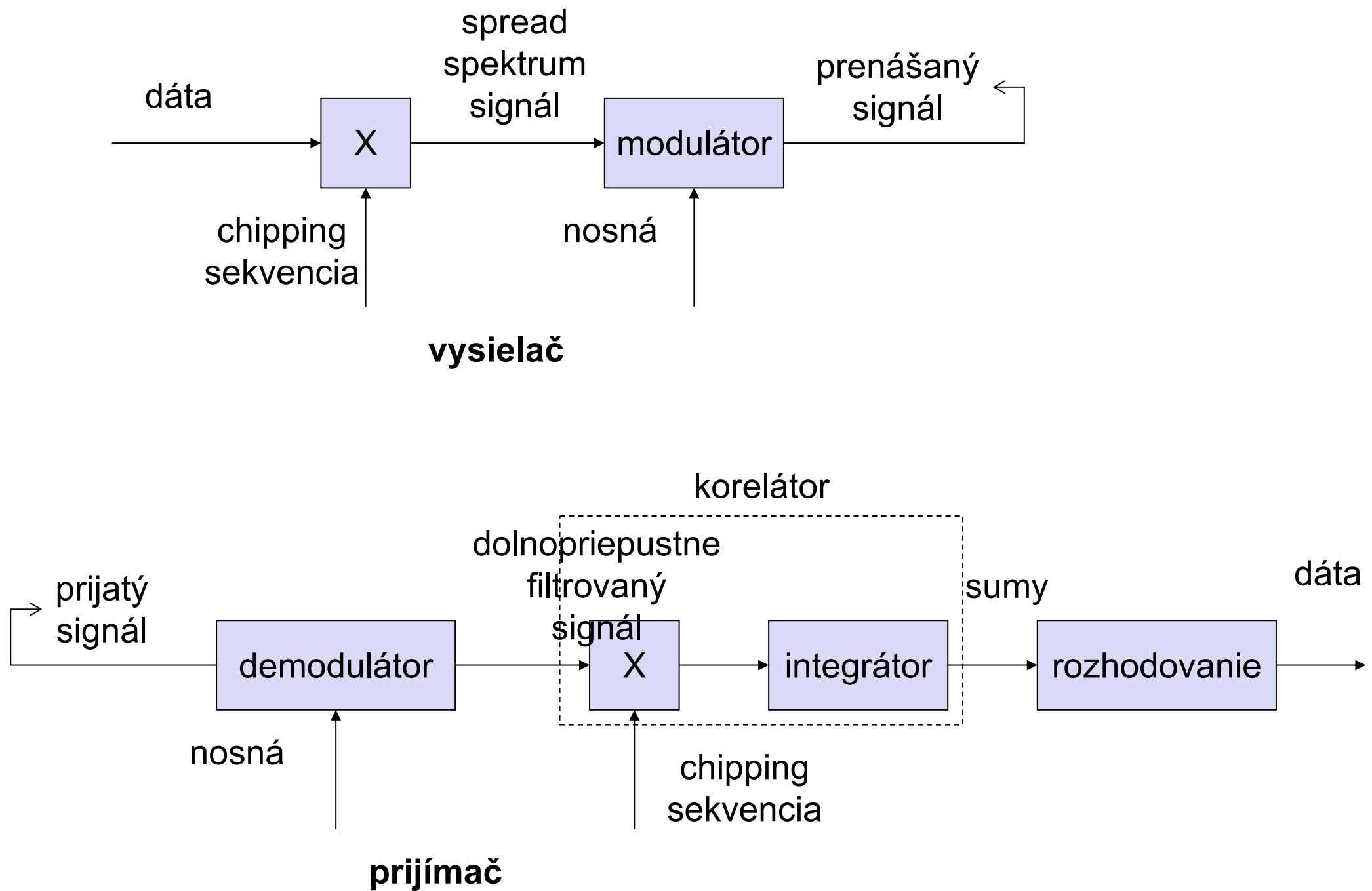
- **Nevýhody**

- je potrebná presná výkonová



t_b : bitová perióda
 t_c : perióda chipu

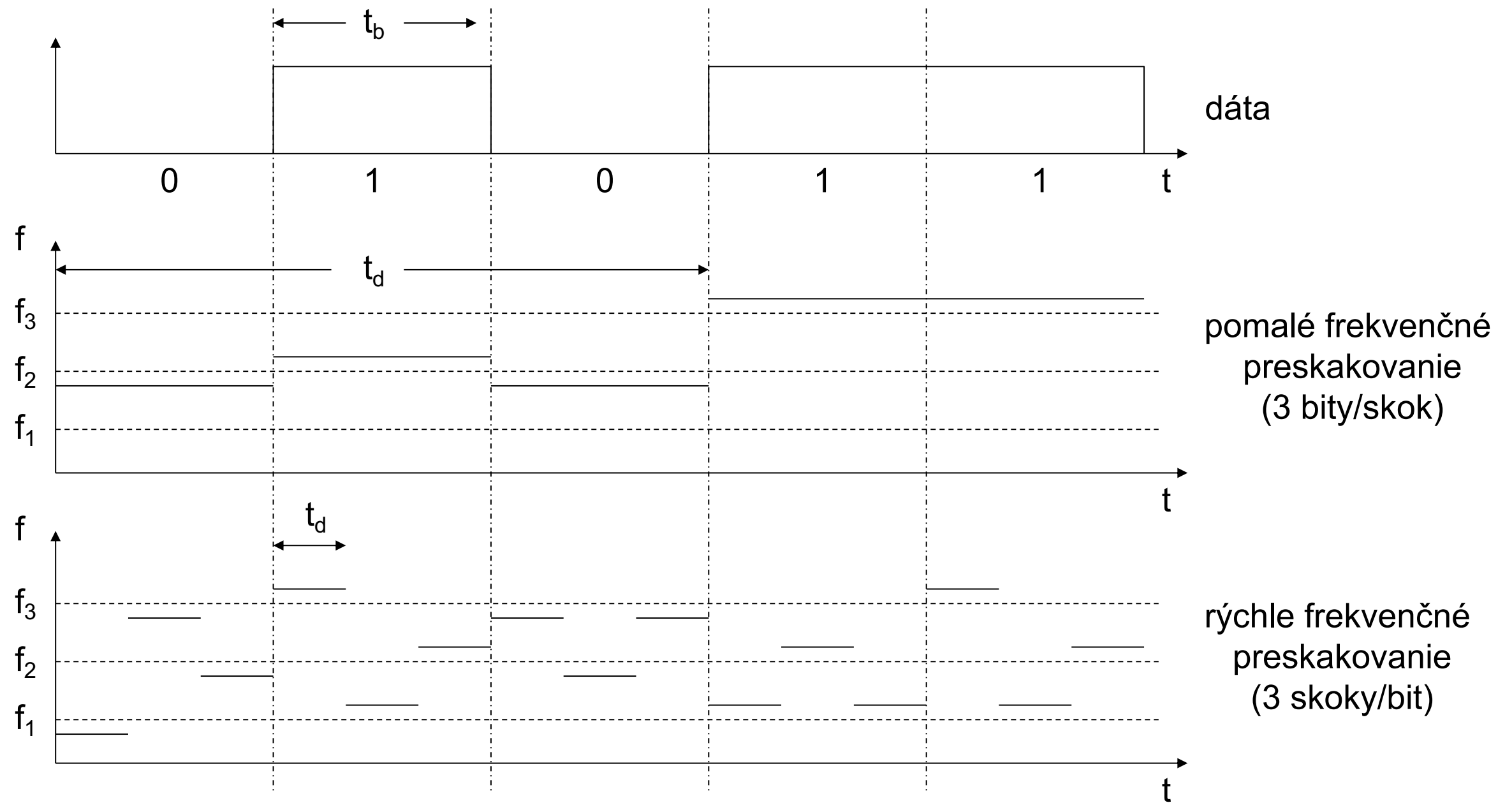
DSSS



FHSS (Frequency Hopping Spread Spectrum)

- Diskrétne zmeny nosnej frekvencie
 - postupnosť frekvenčných zmien je určená prostredníctvom sekvencie pseudo-náhodného čísla
- Dve možnosti
 - Fast Hopping (rýchle frekvenčné preskakovanie): niekoľko frekvencií na používateľský bit
 - Slow Hopping (pomalé frekvenčné preskakovanie): niekoľko používateľských bitov na frekvenciu
- Výhody
 - frekvenčný fading a rušenie je obmedzené len na krátku periódu
 - jednoduchá implementácia voči DSSS
 - využíva iba malú časť spektra v určitom čase voči DSSS
- Nevýhody
 - nie je až také robustné (odolné voči rušeniu) ako DSSS
 - jednoduchšie na detekovanie

FHSS



t_b : trvanie bitu t_d : doba pokoja

802.11 – Vrstvy a funkcie

- MAC
 - prístupové mechanizmy, fragmentácia, šifrovanie
- Riadenie MAC
 - synchronizácia, roaming, MIB, power management

DLC	LLC		Station Management
	MAC	MAC Management	
PHY	PLCP	PHY Management	
	PMD		

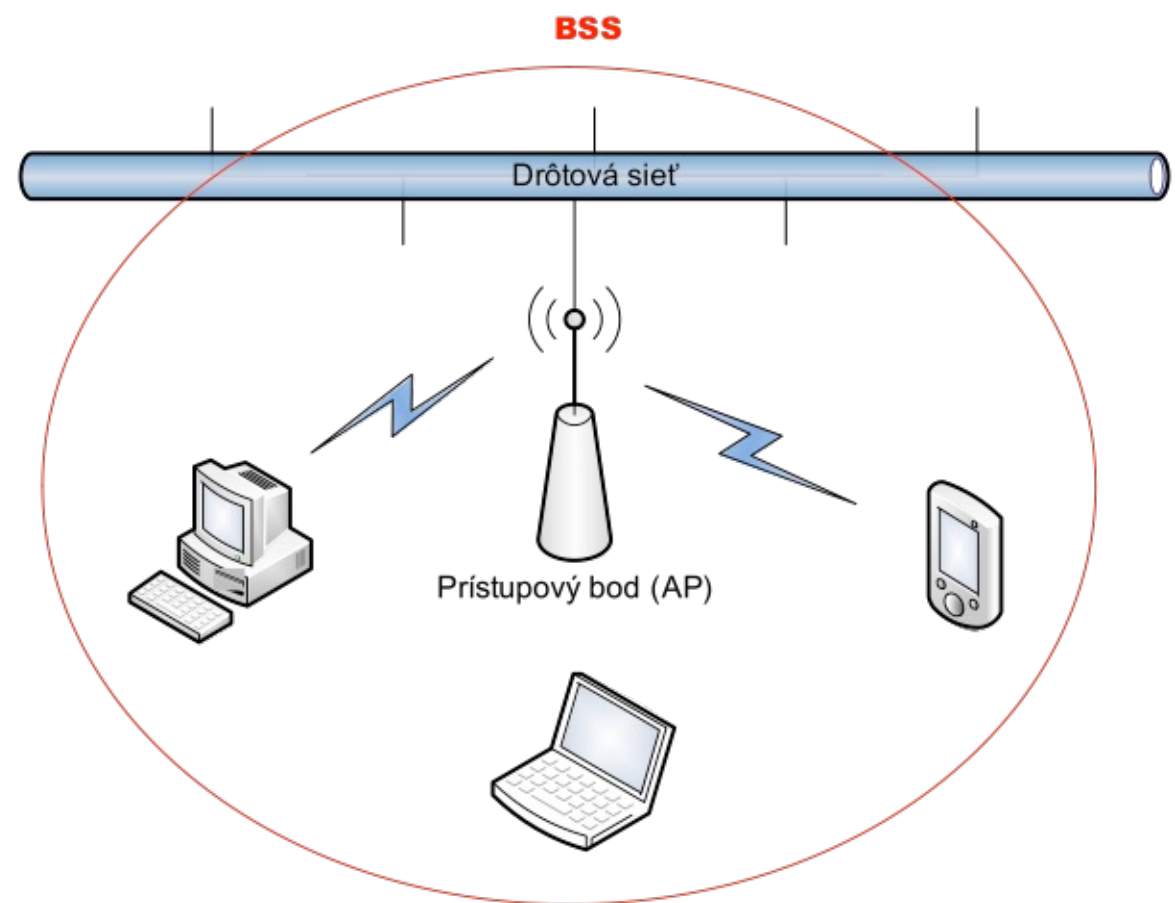
- PLCP Physical Layer Convergence Protocol
 - snímanie nosnej
- PMD Physical Medium Dependent (závislé na fyzickom médiu)
 - modulácia, kódovanie
- PHY Management
 - výber kanála, MIB
- Station Management
 - koordinácia všetkých funkcií riadenia

Séria štandardov 802.11

	802.11a	802.11b	802.11g	802.11n	802.11ac
Štandard schválený	Júl 1999	Júl 1999	Jún 2003	Október 2009	2013
Maximálna prenosová rýchlosť	54 Mb/s	11 Mb/s	54 Mb/s	150 Mb/s MIMO 4x	860 Mb/s MIMO 8x; viacantenový prístup
Modulácia	OFDM	DSSS	DSSS, OFDM	OFDM 64QAM	OFDM, 256QAM
Prenosové pásmo	5 GHz	2,4 GHz	2,4 GHz	2,4, alebo 5 GHz	5 GHz
Počet priestorových tokov	1	1	1	1,2,3, alebo 4	8
Šírka kanála	20 MHz	20 MHz	20 MHz	20, alebo 40 MHz	20-160 MHz

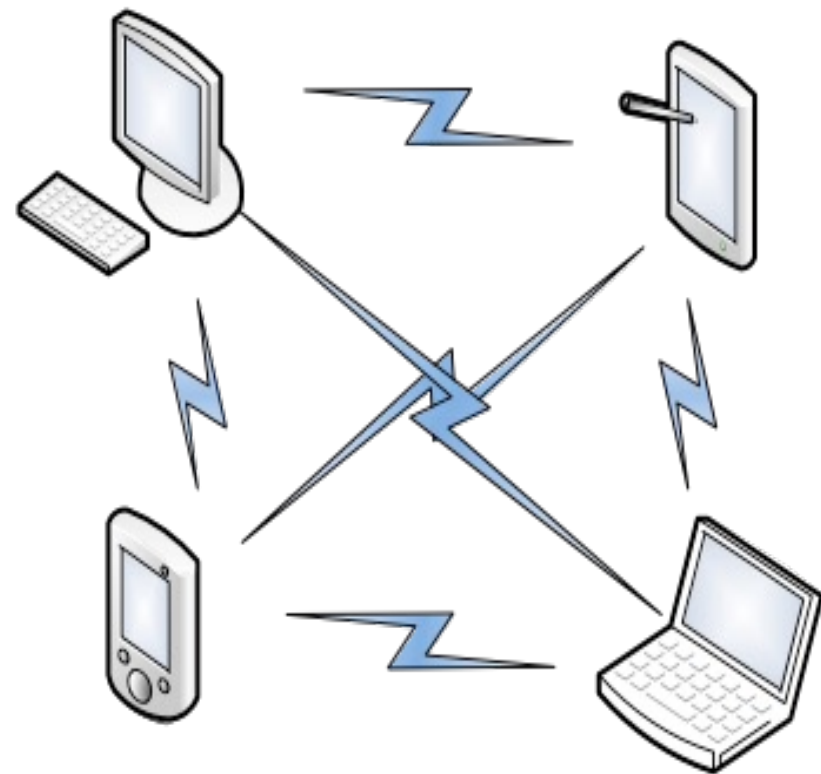
Logická architektúra - infraštruktúra

- BSS (Basic service set) –
Základná servisná jednotka
- BSS je základným stavebným
blokom pre siete 802.11.
- Ak sa stanica vzdaľuje od AP, jej
prenosová rýchlosť klesá.
- V prípade, že sa dostane za
hranicu BSS, komunikácia s AP
bude prerušená.
- Všetky zariadenia komunikujú
prostredníctvom AP, teda nemôžu
komunikovať medzi sebou
priamo.
- BSS má jedno Service Set ID
(SSID).



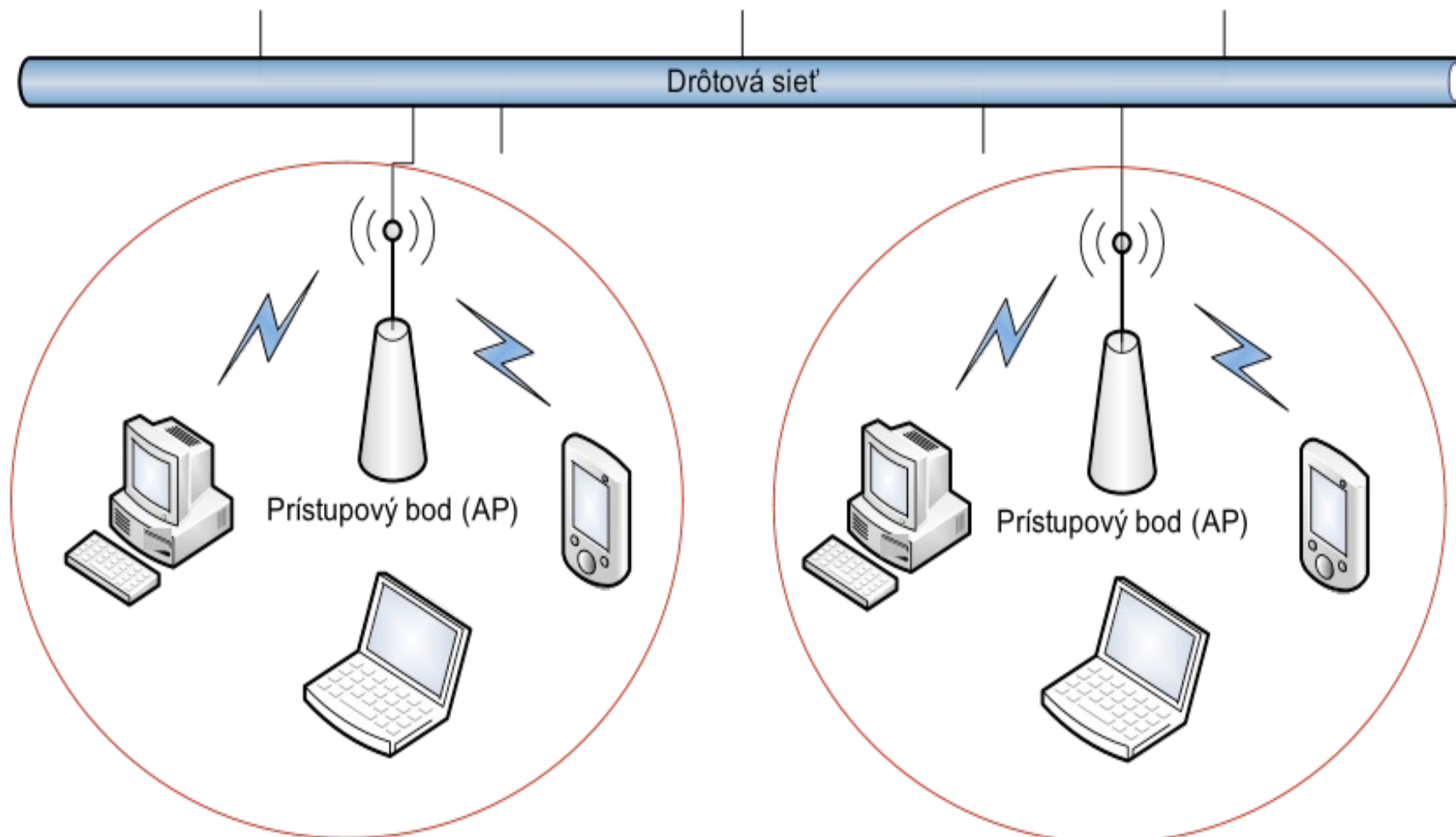
Logická architektúra - bez infraštruktúry

- Nezávislé BSS (IBSS – Independent Basic Service Set)
- Stanice komunikujú priamo medzi sebou.
- Takéto typy sietí vznikajú ako dočasné riešenia spojenia medzi koncovými bodmi a tento typ sietí je známy pod pojmom „ad-hoc“.



Logická architektúra - distribučný systém

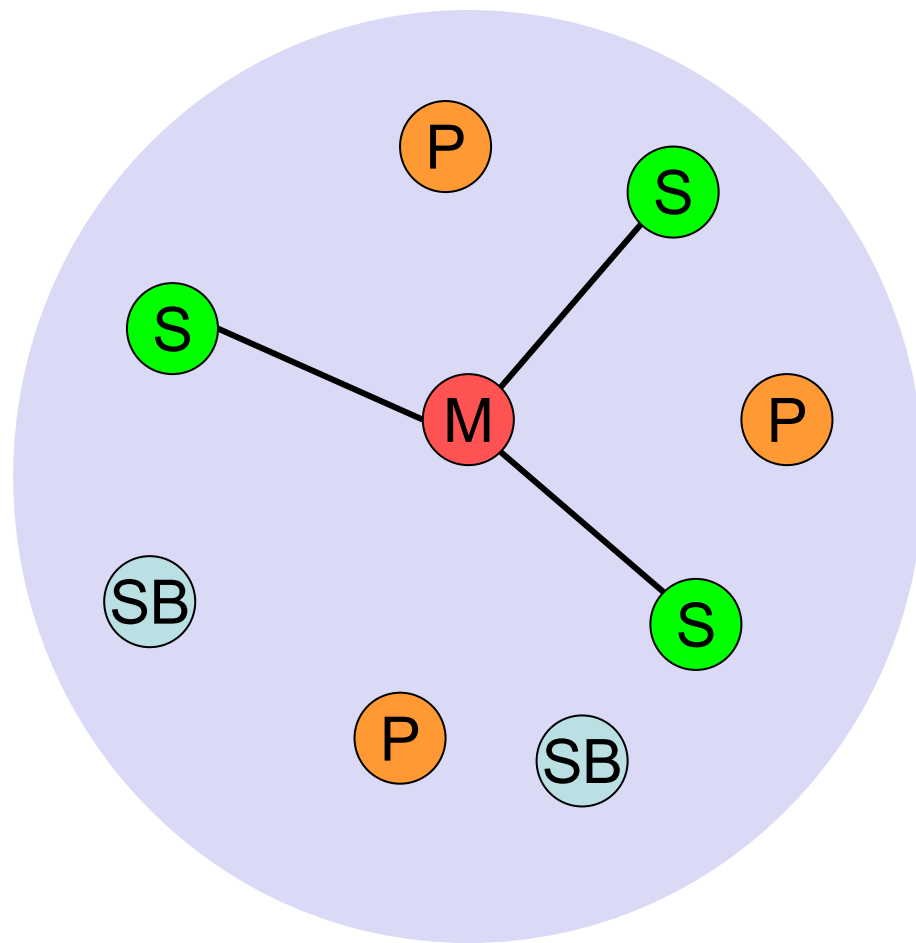
- Distribučný systém (DS – Distribution System) a Rozšírená servisná jednotka (ESS – Extended Service Set)
- Ak pokrytie jednej BSS nie je dostačujúce, spojením viacerých vzniká ESS.
- ESS je pripojená k spoločnému DS (LAN, alebo WAN sieť).



Architektúra BT - Piconet

- Súbor zariadení zapojených v ad hoc tvare
- Jedno zariadenie funguje ako master a ostatné ako slave po čas života piconetu. (volané zariadenie je masterom)
- Master určuje skokovú vzorku, slaveovia sa musia synchronizovať.
- Každý piconet má jedinečnú skokovú vzorku (FHS) a TDD v časových slotoch
- Zapojenie v piconete = synchronizácia na skokovú sekvenciu.
- Každý piconet má jedného mastera a do 7 simultánných aktívnych staníc (>200 môže byť zaparkovaných)

Piconet - obrázok



M=Master P=Parked
S=Slave SB=Standby

Vytvorenie Piconetu

- Master dáva slaveovi svoje hodiny a ID zariadenia (jednoznačná identifikácia BT zariadenia – 48 bit)
 - Hopping pattern: určená cez ID zariadenia (48 bit, svetovo jedinenčné)
 - Fáza v skokovej vzorke určená hodinami -
--Phase in hopping pattern determined by clock
- Adresovanie
 - Active Member Address (AMA, 3 bit)
 - Parked Member Address (PMA, 8 bit)

Rádiová fyzická vrstva

- FHSS ((Frequency Hopping Spread Spectrum):
 - min. 2.5 frequency hops/s (USA), two-level GFSK modulácia
- DSSS (Direct Sequence Spread Spectrum)
 - DBPSK modulácia pre 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK pre 2 Mbit/s (Differential Quadrature PSK)
 - preambula a hlavička rámca je vždy prenesená rýchlosťou 1 Mbit/s, zvyšok prenosu 1 alebo 2 Mbit/s
 - chipová sekvencia: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barkerov kód)
 - max. vyžiarený výkon 1 W (USA), 100 mW (EU), min. 1mW

Spread spektrum

- „Rozprestretie“ signálu do širšieho frekvenčného pásma
 - Bezpečnosť, zvýšenie odolnosti prenosu
- Dva prístupy:
 - Direct Sequence Spread Spectrum (DSSS)
 - Frequency Hopping Spread Spectrum (FHSS)

DSSS (Direct Sequence Spread Spectrum)

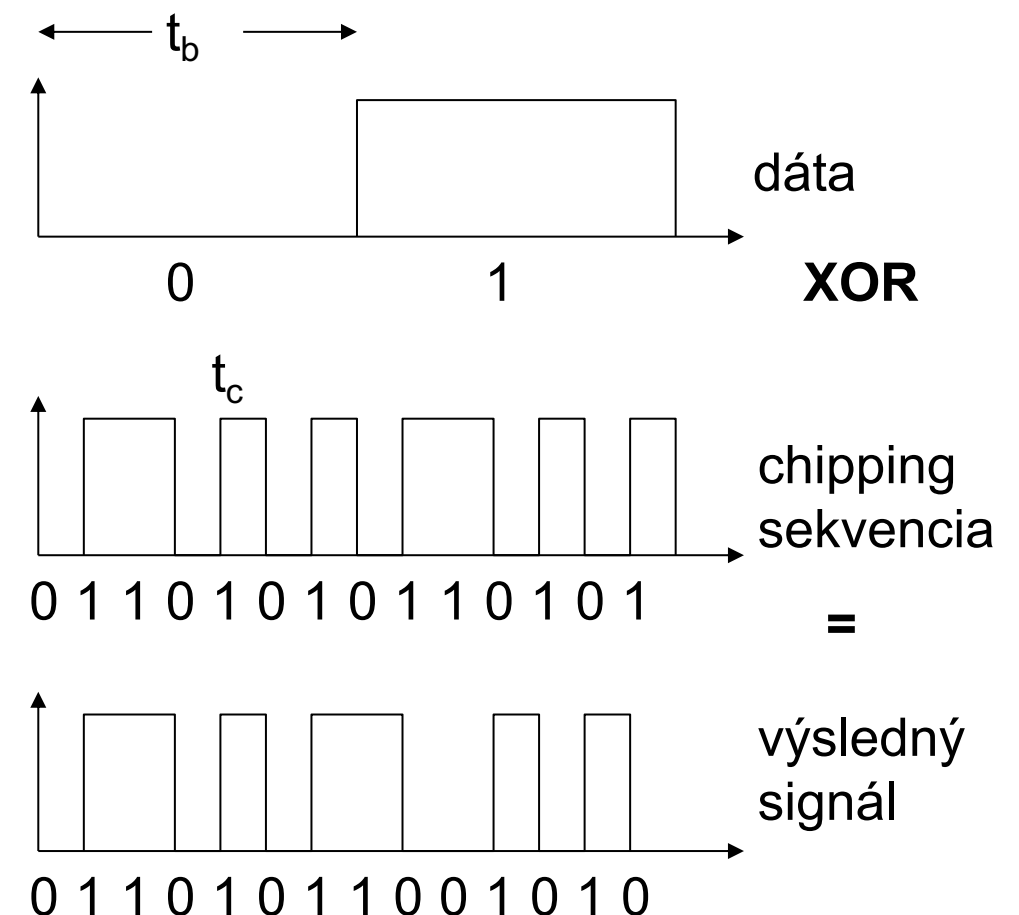
- “XORovanie” signálu so pseudonáhodným číslom (chipping sekvencia)
 - veľa “chipov” na bit (napr. 128) má za výsledok väčšiu šírku pásma signálu

- Výhody

- znižuje frekvenčný fading
- v celulárnych sieťach
 - základňové stanice môžu využívať rovnaké frekvenčné pásmo
 - niekoľko základňových staníc môže detekovať a obnoviť signál
- soft handover

- Nevýhody

- je potrebná presná výkonová kontrola



t_b : bitová perióda

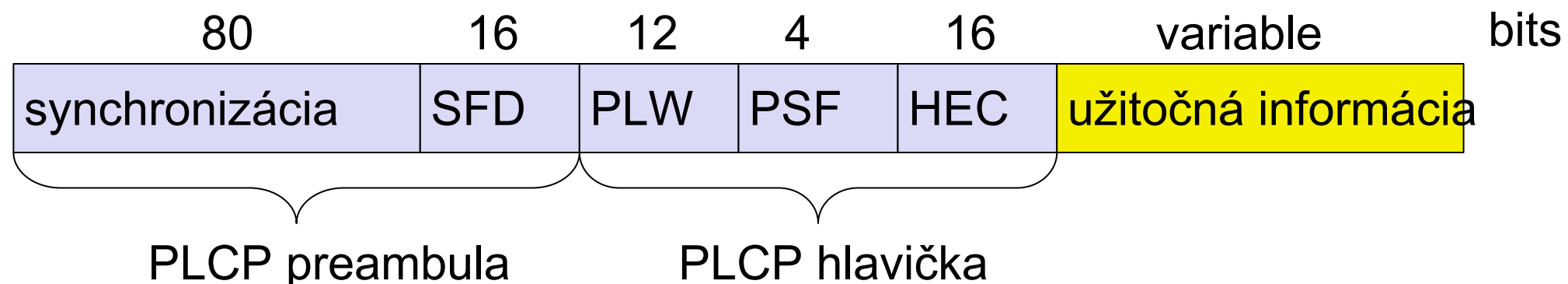
t_c : perióda chipu

FHSS (Frequency Hopping Spread Spectrum)

- Diskrétne zmeny nosnej frekvencie
 - postupnosť frekvenčných zmien je určená prostredníctvom sekvencie pseudo-náhodného čísla
- Dve možnosti
 - Fast Hopping (rýchle frekvenčné preskakovanie): niekoľko frekvencií na používateľský bit
 - Slow Hopping (pomalé frekvenčné preskakovanie): niekoľko používateľských bitov na frekvenciu
- Výhody
 - frekvenčný fading a rušenie je obmedzené len na krátku periódu
 - jednoduchá implementácia voči DSSS
 - využíva iba malú časť spektra v určitom čase voči DSSS
- Nevýhody
 - nie je až také robustné (odolné voči rušeniu) ako DSSS
 - jednoduchšie na detekovanie

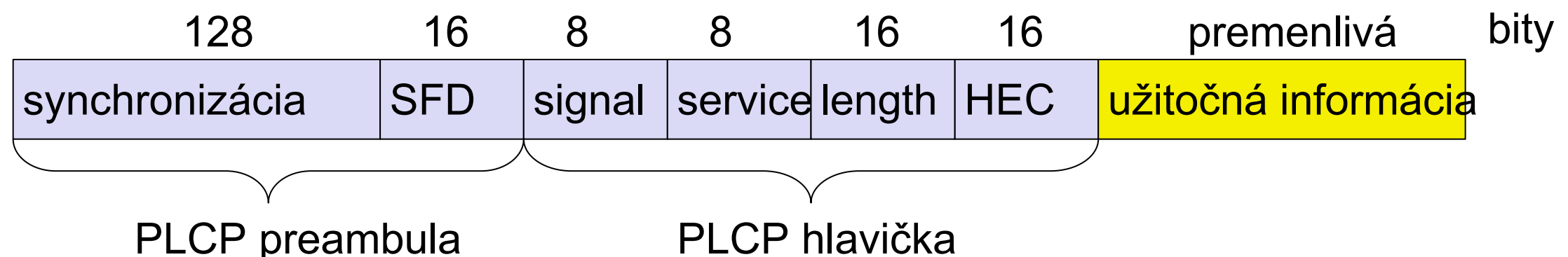
FHSS PHY packet format

- Synchronizácia
 - synchronizuje sa so vzorkou 010101...
- SFD (Start Frame Delimiter) Oddelovač začiatku rámca
 - 0000110010111101 start pattern (štartovacia vzorka)
- PLW (PLCP_PDU Length Word)
 - dĺžka užitočnej informácie zahŕňa 32 bitové CRC užitočnej informácie, $PLW < 4096$
- PSF (PLCP Signaling Field) Signalizačné pole
 - užitočné dáta (1 alebo 2 Mbit/s)
- HEC (Header Error Check) Kontrola chyby hlavičky
 - CRC s $x^{16}+x^{12}+x^5+1$



DSSS PHY packet format

- Synchronizácia
 - synch., nastavenie zosilnenia, detekcia energie, kompenzácia frekvenčného posunu
- SFD (Start Frame Delimiter) Oddelovač začiatku rámca
 - 1111001110100000
- Signál
 - užitočná prenosová rýchlosť (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- Služba: pre budúce použitie, 00: 802.11 compliant
- Dĺžka: dĺžka užitočnej informácie
- HEC (Header Error Check) Kontrola chyby hlavičky
 - ochrana signálu, service and length, $x^{16}+x^{12}+x^5+1$

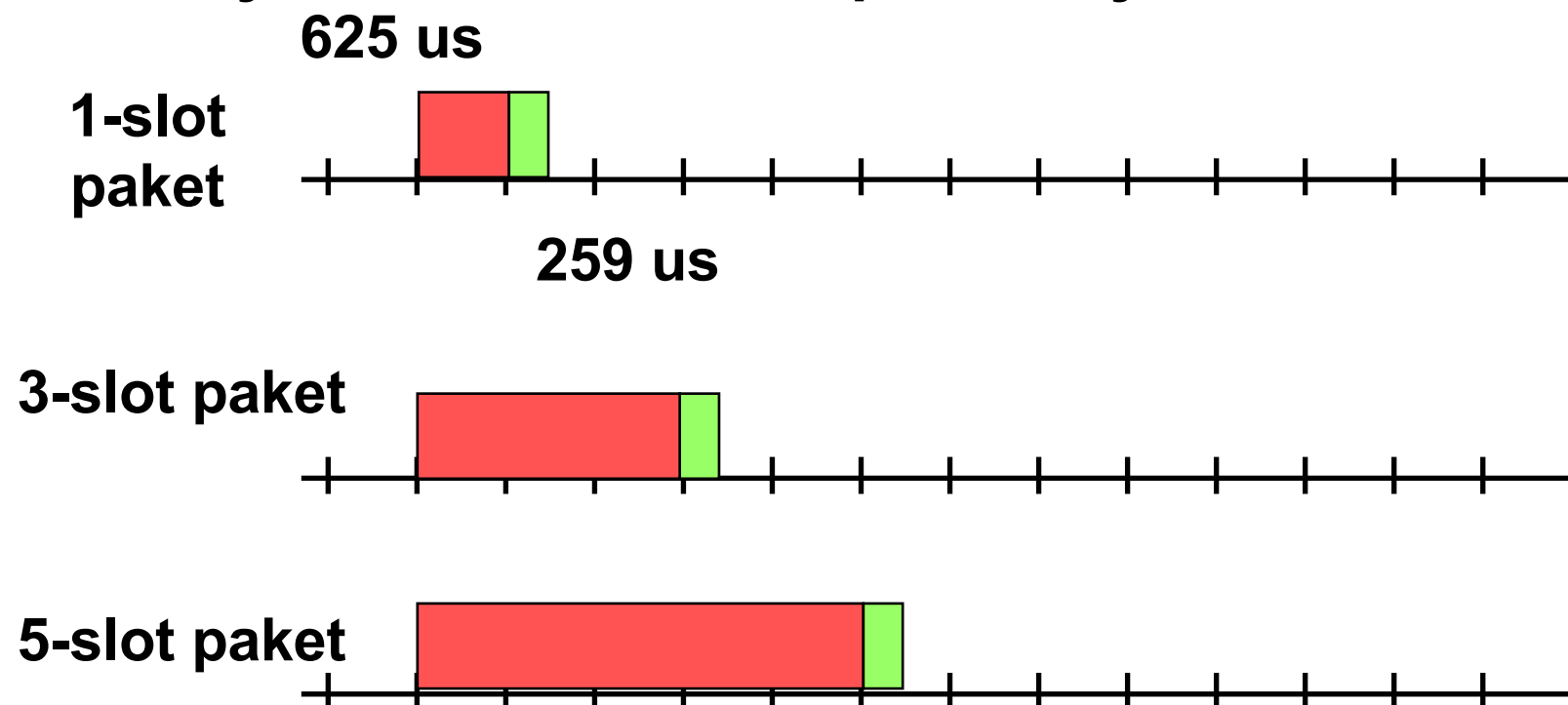


Fyzická vrstva

- Štandard z roku 1999 definoval 3 rozhrania:
 1. Frequency-hopping (FH) spread-spectrum radio PHY
 2. Direct-sequence (DS) spread-spectrum radio PHY
 3. Infrared light (IR) PHY
- Rozšírenia dodefinovali:
 1. 802.11a: Orthogonal Frequency Division Multiplexing (OFDM) PHY
 2. 802.11b: High-Rate Direct Sequence (HR/DS or HR/DSSS) PHY
 3. 802.11g: Extended Rate PHY (ERP)
 4. 802.11n, which is colloquially called the MIMO PHY or the High-Throughput PHY

Typy BT paketov

- Základný paket: 625 us (625 bit pri 1Mbit/s)
- 259 us je čas potrebný na zmeny z vysielacza na prijímač a na novú frekvenciu
- Pre podporu vyšších rýchlostí sú definované 3 slot pakety a 5 slotové pakety

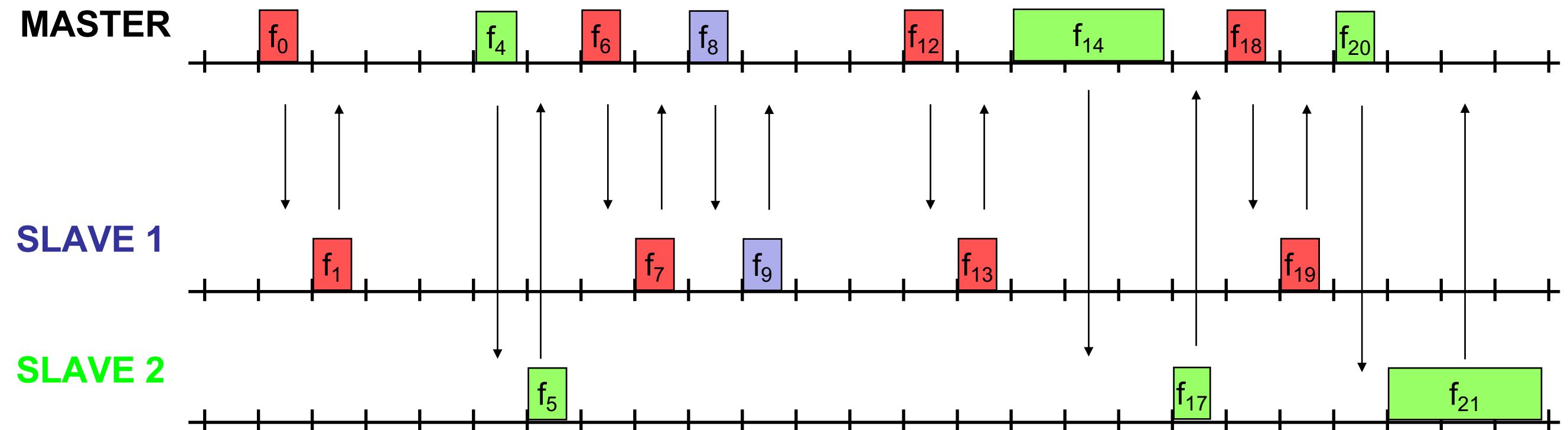


Dátové rychlosti základného pásma

Payload Header		User Payload	Symmetric max. Rate			Asymmetric max. Rate	
Type	[byte]	[byte]	FEC	CRC	[kbit/s]	Forward	Reverse
DM1	1	0-17	2/3	yes	108.8	108.8	108.8
DH1	1	0-27	no	yes	172.8	172.8	172.8
DM3	2	0-121	2/3	yes	258.1	387.2	54.4
DH3	2	0-183	no	yes	390.4	585.6	86.4
DM5	2	0-224	2/3	yes	286.7	477.8	36.3
DH5	2	0-339	no	yes	433.9	723.2	57.6
AUX11		0-29	no	no	185.6	185.6	185.6
HV1		na	10	1/3	no	64.0	
HV2		na	20	2/3	no	64.0	
HV3		na	30	no	no	64.0	
DV	1 D	10+(0-9) D	2/3 D	yes D		64.0+57.6 D	

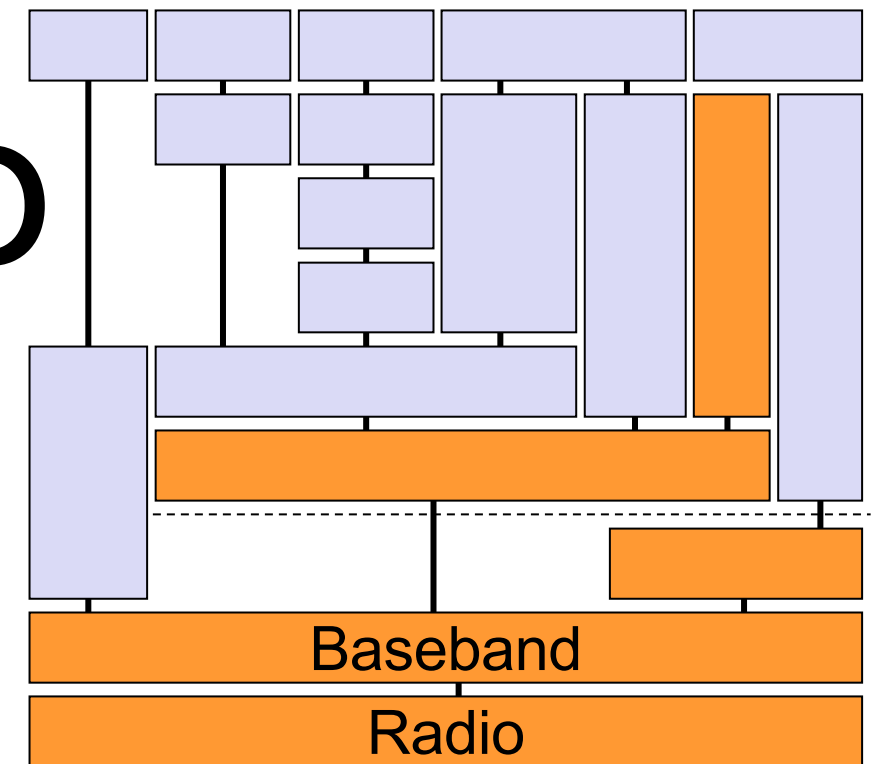
Vysielaie BT

- Polling-based TDD vysielaie pre ACL
 - 625 μ s slots, master polls slaves
- SCO (Synchronous Connection Oriented) po broadcaste od mastera
 - Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point

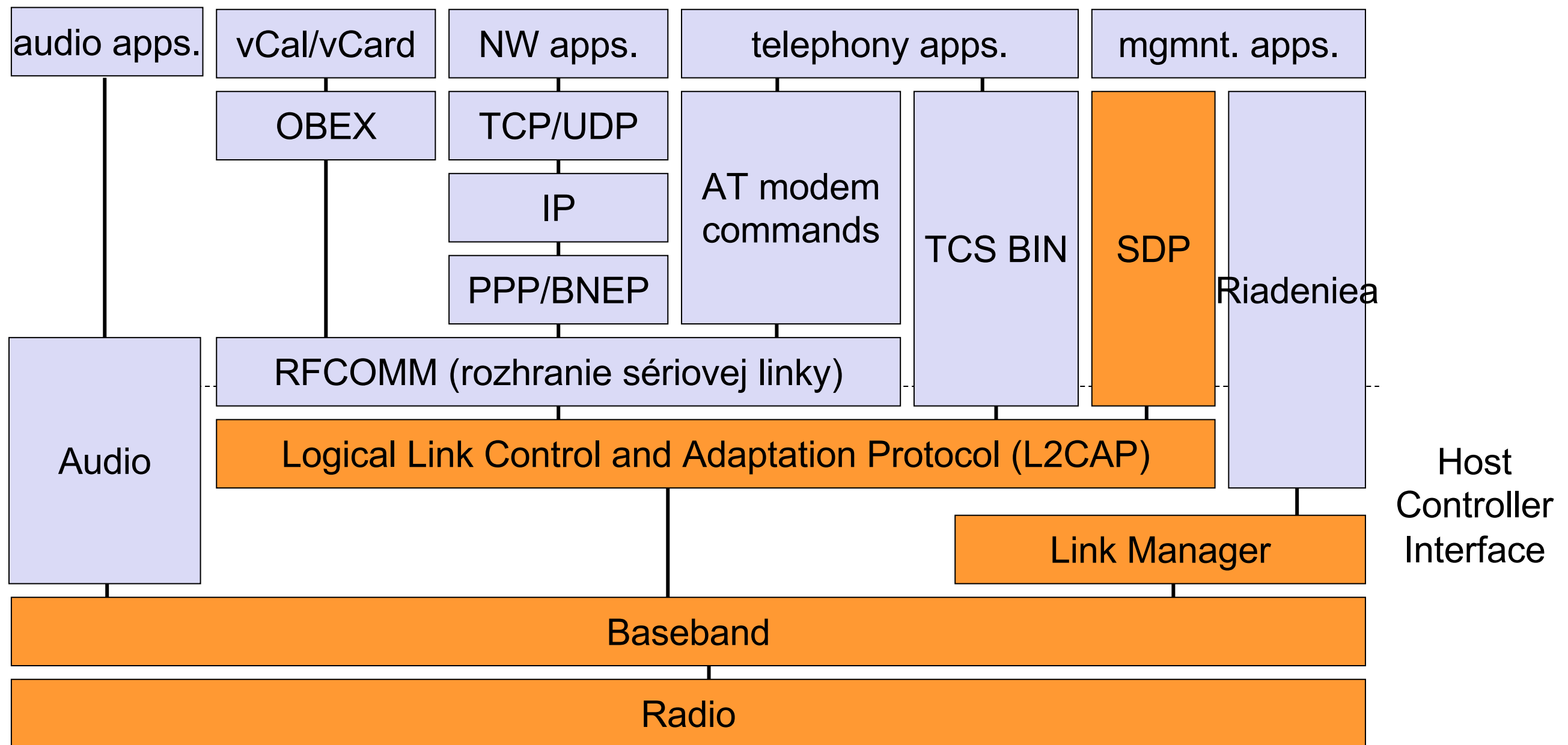


Vrstva radio

- Definuje charakteristiky pre BT rádio rozhranie
- Je definované pre nelicencované pásmo (2.4 GHz) – prichádza k interferenciám s inými technológiami
- Používa FEC
- Nominálna dosah je 10m – 0dBm
- Rozšírený dosah 20dBm (100mW)
- Používa BFSK moduláciu



Bluetooth protocol stack



AT: attention sequence

OBEX: object exchange

TCS BIN: telephony control protocol specification – binary

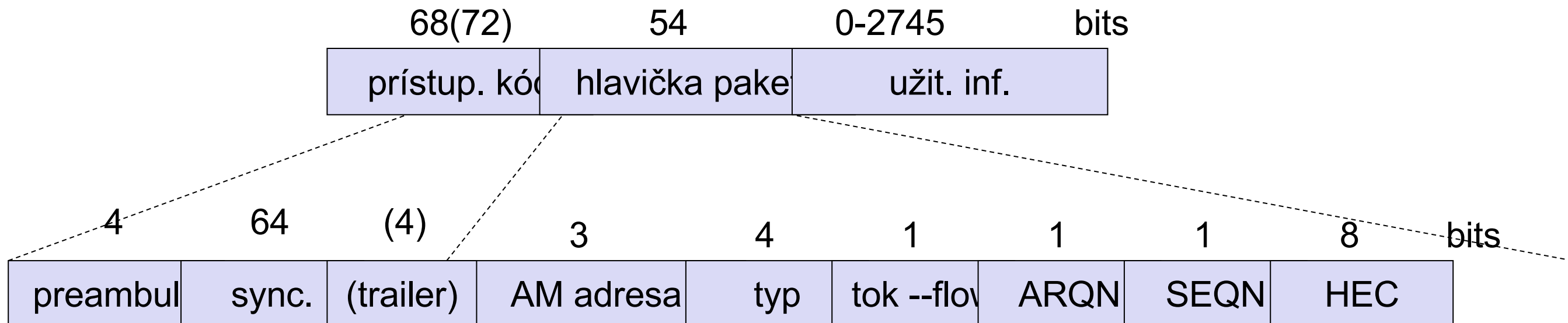
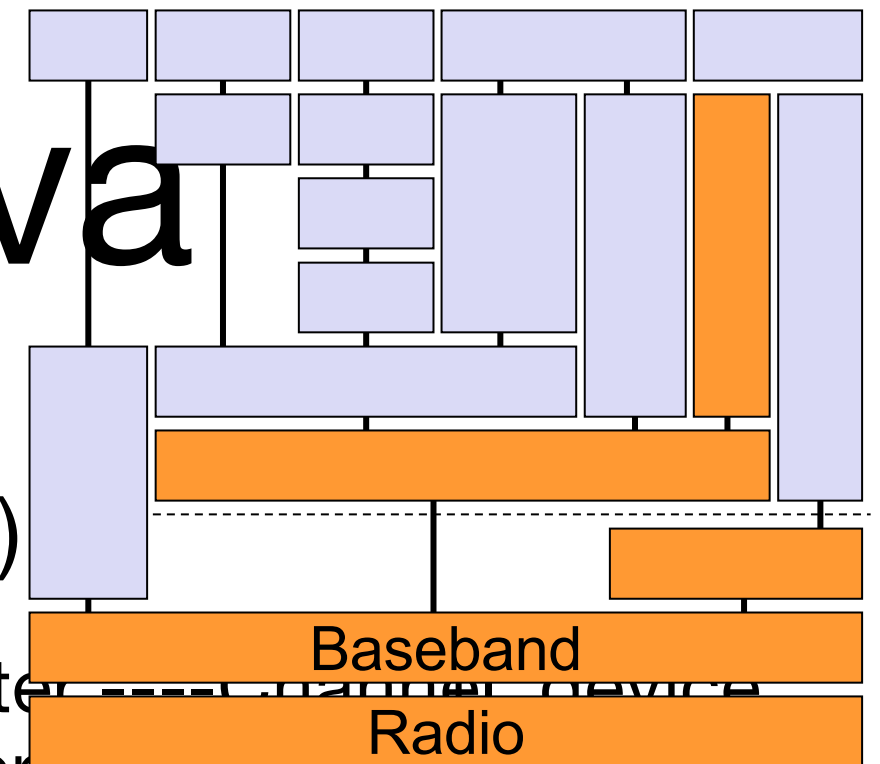
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol

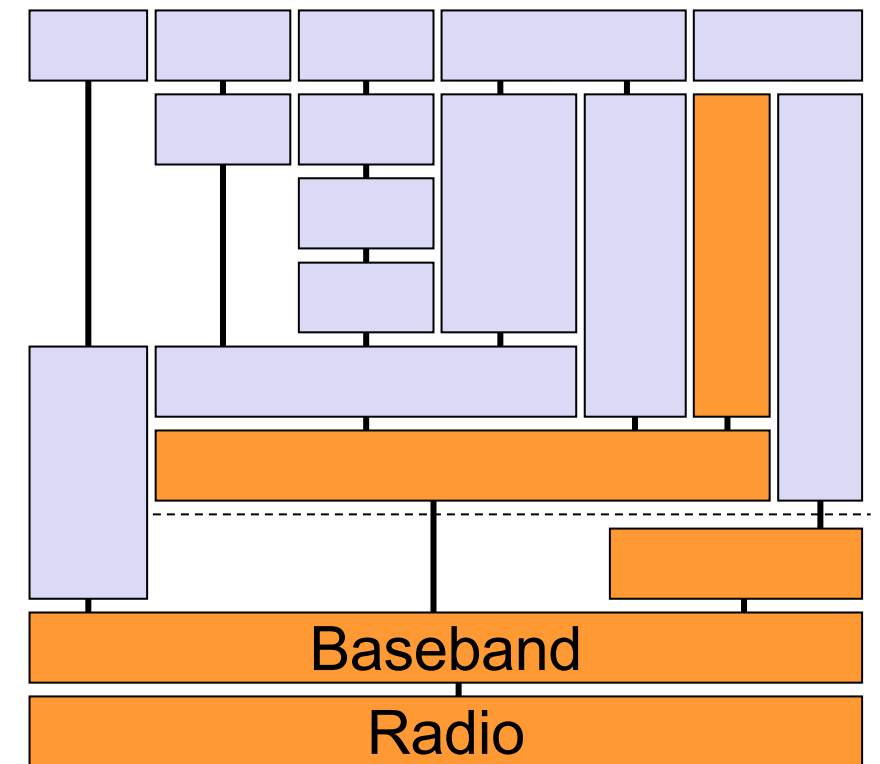
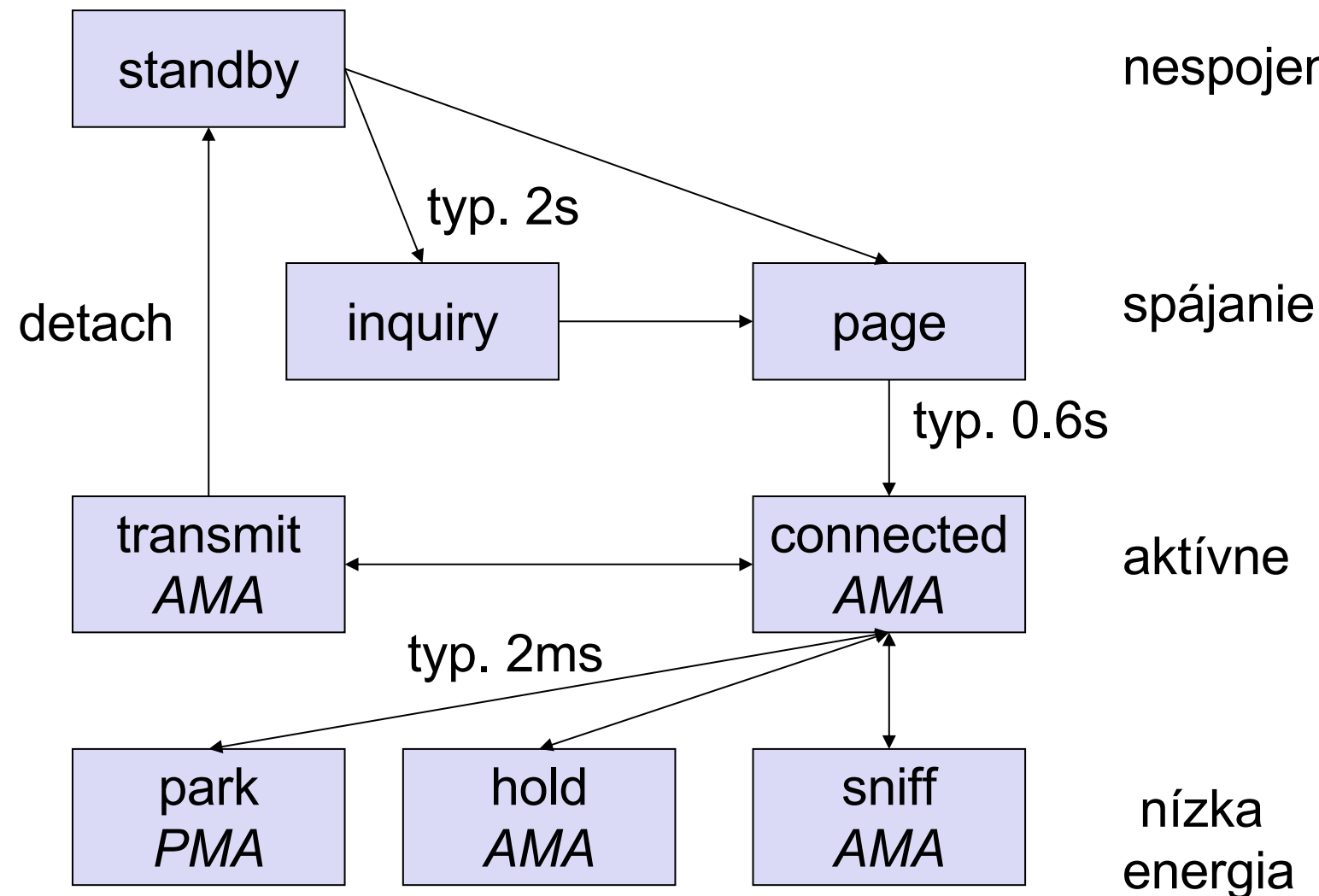
RFCOMM: radio frequency comm.

Baseband vrstva

- Low-level packet definition
- Prístupový kód (Access code)
 - Kanál, , napr. odvodené od master access, e.g., derived from master
- Hlavička paketu (Packet header)
 - 1/3-FEC, aktívna členská adresa (1 master, 7 slaveov), typ linky, alternating bit ARQ/SEQ, kontrolný súčet



Stavy základného pásma BT



Standby: nič nerobí
 Inquire: hľadať ďalšie zariadenia
 Page: pripoj sa k špecifickému zar.
 Connected: zapojenie sa do piconetu
 Park: release AMA, get PMA
 Sniff: počúva periodicky, nie každý slot
 Hold: stop ACLs, SCO still possible, possibly participate in another piconet

802.11a PHY - modulácie a prenosové rýchlosti

- IEEE 802.11a používa OFDM (Orthogonal Frequency Division Multiplexing) – ortogonálnu moduláciu s frekvenčným multiplexom.
- Táto technológia rozdelí komunikačný kanál na niekoľko podkanálov s totožnou šírkou pásma a konštantnými odstupmi medzi jednotlivými podkanálmi.
- používa 52 nosných frekvencií s rozstupom 312,5 KHz.
- Dáta sú zasielané súčasne na 48 nosných, pričom každá nosná prenáša istú časť dát od užívateľa
- 4 nosné sú použité ako pilotné
- Každá nosná je ortogonálna (a teda nezávislá) od ostatných.

802.11a PHY - modulácie a prenosové rýchlosti – meniac sa kvalita

Kódovacia technika	Modulačná technika	Prenosová rýchlosť
OFDM	BPSK	6 Mb/s
OFDM	BPSK	9 Mb/s
OFDM	QPSK	12 Mb/s
OFDM	QPSK	18 Mb/s
OFDM	16QAM	24 Mb/s
OFDM	16QAM	36 Mb/s
OFDM	64QAM	48 Mb/s
OFDM	64QAM	54 Mb/s

802.11 MAC vrstva

- Definuje 3 služby:
 1. Asynchrónne dátové služby
 2. Služby pre zabezpečenie bezpečnosti
 3. Riadenie MSDU

Typy MAC rámcov

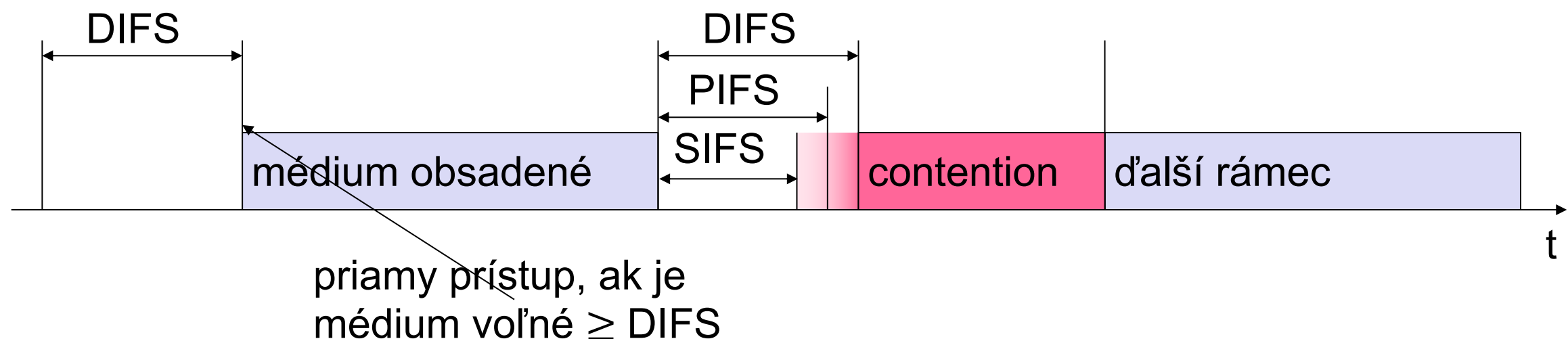
- Existujú tri základné typy MAC rámcov :
- Dátové rámce
 - prenášajú samotné dáta poskytované vyššími vrstvami
- Kontrolné rámce
 - zabezpečujú kontrolu prístupu k médiu (CTS, RTS, ACK)
- Riadiace rámce
 - prenášajú tak ako dátové rámce, avšak nie sú postúpené vyšším vrstvám (napr. signálne rámce)

Prístupové metódy

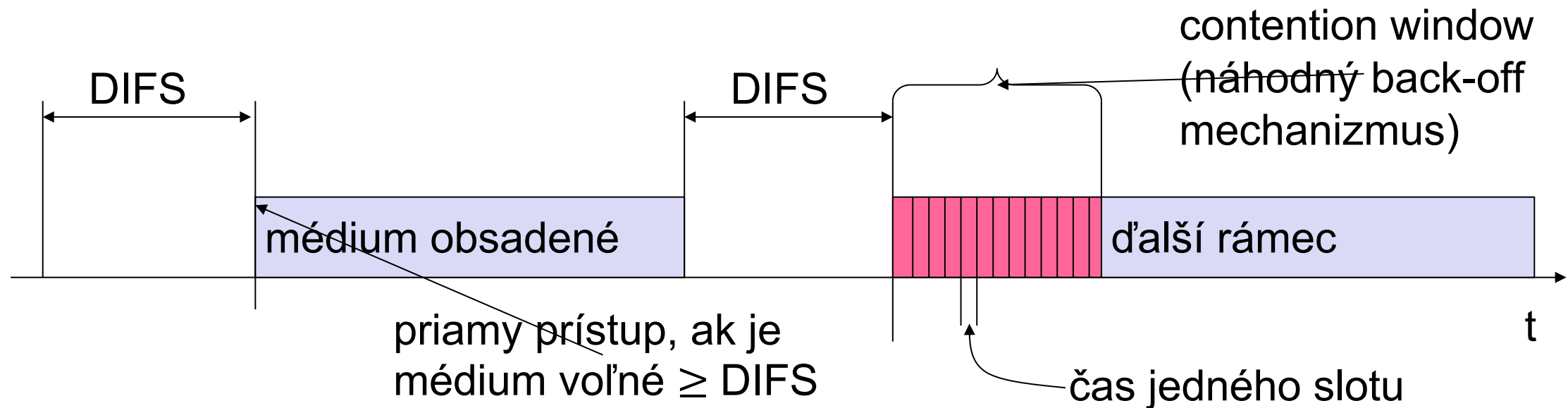
- **DFWMAC-DCF CSMA/CA (povinná)**
- vyvarovanie sa kolízii náhodným „back-off“ mechanizmom
- minimálna vzdialenosť medzi nasledujúcimi paketmi
- ACK paket pre potvrdenia (nie pre broadcasty)
- **DFWMAC-DCF w/ RTS/CTS (voliteľná)**
- Distributed Foundation Wireless MAC
- vyvaruje sa problému skrytého terminálu –avoids hidden terminal problem
- **DFWMAC- PCF (voliteľná)**
- prístupový bod vyberá terminály podľa zoznamu

802.11 - MAC layer II

- IFS - Inter Frame Space
 - definované rozdielnymi medzirámcovými medzerami
 - no guaranteed, hard priorities
 - SIFS (Short Inter Frame Spacing)
 - najvyššia priorita, pre ACK, CTS, polling response
 - PIFS (PCF IFS)
 - stredná priorita, pre časovo ohraničenú službu používa PCF
 - DIFS (DCF, Distributed Coordination Function IFS)
 - najnižšia priorita, pre asynchrónnu dátovú službu
 - EIFS – je rozšírený medzi-rámcový priestor

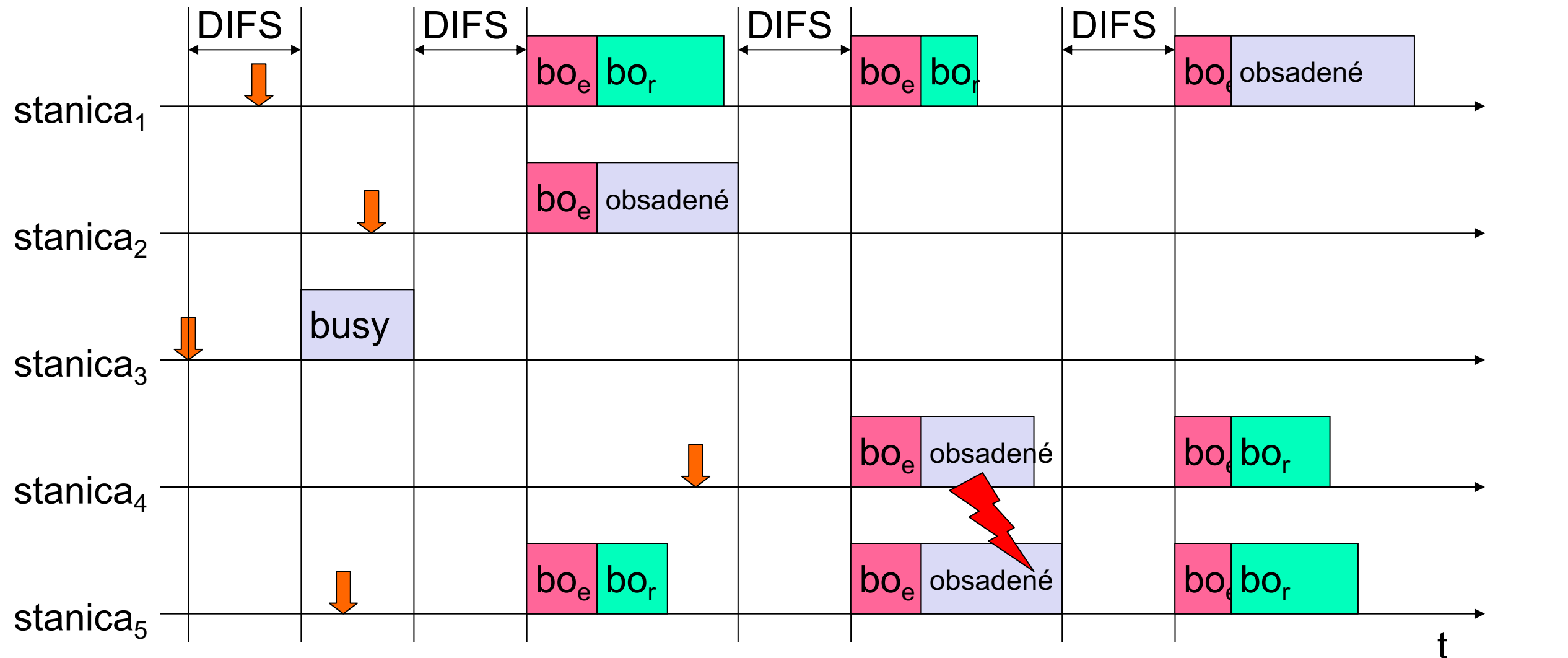


802.11 – Prístupová metóda CSMA/CA I



- stanica je pripravená na vysielanie, začína snímať médium (snímanie nosnej založené na CCA - Clear Channel Assessment)
- ak je médium voľné na čas trvania medzirámцovej medzery (Inter-Frame Space, IFS), stanica môže začať vysielat' (IFS závisí na type služby)
- ak je médium obsadené, stanica musí čakať na voľnú IFS, potom musí ešte čakať na náhodný „back-off“ čas (vyvarovanie sa kolízie, násobok času jedného slotu)
- ak sa ďalšia stanica pokúša dostať na médium počas „back-off“ času, „back-off“ časovač sa zastaví (spravodlivosť - fairness)

802.11 – súťažiace stanice – jednoduchá verzia



obsadené médium nie je voľné (rámec, ack atd.)

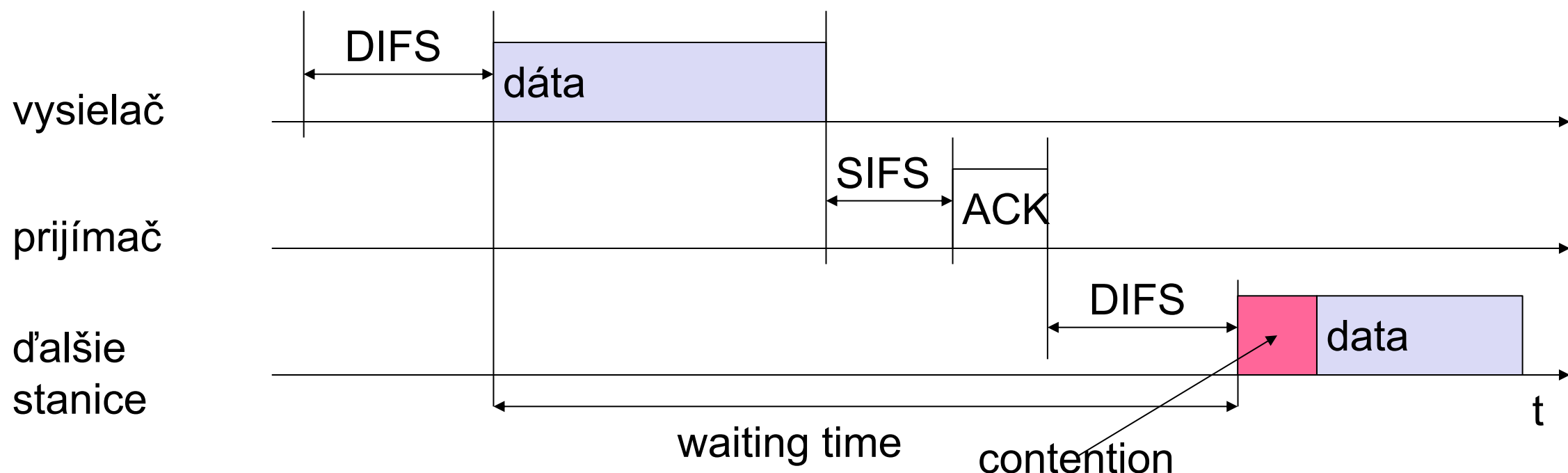
bo_e uplynutý „backoff“ čas

↓ príchod paketu do MAC

bo_r zvyškový (residual) „backoff“ čas

802.11 – Prístupová metóda CSMA/CA II

- Posielanie unicastových paketov (Sending unicast packets)
 - stanica musí čakať na DIFS predtým, ako pošle dáta
 - prijímače potvrdzujú okamžite (po čakaní na SIFS), ak bol paket prijatý správne (CRC)
 - automatická retransmisia dátových paketov v prípade prenosových chýb

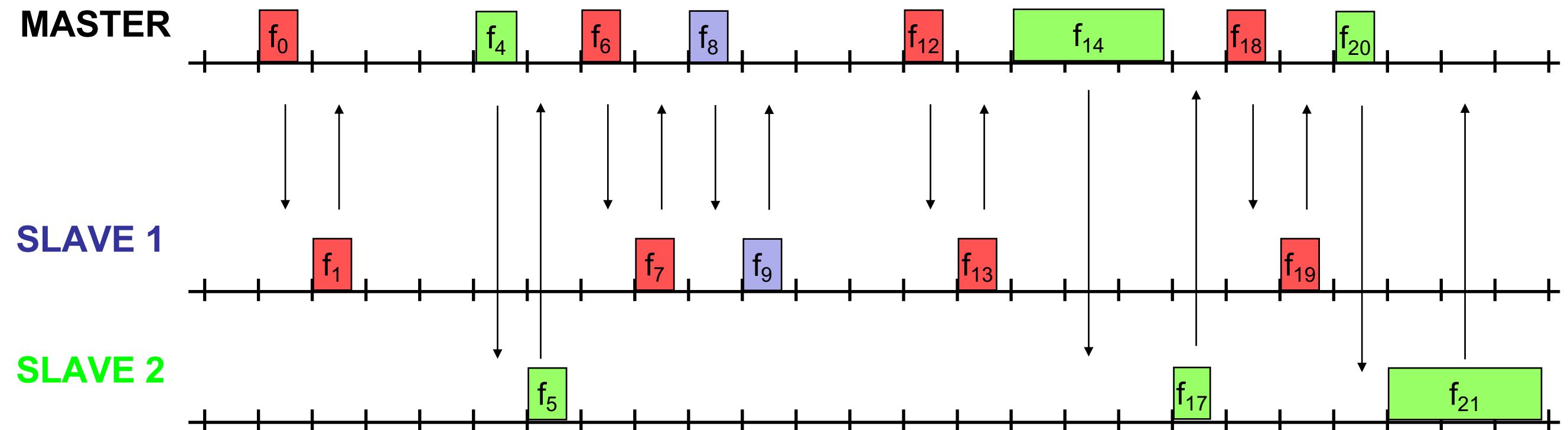


Mechanizmus detekcie vysielania (carrier sense)

- MAC zabezpečuje virtuálnu detekciu vysielania.
- Tento mechanizmus je známy pod pojmom NAV (Network allocation vector) – sieťový alokačný vektor.
- NAV zabezpečuje predpovedanie budúcej prevádzky na médiu z informácií založených na dĺžke trvania rámca získaných z unicast rámcov.
- Každá stanica udržiava svoj vlastný NAV vektor a aktualizuje ho podľa Duration poľa z hlavičky paketu
- Stanica môže vysielat' až keď je NAV=0

Vysielanie

- Polling-based TDD vysielanie pre ACL
- 625 μ s slots, master polls slaves
- SCO (Synchronous Connection Oriented) po broadcaste od mastera
- Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point

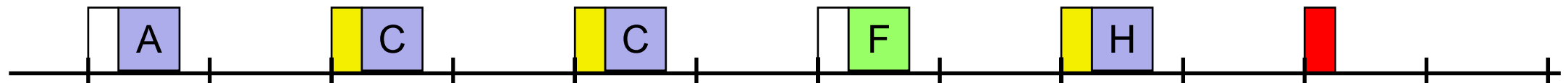


Robustnosť

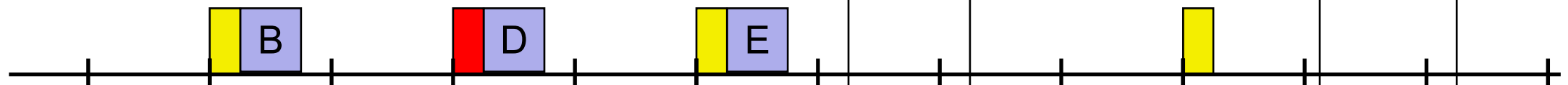
- Pomalé frekvenčné skákanie so skokovými vzorkami určenými masterom
- Ochrana proti interferencii na niektorých frekvenciách
- Oddelenie od ostatných piconetov (FH-CDMA)
- Retransmisia
- len ACL, veľmi rýchle
- Dopredná oprava chýb (Forward Error Correction)
- SCO a ACL

Robustnonst'

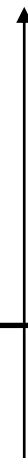
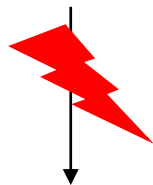
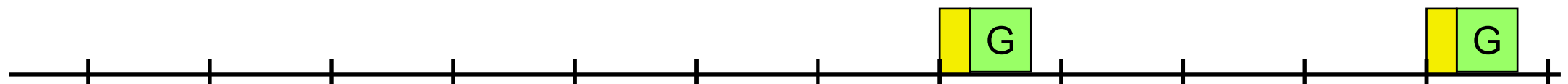
MASTER



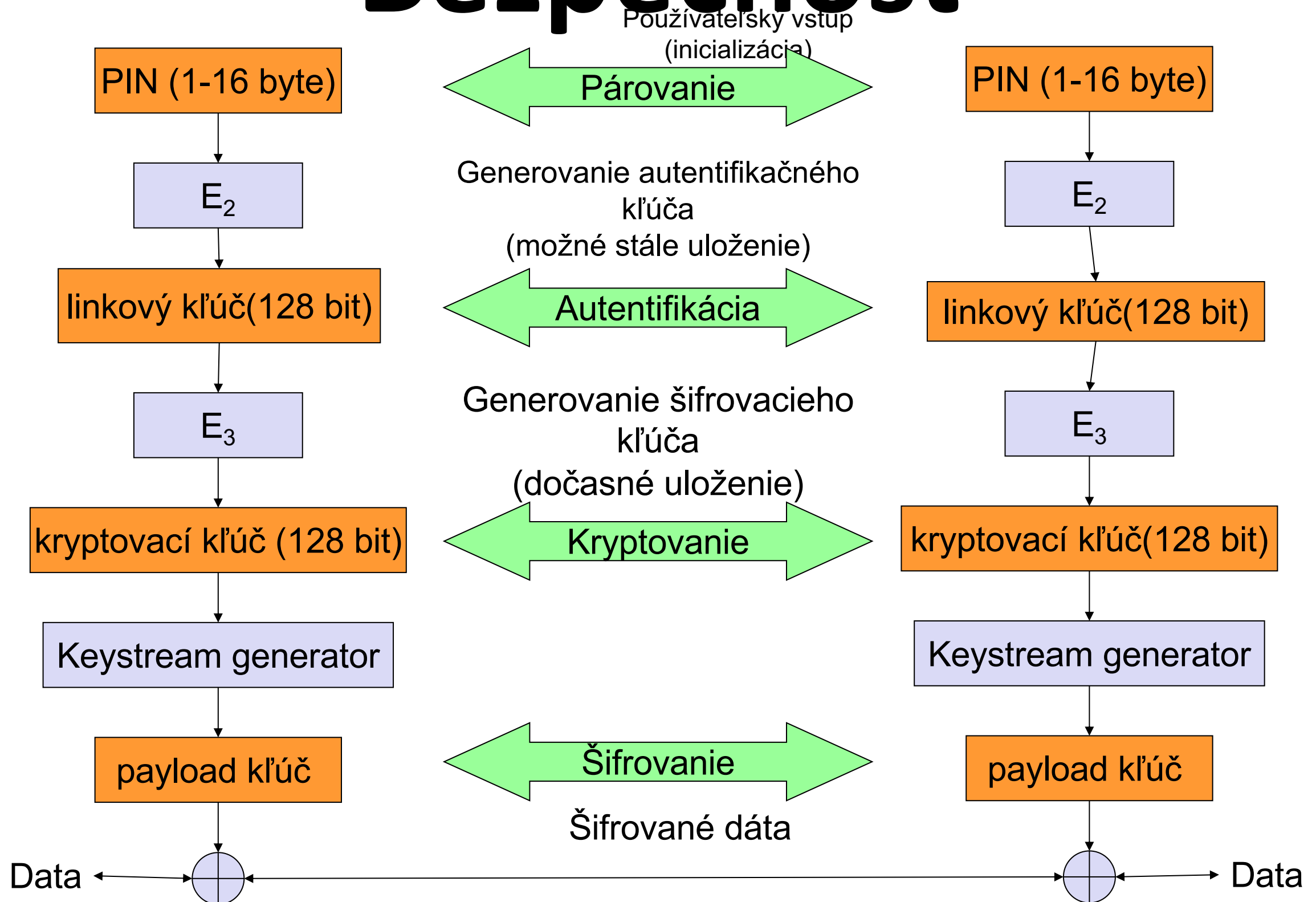
SLAVE 1



SLAVE 2



Bezpečnosť



Bluetooth 2.0 EDR

- 3 Mbit/s
- Vyššia spotreba (nižšia spotreba na bit)
– výhoda?
- Schválený štandard 2.1
- Lepšie párovanie zariadení
- EDR využíva GMSK, QPSK a 8-QPSK

Bluetooth 3.0 + HS

- Štandard z roku 2009, HS – High Speed Umožňuje párovať zariadenia cez Bluetooth a preniesť informáciu cez 802.11 (24Mbit/s)
- Zmena MAC/PHY vrstvy tak, aby umožnila prenos cez WiFi
- Vylepšenie riadenia spotreby energie

Bluetooth 4.0

- Štandard z roku 2010, obsahuje:
 - predchádzajúce štandardy
 - High Speed (HS)
 - Low Energy - WiBree

Bluetooth 5.0

- 2016
- Spätne kompatibilný
- Zvýšenie dosahu, prenosovej rýchlosti,
Prenosová rýchlosť do 2Mbit/s (BLE)
- Zameraný aj na IoT
- Zlepšenia využitia broadcastových kanálov

802.15.4 - Zigbee

- Ciel': definovať globálny štandard pre spoľahlivé, cenovo efektívne a energeticky nenáročné aplikácie
- Požiadavky:
 - 10k-250 kbps
 - Dosah 10-75 metrov
 - Výdrž 2 roky na alkalickú baterku
 - 65k slave uzlov a 10² kolokovaných sietí



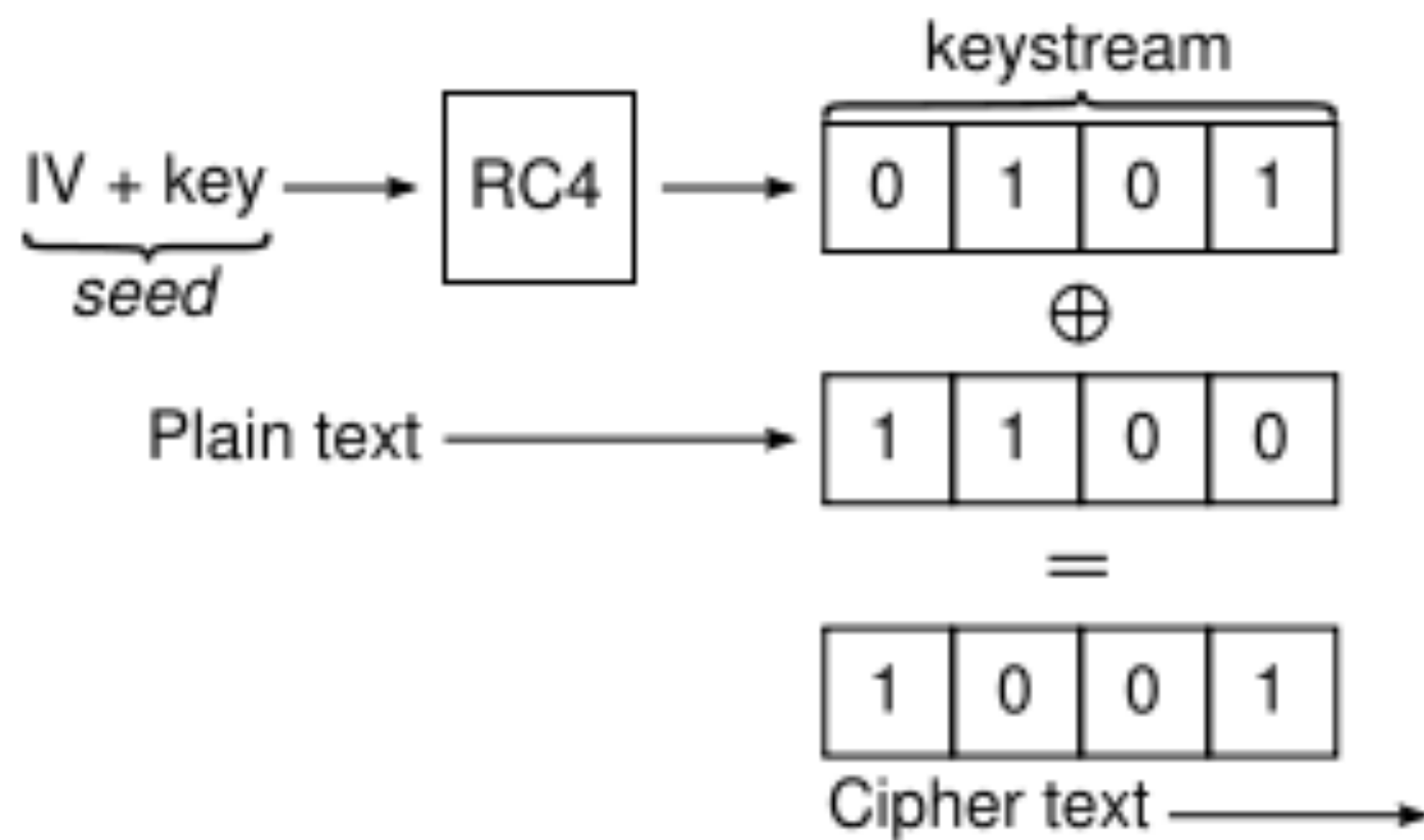
ZigBee Alliance

Wired Equivalence Privacy (WEP)

- Pôvodný algoritmus pre zabezpečenie komunikácie v bezdrôtovom prostredí
- Pochádza z roku 1999
- V 2003 bol WEP štandard nahradený podmnožinou 802.11i známou ako WPA (WiFi Protected Access)
- V 2004 bol prijatý štandard 802.11i známy aj ako WPA2

WEP - ako to funguje

- 64 bitový WEP používa 24bitový inicializačný vektor a 40bitový kľúč
- IV+kľúč tvoria RC4 kľúč
- Po uvoľnení reštrikcií na export šifrovacích technológií bol prijatý WEP104
 - Používateľ zadáva 26 hexadecimálnych znakov



Riveston Cipher 4

- Známa ako RC4, arc4, alebo arcfour šifra
- Patrí medzi najpoužívanéjšie prúdové šifry
 - používa ju napr. SSL a WEP
- Nie je bezpečná, keď sa inicializačný vektor nezničí, alebo sa používa viacnásobne

RC4 – história

- Bola navrhnutá v roku 1987 Ronom Rivestonom
- Do roku 1994 bola vedená ako obchodné tajomstvo, ale bola prelomená a zverejnená na Internete
- Neoficiálne implementácie sú legálne, ale nesmú niesť meno RC4 (preto sa používa ARC4 – Alleged)
-

Ako to funguje

- RC4 generuje pseudonáhodný tok bitov (keystream)
- Keystream je XOR ovaný so šifrovaným textom
- Dešifrovanie sa robí presne tak isto
- Na generovanie Keystreamu potrebujeme dve súčasti:
 - Pole permutácií S
 - Dva 8 bitové indexy (pointre)
 - Pseudonáhodný generátor

Key scheduling algorithmus

- Parameter dĺžka kl'úča (keylength) v bajtoch
- Hraničné hodnoty sú 1 - 256
- Typicky nadobúda hodnoty 5-16 (40-128 bit)

```
for i from 0 to 255
    S[i] := i
end
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength])
    mod 256
    swap(S[i], S[j])
endfor
```

Pseudonáhodný generátor (PRGA)

- `i := 0`
- `j := 0`
- `while GeneratingOutput:`
- `i := (i + 1) mod 256`
- `j := (j + S[i]) mod 256`
- `swap(S[i], S[j])`
- `output S[(S[i] + S[j]) mod 256]`
- `endwhile`

$j = 0$

for $i = 0$ to 7

{ $j = [j + S(i) + T(i)] \bmod 8$

vymena $S(i), S(j)$

$S:$

0	1	2	3	4	5	6	7
---	---	---	---	---	---	---	---

$T:$ 3 7 4 1 6 5 2 0

	j	i	0	1	2	3	4	5	6	7
0,	0	0	3	1	2	0	4	5	6	7
1,	3	1.	3	0	2	1	4	5	6	7
2,	1	2.	3	2	0	1	4	5	6	7
3,										

...

3 2 0 7 4 6 5 1

3	4	5	6	2	7	0	1
---	---	---	---	---	---	---	---

$j = 0$

for $i = 0$ to 7 {

$j = [j + S(i)] \bmod 8$

vy'menn $S(i) \neq S(j)$

$t = [S(i) + S(j)] \bmod 8$

$S_{out} = S(t)$

}

S_{out}

4

47

$j \quad i \quad 3 \ 4 \ 5 \ 6 \ 2 \ 7 \ 0 \ 1 \ t$

3 0 6 4 5 3 2 7 0 1 1

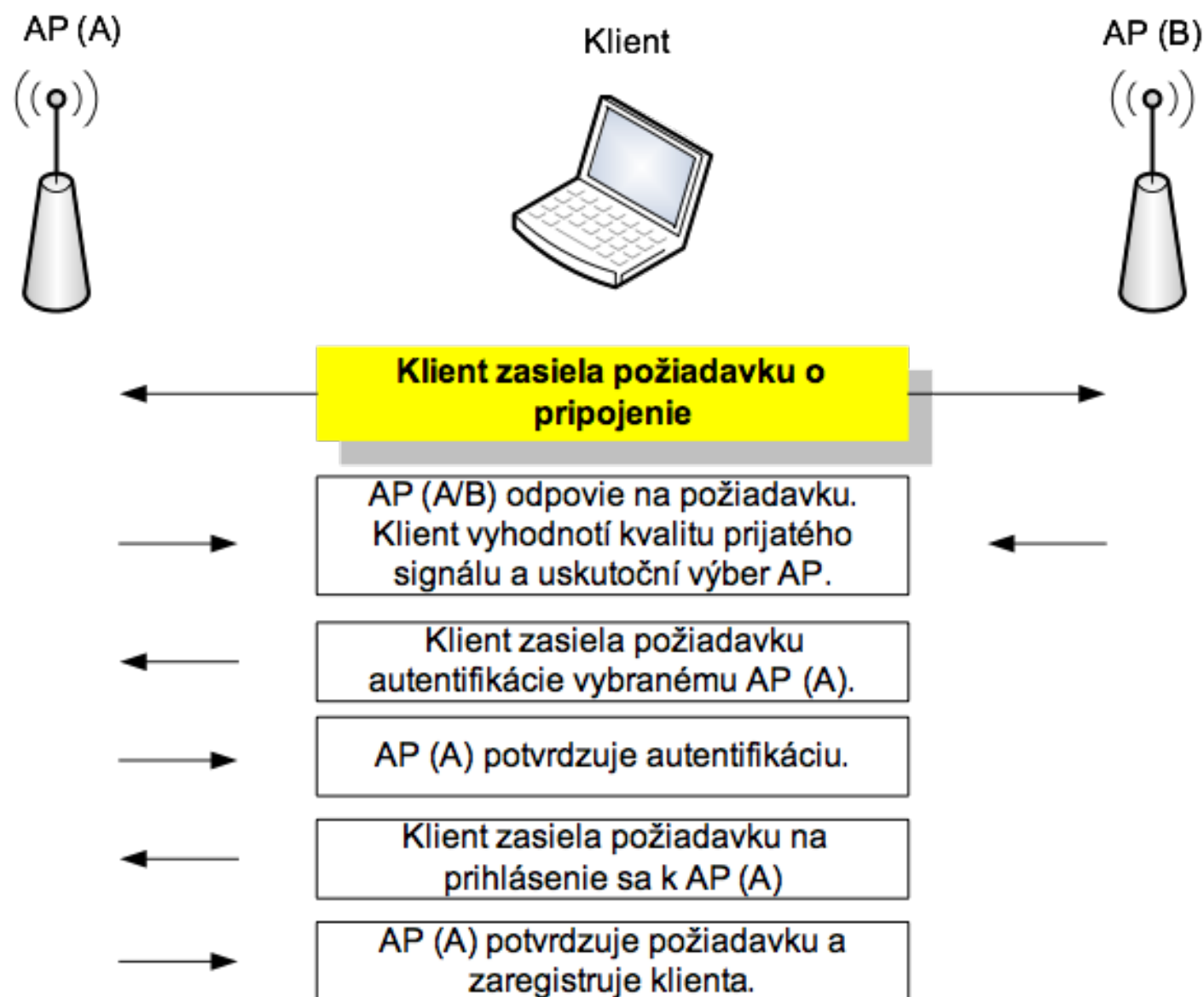
7 1 6 1 5 3 2 7 0 4 ~~5~~

WPA – WiFi Protected Access

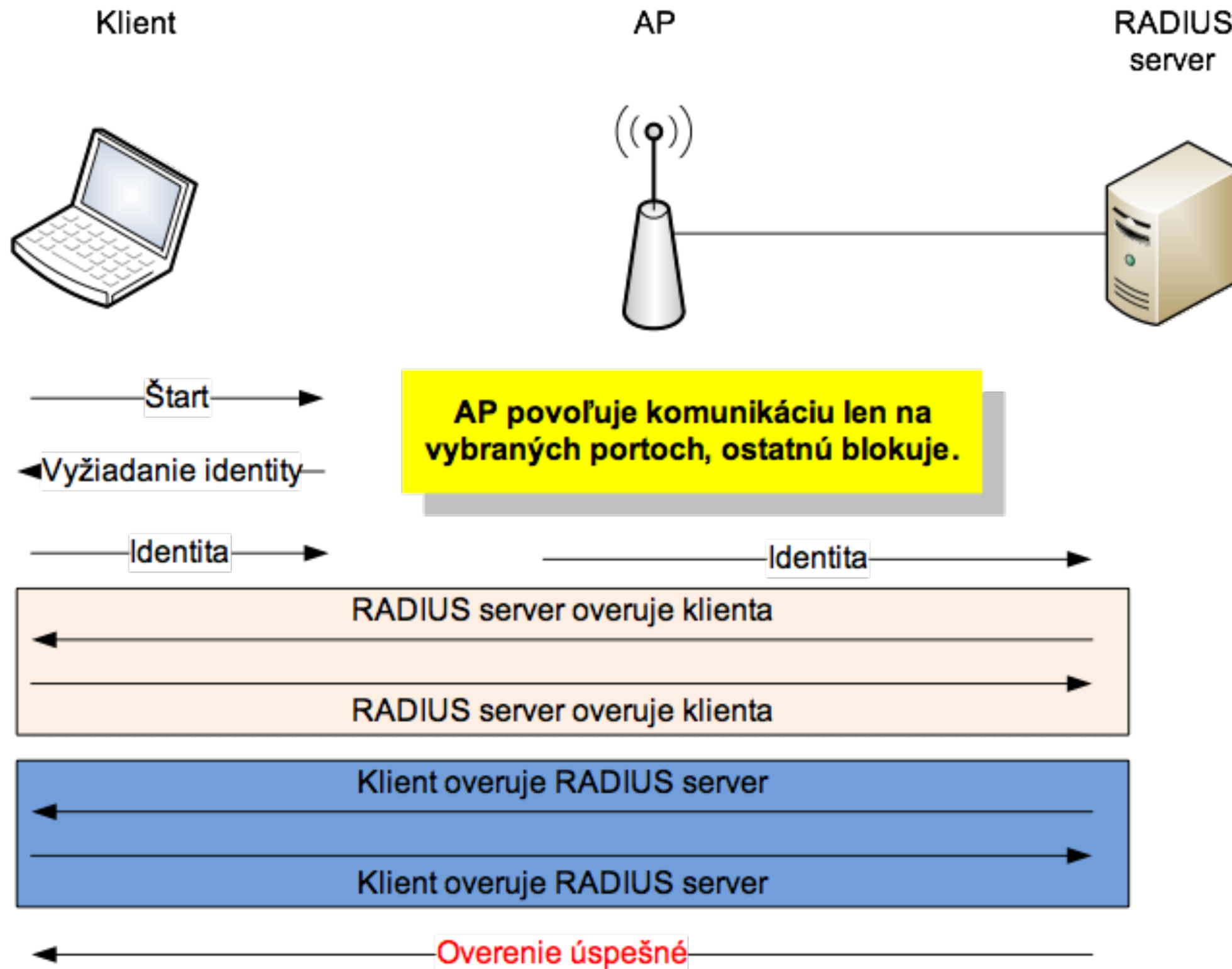
- Definovaný WiFi alianciou
- Má sa používať pre:
 - Spoločnosti s využitím 802.1X
 - Osobné potreby s preddefinovaným kľúčom (PSK – PreShared Key)
- WPA je založené na drafte 3 štandardu 802.11i
- WPA2 je de-facto štandard 802.11i
- Používa 128 bit kľúč a 48 bit. IV (RC4)
- Na zvýšenie bezpečnosti používa TKIP (Temporal Key Integrity Protocol) pre dynamickú zmenu kľúčov

Otvorená Autentifikácia

- Nepoužíva sa na autentifikáciu
- Pri použití WEP sa totižto kóduje len dátová časť



802.1x



802.11 - Roaming

- Žiadne alebo zlé spojenie? Tak urob:
- Scanning
 - prehľadaj prostredie, t.j, počúvaj médium
- Reassociation Request Požiadavka na znovuspojenie
 - stanica posiela požiadavku k jednému alebo niekoľkým AP
- Reassociation Response Odpoveď na znovuspojenie
 - úspech: AP odpovedalo, stanica sa môže pripojiť
 - chyba: pokračuj v prehľadávaní
- AP accepts Reassociation Request
 - signalizuje novú stanicu do distribučného systému
 - distribučný systém aktualizuje svoju databázu (t.j. lokalizačné informácie)
 - zvyčajne distribučný systém teraz informuje starý AP, takže ten môže uvoľniť prostriedky