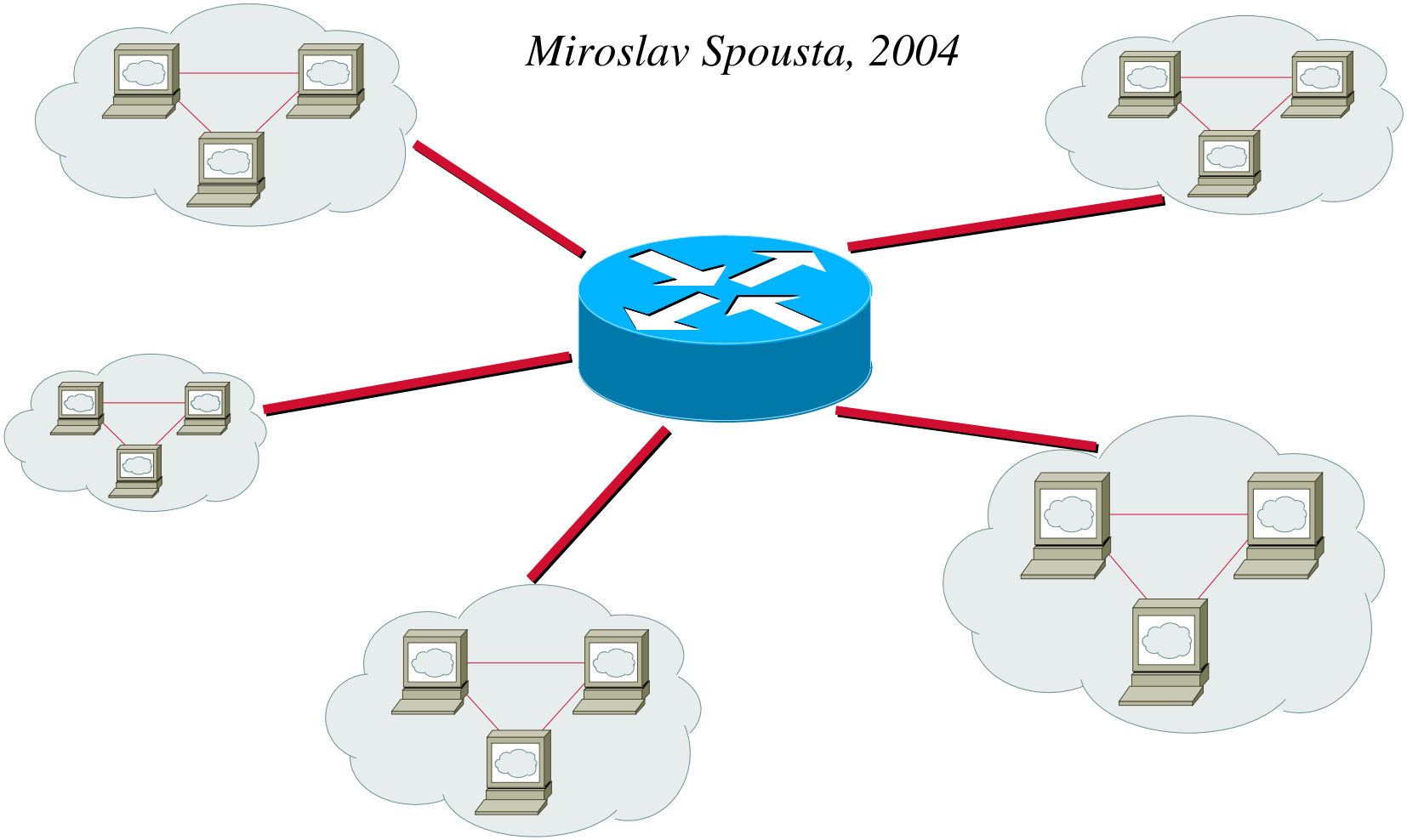
Počítačové sítě I

8. Bezdrátové sítě, GSM

Miroslav Spousta, 2004



Bezdrátové sítě

- přenosové médium: atmosféra (vzduch)
- sdílené: je potřeba řídit přístup (vysílání)
- v rámcí IEEE 802

  IEEE 802.11 (WLAN) bezdrátové lokální sítě (uvnitř budovy)

  IEEE 802.15 (WPAN) bezdrátové osobní sítě (v jedné kanceláři)

  IEEE 802.16 bezdrátové metropolitní sítě

- připojení zařízení přes digitální telefonní síť (GSM)

  většinou pouze dvoubodové spoje

  využívá se digitální přenosový kanál (místo analogového v případě modemu a telefonní linky

WLAN

- Wireless LAN, bezdrátová lokální síť
- stanice vybaveny bezdrátovou síťovou kartou
- hub (koncentrátor) je nahrazen AP (Access Point)

  základnová stanice a datový most pro asociované (připojené) klienty
- nebo může fungovat WLAN jako síť peer-to-peer (ad-hoc) bez AP
- v roce 1990 vzniká skupina IEEE 802.11

  cíl: „bezdrátový Ethernet“

  v bezlicenčním pásmu 2.4 GHz

  předpokládané využití: uvnitř budov

IEEE 802.11

- IEEE 802.11: 1997
- pásmo 2.4 GHz: 2.4 – 2.4835 GHz

  2.45 GHz používají mikrovlnné trouby
- pouze 1 a 2 Mbps (ve srovnání s LAN: 10/100 Mbps)
- oproti Ethernetu jiná přístupová metoda: CSMA/CA

  nemožnost spolehlivé detekce kolizí (stanice se vzájemně nemusí slyšet)

  Carrier Sense Multiple Access with Collision Avoidance
- na fyzické vrstvě používá:

  DSSS, FHSS, infračervené světlo (DFIR) – nepoužívá se

IEEE 802.11

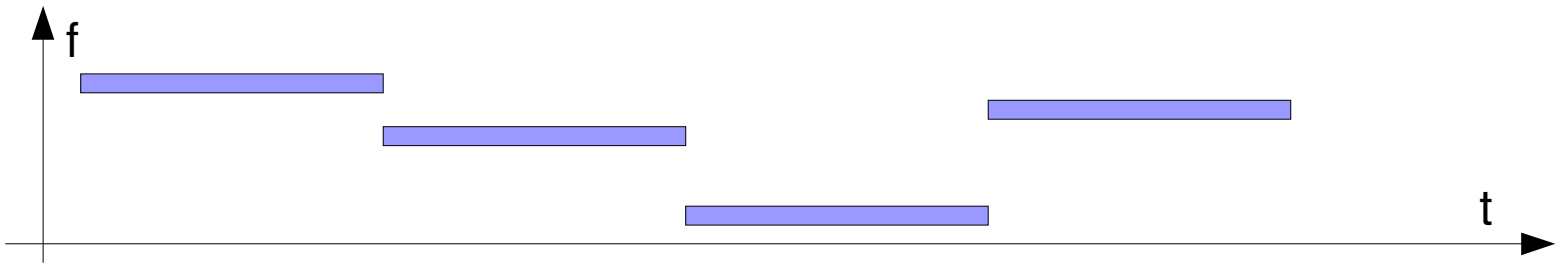
- DSSS

  používá oddělená pásma pro příjem a vysílání (umožňuje full-duplex)

  kódový multiplex: používá bitové posloupnosti pro 1 a 0

- FHSS

  frequency hoping – přepínají se frekvence



CSMA/CA

- předcházení kolizím (řešení problému skrytého uzlu)

  je možné vypnout/zapnout

- stanice, která chce vysílat vyšle krátký paket RTS (Ready to Send)

  součástí je velikost budoucích přenášených dat

- příjemce potvrdí zasláním zpět paketu CTS (Clear to Send)

  opět je velikost dat součástí dat

- ostatní stanice slyší CTS a/nebo RTS+CTS, počká na skončení domlouvaného přenosu dat

- po úspěšném přenosu dat příjemce potvrdí odésílateli příjem paketem ACK (Acknowledge)

Wi-Fi

- IEEE 802.11b, Wireless Fidelity, 1997
- stejné pásmo: 2.4 GHz
- vzdálenost kolem 100 m
- zrychlení na 11 Mbps (nebo 5.5, 2, 1 Mbps, podle stupně rušení)

  efektivní rychlost o 30 – 40% nižší, běžně kolem 6 Mbps
- používá se pouze DSSS, kódování CCK (Complemetary Code Keying)
- o testování kompatibility se stará WECA (Wireless Ethernet Compatibility Alliance), ta také zavedla označení Wi-Fi

Wi-Fi5

- IEEE 802.11a, 1999
- vyšší pásmo: 5.2 GHz, méně zarušené, není všude bezlicenční
- vyšší rychlost: až 54 Mbps (30 – 36 Mbps reálně)
- pásmo rozděleno na 8 nepřekrývajících se kanálů
- OFDM – Orthogonal Frequency-Division Multiplexing

  rozdělí data do několika toků bitů, které poté moduluje na různé nosné frekvence

  něco jako frekvenční multiplex, ale kanály se částečně překrývají
- podporované rychlosti: 64, 48, 36 a 24 Mbps (16-QAM), 18 a 12 Mbit/s (QPSK), 9 a 6 Mbps (BPSK, BiPhase Shift Keying)

IEEE 802.11g

- IEEE 802.11g, 2003, rozšíření Wi-Fi (802.11b)
- opět pásmo 2.4 GHz, není problém s licencí
- vyšší rychlost: až 54 Mbps (30 – 36 Mbps reálně), používý OFDM
- zpětně kompatibilní s Wi-Fi

  v režimu kompatibility musí použít RTS/CTS mechanizmus

  potřebuje detekovat kolize, Wi-Fi bere vysílání 802.11g jako šum

Porovnání IEEE 802.11x

Typ	Kmitočet	Maximální přenosová rychlost	Přenosový výkon	Mechanismus přenosu
802.11b (Wi-Fi)	2.4 – 2.485 Ghz	11 Mbps	do 6 Mbps	DSSS
802.11g	2.4 – 2.485 Ghz	54 Mbps	do 22 Mbps	OFDM/DSSS
802.11a	5.1-5.3 Ghz a 5.725 – 5.825 Ghz	54 Mbps	do 25 Mbps	OFDM

Zabezpečení

- SSID (ESSID)

  32-bajtový sdílený klíč, nutný pro připojení k síti

  přenáší se v každém paketu, který běží po síti

  klient ho musí znát, aby se mohl připojit k síti

  ale může ho odposlechnout

- BSSID

  48-bitový klíč, MAC adresa zařízení

WEP

- Wire Equivalent Privacy
- součástí standardu 802.11
- cíl: zabezpečit utajení a kontrolu integrity dat
- utajení:

  proudová šifra RC4

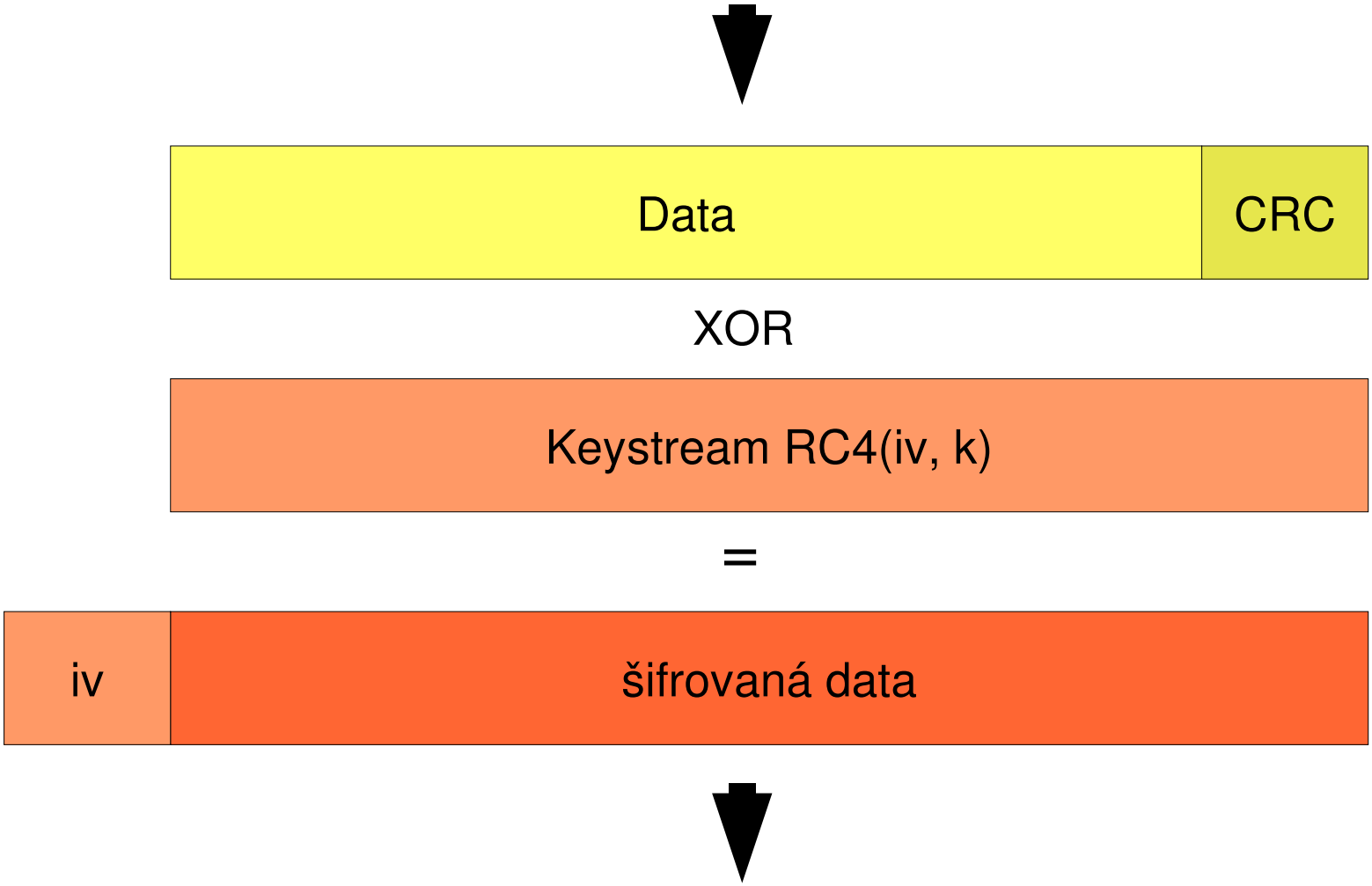
  používá se 64(40)-bitový nebo 128(104)-bitový klíč

  inicializační vektor se přenáší současně s daty

- integrita:

  CRC-32

WEP



Problém 1: krátký IV

- pro každý paket se používá jiný inicializační vektor (IV)
- někteří výrobci to implementovali jako sequence number

  po restartu karty se začíná od 0 a zvyšuje se po 1

- IV je jen 24 bitů dlouhý: na vytížené síti se zopakuje za půl dne
- problém: pokud víme. že byl použit stejný IV a stejný klíč pro dva šifrové texty, pomocí XOR na nich operace dostaneme XOR plaintextů obou původních zpráv.

  pokud známe formát (lépe celý plaintext) jedné zprávy, můžeme dešifrovat druhou

- často se používá sdílený klíč pro více stanic – jednodušší útok

Problém 2: CRC

- CRC-32 není kryptologicky bezpečné
- CRC nezávisí na klíči (toto neplatí pro SHA1, MD5, …)

  CRC bylo konstruováno pro detekci chyb přenosu, ne pro detekci úmyslného podvržení

- pokud změníme (xor) bit ve zprávě, vyvolá to předem spočitatelné změny (xor) v CRC-32
- CRC-32 je lineární funkce: CRC(X xor Y) = CRC(X) xor CRC(Y)

Aktivní útok

- platí: RC4(X) xor X xor Y = RC4(Y)

  známe-li jednu clear-textovou zprávu, můžeme konstruovat další, které jsou korektní (umíme spočítat CRC)

- změny v bitech (xor) se přenášejí přes RC-4: můžeme měnit obsah zprávy i CRC, pokud známe původní zprávu

- co takhle odchytit paket a změnit cílovou adresu v IP paketu?

  a poslat ho přes AP do Internetu?

- můžeme si vytvořit tabulku RC4 podle všech IV

  pakumíme dešifrovat vše

  tabulka bude mít velikost řádu GB

Aktivní útok

$C' = C \oplus \langle D, c(D) \rangle$

$= RC4(iv, key) \oplus \langle M$

GSM

- GSM (vytvářela skupina Groupe Spécial Mobile)

  od roku 1982, dnes vyvíjí ETSI (European Telecomunication Standard Institute)

- celoevropský komunikační systém na buňkové bázi v pásmu 900 MHz
- 1990: GSM Phase 1

  první používaná verze GSM, přesměrování hovorů, hlasová schránka, ...

- 1992: GSM Phase 2

  tarifikace hovorů, identifikace hovorů, konference, ...

- rozšíření na pásmo 1800 Mhz
- u nás: nejdříve analogová síť Eurotel (NMT), později GSM

GSM kanály

- síť GSM používá kanály o šířce 200 kHz
- kanály jsou v pásmu 900 nebo 1800 Mhz

  oddělené směry komunikace (k telefonu: downlink, od telefonu: uplink)

  890 – 915 MHz uplink a 935 – 960 MHz downlink: 2 x 125 kanálů

  1710 – 1785 MHz a 1805 – 1880 MHz, 2 x 375 kanálů

  jednotlivé kanály jsou přiděleny operátorům

pásmo 900 MHz

Český Mobil: 1-20

Eurotel: 36-49, 61-70, 81-96, 110-114

T-Mobile: 22-35, 50-60, 71-80, 97-107

AČR: 115-124, měřicí kanály: 21, 108, 109

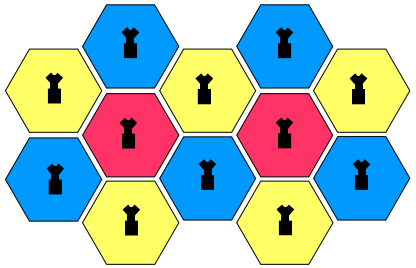
pásmo 1800 MHz

Eurotel: 548-570, 581-597

T-Mobile: 571-596, 613-643, 735-774

Český Mobil: 776-845

Buňková síť



- vyhrazená pásma (kanály) pro jednotlivé operátory nestačí
- je potřeba použít dané pásmo opakovaně

  ale nesmí se používat u vysílačů, které na sebe „vidí“ – docházelo by k rušení

  často se používají šestihranné buňky – stačí mít tři sady navzájem různých frekvencí

  počet hovorů v jedné buňce omezen počtem kanálů přidělených dané buňce

- v centru každé buňky je vysílač – základnová stanice

  stanice se může pohybovat, může přecházet z buňky do jiné – tzv. handover

  základnové stanice jsou propojeny pevnou (i když třeba bezdrátovou) sítí

GSM: struktura

- síť používá systém základnových stanic (BSS, Base Station Subsystem)

  s nimi komunikují mobilní zařízení (MS – Mobile Station) – telefony, ...

  k přenosu se používá rádiový signál (900/1800 MHz)

- NSS (Network and Switching Subsystem)

  obdoba telefonní ústředny (spojování hovorů, vyhledávání účastníků)

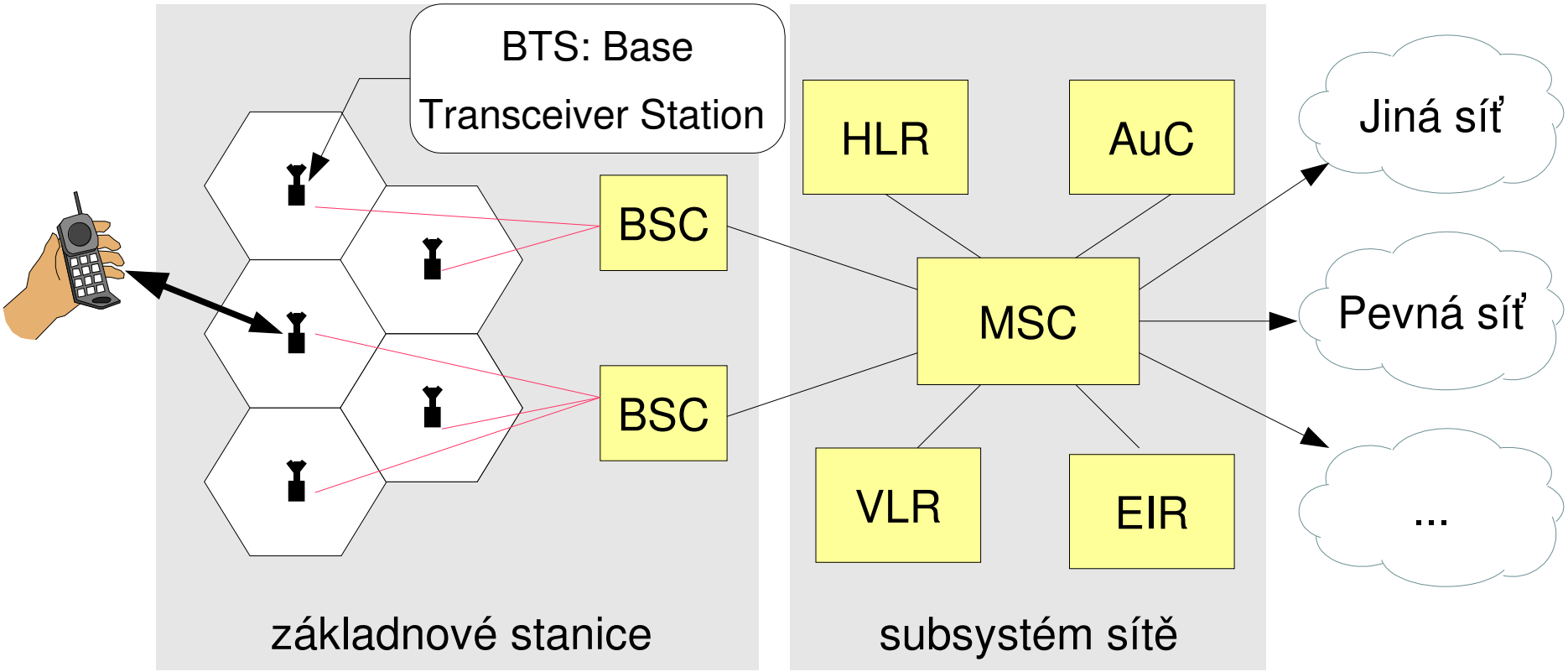
- OSS (Operation Subsystem)

  globální dohlížení, tarifikace

  provoz předchozích subsystémů

- všechno to jsou stacionární složky (nehýbou se)

Mobilní síť GSM

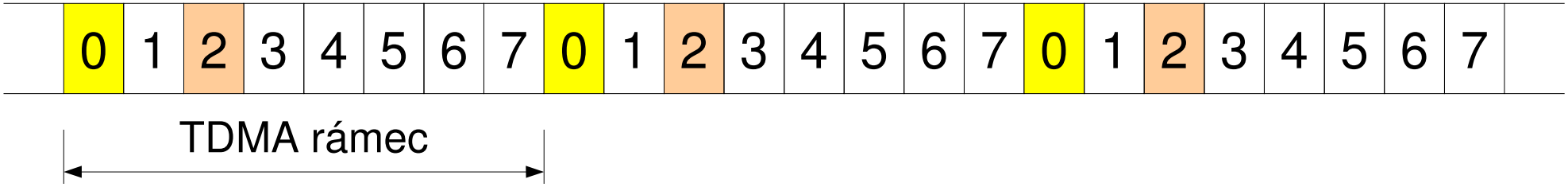


- BSC: Base Station Controller, MSC: Mobile Services Switching Center
- HLR: Home Location Register, VLR: Visitor Location Register
- EIR: Equipment Identity Register, AuC: Authentication Center

Časový multiplex

- jednotlivé 200 kHz kanály jsou dále děleny na menší části

  8 slotů, dělí se pomocí TDMA (časový multiplex)



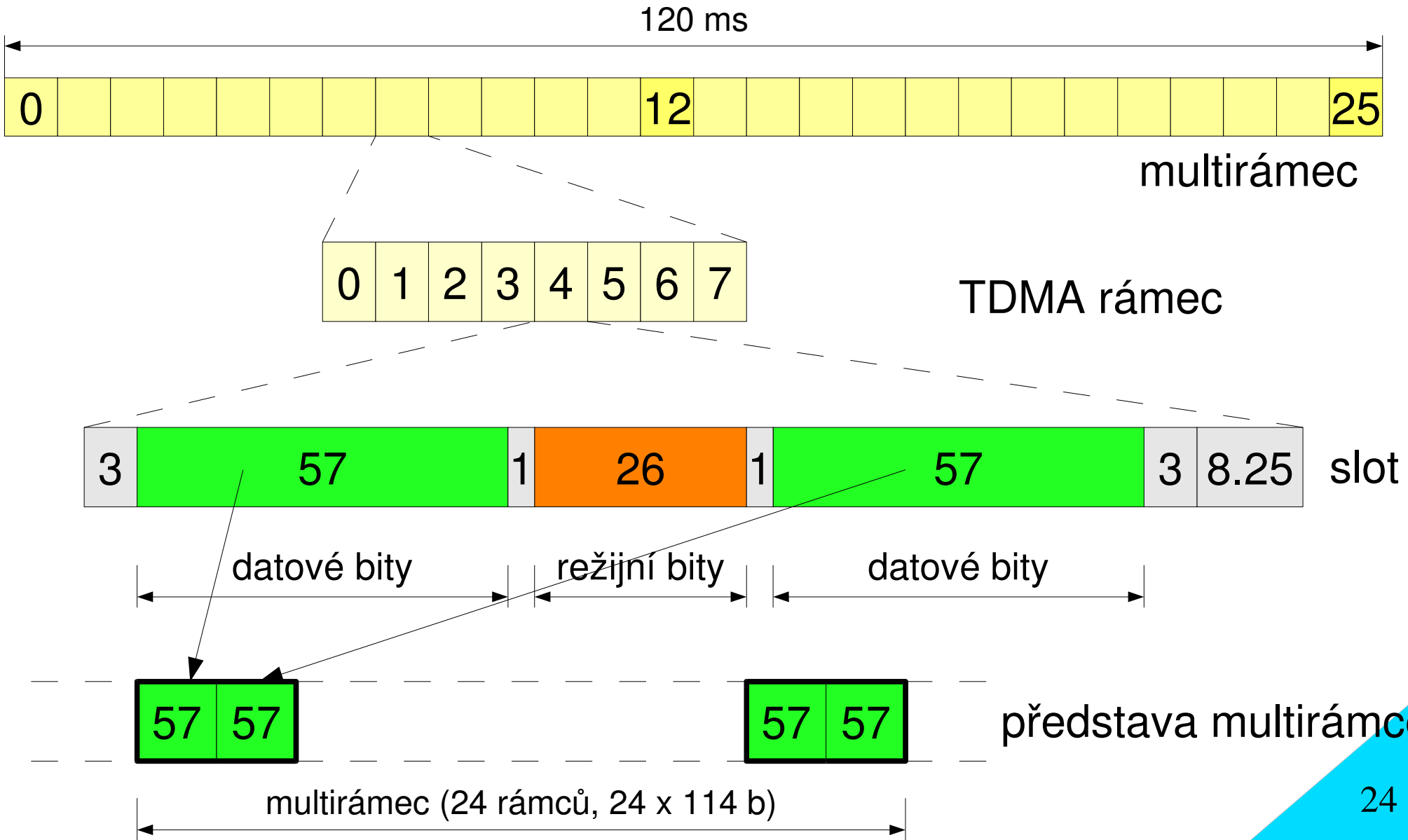
- 8 slotů tvoří rámec – trvá asi 4.615 ms
- rámce se sdružují do multirámců (26 rámců)

  jeden multirámec trvá 120 ms

  multirámce jsou odděleny prodlevou odpovídající 3 slotům

  využívá se jen 24 rámců, 13. je řídící, 25. je rezervovaný

GSM sloty


120 ms
0
12
25
multirámec
0 1 2 3 4 5 6 7
TDMA rámec
3
57
1
26
1
57
3
8.25
slot
datové bity
režijní bity
datové bity
57 57
57 57
představa multirámce
multirámec (24 rámců, 24 x 114 b)

GSM hovor

- každému hovoru je přidělen jeden slot (1/8 rámce)
- sloty mohou mít různý formát, nejčastěji 156.25 bitů

  z toho 2x57 bitů datových, ostatní je režie

- v multirámci je 24 datových rámců, přenese se za 120 ms

  24 x 114 datových bitů (2736 b) pro daný hovor

  2736/0.120 => 22.8 kbps (na jeden slot)

  na režii sítě GSM zbývá asi 11 kbps

- digitalizace hlasu

  klasicky: 8000 x 8b = 64 kbps

  GSM: 50 x 260b = 13 kbps

GSM hovor

- k datovému toku 13 kbps se přidává ještě redundance kvůli možné ztrátě nebo poškození dat

  260 b => 456 b, tedy za 120 ms 6 x 456 = 2736 bitů dat (což je přesně tolik, kolik pojme jeden logický kanál v multirámci)

  neboli z 13 kbps dostaneme tok 22.8 kbps

GSM data

- pro přenos dat můžeme použít rovnou digitální přenosový kanál
  - 22.8 kbps, ale stejně potřebujeme nějakou režii (oprava chyb, potvrzování)
- zpočátku se využívalo jen toku stejného jako má hlas: 13 kbps
  - zaokrouhlilo se dolů na běžně používaný datový tok 9.2 kbps
  - zbytek pro korekce, zajištění spolehlivosti, atd.
  - takto fungují základní datové přenosy v GSM
- data nemusíme zabezpečovat na linkové úrovni jako hlas
  - mohou se použít mechanismy vyšších vrstev (příp. přenést data znovu)
  - alespoň máme-li kvalitní spojení
  - 14.4 kbps: odstraněním některých ochranných mechanismů (redundance)

GSM datové přenosy

- při přenosech v počítačových sítích nejsme zvyklí na velkou redundanci

  max. CRC, poškození a ztráta dat se řeší opětovným posláním

  to vadí v případě telefonování (zpoždění), ale ne tolik u dat

- datové přenosy v síti GSM mohou být „transparentní“

  kanál se tváří jako bitová roura, data jsou dodávány pravidelně (ale možná poškozené)

- „netransparentní“

  používá se protokol RPL (Radio Link Protocol)

  dále ukrajuje z 9.2 (14.4) kbps – zpomaluje spojení

  mechanismus, který zajišťuje přeposlání poškozených dat, může způsobovat nestejnoměrný tok dat

Rychlejší datové přenosy

- doposud jsme využívali GSM pro přenos dat stejně jako hovory

  místo digitalizovaného hovoru jsme přenášeli data (maximálně s vypuštěním redundance)

  chceme zachovat koncepci a fungování GSM, jak zrychlit datové přenosy?

- používat několik slotů (hovorů) najednou pro přenos dat
- HSCSD (High Speed Circuit Switched Data)

  pevně vyhradíme více slotů pro komunikaci

- GPRS (General Packet Radio Service)

  přidělovat volné sloty datovým přenosům podle potřeby

HSCSD

- vlastně jen několikanásobné zrychlení použitím více slotů
- vždy se myslí plně duplexní komunikace

  tedy aspoň dva sloty, jeden tam a druhý zpět
- je definováno několik tříd, podle počtu slotů, které se použijí
- základní jednotka je zde 14.4 kbps
- v ČR: Eurotel nabízel třídu 6

Třída	Rx	Tx	Celkem
1	1	1	2
2	2	1	3
3	2	2	3
4	3	1	4
5	2	2	4
6	3	2	4
9	3	2	5
10	4	2	5
12	4	4	5

GPRS

- podpora „přepínání paketů“
- je potřeba změnit strukturu sítě
- koncová zařízení zůstávají stejná (BTS, BSC)
- přibyly dva nové typy uzlů:

  SGSN (Serving GPRS Support Node)

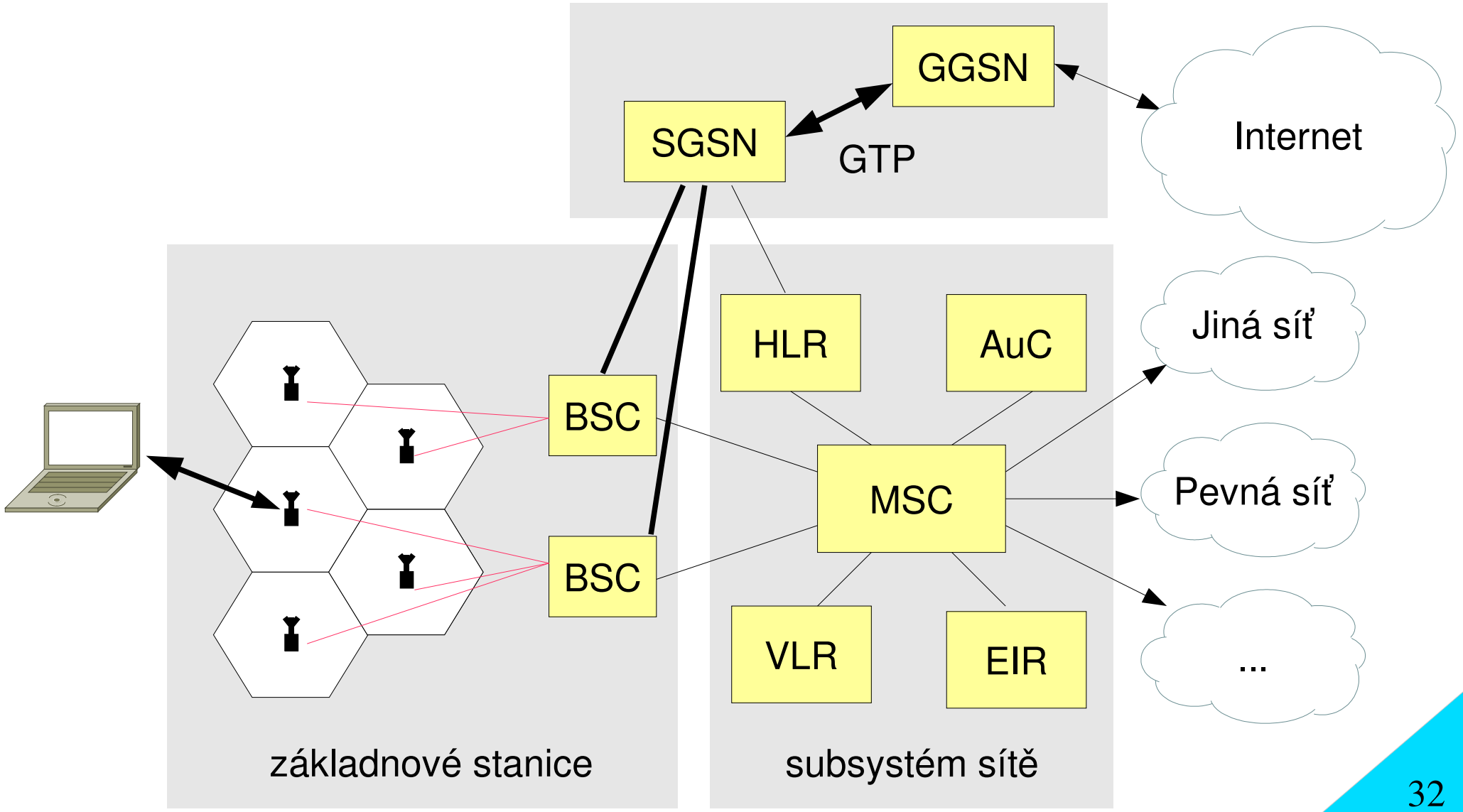
  doručování paketů (něco jako MSC pro hovory), jsou propojeny s HLR (tarifikace, ověřování identity, atd.)

  GGSN (Gateway GPRS Support Node)

  brána mezi IP (tedy Internetem) nebo X.25 a GSM sítí

  oba prvky jsou spojeny přes GPRS Tunelling Protocol (GTP), který běží nad IP

GPRS


GGSN
SGSN
GTP
Internet
HLR
AuC
Jiná síť
BSC
MSC
Pevná síť
BSC
VLR
EIR
...
základnové stanice
subsystém sítě

Rychlost GPRS

- GPRS mění oproti hlasovým přenosům GSM pouze režii v rámci jednotlivých slotů
- vychází z 22.8 kbps, což je maximální rychlost pro jeden slot
- definuje 4 třídy (Coding Scheme), liší se zajištěním přenosu

  která se použije záleží na kvalitě signálu

  CS-1: 9.05 kbps, CS-2: 13.4 kbps, CS-3: 15.6 kbps, CS-4: 21.4 kbps
- pokud bychom využili všech 8 slotů při CS-4, dostaneme rychlost 8 x 21.4 = 171.2 kbps, v praxi bude nižší
- GPRS data mají nejnížší prioritu (po hlasu a HSCSD)
- umožňuje zpoplatňovat přenesená data, ne čas!

Jak dál?

- zachování plné kompatibility s GSM nedává žádný prostor pro další zrychlování přenosu dat

  změnit kompletně metodu přístupu ke sdílenému kanálu, kódování, atd.

  3. generace mobilních sítí – UMTS (Universal Mobile Telephone Standard)

  změnit (zefektivnit) kódování dat při přenosu v GSM – EDGE (Enhanced Data Rates for GSM Evolution)

- EDGE je považována za mezistupeň mezi 2. a 3. generací mobilních sítí
- problémy s cenou licencí UMTS tlačí na zavádění technologie EDGE i u nás

EDGE

- jedná se vlastně o rozšíření GPRS (vychází ze zkušeností s GPRS)

  změna modulace a změna kódovacího schématu, někdy označováno EGPRS

  pouze na rozhraní BTS – MS, zbytek sítě zůstává stejný

- změna modulace

  kromě GMSK (fázová modulace) používané v GSM

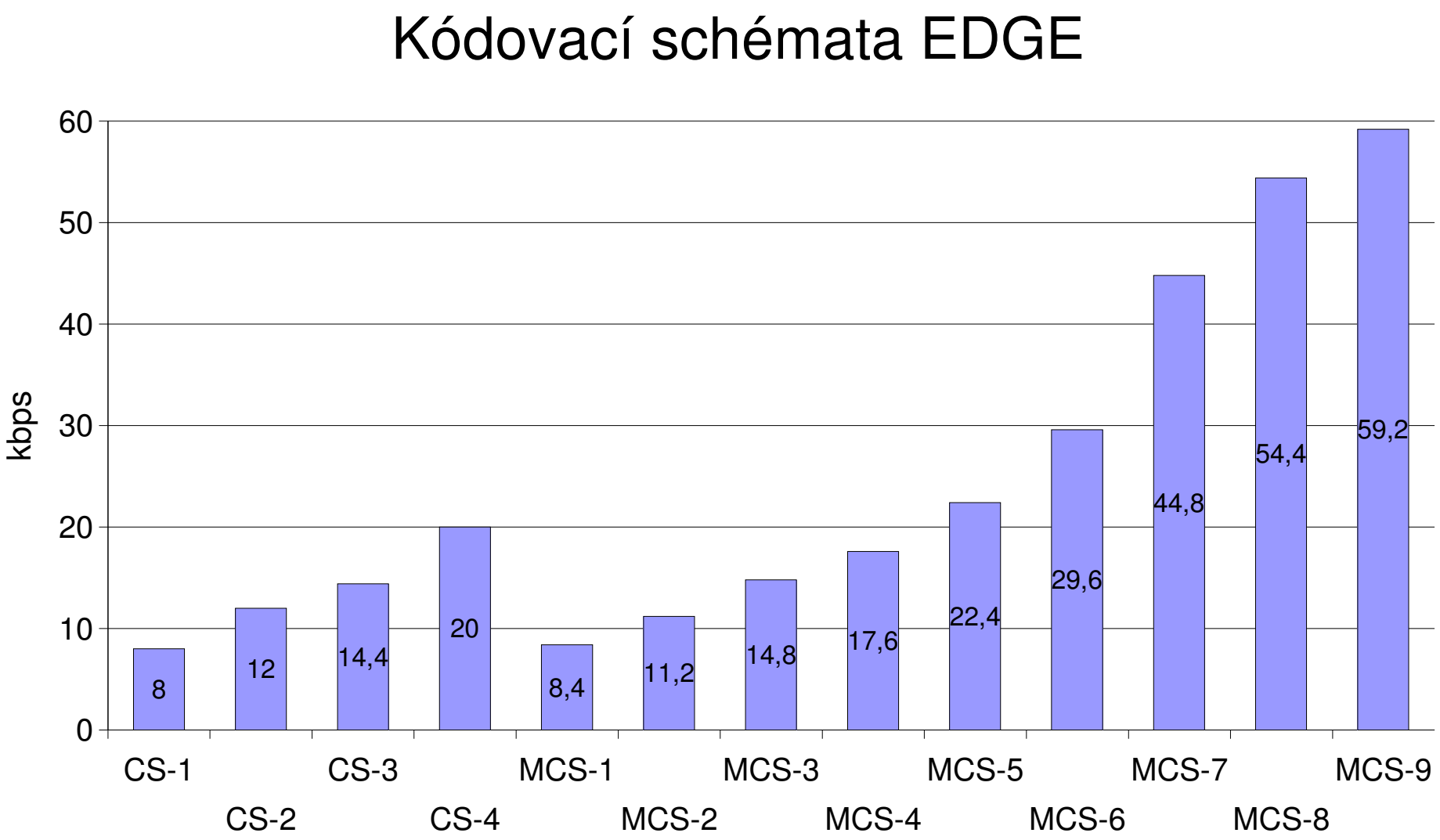
  8-PSK, umožňuje zakódovat 3 bity místo jednoho – trojnásobné zrychlení

- nová kódovací schémata: MCS1 – MCS9

  MCS-1 – MCS-4 jsou obdobou CS-1 – CS-4, používají GMSK modulaci, ale liší se trochu ve formátu hlavičky

  MCS-5 – MCS-9 používají 8-PSK modulaci

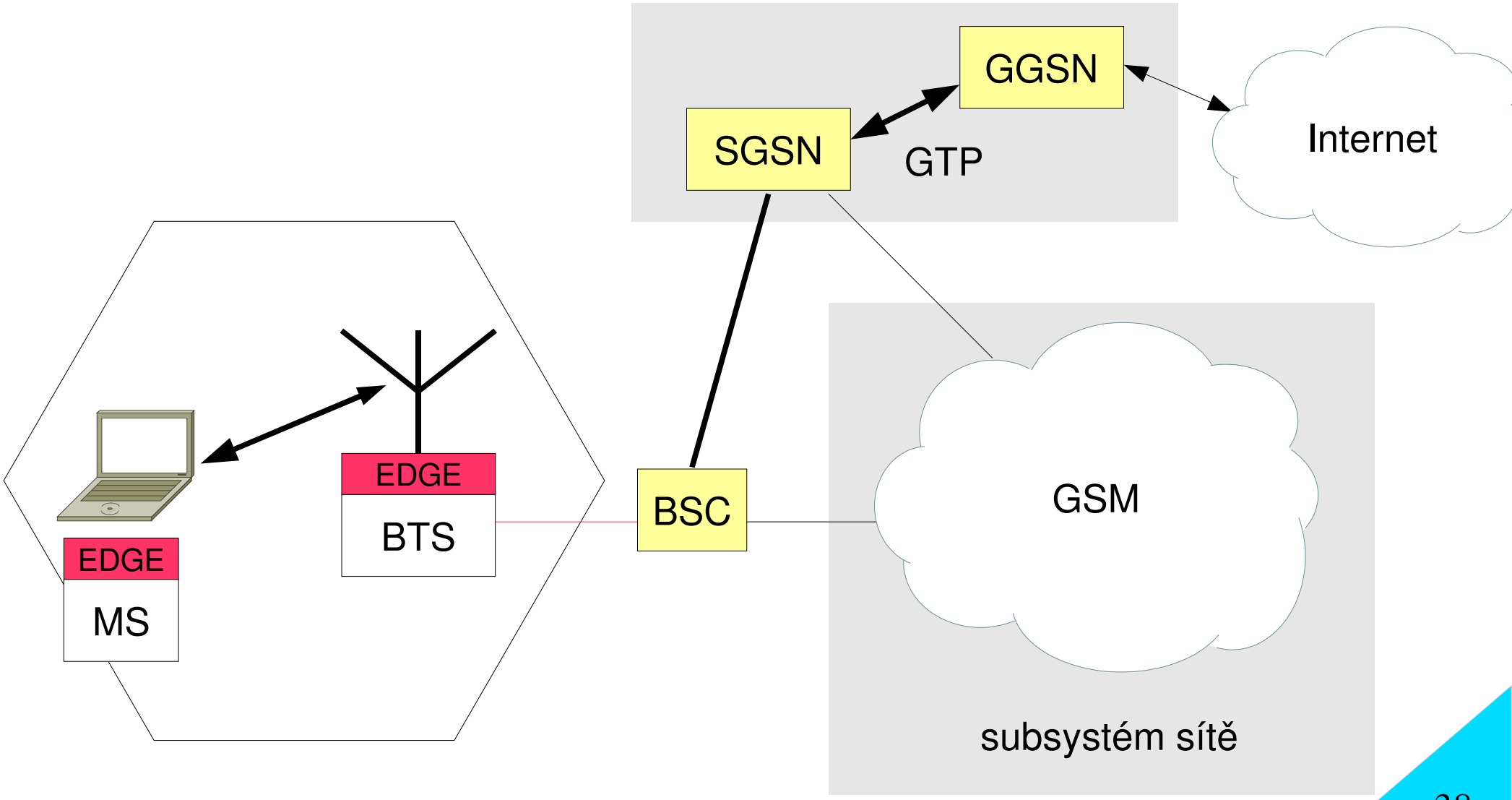
Kódovací schémata



EDGE

- až trojnásobné zrychlení oproti GPRS
- na rozdíl od GPRS umožňuje přeposlat poškozená data pomalejším (ale lépe zabezpečeným) schématem
  - GPRS muselo použít pro stejný paket stejné schéma
- zvětšení rozsahu pro číslování paketů ze 128 (GPRS) na 2048
  - problém s krátkým polem číslování paketů při opětovném posílání
- EDGE častěji měří kvalitu signálu
  - GPRS maximálně jednou za 120 ms
- přechod na EDGE znamená pro operátora pouze úpravu BTS
  - přidání transceiveru podporujícího 8-PSK modulaci

EDGE


GGSN
SGSN
GTP
Internet
EDGE
BTS
EDGE
MS
BSC
GSM
subsystém sítě

GPRS vs EDGE

	GPRS	EDGE
Typ modulace	GMSK	8-PSK/GMSK
Modulační rychlost	270 kBaud	270 kBaud
Přenosová rychlost	270 kbps	810 kbps
Rychlot pro slot	22.8 kbps	69.2 kbps
Data pro slot	20 kbps	59.2 kbps
Data max. (8 slotů)	160 kbps	472.6 kbps

Srovnání

	Maximální datový tok
GSM	14,4 kbps
GPRS	171,2 kbps
EDGE	384 kbps
UMTS	144 kbps (automobil)
	384 kbps (chůze)
	2 Mbps (pevné)