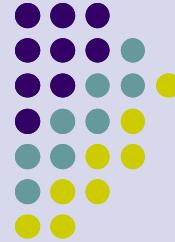


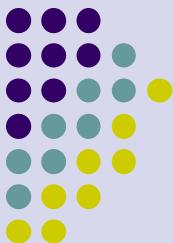
# Úvod



Úvod do počítačových sítí

Lekce 01

Ing. Jiří lédvina, CSc.



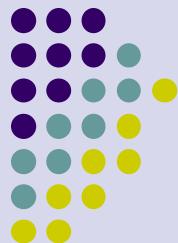
# Administrativa

- Přednášky EP-110
  - Pá 12.05 až 14.40 Ing. Jiří Ledvina, CSc ([ledvina@kiv.zcu.cz](mailto:ledvina@kiv.zcu.cz))
- Cvičení UL-402
  - Út 8.25 až 10.05 Ing. Jiří Ledvina, CSc ([ledvina@kiv.zcu.cz](mailto:ledvina@kiv.zcu.cz))
  - Út 13.00 až 14.40 Ing. Jindřich Skupa ([skupaj@kiv.zcu.cz](mailto:skupaj@kiv.zcu.cz))
  - Út 14.50 až 16.30 Ing. Jindřich Skupa ([skupaj@kiv.zcu.cz](mailto:skupaj@kiv.zcu.cz))
  - St 7.30 až 9.10 Ing. Luboš Matějka ([lmatejka@kiv.zcu.cz](mailto:lmatejka@kiv.zcu.cz))
  - St 9.20 až 11.00 Ing. Luboš Matějka ([lmatejka@kiv.zcu.cz](mailto:lmatejka@kiv.zcu.cz))



# Literatura

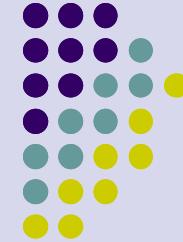
- Literatura:
  - Kállay, F.: Počítačové sítě a jejich aplikace, Grada 1999
  - Tanenbaum, A.,S.: Computer Network, Prentice Hall Inc
  - Stallings, W.: Data and Computer Communications, Prentice Hall Inc
  - Janeček, J.: Počítačové sítě, ČVUT Praha
  - Janeček, J.: Distribuované systémy, ČVUT Praha
  - Habraken,J.:Průvodce úplného začátečníka pro Počítačové sítě, Grada 2009
- Elektronické zdroje
  - Oficiální stránky předmětu (*portal.zcu.cz*), *kiv/ups*
  - Stránky vyučujících (*www.kiv.zcu.cz/~jmeno*)
  - Stránky Jiřího Peterky (MFF UK Praha) (*www.eearchiv.cz*)



# Návaznosti

- Navazuje na předměty
  - PPA (programování, Java), PT (programovací techniky), ZOS (základy operačních systémů), Programování v C
- Navazující předměty
  - PD (přenos dat) – přenosové protokoly (úroveň 1, 2 a přístupová)
  - PSI (počítačové sítě) – zásobník TCP/IP, bezpečnost
  - DS (distribuované systémy) – principy distribuovaných systémů
- Doplňující předměty
  - OS (operační systémy) – znalosti konfigurace op. systémů a síťových serverů
  - DB (databázové systémy) – vazba na další síťové servery
  - SWI (softwarové inženýrství) – jak vytvářet větší programové celky
  - ACS, NMS (architektury číslicových systémů, mikroprocesorové systémy)
- Požadavky praxe
  - C, C++, Python, PHP, Linux, Windows, databáze, softwarové inženýrství, počítačové sítě, databáze.

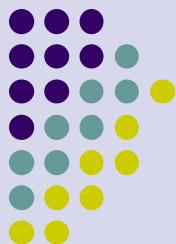
# Úvod do počítačových sítí



Úvod do počítačových sítí

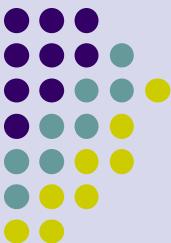
Lekce 01

Ing. Jiří lédvina, CSc.



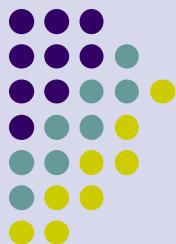
# Úvod do počítačových sítí – přehled

- Úvod, síťové protokoly, architektury, standardy
- Fyzická úroveň
- Linková úroveň, protokoly linkové úrovni
- Lokální počítačové sítě, příklady
- Rozlehlé počítačové sítě, adresování a směrování
- Transportní a aplikační protokoly
- Internet
- Bezpečnost



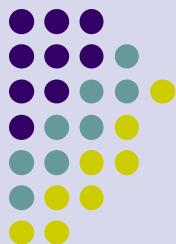
# Úvodem

- Výpočetní systémy
  - Centralizované
    - Procesor, paměť, periferie
  - Decentralizované
    - Těsně vázané – více procesorů, komunikace prostřednictvím sdílené paměti, multiprocesory, matematické výpočty
    - Volně vázané – vícepočítáčové systémy, propojení komunikačními linkami



# Úvodem

- Možnosti propojení systémů
  - Vzdálený přístup
    - Přístup k počítači ze vzdáleného terminálu (typicky telefonní linka a modem)
  - Počítačová síť
    - Vzájemné propojení více počítačů a terminálů s cílem provádět výpočet na některém z počítačů
  - Distribuovaný systém
    - Vzájemné propojení více počítačů, kde výpočet probíhá rozprostřeně na více uzlech, které navíc spolupracují (sdílení dat, souběžně probíhající výpočet).



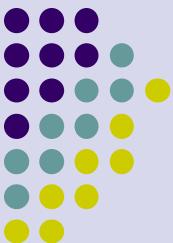
# Úvodem

- Definice
  - Počítačová síť je soubor počítačů propojených komunikační sítí, dovolující sdílet prostředky, jako jsou programy, data, soubory, periferní zařízení.
- Počítačovou síť zobrazujeme jako graf
  - Uzly – výpočetní prostředky, komunikační prvky
  - Hrany – propojovací vedení, komunikační linky



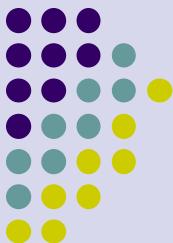
# Úvodem

- Propojení
  - Dvoubodové (jeden vysílač, jeden přijímač)
  - Mnohabodové (více vysílačů, více přijímačů)
    - Pasivní připojení (sběrnice)
    - Aktivní připojení (kruhové sítě)
- Topologie
  - Úplná polygonální síť
  - Neúplná polygonální síť
  - Hierarchické propojení (stromová síť, hvězdicová síť)
  - Lineární síť, kruhová síť



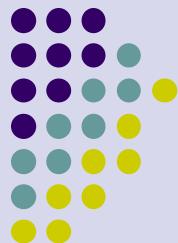
# Úvodem

- Lokální počítačové sítě
  - Mnohabodové spoje
    - Sběrnicové (CAN, Ethernet)
    - Kaskádní propojení
    - Kruhové (Token Ring, FDDI)



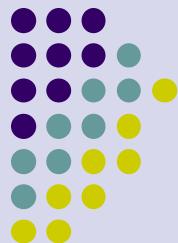
# Rozdělení sítí podle rozlehlosti

- Body area networks (BAN) – 2 až 5m, 100 zařízení, 1mW
- Personální počítačové sítě – PAN
  - WPAN-LR (2,5GHz, 100kb/s, 100m) - ZigBee
  - WPAN-HR (2,5GHz, 1Mb/s, 10m) - Bluetooth
- Lokální počítačové sítě – LAN (100Mb/s až 1Gb/s, stovky metrů až km, dvojlinka, optická vedení, bezdrátové přenosy)
- Metropolitní počítačové sítě – MAN (desítky až stovky km), kabelová televize, optické sítě
- Rozlehlé počítačové sítě – WAN (stovky až tisíce km)
- Propojení počítačových sítí – internet (Země) – ? 800mil počítačů
- Bezdrátové lokální sítě (stovky metrů) – WLAN (Wireless LAN), WiFi
- Bezdrátové personální sítě - WPAN



# Multiplexování

- Přepínání na úrovni datových přenosů
  - Sítě s přepínáním kanálů
  - Sítě s přepínáním zpráv
  - Sítě s přepínáním paketů
- Přepínání na úrovni kanálu
  - Časový multiplex (synchrozní, asynchronní) - TDMA
  - Frekvenční multiplex – FDMA
  - Vlnový multiplex – různé „barvy“



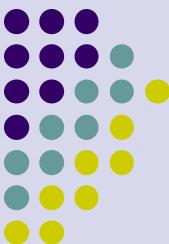
# Multiplexování v rádiových sítích

- Přenos v rozprostřeném pásmu
  - Používá se zejména v bezdrátových sítích
  - Snížení vlivu rušení, zvýšení bezpečnosti (odposlech)
  - DSSS – přímá modulace
    - Čipové sekvence, „roztažení pásma“, např. ZigBee
  - FHSS – frekvenční přeskoky
    - Náhodná volba přenosové frekvence
    - Např. Bluetooth – 79 kanálů po 1MHz
  - CDMA – ortogonální frekvenční multiplex
    - Umožňuje souběžné vysílání více stanic najednou

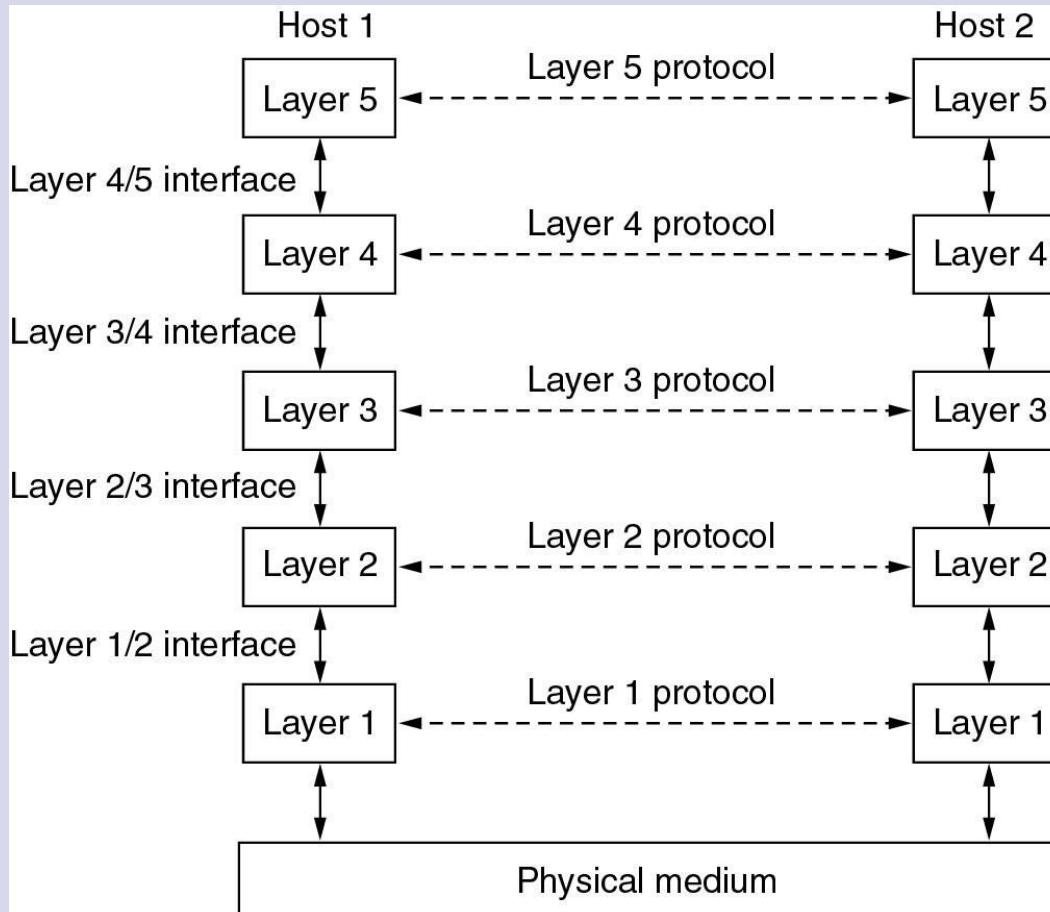


# Programové vybavení poč. sítí

- Hierarchie protokolů
- Důvody pro zavedení hierarchie úrovní
- Spojované a nespojované služby
- Primitivní služby
- Vztah mezi službami a protokoly

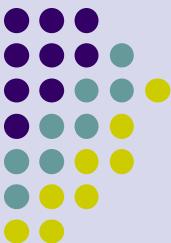


# Hierarchie protokolů

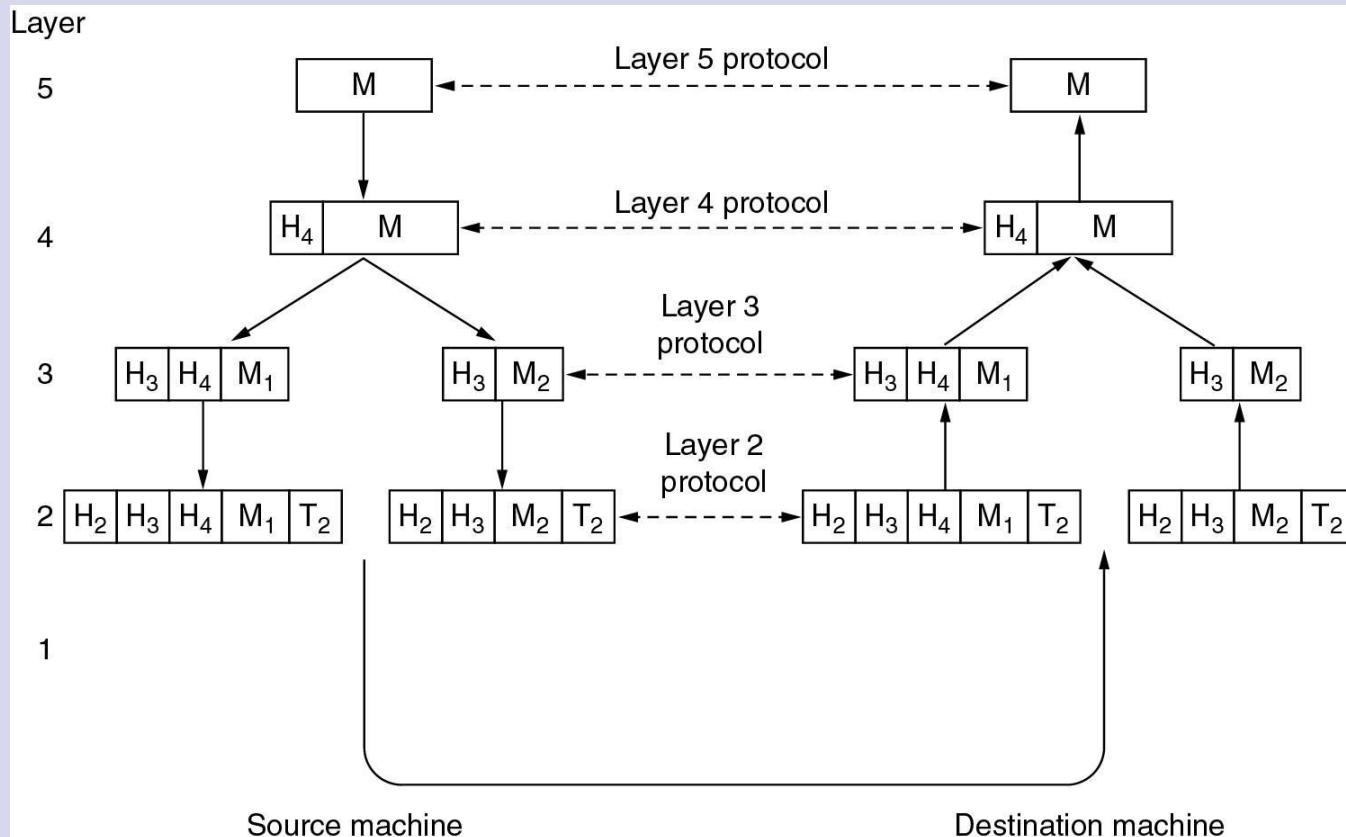


Úrovně, protokoly a rozhraní

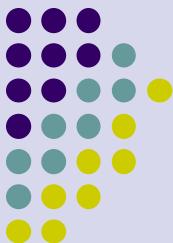
Úvod do počítačových sítí - lekce 1



# Příklad hierarchie protokolů

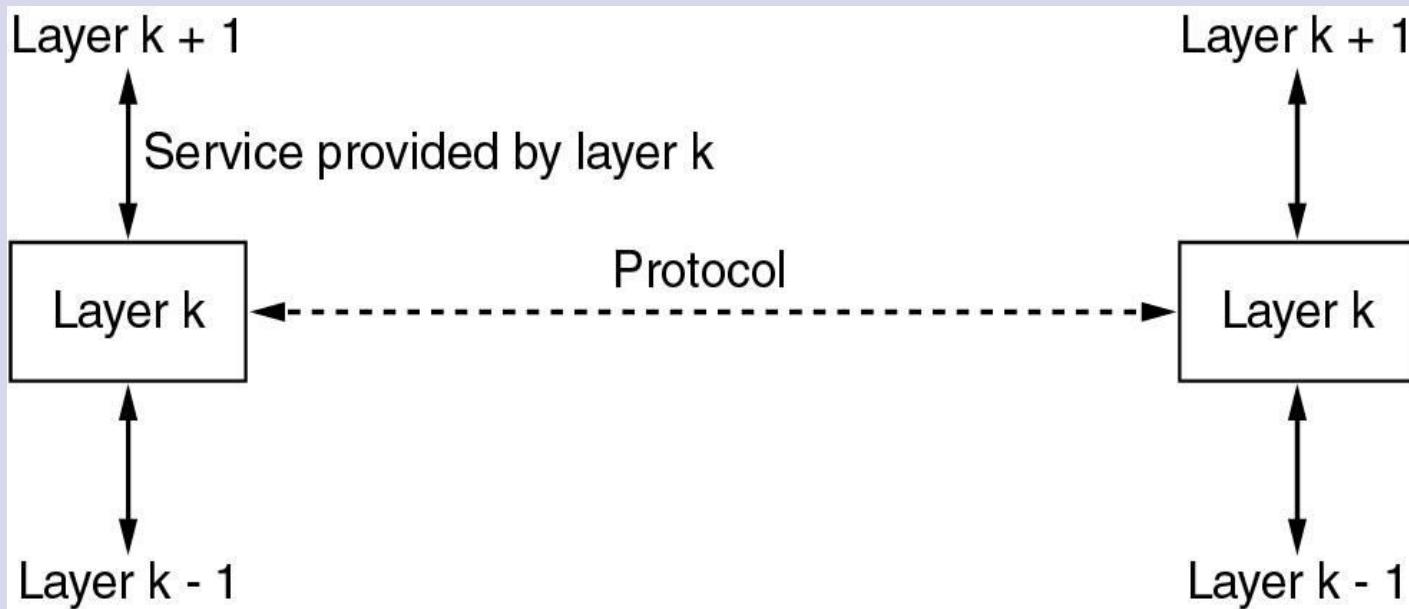


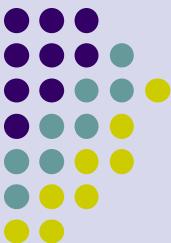
Informační tok, podporující komunikaci vrstvy č.5



# Vztah mezi službami a protokoly

- Základní služby
  - Request, Indication
  - Response, Confirm

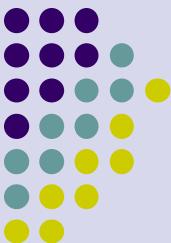




# Spojově orientované a nespojované služby

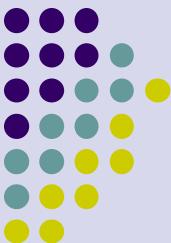
	<b>Service</b>	<b>Example</b>
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
Connection-less	Unreliable connection	Digitized voice
	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Různé typy služeb

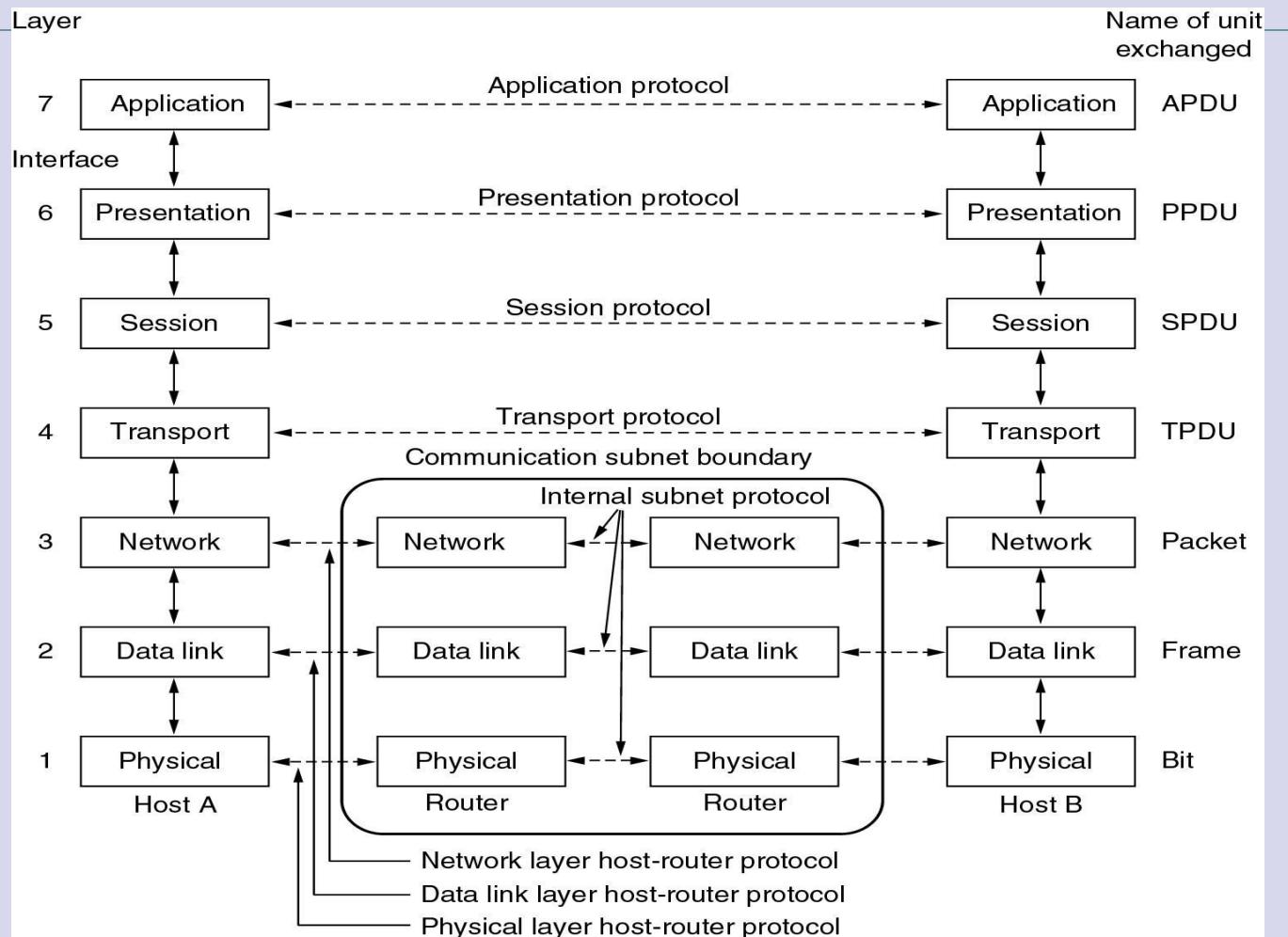


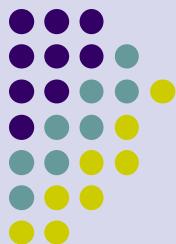
# Referenční modely

- Referenční model ISO/OSI
- Referenční model TCP/IP



# Referenční model ISO



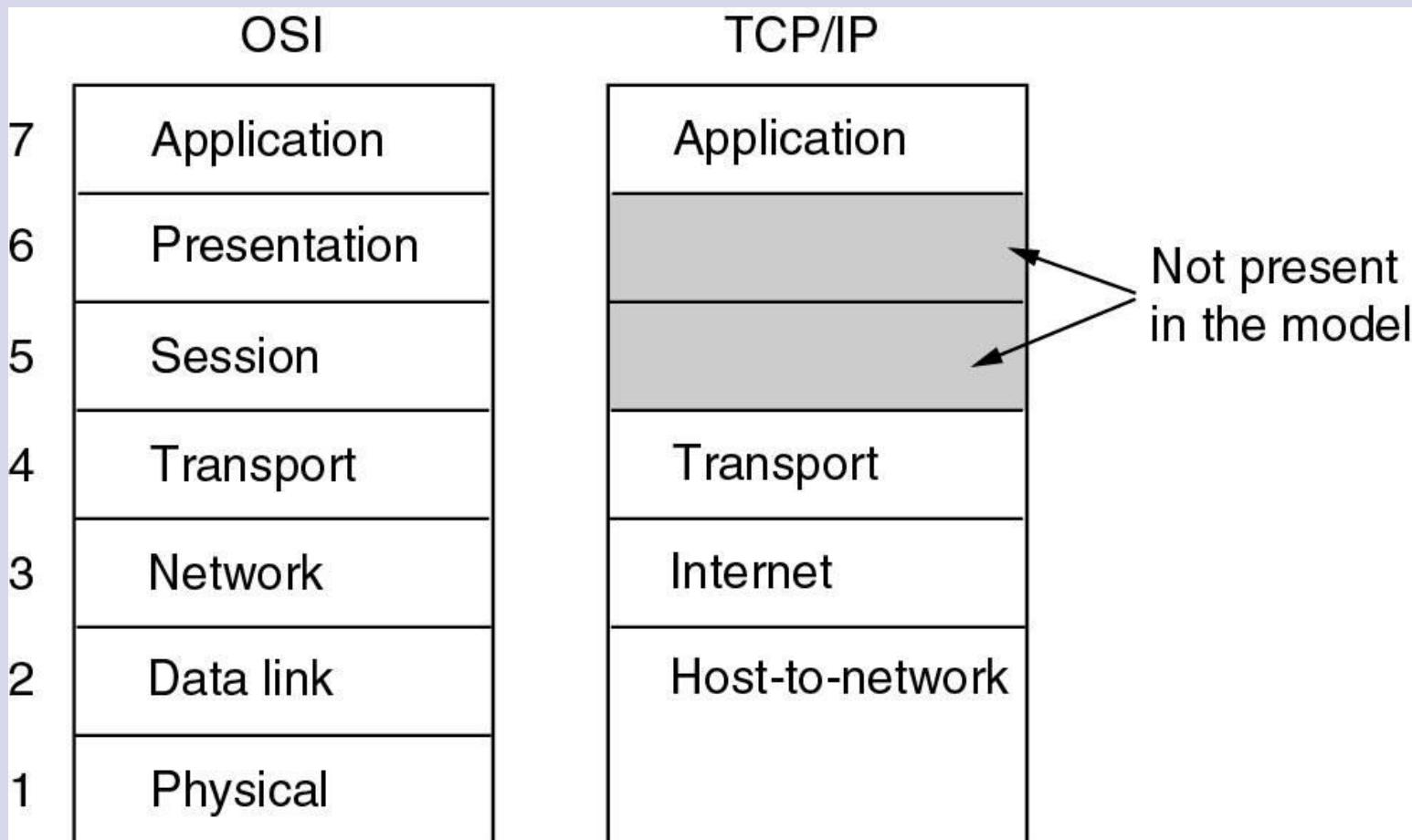


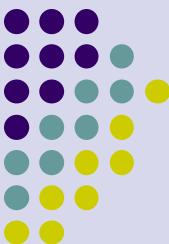
# Referenční model ISO

- **Aplikační (7)**
  - obecné a speciální služby pro aplikace, např. přenos souborů, terminál, ...
- **Prezentační (6)**
  - Převod aplikačních dat na data vhodná pro přenos (heterogenita, komprese, šifrování)
- **Relační (5)**
  - Řešení problému chyb nad přenosovými protokoly (výpadek spojení)
- **Transportní (4)**
  - Přizpůsobení různorodých síťových služeb potřebám aplikace (řešení chyb)
- **Síťová (3)**
  - Přenos dat mezi koncovými uzly sítě (směrování, adresování, řízení toku dat)
- **Linková (2)**
  - Přenos dat mezi sousedními uzly sítě (zabezpečení proti chybám)
- **Fyzická (1)**
  - Definice signálů, konektorů, vedení, rychlostí, ...

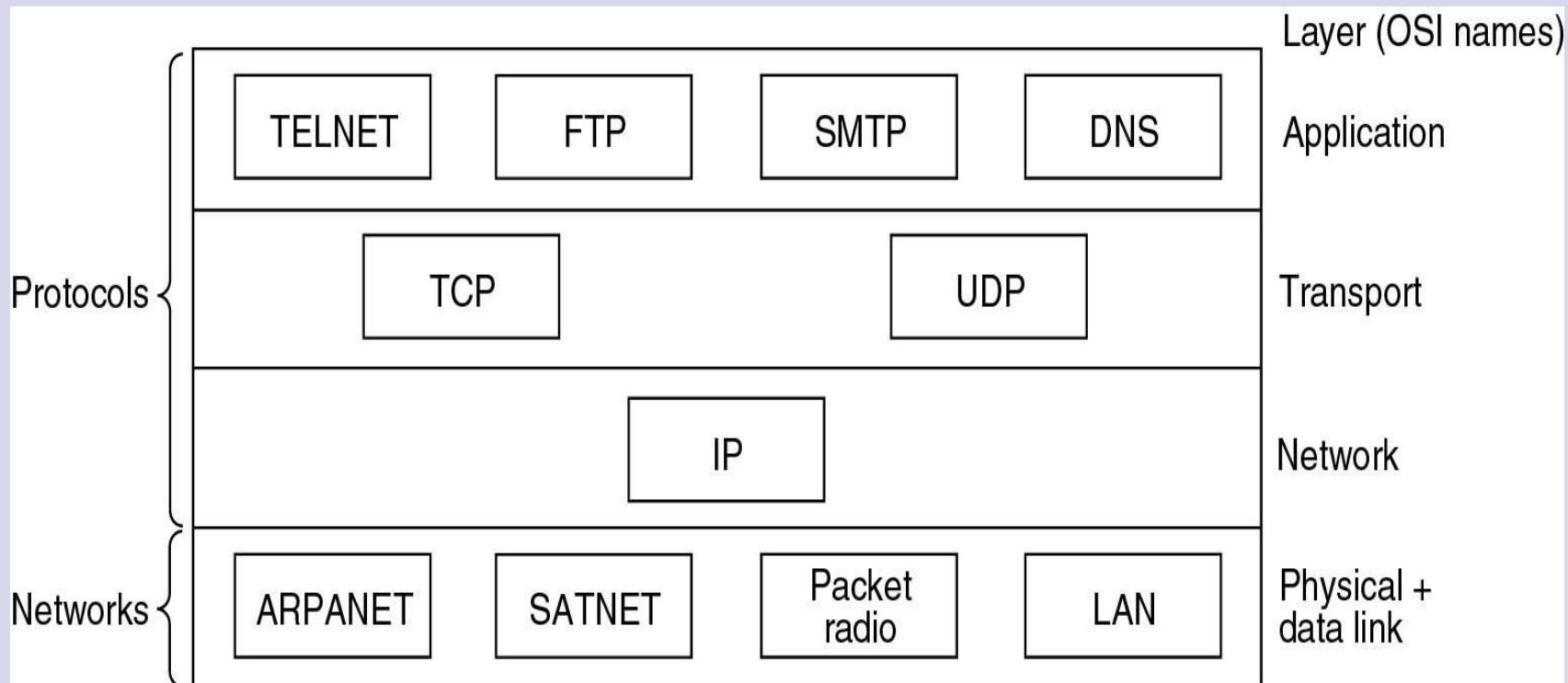


# Referenční model TCP/IP

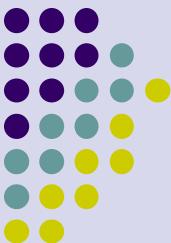




# Protokoly TCP/IP

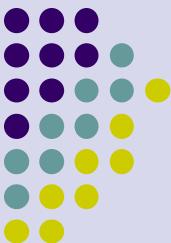


## Původní protokoly TCP/IP



# Příklady sítí

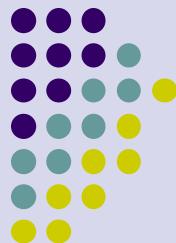
- The Internet
- Connection-Oriented Networks:  
X.25, Frame Relay, and ATM
- Ethernet
- Wireless LANs: 802:11



# Internet

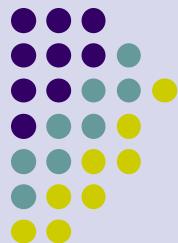
## Tradiční aplikace

- Elektronická pošta (e-mail)
- Elektronické „noviny“ News
- Vzdálený přístup (telnet, ssh)
- Přenos souborů (ftp)
- Webové služby (http)
- Adresářové služby (DNS, LDAP)



# Jednotky

Exp.	Explicit	Prefix	Exp.	Explicit	Prefix
$10^{-3}$	0.001	milli	$10^3$	1,000	Kilo
$10^{-6}$	0.000001	micro	$10^6$	1,000,000	Mega
$10^{-9}$	0.000000001	nano	$10^9$	1,000,000,000	Giga
$10^{-12}$	0.000000000001	pico	$10^{12}$	1,000,000,000,000	Tera
$10^{-15}$	0.000000000000001	femto	$10^{15}$	1,000,000,000,000,000	Peta
$10^{-18}$	0.000000000000000001	atto	$10^{18}$	1,000,000,000,000,000,000	Exa
$10^{-21}$	0.000000000000000000001	zepto	$10^{21}$	1,000,000,000,000,000,000,000	Zetta
$10^{-24}$	0.0000000000000000000000000000000001	yocto	$10^{24}$	1,000,000,000,000,000,000,000,000,000	Yotta



# Jednotky

- Nově zavedené jednotky pro mocniny dvou
  - zdroj:  
<http://physics.nist.gov/cuu/Units/binary.html>
  - In December 1998 the International Electrotechnical Commission (IEC), the leading international organization for worldwide standardization in electrotechnology, approved as an IEC International Standard names and symbols for prefixes for binary multiples for use in the fields of data processing and data transmission. The prefixes are as follows:

Fak	Název	Sym	Hodnota	
$2^{10}$	kibi	Ki	kilobinary	Ki <sup>1</sup>
$2^{20}$	mebi	Mi	megabinary	Ki <sup>2</sup>
$2^{30}$	gibi	Gi	gigabinary	Ki <sup>3</sup>
$2^{40}$	tebi	Ti	terabinary	Ki <sup>4</sup>
$2^{50}$	pebi	Pi	petabinary	Ki <sup>5</sup>
$2^{60}$	exbi	Ei	exabinary	Ki <sup>6</sup>



# Otázky

- Vysvětlete rozdíl mezi systémem vzdáleného přístupu, počítačovou sítí a distribuovaným systémem.
- Uveďte rozdělení počítačových sítí podle rozlehlosti. Uveďte i jejich další vlastnosti.
- Rozdíl mezi dvoubodovými a mnohabodovými spoji, výhody, nevýhody, použití.
- Nakreslete sběrnicovou a kruhovou topologii počítačové sítě, vysvětlete princip přenosu dat a řízení přenosu (sdílení komunikačního média)
- Sdílení komunikačního média, sítě s přepínáním kanálů, zpráv a paketů. Znázorněte rozdíl při přenosu dat přes mezilehlý uzel.
- Na jednoduchém obrázku znázorněte rozdíl mezi časovým a frekvenčním multiplexem při souběžném přenosu 4 datových toků.



# Otázky

- Co je to úrovňová architektura, jaké má výhody a nevýhody, kde se obecně používá.
- Vysvětlete, co v referenčním modelu ISO znamenají pojmy úroveň nebo vrstva, n-tita, služba, protokol, datová jednotka n-té vrstvy a přístupový bod.
- V sedmiúrovňovém modelu ISO/OSI vyjmenujte jednotlivé vrstvy od nejnižší po nejvyšší a vyjmenujte jejich funkci při přenosu dat.
- Která vrstva zajišťuje směrování v síti
- Která vrstva zajišťuje převod logického signálu na napětí
- Která vrstva zajistí, aby byla data přenesena bezchybně mezi sousedními uzly
- Kterou vrstvu nemusíme realizovat v lokální počítačové síti a proč
- Která vrstva odstraňuje výpadky (rozpad) transportního spojení



# Otázky

- Zakreslete schematicky referenční model TCP/IP, vysvětlete význam jednotlivých vrstev a uveďte příklady protokolů.
- Porovnejte referenční model ISO/OSI s modelem TCP/IP. Které vrstvy v modelu TCP/IP chybí a jak jsou nahrazovány.
- Uveďte základní aplikační protokoly TCP/IP.
- Co znamená zkratka TCP a co IP. Kde se TCP/IP používá.
- Co jsou to spojované a nespojované služby. Kterým protokoly jsou v zásobníku TCP/IP realizovány
- Uveďte výhody a nevýhody spojovaných služeb. Kdy (v jakých typických aplikacích) se zejména používají
- Uveďte výhody a nevýhody nespojovaných služeb. Kdy (v jakých typických aplikacích) se zejména používají.

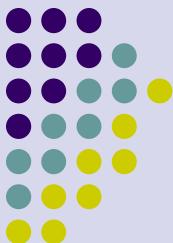
# Zásobník protokolů TCP/IP



Úvod do počítačových sítí

Lekce 2

Ing. Jiří lédvina, CSc.



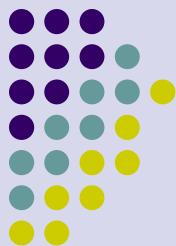
# Úvod

- Vysvětlení základních pojmů a principů v protokolovém zásobníku TCP/IP
- Adresování v Internetu
- Jmenné služby
- Protokoly
- Referenční model ISO/OSI
- Porovnání s modelem TCP/IP s modelem ISO/OSI



# Protokolový zásobník TCP/IP

- **TCP/IP** – Transport Control Protocol/Internet Protocol
- Základ protokolů Internetu
- Vznik v 70 letech minulého století
- Zásobník se 4 až 5 vrstvami
  - Přenosová (Fyzická a přístupová) – závislá na médiu
  - Sítová – nezávislá na médiu, adresování, směrování
  - Transportní – přenos dat mezi procesy,
  - Aplikační – komunikace mezi aplikacemi



# Protokolový zásobník TCP/IP

- Přenosové protokoly
  - **Ethernet** (nejčastější)
  - **Protokoly IEEE** 802.3, 802.4, 802.5, 802.6, 802.11, ...
  - **PPP** (Point to Point Protocol)
  - **SLIP** (Seriál Link Internet Protocol)
  - **ATM** (Asynchronous Transfer Mode)
  - A mnoho dalších ...
- Síťový protokol
  - **IP** (Internet Protocol) – nespojovaný protokol, nepotvrzované služby, přenáší pakety a směruje je podle cílové adresy.



# Protokolový zásobník TCP/IP

## ● Pomocné protokoly

- Kromě „přenosových“ protokolů existují i protokoly pomocné, které se používají pro řízení a oznamování chyb
- **ARP** (Address Resolution protocol) – převod síťové adresy na fyzickou (Ethernet)
- **ICMP** (Internet Control Message Protocol) – přenos zpráv o chybách, test dosažitelnosti vzdáleného uzlu, přenos parametrů, synchronizace času
- **BOOTP** (Bootstrap Protocol) – pracuje nad UDP, slouží k získání IP adresy a dalších parametrů potřebných pro zapojení uzlu do sítě
- **DHCP** (Dynamic Host Configuration Protocol) – obdoba BOOTP ale s tím, že se nepoužívá statická konfigurace – při každém připojení do sítě může uzel obdržet jinou adresu.



# Protokolový zásobník TCP/IP

- Transportní protokoly
  - **TCP** (Transport Control Protocol) – spojované služby, potvrzované, obnova po chybě
  - **UDP** (User Datagram protocol) – nespojované služby, nepotvrzované
- Aplikační protokoly
  - **Telnet** – (telecommunication network) – emulace terminálu, vzdálený přístup
  - **FTP** (File Transfer Protocol) – přenos souborů, přístup ke vzdálenému serveru
  - **HTTP** (HyperText Transport Protocol) – přístup k webovým stránkám
  - **DNS** (Domain Name Services) – jmenné služby
  - A mnoho dalších ...



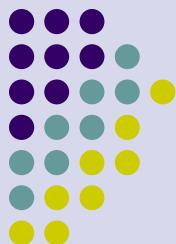
# Adresy a adresování

- Počítač je objekt
  - Objekt se identifikuje jednoznačným identifikátorem – např. číslo, ale většinou se špatně pamatuje
    - Rodné číslo – 865319/0123
    - IP adresa (Internet adresa) – 147.228.67.106
  - Objekt se identifikuje jménem – snadno se pamatuje, ale nemusí být obecně jednoznačné
    - Jméno a příjmení – Jana Malá, jr.
    - Doménové jméno počítače – eryx.zcu.cz
- Adresování v Internetu
  - Globálně rozlišitelná adresa – jednoznačné přiřazení počítači
  - Existují ale i privátní adresy – použití lokálně, mimo Internet
    - Např. rozsahy 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
  - Stejný formát, rezervovaný rozsah (dáno dohodou)



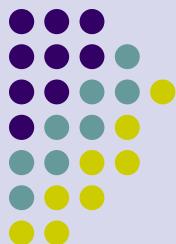
# Adresy a adresování

- Vývoj adresování
  - Původní verze – IPv4
    - Vytvořena počátkem 70 let minulého století
  - Nová verze – IPv6
    - Vytvořena v 90 letech minulého století (1994-1998)
    - Důvodem byl rychlý rozvoj Internetu a nedostatek IP adres
    - Počet adres by měl stačit již nápořád
    - Pokud je povrch Země  $511,263,971,197,990 \text{ m}^2$
    - Pak na 1 m<sup>2</sup> připadá  $665,570,793,348,866,943,898,599$  adres



# Adresy a adresování

- Dnes existují dva typy protokolu IP
  - Původní verze - IPv4
    - Adresa délky 32 bitů, zapisovaná ve tvaru a.b.c.d
    - a, b, c, d – dekadická čísla v rozsahu 0 až 255 (8 bitů)
    - $2^{32}$  (4,294,967,296) adres
    - **147.228.54.10**
  - Nová verze – IPv6
    - Adresa délky 128 bitů, zapisovaná ve tvaru
      - abcd:efgh: ... :stuv:wxyz
      - abcd – hexadecimální čísla v rozsahu 0 až FFFF
      - $2^{128}$  (340,282,366,920,938,463,463,374,607,431,768,211,456)
      - **2002:93e4:406a::93e4:406a**
  - Změna není pouze ve změně adresy (ta je ale nejvíce patrná)

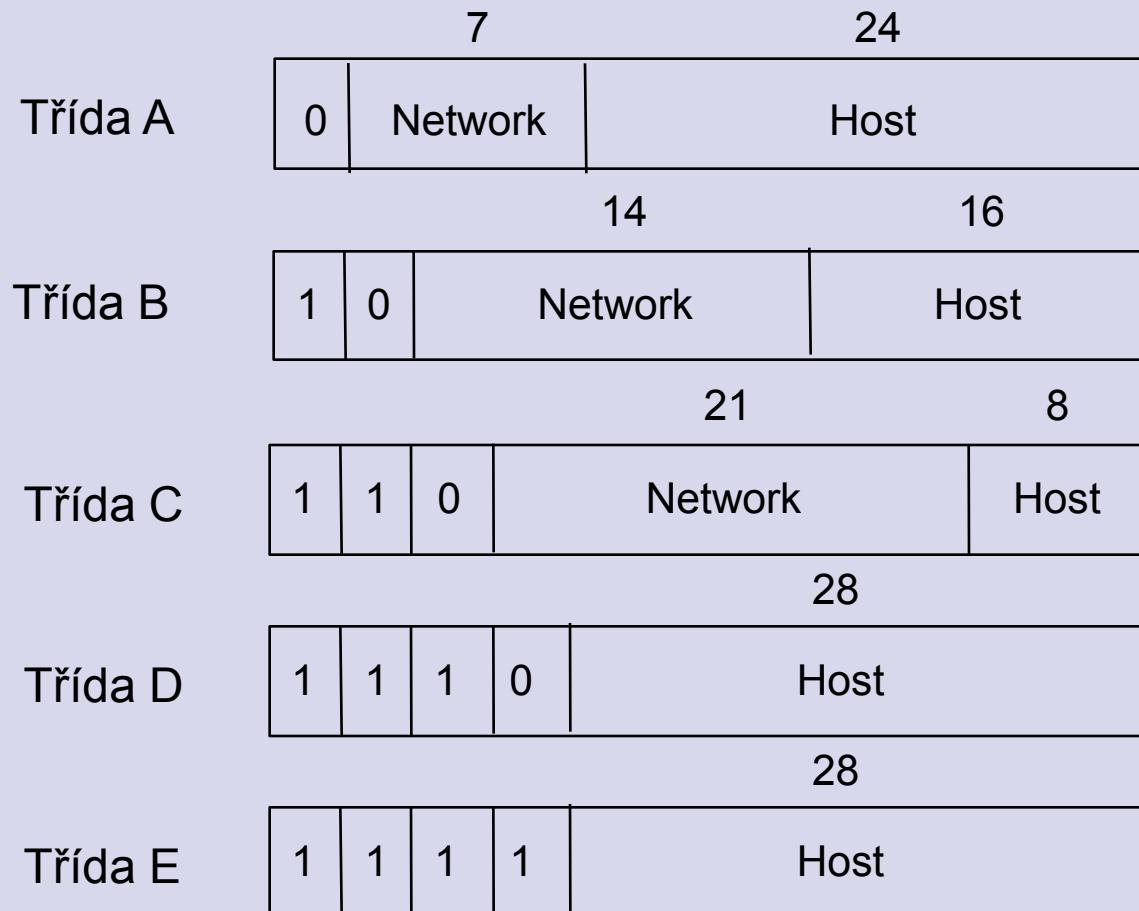


# Adresy a adresování

- Typy síťových adres (IPv4)
  - Individuální adresa – jednoznačně určuje adresu počítače (uzlu)
    - Třída A (1.0.0.0 – 126.255.255.255)
    - Třída B (128.1.0.0 – 191. 254.255.255)
    - Třída C (192.0.1.0 – 223.255.254.255)
  - Skupinová adresa – určuje skupinu uzlů
    - Třída D (224.0.0.0 – 239.255.255.255)
  - Všeobecná adresa – přenos zpráv pro všechny
    - (limitováno lokálním segmentem sítě)
    - 255.255.255.255



# Adresy a adresování





# Adresy a adresování

- Vyhrazená část (IPv4)

- 0.0.0.0
- 127.0.0.0
- 128.0.0.0
- 191.255.0.0
- 192.0.0.0
- 223.255.255
- 255.255.255.255

- Privátní adresy (IPv4)

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255



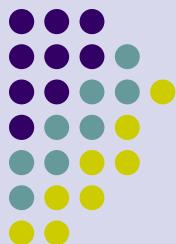
# Adresy a adresování

- Maska sítě
  - Rozděluje adresu na část síťovou a část pro hostitelský systém
  - Např. 255.255.255.0
  - 147.228.67.0 \* 255.255.255.0 dává stejný výsledek pro všechny adresy začínající 147.228.67
  - Důvodem rozdelení na dvě části je minimalizace počtu položek ve směrovačích (jedna položka zahrnuje více adres počítačů)
- CIDR (ClassLess InterDomain Routing)
  - Umožňuje použít pro adresování v podsíti takový počet bitů, který není na hranici 8.
  - Adresa se udává ve tvaru adresa/počet bitů síťové části
  - Např. 147.228.67.0/24

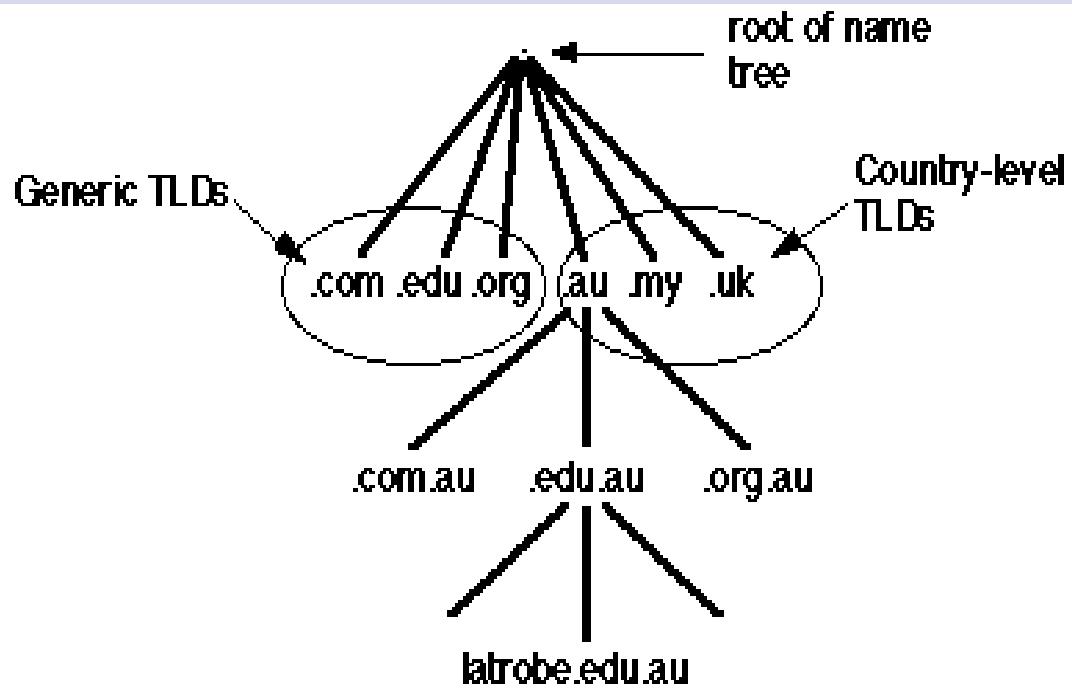


# Jména a jmenné služby

- Každý počítač má přiřazené jednoznačné doménové jméno
  - Jméno obsahuje informaci o doméně, ve které je definováno – tím se docílí toho, že ve dvou různých doménách mohou být stejná jména
  - Toto jméno má tvar
  - <host>.<subdoména>.<subdoména>. ... .<doména>
  - Např. eryx.zcu.cz



# Jména a jmenné služby

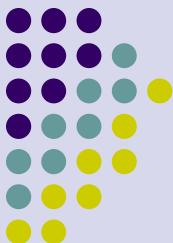


Kořen (.)

Doména nejvyšší úrovně (TLD)

Doména druhé úrovně (SLD)

Doména třetí úrovně



# Jména a jmenné služby

- Domény nejvyšší úrovně (původní)
  - edu – výukové organizace USA
  - com – společnosti
  - net – organizace poskytující síťové služby
  - gov – vládní organizace
  - mil – vojenská část sítě
  - org – různé organizace (ieee, acm)
- Nové domény
  - .aero .biz .coop .info .name .pro .eu



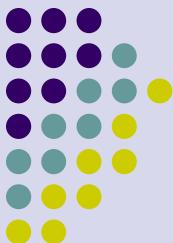
# Domény nejvyšší úrovně

- .aero – rezervováno pro letecký průmysl a sponzorováno Société Internationale de Télécommunications Aéronautiques (SITA).
- .biz – omezeno na obchod a řízeno NeuLevel, Inc.
- .com – řízeno VeriSign Global Registry Services.
- .coop – rezervováno pro spolupracující společnosti a sponzorováno Dot Cooperation LLC.
- .info – řízeno Afilias Limited.
- .museum – rezervováno pro musea, sponzorováno Museum Domain Management Association.
- .name – rezervováno pro jednotlivce, spravováno Global Name Registry.
- .net – spravováno VeriSign Global Registry Services.
- .org – nekomerční skupiny, spravováno Public Interest Registry.
- .pro – využití omezeno pro vybrané profesionály a podobné entity, spravováno RegistryPro.



# Jména a jmenné služby

- Domény nejvyšší úrovně podle geografického rozdělení
  - cz – Česká republika
  - sk – Slovenská republika
  - pl – Polsko
  - uk – Velká Británie
  - au – Austrálie.
- Aliasy – zavedení funkčních jmen pro jejich ještě lepší zapamatování
  - Např. www, ftp, time, clock, ns, ...
- Absolutní a relativní jména
  - Relativní (neúplné) jméno - www - platí v doméně zcu.cz
  - Absolutní (úplné) jméno www.zcu.cz.



# Jména a jmenné služby

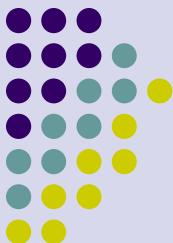
- Systém jmenných domén (DNS – Domain Name System)
  - Slouží k převodu jména na adresu a opačně
  - Poskytuje i další informace (jmenné servery, poštovní servery, informace o doméně, o počítačích, ... )
  - Základem je distribuovaná databáze
  - Protokol využívá služeb UDP i TCP
  - V každé oblasti jeden primární jmenný server a alespoň jeden sekundární jmenný server
  - Oprava databáze se provádí na primárním jmenném serveru
  - Sekundární jmenné servery získávají informaci z primárního
  - Důvodem je zvýšení spolehlivosti DNS



# Jména a jmenné služby

## • Hierarchie domén

- Domény tvoří hierarchickou strukturu (úroveň katedry, fakulty, univerzity, poskytovatele)
- Každou doménu má na starost jmenný server
- Servery také tvoří hierarchii
- Kořenová část sítě – GTLD (General Top-Level-Domain)
  - 13 jmenných serverů – kořenových jmenných serverů, centrální distribuce informací
  - A.ROOT-SERVERS.NET, B.ROOT-SERVERS.NET, … , M.ROOT-SERVERS.NET
  - Poskytuje informace o doménách druhé úrovně
- Domény druhé úrovně
  - Jmenné servery poskytují informace doménám třetí úrovně
- Domény třetí, čtvrté, páté úrovně

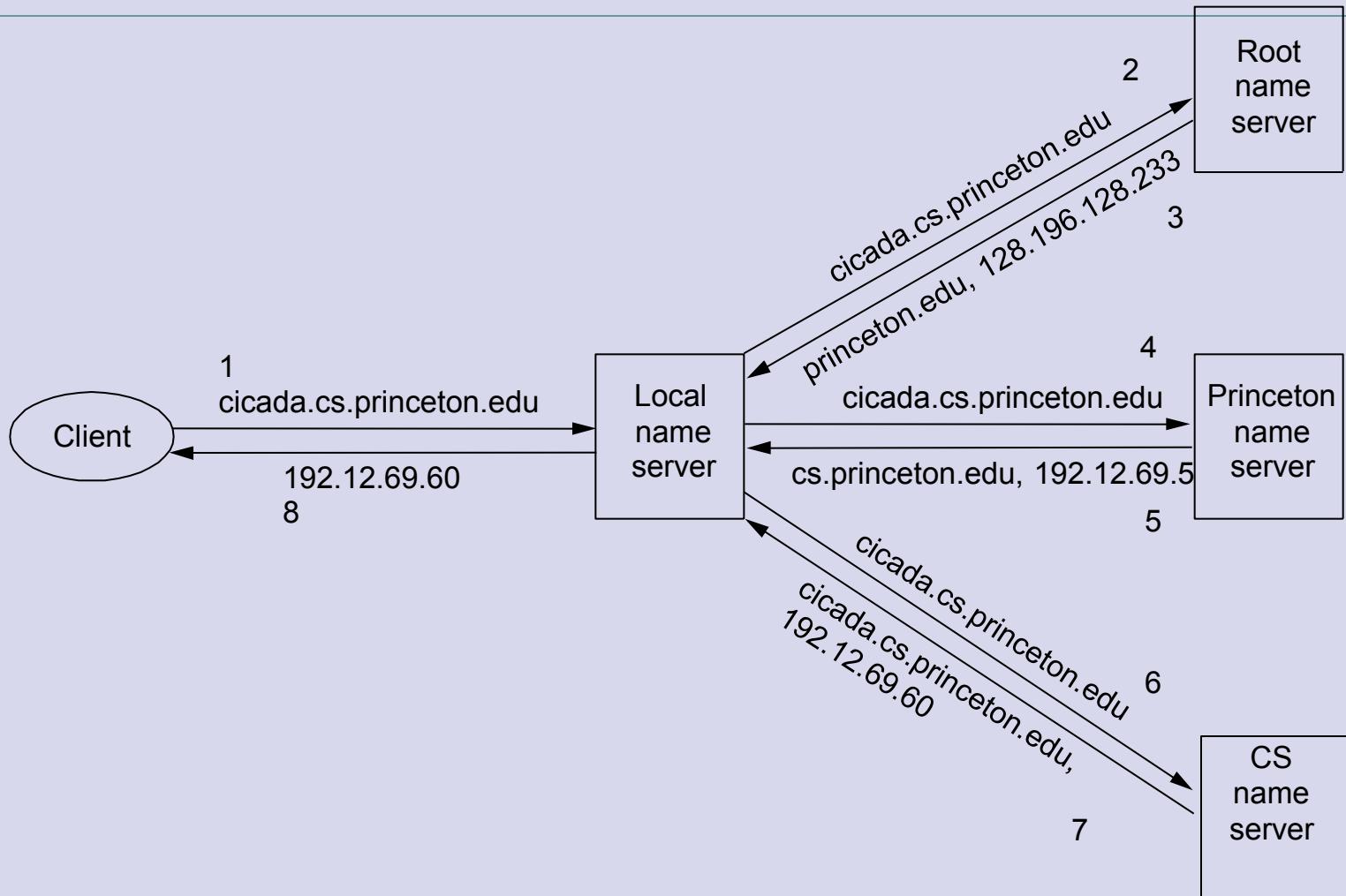


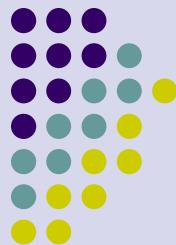
# Jména a jmenné služby

- Postup dotazování
  - Program → klient jmenných služeb (resolver)
  - Klient → jmenný server oblasti (nakonfigurovaný)
  - Jmenný server oblasti → jmenný server nadřazené oblasti ...
  - Jmenný server nadřazené oblasti → vrátí adresu jmenného serveru cílové oblasti
  - Jmenný server → jmenný server cílové oblasti
  - Jmenný server → klient (v lokálním uzlu)



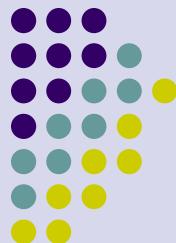
# Postup dotazování





# Některé základní služby TCP/IP

- ifconfig (ipconfig)
  - Rozhraní, fyzická adresa, síťová adresa, ...
- arp – tabulka přiřazení síťová – fyzická adresa
- route – výpis směrovací tabulky
- netstat – zjištění stavu spojení (TCP, UDP)
- ping – test dostupnosti vzdáleného počítače
- traceroute (tracert) – výpis cesty ke vzdálenému počítači
- nslookup, dig, host – práce s doménovými jmény a adresami



# Úvod - protokoly

- pravidla podle kterých síťové komponenty vzájemně komunikují představují protokol
- protokoly definují formáty vyměňovaných zpráv a akce spojené s přenosem zpráv mezi entitami
- protokoly známé z běžného života
  - pravidla podle kterých dva nebo více lidí komunikují
  - řízení dopravy
  - problém souběžného přístupu
  - další ....



# Úvod - úrovňová architektura

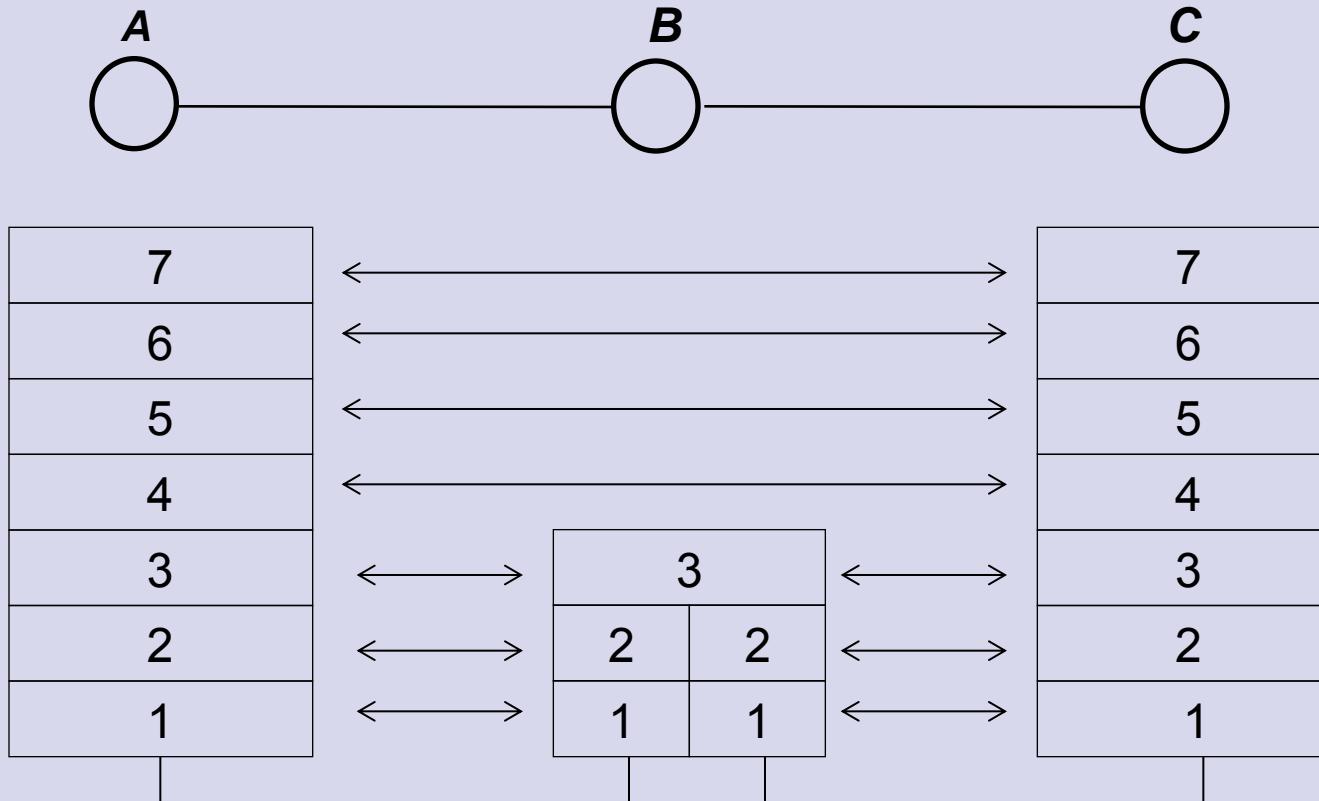
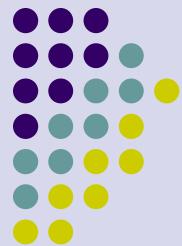
- architektura složitých systémů může být zjednodušena rozdělením do více úrovní
- úroveň N využívá služeb úrovně N-1 a zajišťuje služby pro úroveň N+1
- služby poskytované nižší úrovní jsou nezávislé na tom, jak jsou tyto služby realizovány
  - *skrytí složitosti nižších úrovní*
  - *změna úrovně N neovlivní ostatní úrovně*
- rozhraní definuje jak lze služby využívat

# Úvod - distribuovaná síťová architektura

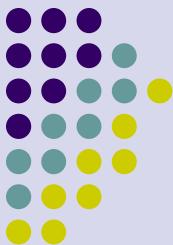


- síť je složena z geograficky distribuovaných technických i programových komponent
- stejnorodé entity (např. procesy) na úrovni N poskytují služby komunikací (posíláním zpráv nebo paketů) sobě navzájem. Používají přitom komunikační služby úrovně N-1
- logická kontra fyzická komunikace

# Úvod - distribuovaná síťová architektura

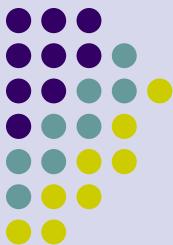


# Úvod - referenční model ISO/OSI



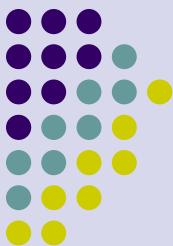
- aplikační úroveň
  - komunikace mezi procesy
  - všechny existující úrovně podporují aplikační úroveň
  - příklady:
    - elektronická pošta
    - telekonferencing
    - www
    - ftp
    - telnet
    - distribuované databáze
- prezentační úroveň
  - konverze dat do společného formátu
  - komprese dat
  - ochrana dat (šifrování)

# Úvod - referenční model ISO/OSI



- relační úroveň
  - spojení dvou aplikací pomocí relace
  - vytvoření relace (ověřování)
  - obnova po chybě
  - sdílení relačního spojení
- transportní úroveň
  - univerzální transportní služby: přenos dat mezi koncovými procesy
  - komunikace mezi koncovými uzly
  - multiplexování toku dat z vyšších úrovní
  - srovnání rychlosti vysílače a přijímače

# Úvod - referenční model ISO/OSI

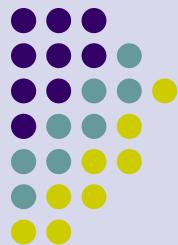


- síťová úroveň
  - přijímání paketů z vyšších úrovní a určení jejich cesty do koncových uzlů
  - řízení směrování
  - předcházení zahlcení, předcházení kolizím
  - adresování v síti
- linková úroveň
  - komunikace mezi dvěma sousedními uzly
  - zajištění bezchybného přenosu
  - řízení rychlosti přenosu mezi sousedními uzly
- fyzická úroveň
  - transport jednotlivých bitů komunikačním vedením
  - kódování přenášených informací



# Úvod - obecné funkce úrovní

- zpracování chyb
  - vytvoření spolehlivějšího kanálu
  - zpracování ztracených paketů a paketů přijatých mimo pořadí
- řízení toku dat
  - předcházení zaplavení sítě pakety
  - vzniká např. při různých rychlostech hostitelských systémů nebo různých kapacitách komunikačních komponent a kanálů
- přidělování zdrojů
  - přidělování fyzických zdrojů (vyrovnávací paměti, šířka přenášeného pásma)
  - přidělování logických zdrojů (datové struktury) mezi odpovídajícími entitami



# Úvod - obecné funkce úrovní

- fragmentace
  - rozdělení velkých datových bloků na menší části a jejich znova sloučení
- multiplexování
  - slučování několika relací vyšší úrovně
- vytváření spojení
  - inicializace logických spojení mezi odpovídajícími entitami



# Úvod - obecné funkce úrovní

- adresování a práce se jmény
  - ovládání identifikátorů spojených s entitami
- komprese
  - redukce velikosti přenášených dat a tím zkracování doby jejich přenosu
- šifrování
  - symetrické kódy (DES)
  - nesymetrické kódy (RSA)
- časové funkce
  - obnova po chybě

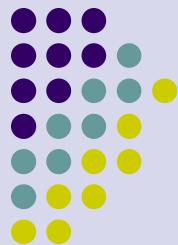


# Fyzická úroveň

Úvod do počítačových sítí

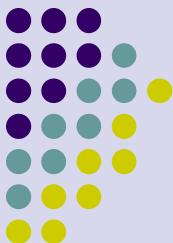
Lekce 03

Ing. Jiří ledvina, CSc.



# Teoretický základ datových komunikací

- Fourierova analýza
- Signály limitované šířkou pásma
- Maximální přenosová rychlosť kanálem



# Fourierova analýza

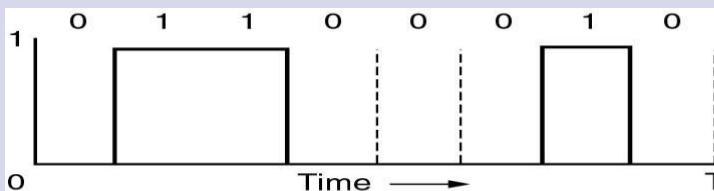
$$f(x) = a_0 + \sum_{n=1}^{\infty} (a_n \cos \omega_0 t + b_n \sin \omega_0 t)$$

$$a_0 = \frac{1}{T} \int_0^T f(t) dt$$

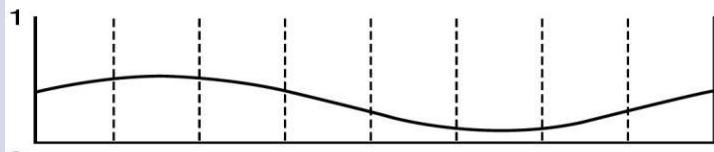
$$a_n = \frac{2}{T} \int_0^T f(t) \cos(n\omega_0 t) dt \quad b_n = \frac{2}{T} \int_0^T f(t) \sin(n\omega_0 t) dt$$



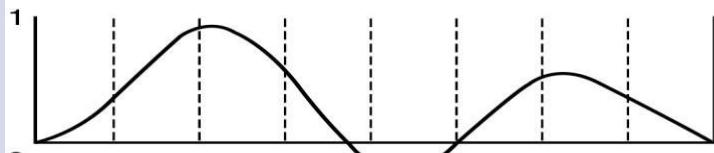
# Signály limitované šířkou pásma



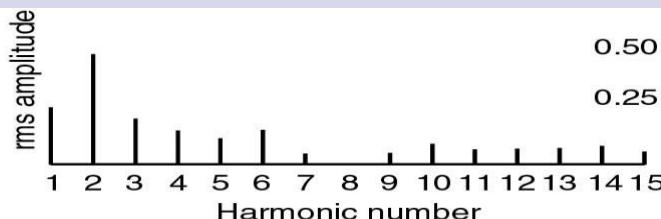
(a)



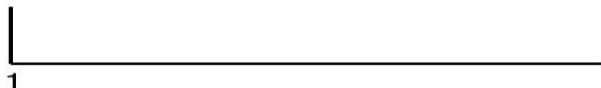
(b)



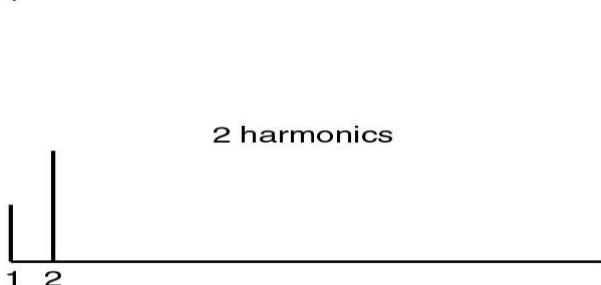
(c)



1 harmonic

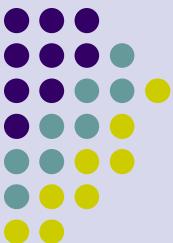


2 harmonics

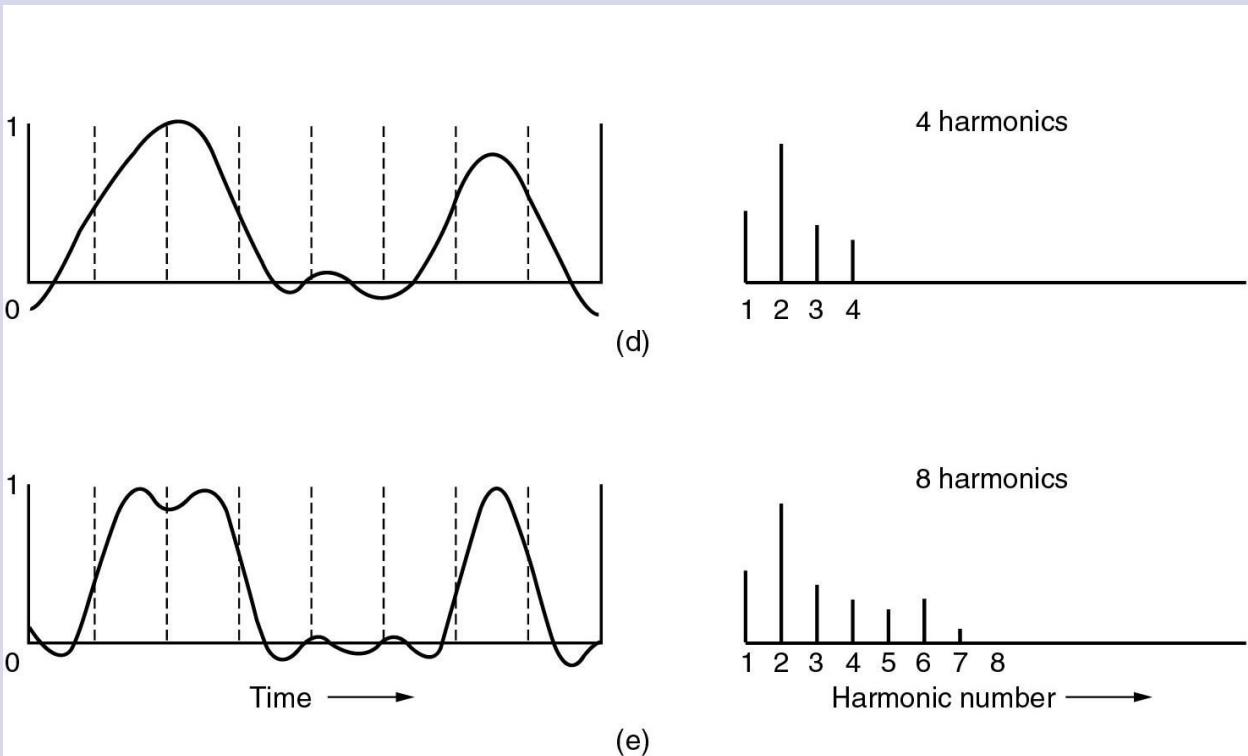


(a) Binární signál a druhá odmocnina součtu kvadrátů amplitud násobků základní frekvence.

(b) – (c) následné aproximace originálního signálu.



# Signály limitované šířkou pásma (2)

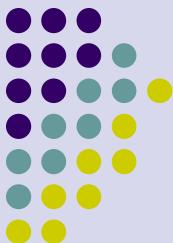


(d) – (e) další aproximace originálního signálu .



# Signály limitované šířkou pásma (3)

Bps	T (msec)	First harmonic (Hz)	# Harmonics sent
300	26.67	37.5	80
600	13.33	75	40
1200	6.67	150	20
2400	3.33	300	10
4800	1.67	600	5
9600	0.83	1200	2
19200	0.42	2400	1
38400	0.21	4800	0



# Nyquistovo kritérium

$$C = 2W \log_2 V \text{ [b/s; Hz, -]}$$

- C – kapacita komunikačního kanálu
- W – šířka pásma
- V – počet úrovní signálu
- Přenosová rychlosť
  - Počet bitů za sekundu [b/s nebo bps]
  - Počet změn za sekundu [Baud]



# Shannonovo kritérium (Shannon – Hartley)

$$C = W \log_2 \left( 1 + \frac{S}{N} \right) \left[ \frac{b}{s}; Hz, - \right]$$

- C – kapacita přenosového kanálu
- S – úroveň signálu
- N – úroveň šumu
- Na přenos působí
  - Zesílení
  - Omezené pásmo
  - Šum
    - Impulzní (spínače, ...)
    - Tepelný (pohyb elektronů)



# Zesílení a decibely

$$A_P = \log_{10} \frac{P_{out}}{P_{in}} \text{ [Bell]}$$

Příklad: S/N = 30 dB

$$A_P = 10 \log_{10} \frac{P_{in}}{P_{out}} = 10 \log_{10} \left( \frac{10}{5} \right)$$

$$A_P = 10 \log_{10} \frac{P_{out}}{P_{in}} \text{ [dB]}$$

$$A_P = 3$$

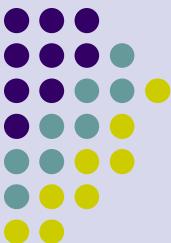
$$A_u = 20 \log_{10} \frac{U_{out}}{U_{in}} \text{ [dB]}$$

Příklad: P<sub>in</sub> = 10 mW, P<sub>out</sub> = 5 mW

$$A_P = 10 \log_{10} \left( 1 + \frac{S}{N} \right) \text{ [dB]} = 30 \text{ dB}$$

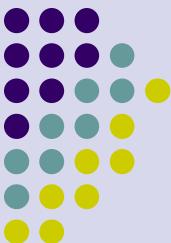
$$P_{dbm} = 10 \log_{10} P_{mW} \text{ [dB; mW]}$$

$$\left( 1 + \frac{S}{N} \right) = 10^3$$



# Typy přenosů

- Přenos
  - Sériový
  - paralelní
- Přenos
  - Synchronní
  - Asynchronní
  - Arytmický
- Přenos
  - Dvouúrovňový
  - Víceúrovňový



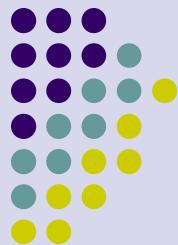
# Typy spojení

- **Spoje**
  - Dvoubodové
    - Jeden vysílač, jeden přijímač
  - Mnohabodové
    - Jeden vysílač, více přijímačů
    - Více vysílačů, více přijímačů
- **Vedení**
  - Nesymetrická
  - Symetrická
- **Přizpůsobení**
  - Impedančně nepřizpůsobené
  - Impedančně přizpůsobené

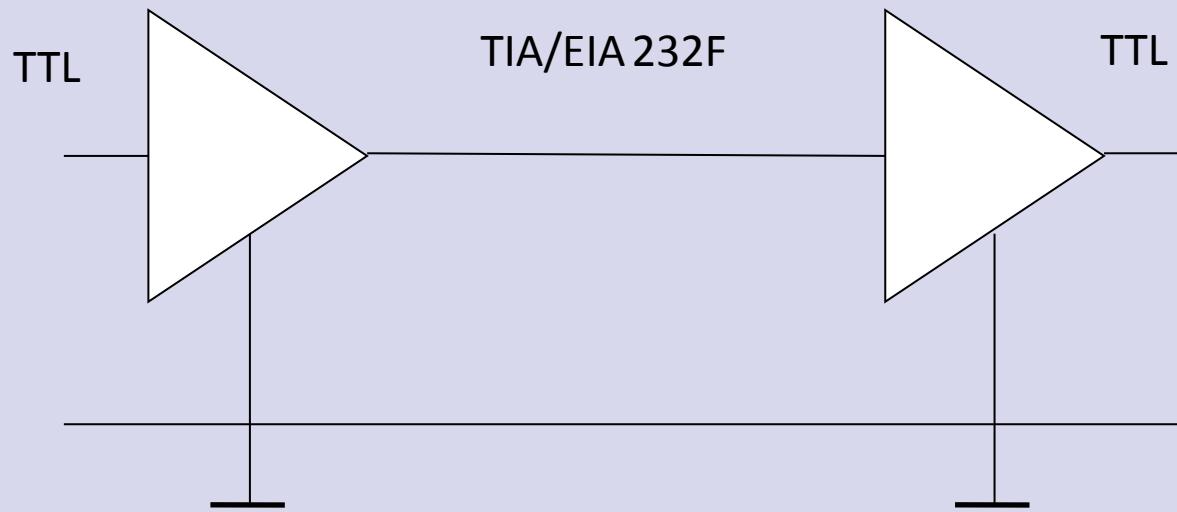


# Příklady rozhraní na fyzické úrovni

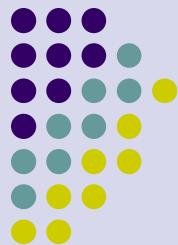
- CCITT (ITU), EIA
- V.24, V.28 (EIA RS232C) – analogové modemy
  - Signálové úrovně V.28
  - Definice okruhů V.24
- X.21, V.10/X.27 (RS 423-A) nebo V.11/X.26 (RS422-A) – číslicové modemy
  - Signálové úrovně V.10, V.11
  - Definice okruhů X.21
- EIA RS 232C – nesymetrické, 20kb/s, 20m, 15V/3V
- EIA RS 423 – nesymetrické, 1000m, 1:10, 6V/0.2V
- EIA RS 422 – symetrické, 1000m, 1:10, 6V/0.2V
- EIA RS 485 – symetrické, 1000m, 12:32, 6V/0.2V



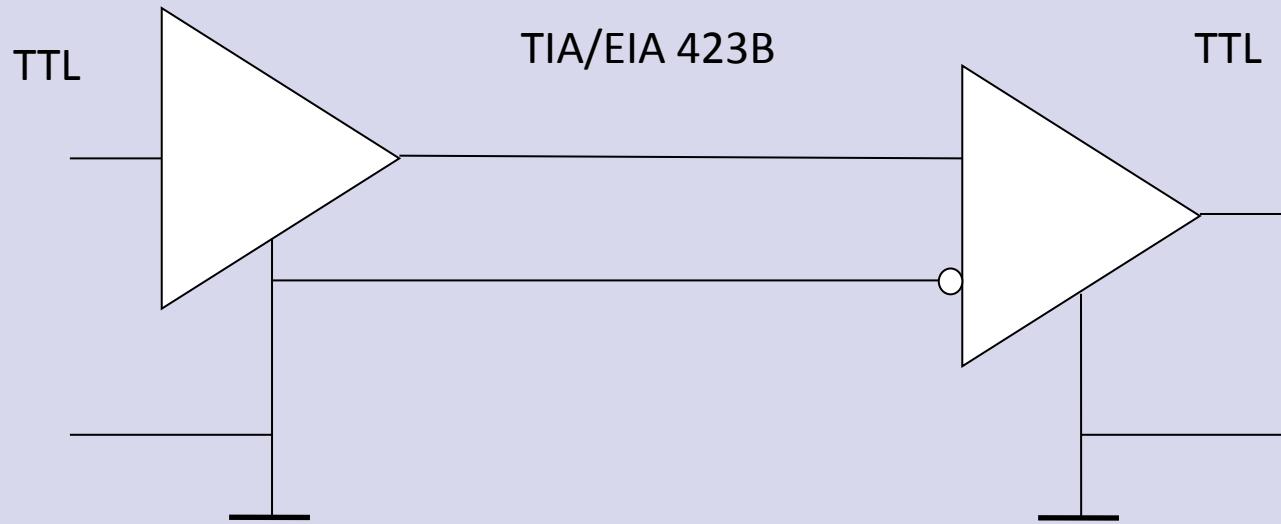
# Příklady rozhraní na fyzické úrovni



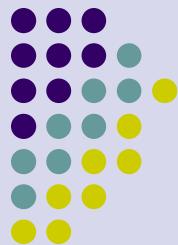
Sériové komunikační rozhraní TIA/EIA 232F (RS 232C, V.28)  
Nesymetrický vstup i výstup



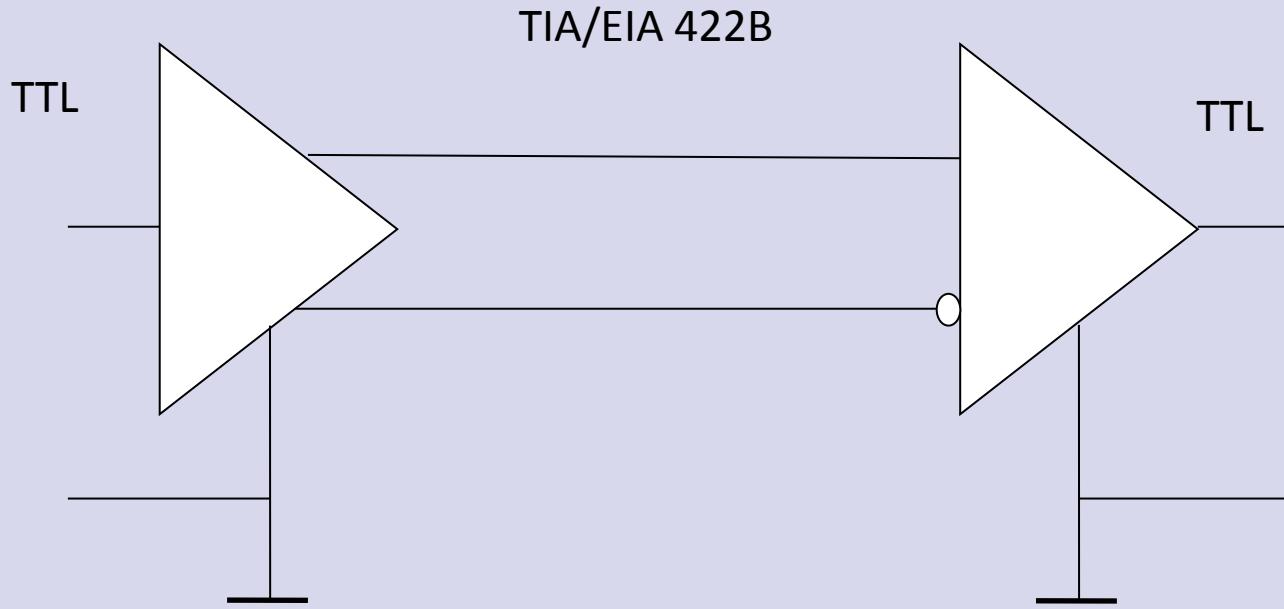
# Příklady rozhraní na fyzické úrovni



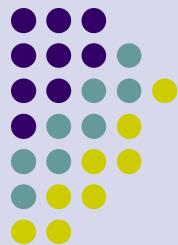
Sériové komunikační rozhraní TIA/EIA 423B (V.11)  
Symetrický vstup nesymetrický výstup



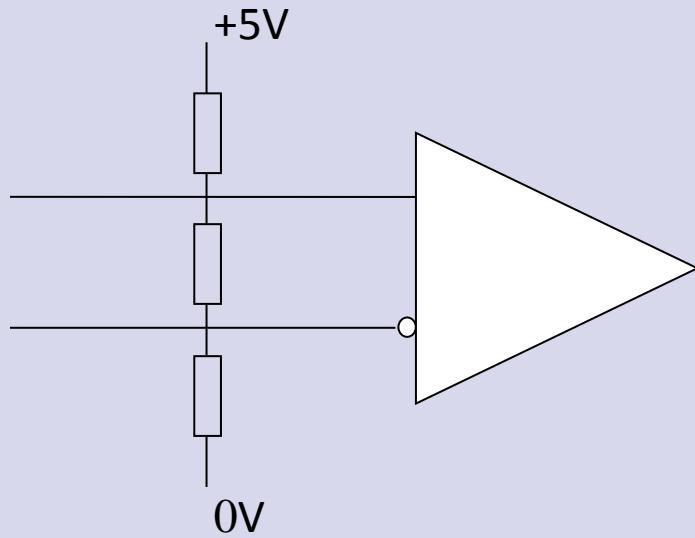
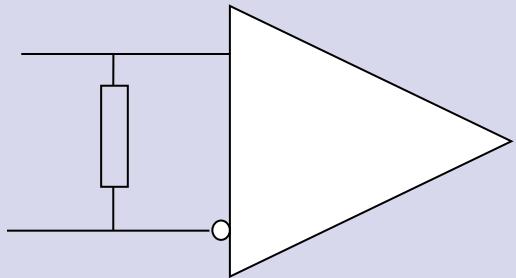
# Příklady rozhraní na fyzické úrovni



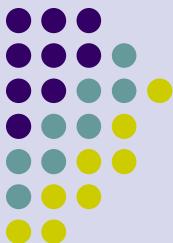
Sériové komunikační rozhraní TIA/EIA 422B (V.10)  
Symetrický vstup i výstup



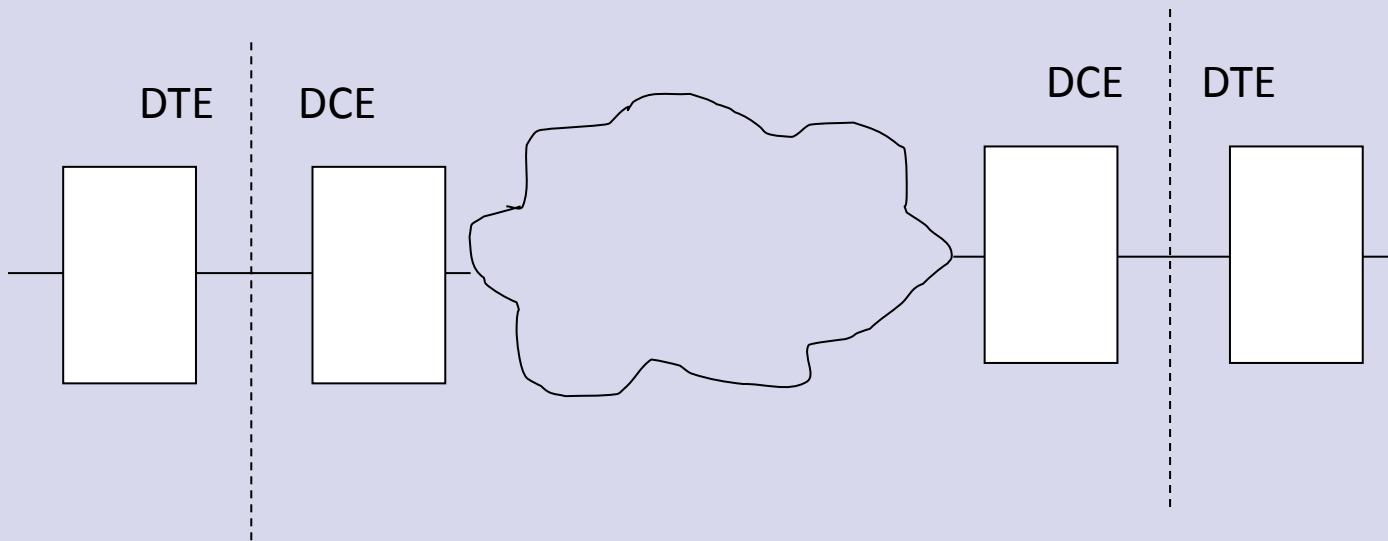
# Příklady rozhraní na fyzické úrovni



Impedanční přizpůsobení vedení, udržení rozdílového napětí na vodičích sběrnice při odpojení všech vysílačů.



# Rozhraní DTE/DCE

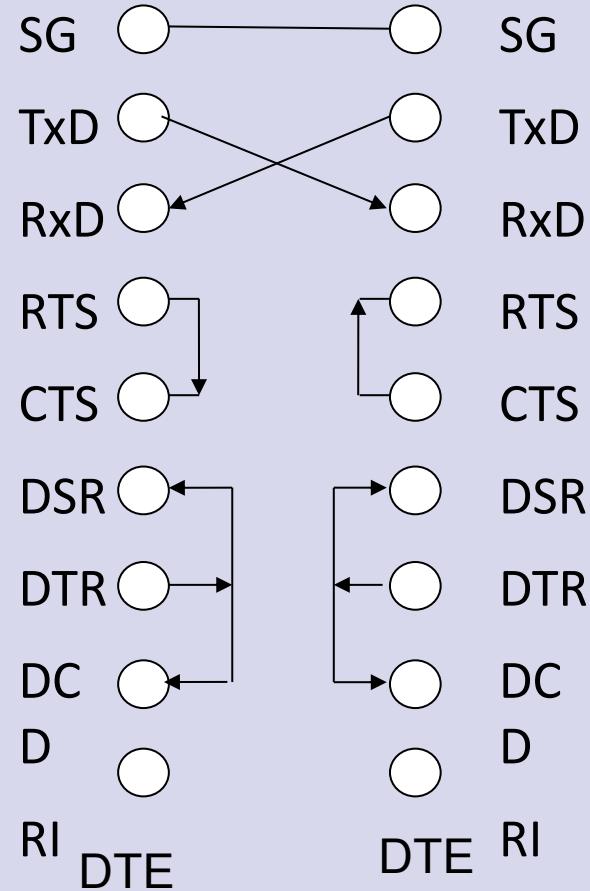
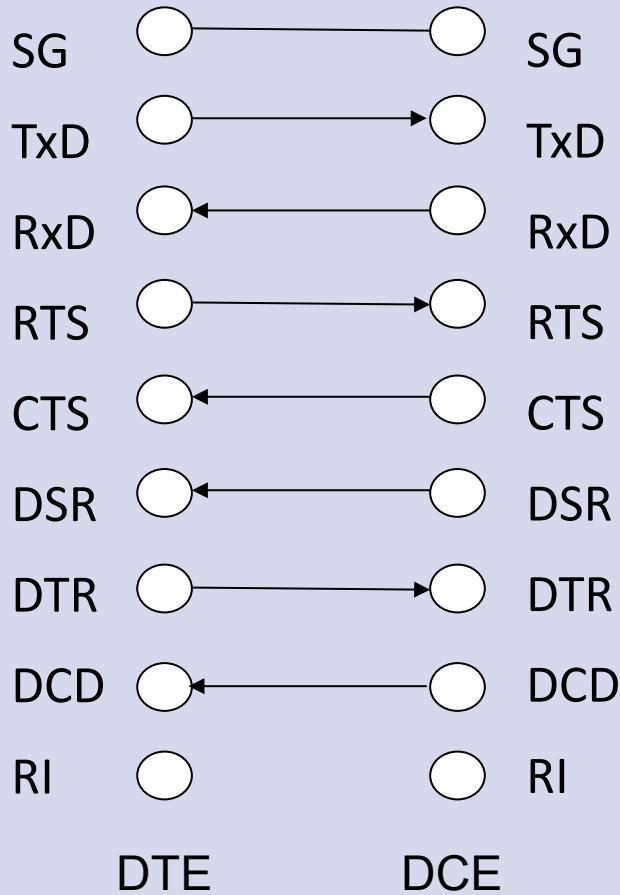


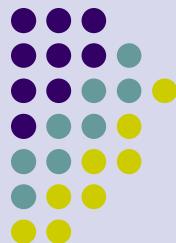
Rozhraní mezi koncovým zařízením (DTE) a ukončovacím zařízením datového okruhu (DCE)

Např. DTE – počítač, DCE - modem



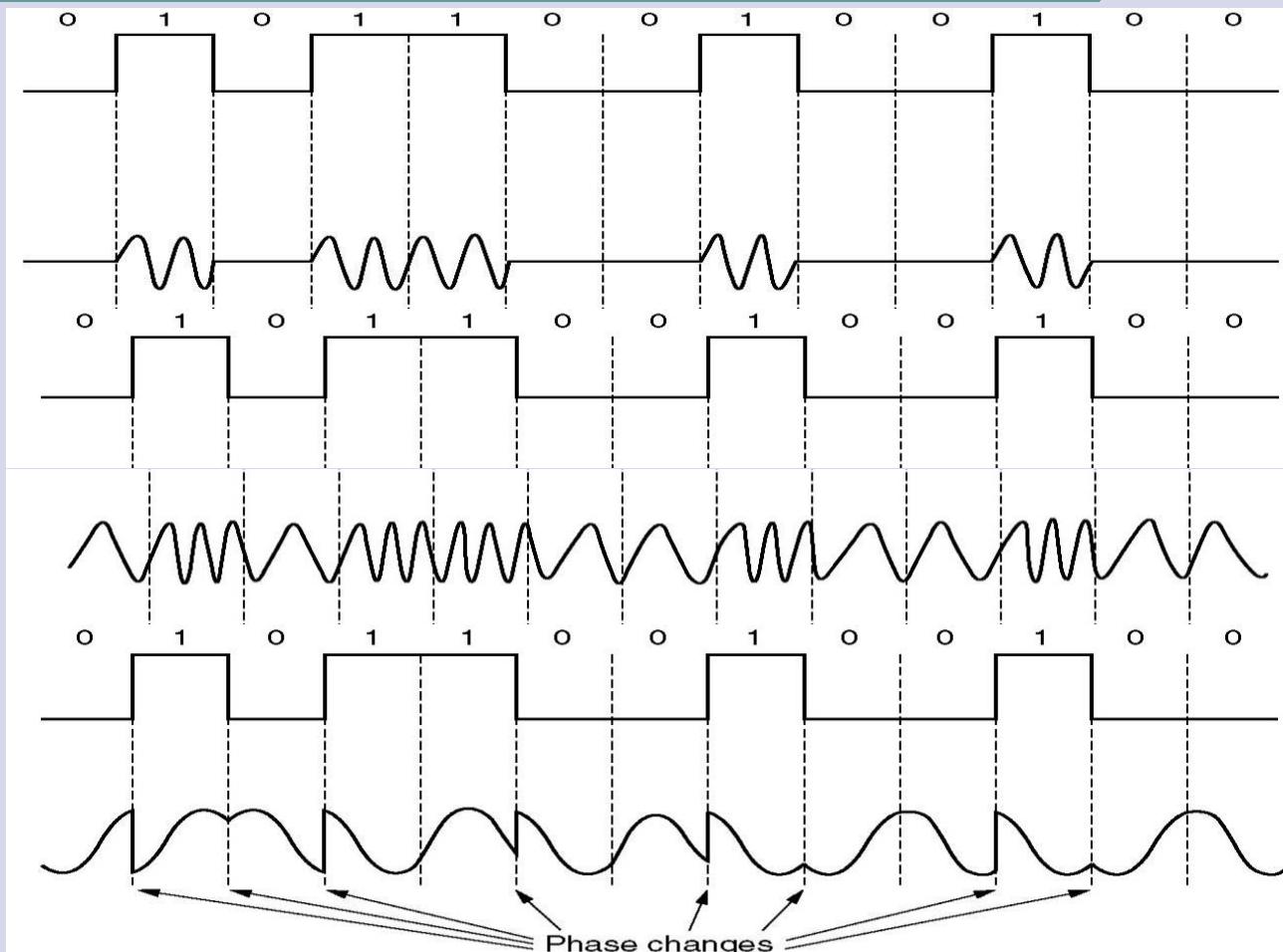
# Rozhraní DTE/DCE - RS232

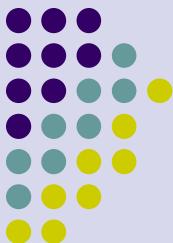




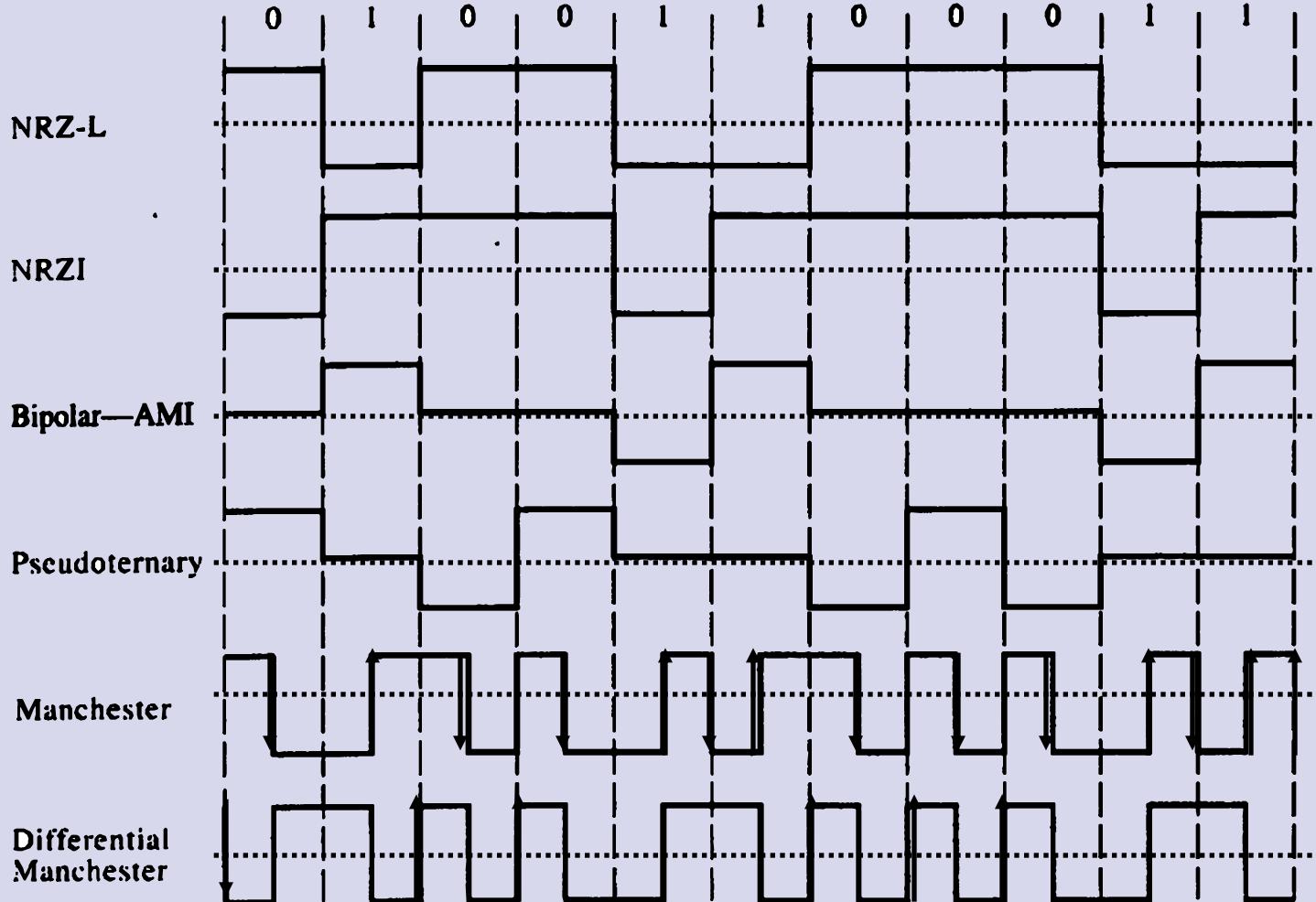
# Modulace, klíčování

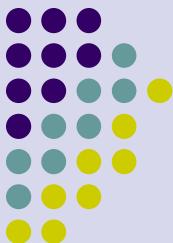
- Amplitudová
- Frekvenční
- Fázová





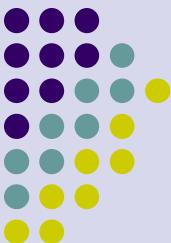
# Kódování





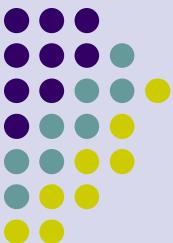
# Kódování

- **Bez návratu k nule - úroveň (NRZ-L)**  
0= vysoká úroveň  
1= nízká úroveň
- **Bez návratu k nule - invertované (NRZI, nebo NRZ-M)**  
0= *bez přechodu na začátku bitového intervalu*  
1= *přechod na začátku bitového intervalu*
- **Manchester**  
0= *přechod z vyšší úrovně na nižší uprostřed bit. intervalu*  
1= *přechod z nižší úrovně na vyšší uprostřed bit. intervalu*
- **Diferenciální Manchester**  
*změna uprostřed intervalu vždy*  
0= *změna úrovně na začátku bitového intervalu*  
1= *beze změny na začátku bitového intervalu*

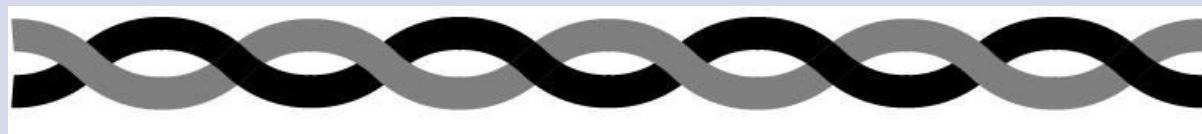


# Přenos dat vedením

- Kroucená dvojlinka
- Koaxiální kabel
- Optická vlákna



# Kroucená dvojlinka

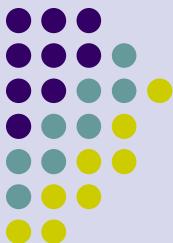


(a)



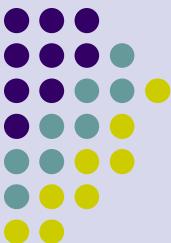
(b)

(a) kategorie 3 UTP.  
(b) kategorie 5 UTP.



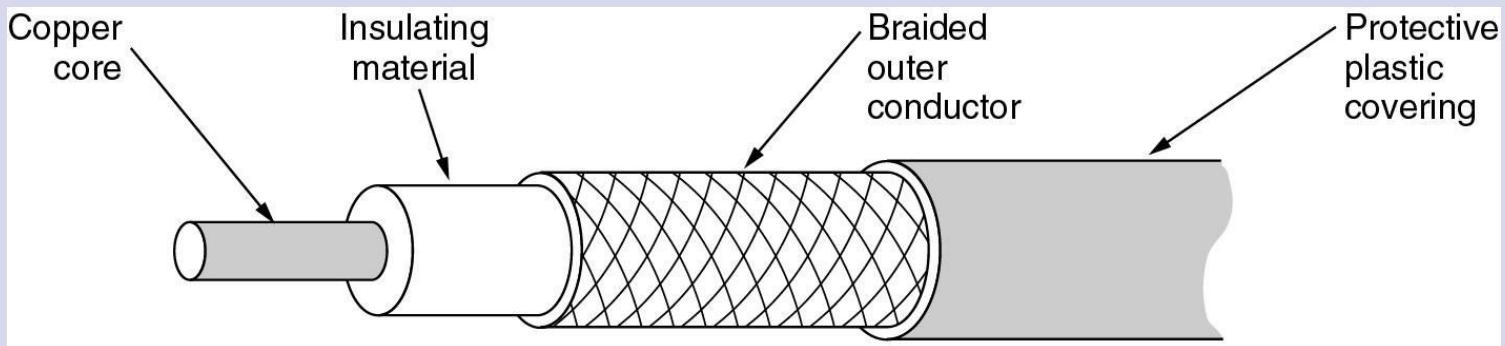
# Kroucená dvojlinka

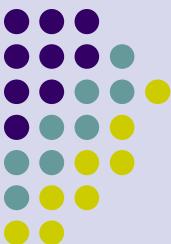
Název	Typ	Mb/s	použití
CAT1	UTP	1	modem
CAT2	UTP	4	Token Ring 4
CAT3	UTP	10	10Base-T Ethernet
CAT4	STP	16	Token Ring 16
CAT5	UTP	100	100Base-T Ethernet
CAT5	STP	100	100Base-T Ethernet
CAT5e	UTP	100	1000Base-T Ethernet
CAT6	UTP	200	1000Base-T Ethernet
CAT7	STP	600	1000Base-T Ethernet



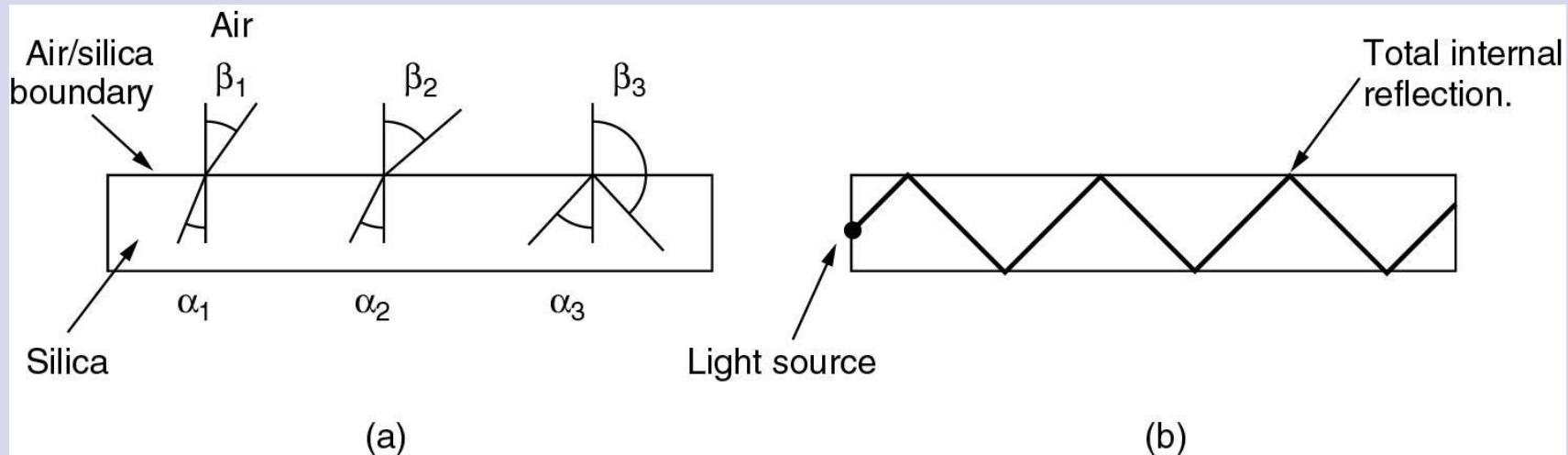
# Koaxiální kabel

Koaxiální kabel.

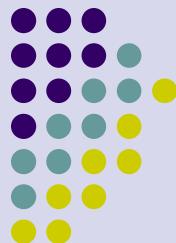




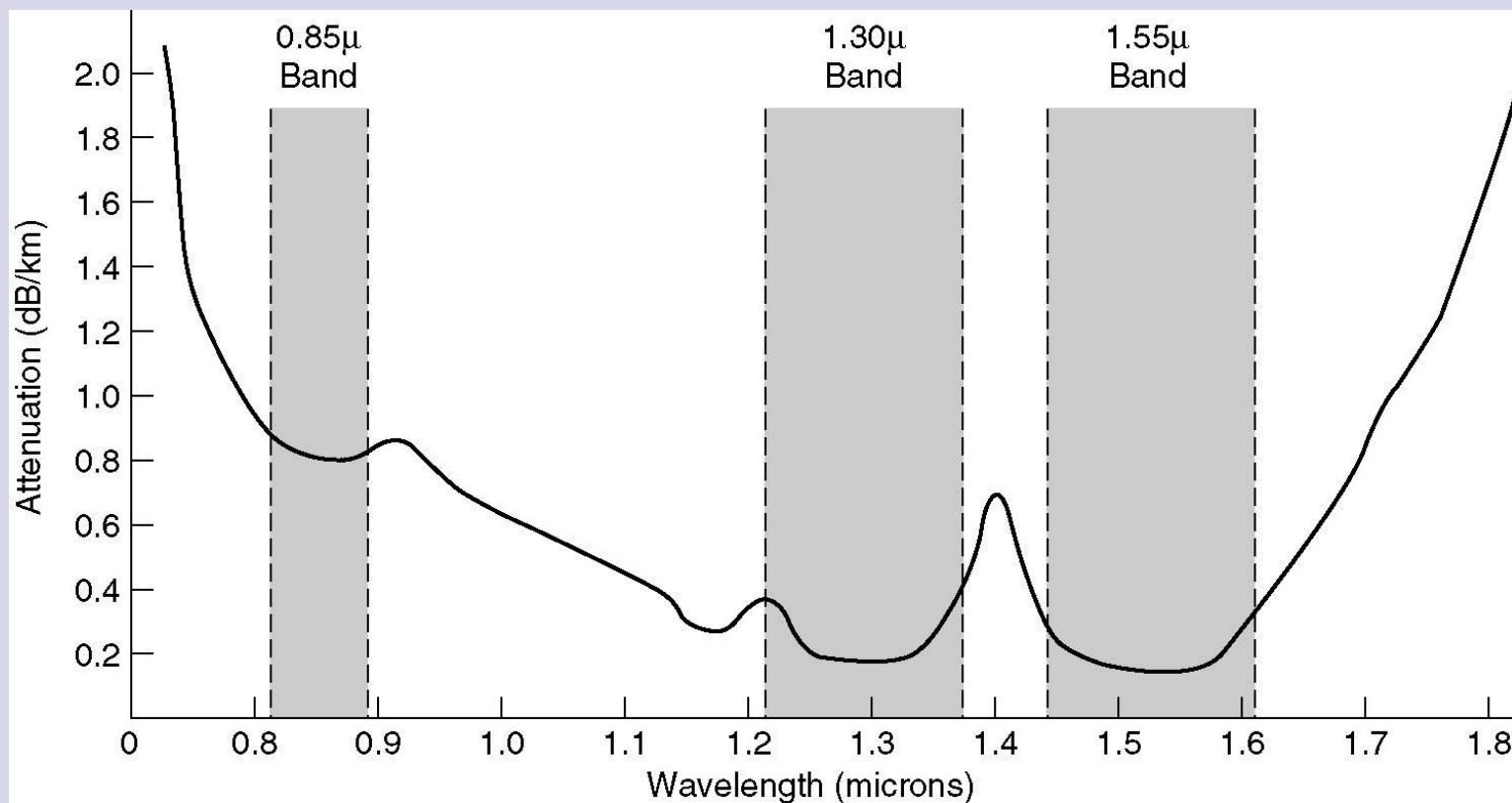
# Vláknová optika



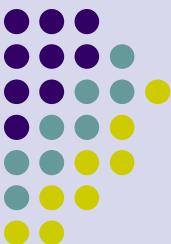
- (a) Příklady odrazu a lomu světelného paprsku na rozhraní skla a vzduchu.
- (b) Šíření světla úplným odrazem.



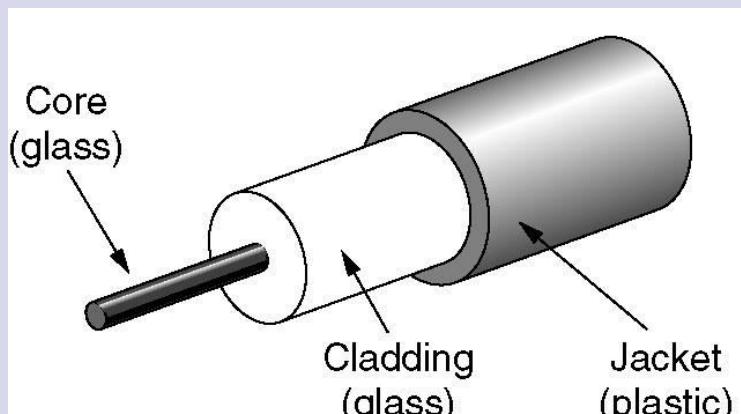
# Přenos světla optickým vláknem



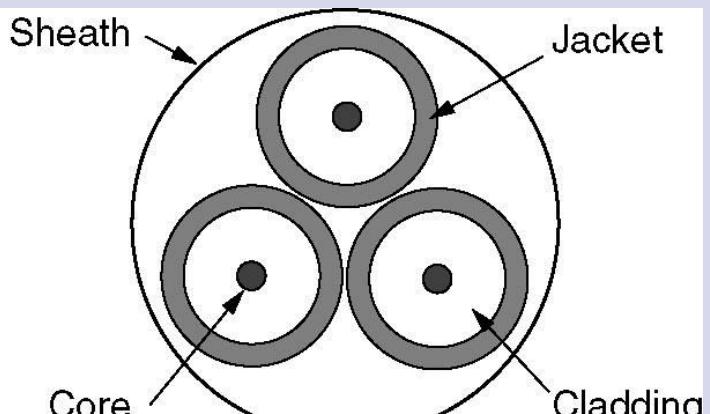
Útlum světla při průchodu optickým vláknem v oblasti infračerveného záření.



# Optické kabely

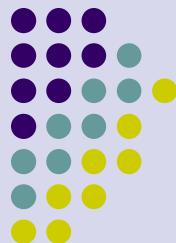


(a)



(b)

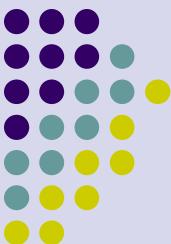
- (a) Struktura jednoho vlákna optického kabelu.  
(b) Optický kabel se třemi vlákny.



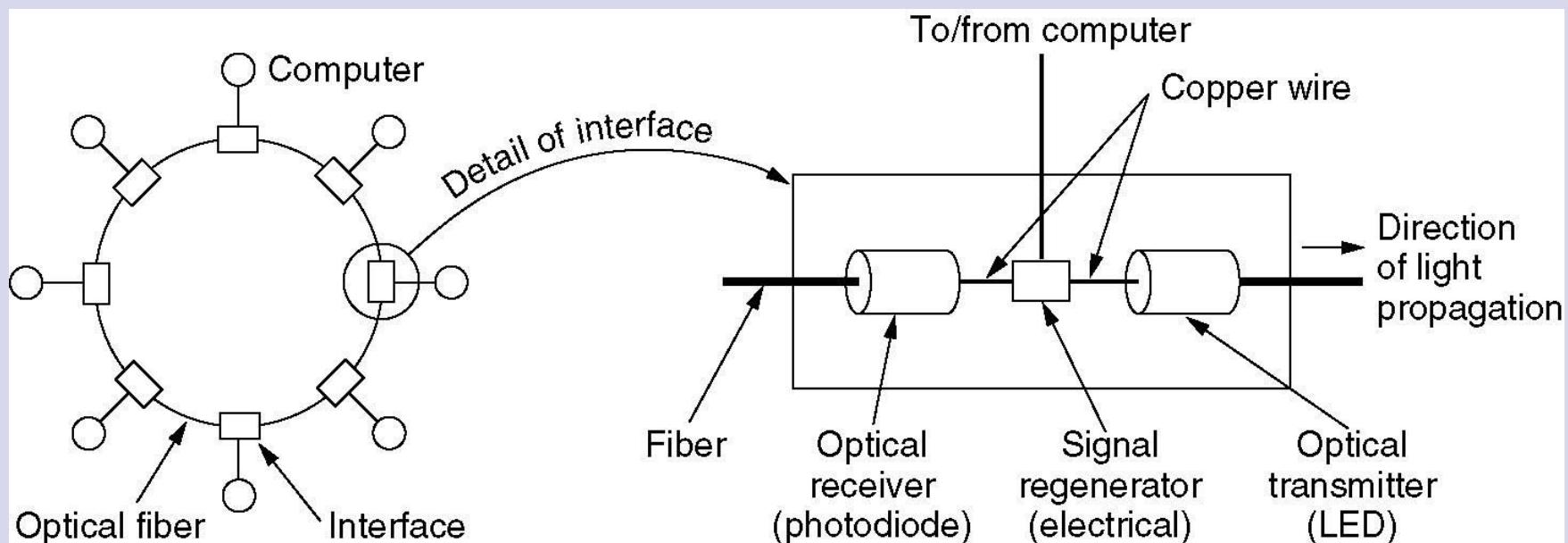
# Optické kabely (2)

Item	LED	Semiconductor laser
Data rate	Low	High
Fiber type	Multimode	Multimode or single mode
Distance	Short	Long
Lifetime	Long life	Short life
Temperature sensitivity	Minor	Substantial
Cost	Low cost	Expensive

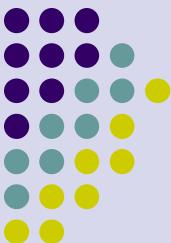
Porovnání zdrojů infračerveného záření – polovodičový laser a LED.



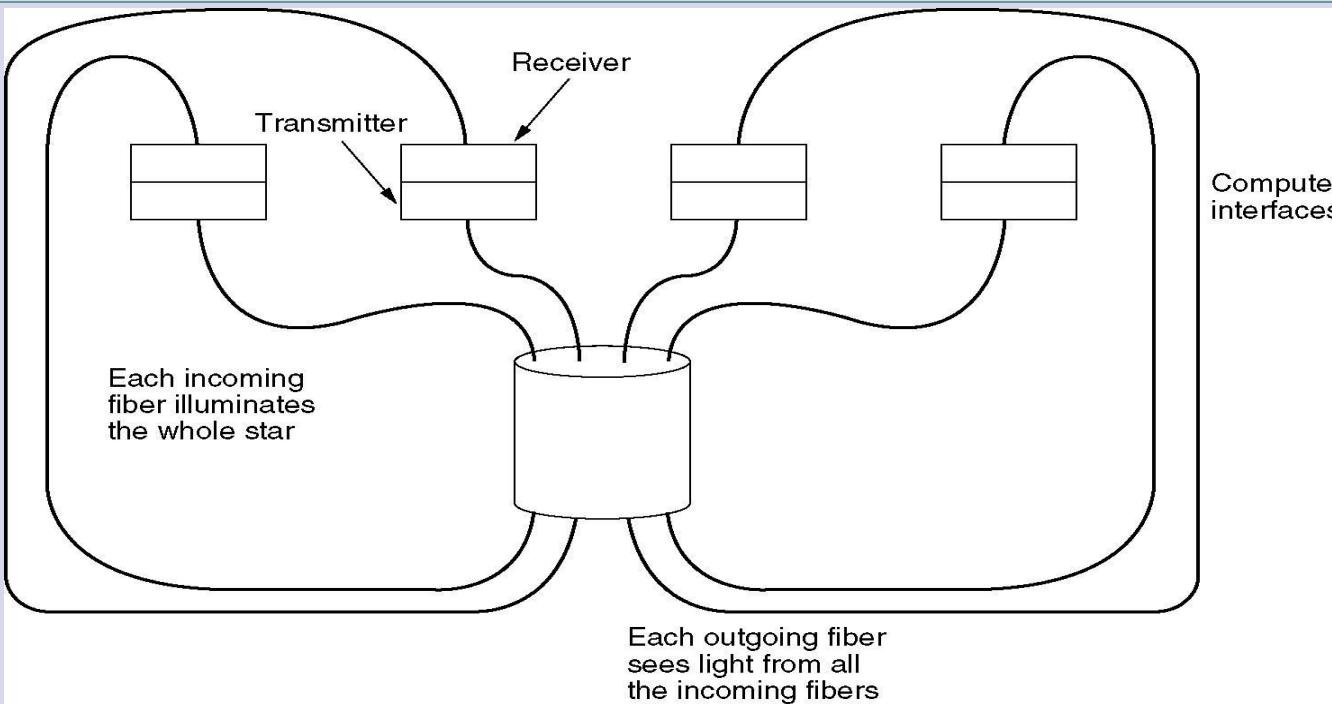
# Optické sítě



Struktura optické sítě ve tvaru kruhu s aktivními opakovači.



# Optické sítě (2)

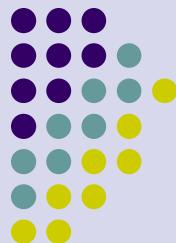


Propojení optických vláken pasivním optickým rozbočovačem ve tvaru hvězdy.

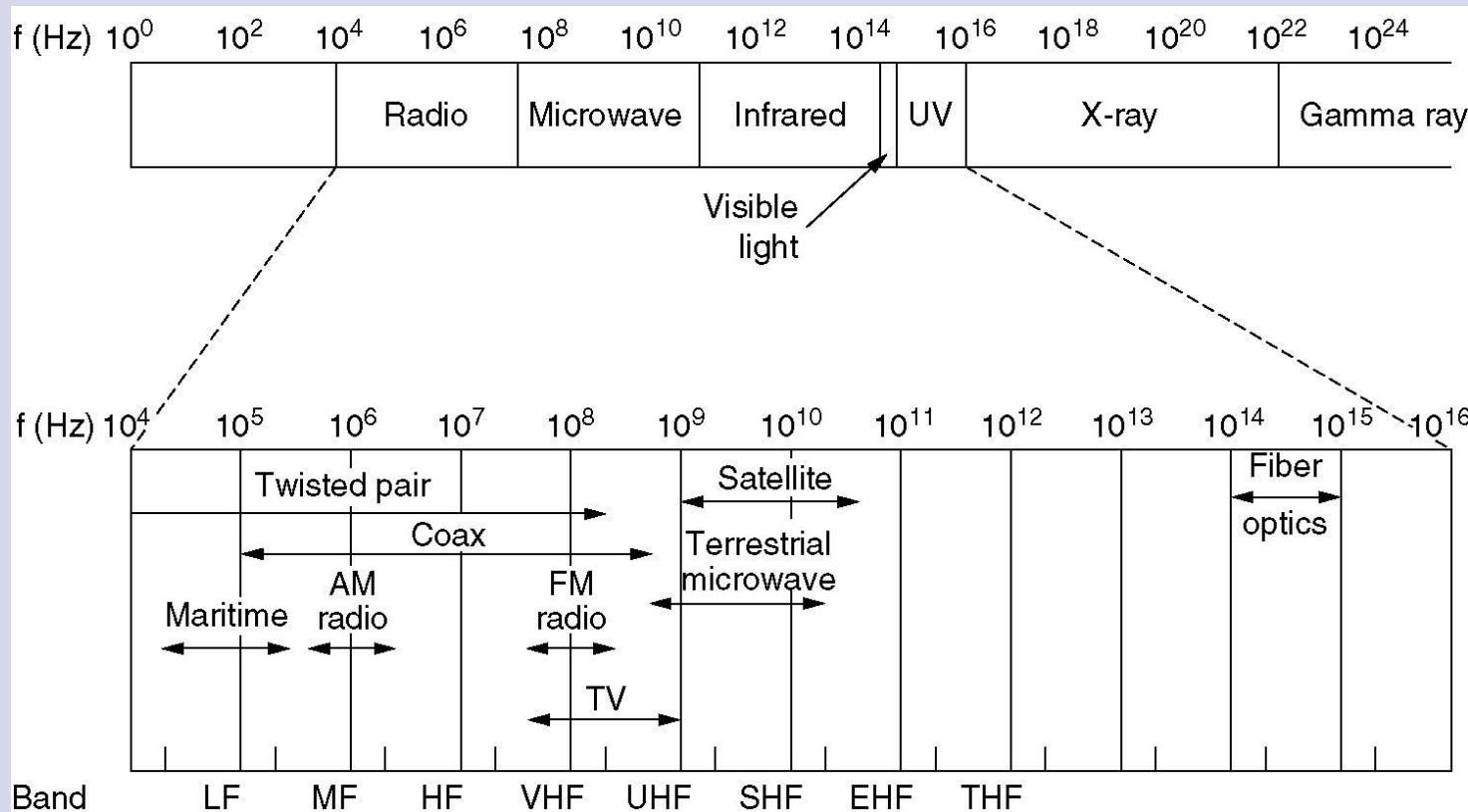


# Bezdrátový přenos

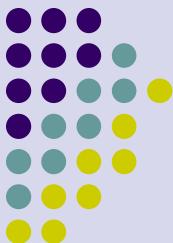
- Elektromagnetické spektrum
- Radiový přenos
- Mikrovlnné přenosy
- Přenos v infračerveném spektru a v mikrovlnném spektru
- Přenos ve viditelném spektru



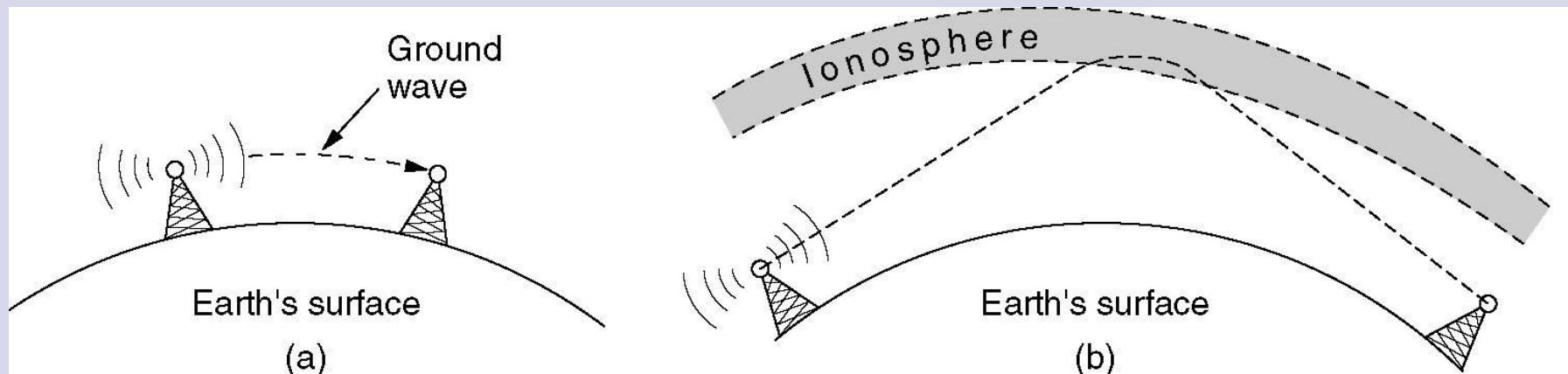
# Elektromagnetické spektrum



Elektromagnetické spektrum a jeho využití pro komunikace.



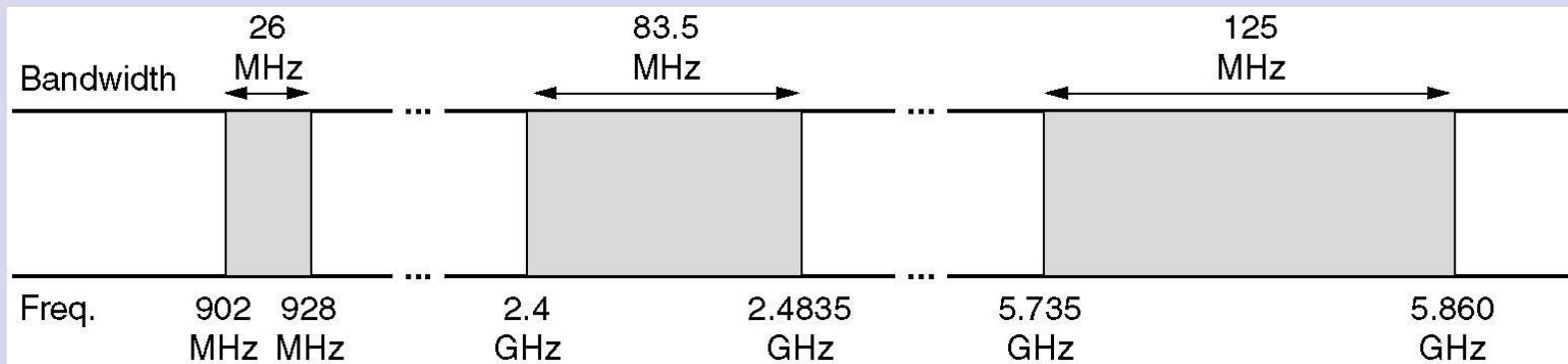
# Radiový přenos



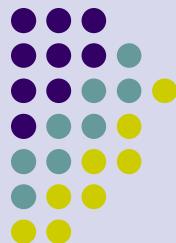
- Na velmi dlouhých, dlouhých a středních vlnách kopírují radiové vlny povrch Země.
- Na krátkých vlnách dochází k odrazům od ionosféry.



# Rozdělení elektromagnetického spektra



Vyšší frekvenční pásma v USA.



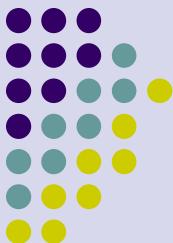
# Radiový bezdrátový přenos dat

- IEEE 802.11      2,4 GHz      2Mb/s
- IEEE 802.11a      5GHz      54Mb/s
- IEEE 802.11b      2,4GHz      11 Mb/s
- IEEE 802.11g      2,4GHz      54Mb/s
- IEEE 802.11n      2,4GHz      až 300 (600Mb/s)
- IEEE 802.15.1      2,4GHz      1Mb/s      Bluetooth
- IEEE 802.15.3      2,4GHz      11 až 55Mb/s      HR-WPAN
- IEEE 802.15.4      2,4GHz      250kb/s      LR-WPAN
- IEEE 802.15.6      2,4GHz      250kb/s      BAN

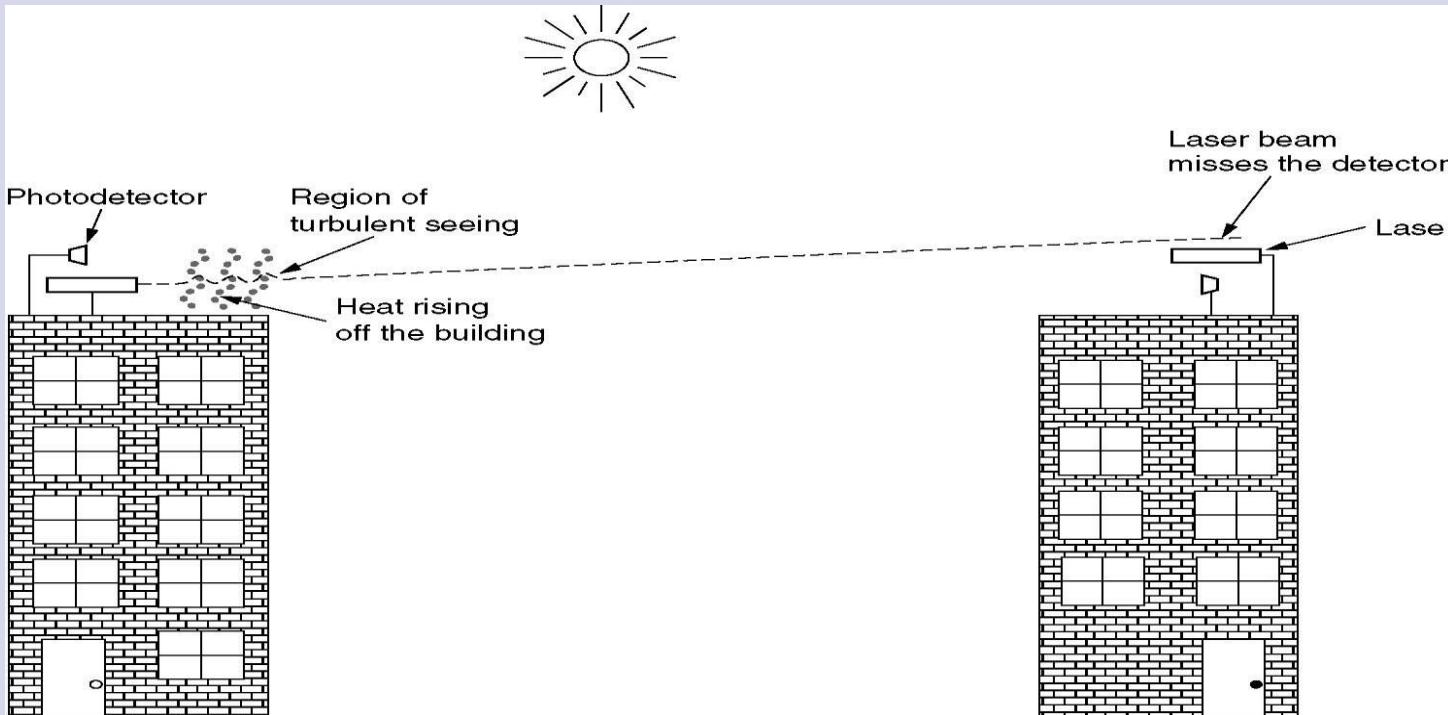


# Radiový bezdrátový přenos dat

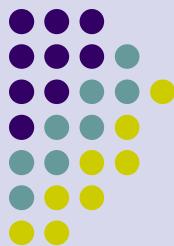
- IEEE 802.16      10 - 66GHz    40Mb/s      WiMAX
  - Worldwide Interoperability for Microwave Access
  - Bezdrátové metropolitní sítě
  - 802.16e-2005 Mobile WiMAX, Mobile Broadband Wireless Access System
  - 802.16m Advanced Air Interface with data rates of 100 Mbit/s mobile & 1 Gbit/s fixed
- IEEE 802.20      do 3,5GHz                  až 80Mb/s
  - Obdoba 802.16
  - Mobile Broadband Wireless Access (MBWA)
- IEEE 802.22      tel. Spektrum    19 Mb/s      WRAN
  - Využití „nevyužitých“ televizních kanálů (6MHz), dosah 30km/19Mb/s



# Světelný přenos

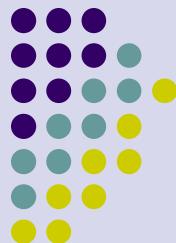


Tepelné proudění vzduchu může ovlivnit laserový komunikační systém.  
Obrázek představuje obousměrný komunikační systém se dvěma lasery.

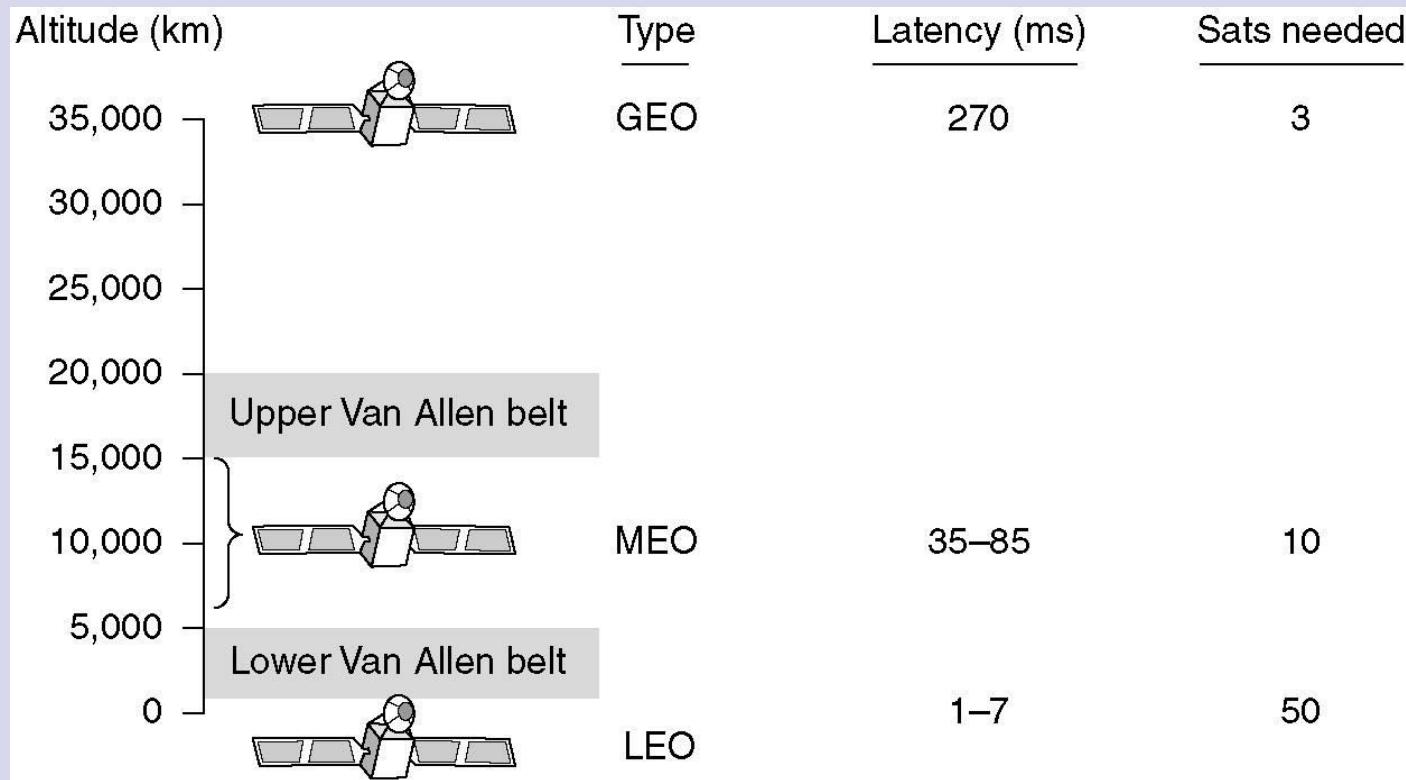


# Komunikační satelity

- Geostacionární satelity
- Satelity na střední oběžné dráze
- Satelity na nízké oběžné dráze
- Porovnání satelitů a optických vláken



# Komunikační satelity



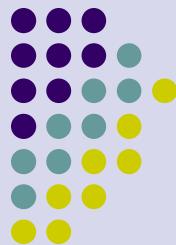
Komunikační satelity a některé jejich vlastnosti, včetně vzdálenosti od Země, doby odezvy a počtu satelitů nutných pro úplné pokrytí.



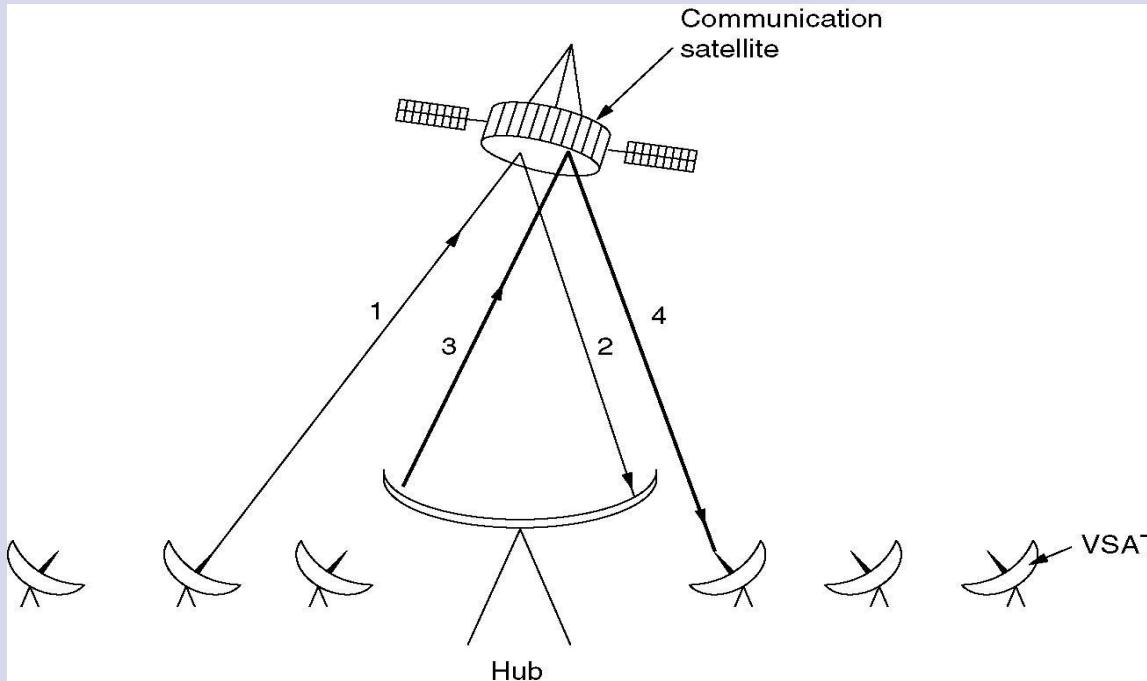
# Komunikační satelity (2)

<b>Band</b>	<b>Downlink</b>	<b>Uplink</b>	<b>Bandwidth</b>	<b>Problems</b>
L	1.5 GHz	1.6 GHz	15 MHz	Low bandwidth; crowded
S	1.9 GHz	2.2 GHz	70 MHz	Low bandwidth; crowded
C	4.0 GHz	6.0 GHz	500 MHz	Terrestrial interference
Ku	11 GHz	14 GHz	500 MHz	Rain
Ka	20 GHz	30 GHz	3500 MHz	Rain, equipment cost

Základní satelitní pásma.



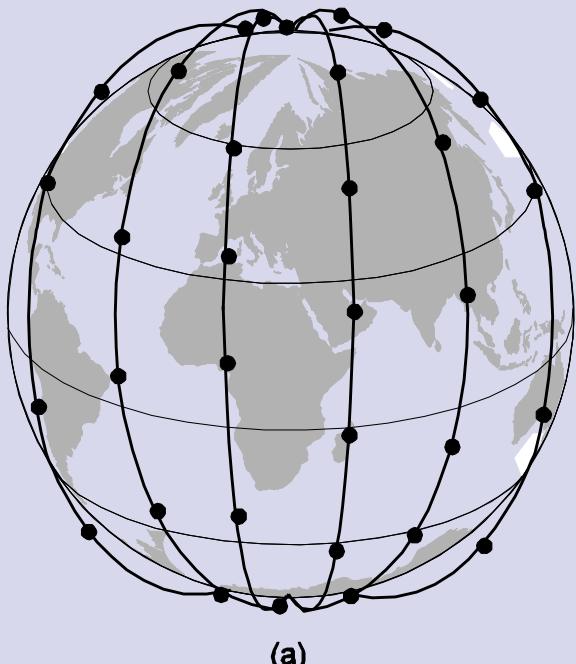
# Komunikační satelity (3)



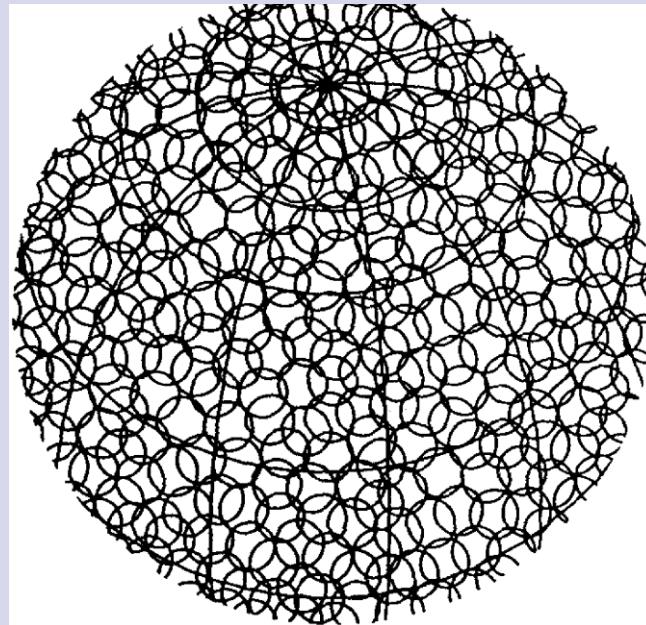
VSATs (Very Small Aperture Terminal) s použitím Hubu.

Velmi malé stanice, běžně menší než 2.4m, používané pro satelitní komunikaci.  
Přenosová rychlosť až 2MB/s oběma směry.

# Satelity na nízké oběžné dráze projekt Iridium

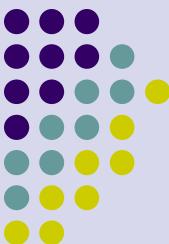


(a)

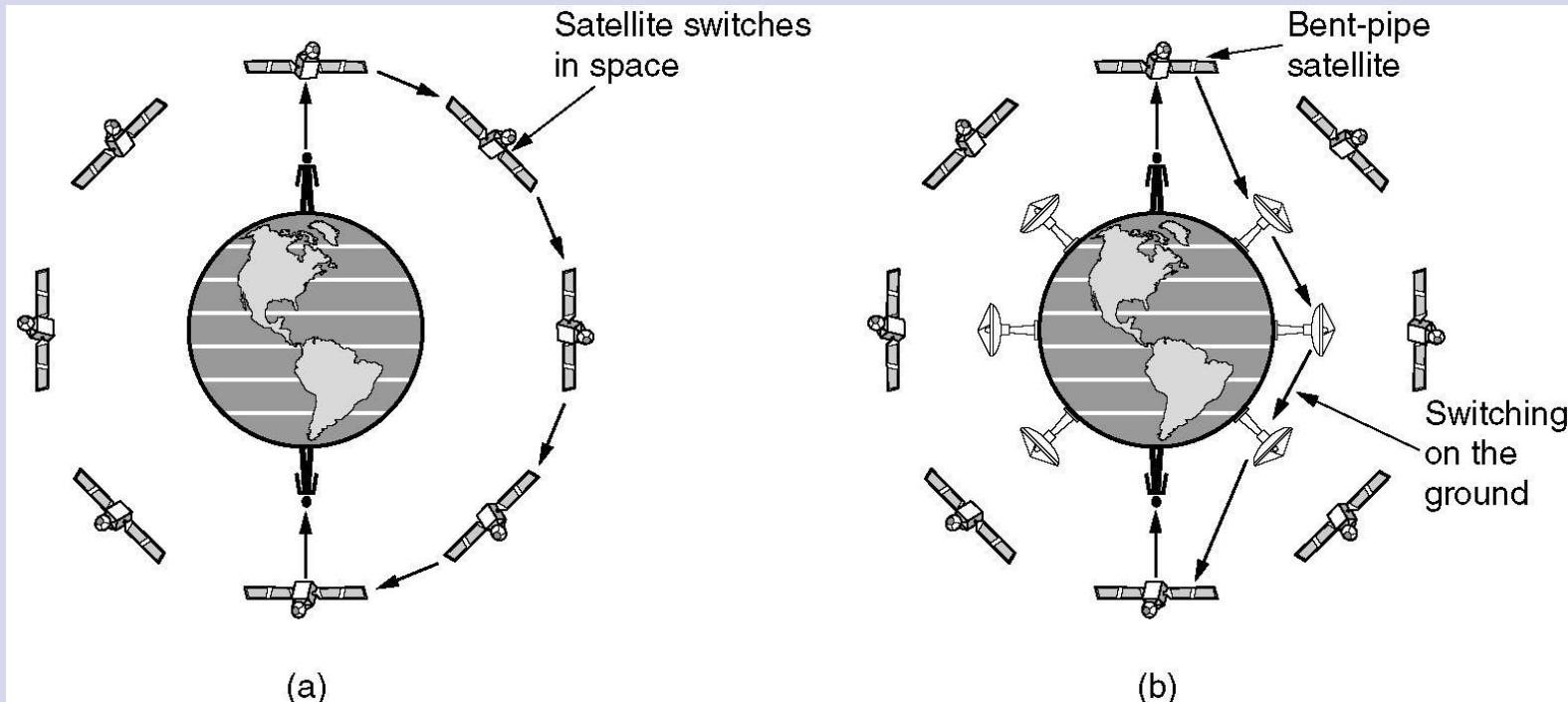


(b)

- Rozmístění satelitů Iridia kolem Země.
- 1628 pohyblivých buněk zahalí celou Zem.



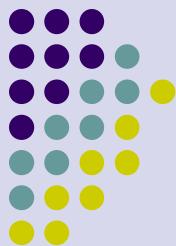
# Globalstar



(a) Přepínání ve vesmíru.

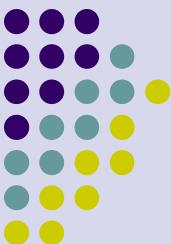
Satelitní telefony, SMS, fax

(b) Přepínání na Zemi

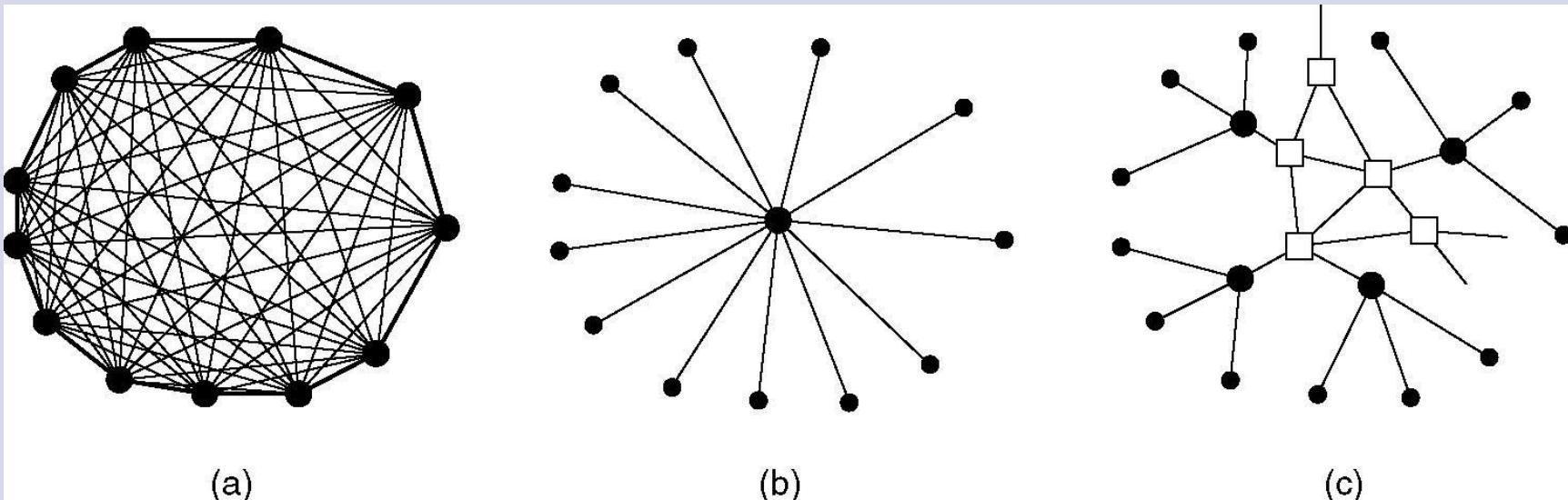


# Veřejné přepínané telefonní systémy

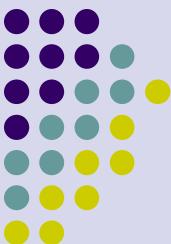
- Struktura telefonního systému
- Rozdělení telefonů
- Lokální smyčka: modemy, ASDL a bezdrátové spoje
- Tranzitní propojení (Trunk) a multiplexování
- Přepínání



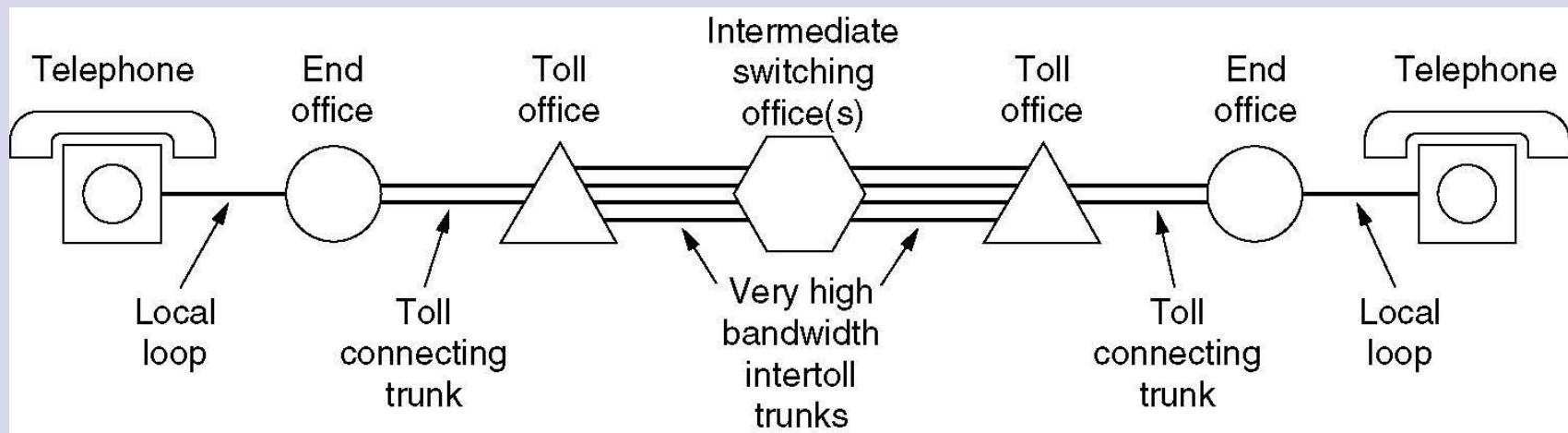
# Struktura telefonního systému



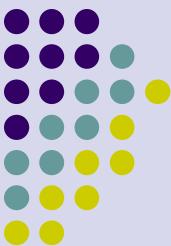
- (a) Úplně propojená síť.
- (b) Centralizovaný přepínač.
- (c) Dvouúrovňová hierarchie.



# Struktura telefonního systému (2)



Typická okruh pro volání na střední vzdálenosti.

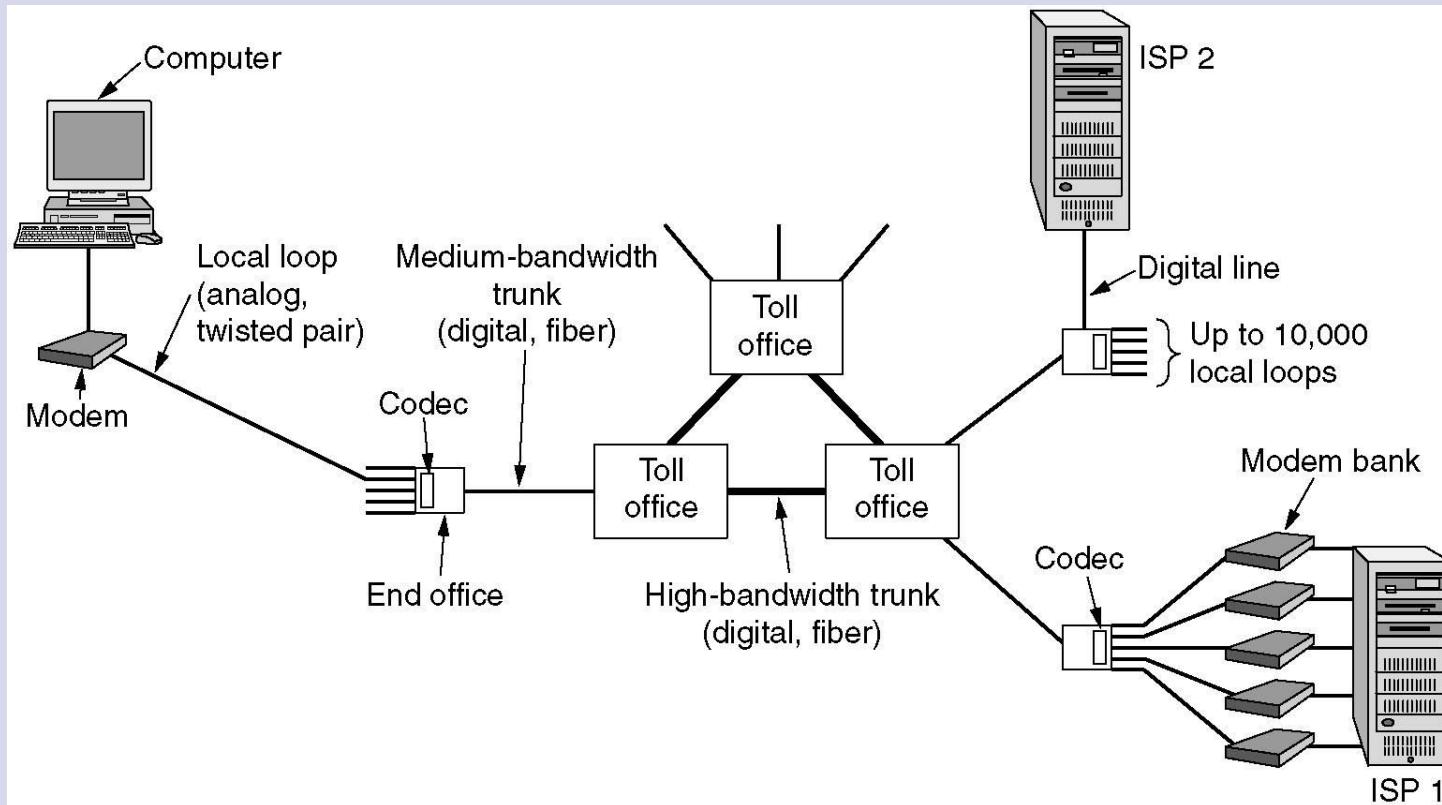


# Hlavní komponenty telefonního systému

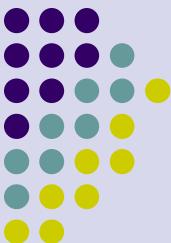
- Lokální smyčky
  - Analogové přenosy kroucenou dvojlinkou
- Dálková vedení (Trunks)
  - Digitální přenosy vláknovou optikou propojující digitální ústředny
- Ústředny
  - Propojení jednotlivých dálkových vedení



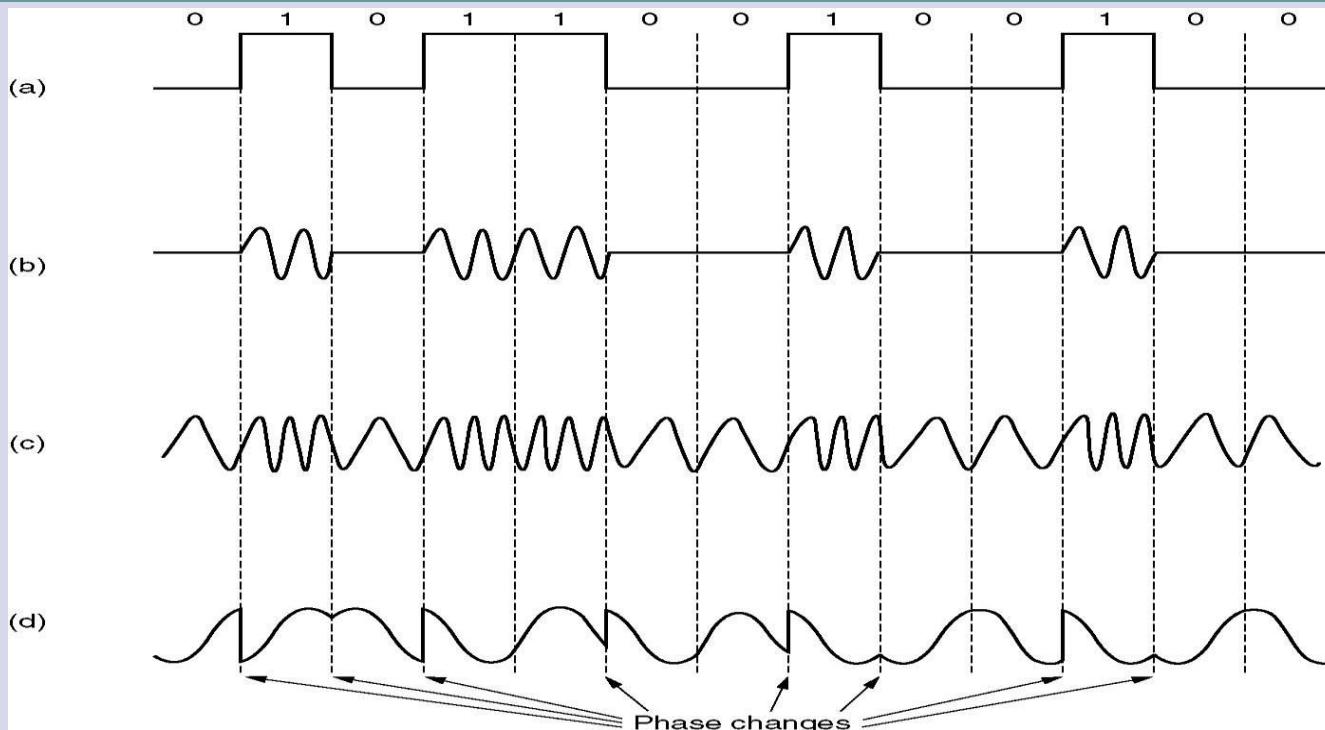
# Lokální smyčky: modemy, ASDL, bezdrátové spoje (wireless)



Použití analogových i digitálních přenosů pro propojení počítačů.  
Převody jsou realizovány modemy a kodeky (codec).



# Modemy



(a) binární signál

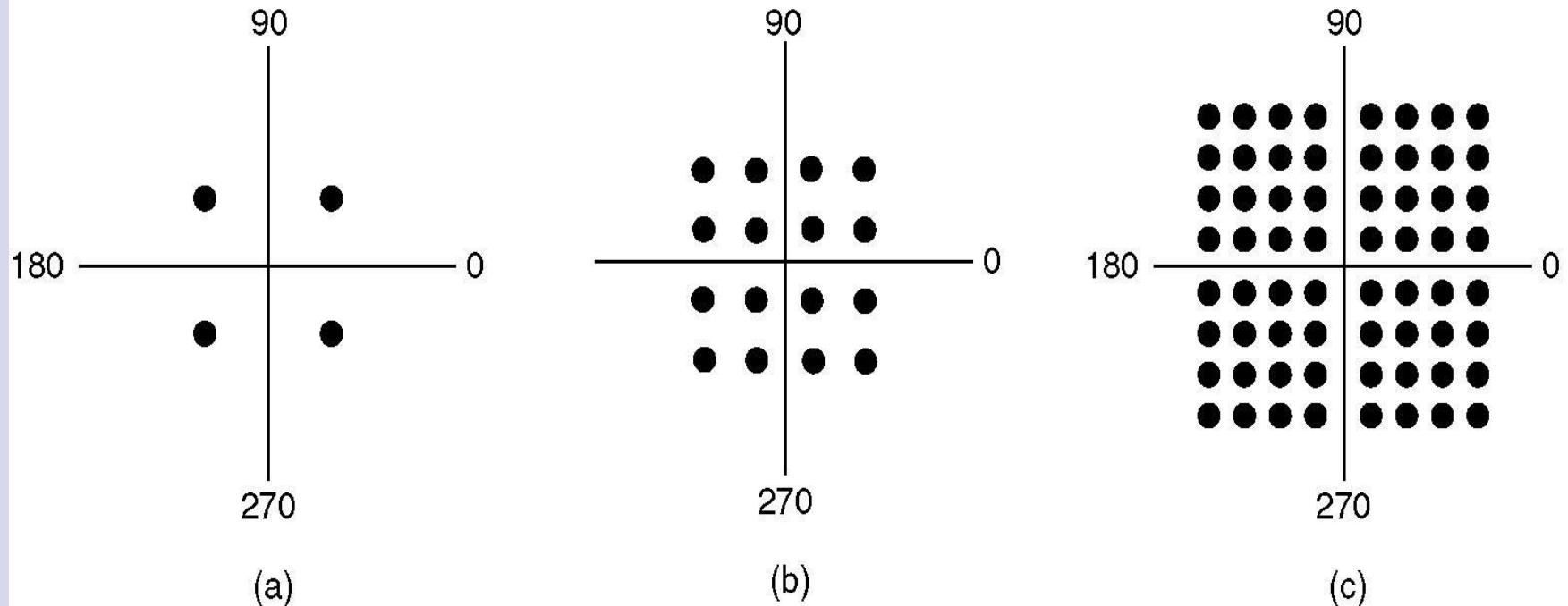
(b) amplitudová modulace

(c) Frekvenční modulace

(d) Fázová modulace

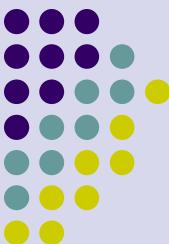


# Modemy (2)

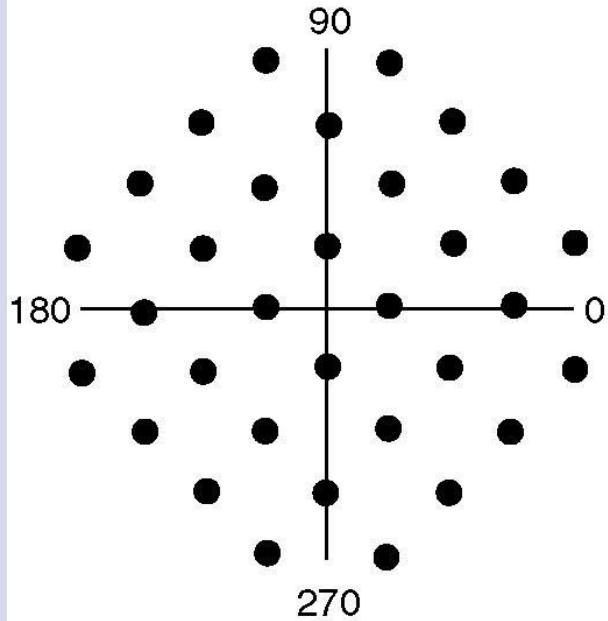


Příklady amplitudo – fázové modulace

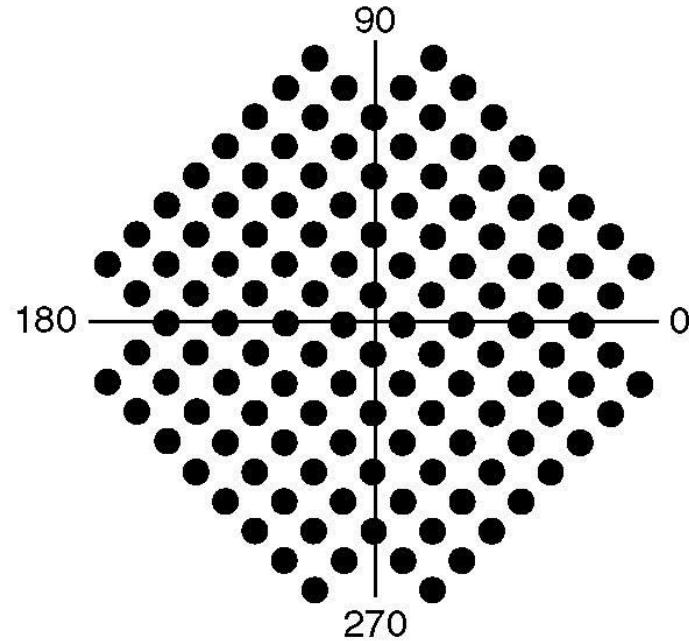
(a) QPSK.    (b) QAM-16.    (c) QAM-64.



# Modemy (3)



(a)



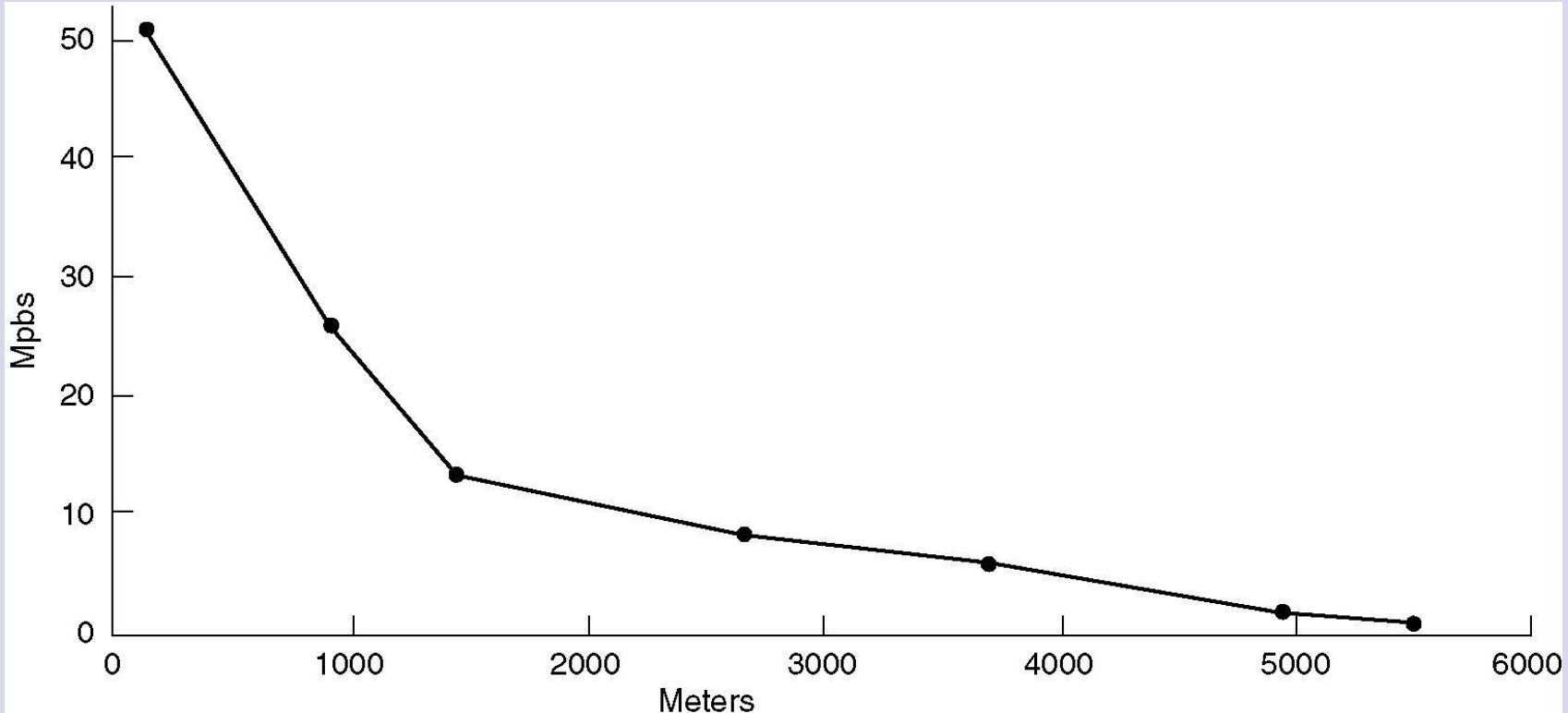
(b)

(a) V.32 pro 9600 b/s.

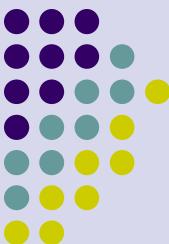
(b) V32 bis pro 14,400 b/s.



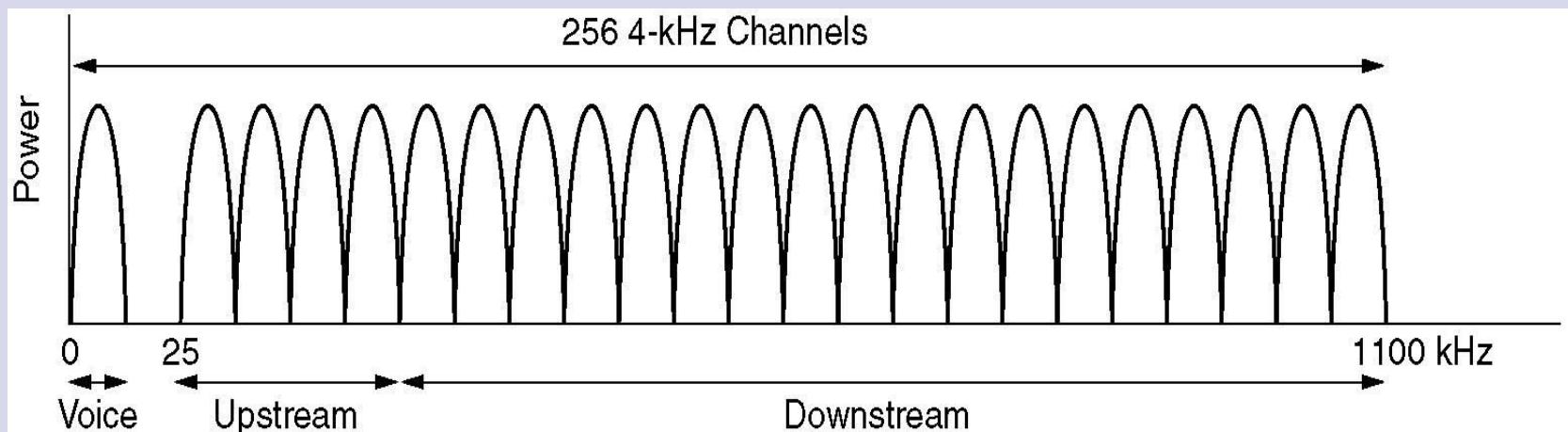
# Digitální účastnické linky (Digital Subscriber Lines - DSL)



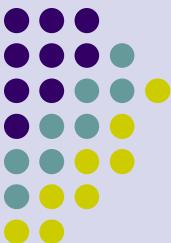
Závislost šířky pásma na vzdálenosti pro přenos DSL kroucenou dvojlinkou (UTP) kategorie 3 (telefonií vedení).



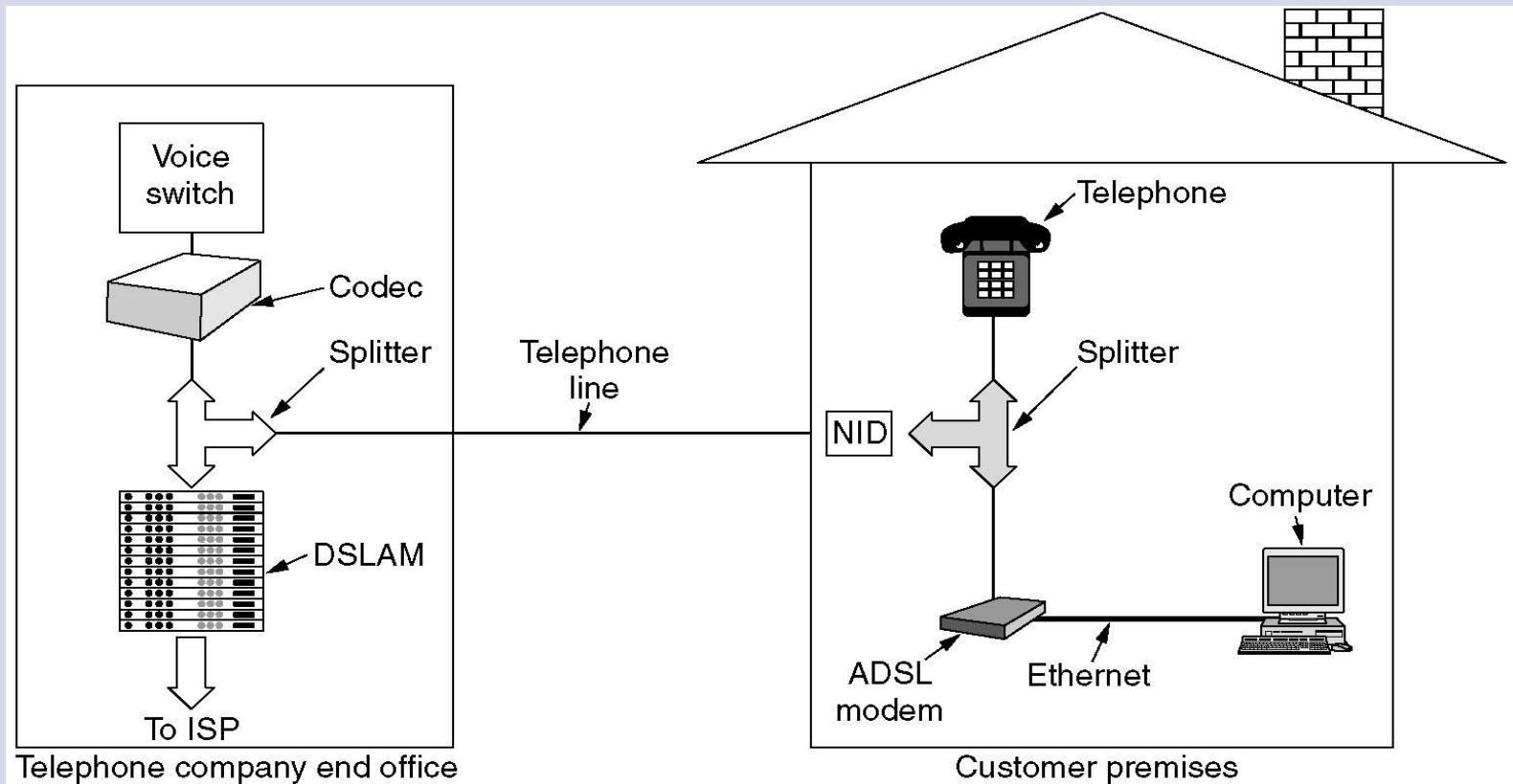
# Digitální účastnické linky (2)



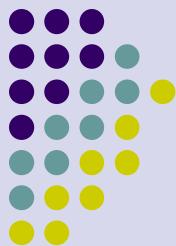
Provoz ADSL s použitím diskrétní víacetónové modulace.



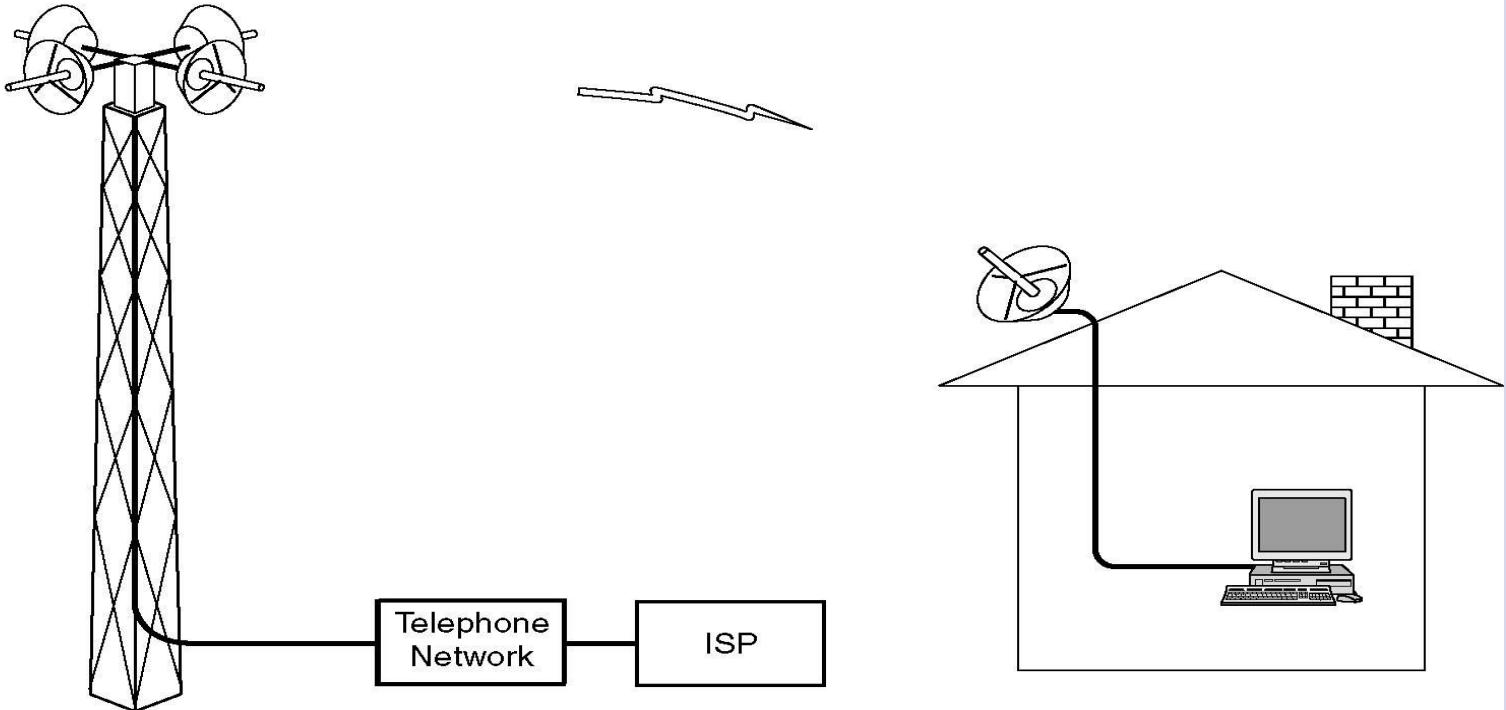
# Digitální účastnické linky (3)



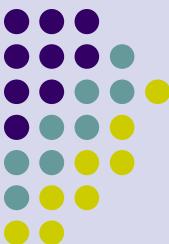
Typická konfigurace ASDL.



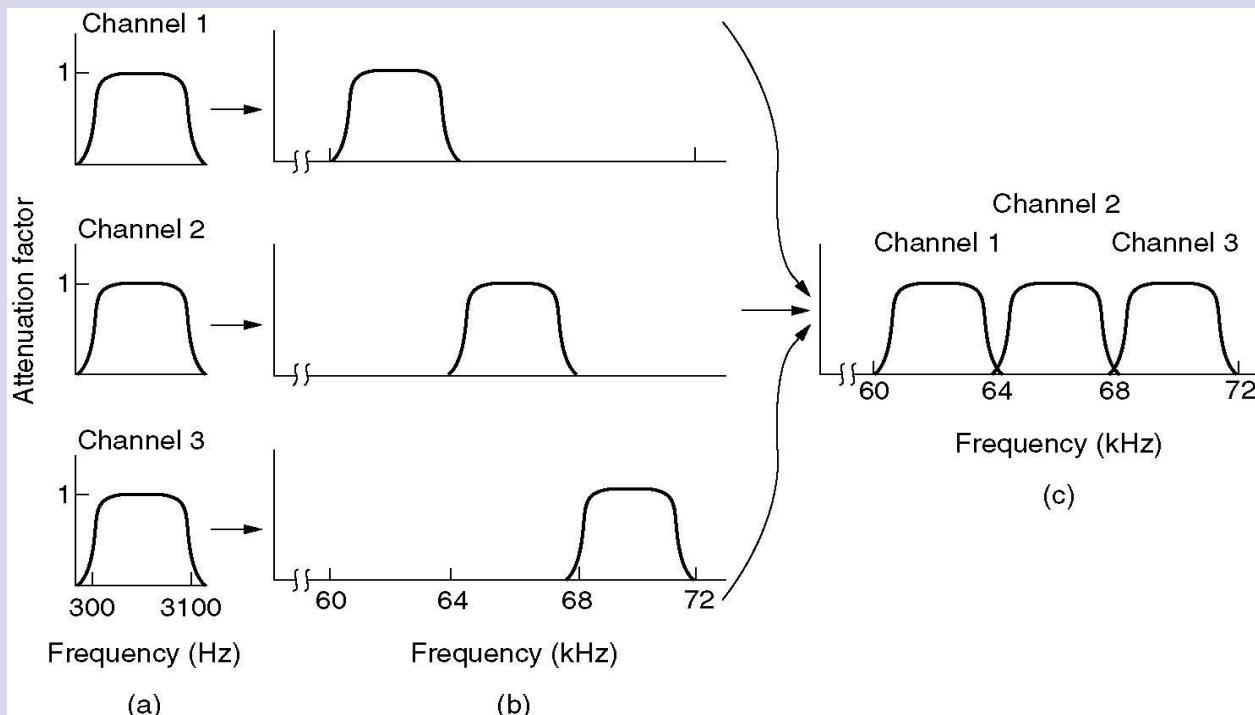
# Bezdrátové lokální smyčky



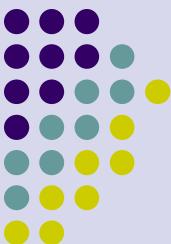
Architektura LMDS (Local Multipoint Distribution Service), 28 & 31 GHz, šířka pásma ve dvou blocích (A a B) 1150MHz (850+150+1150) a 150MHz (75+75).



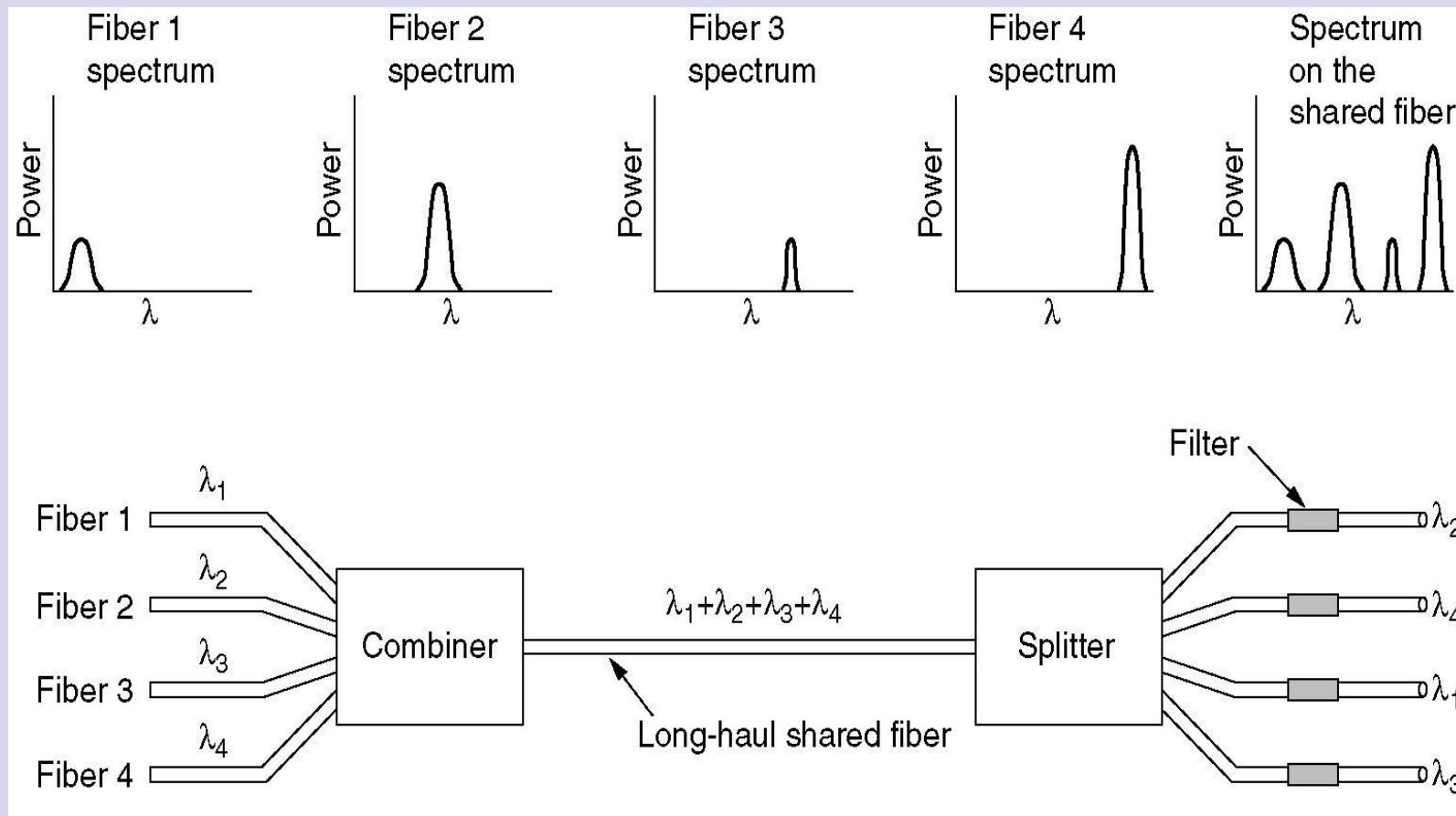
# Frekvenční multiplexování

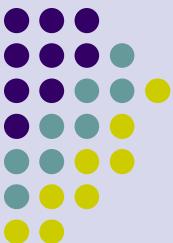


- (a)** Originální pásmo.
- (b)** Posunuté pásmo.
- (c)** Multiplexovaný kanál.

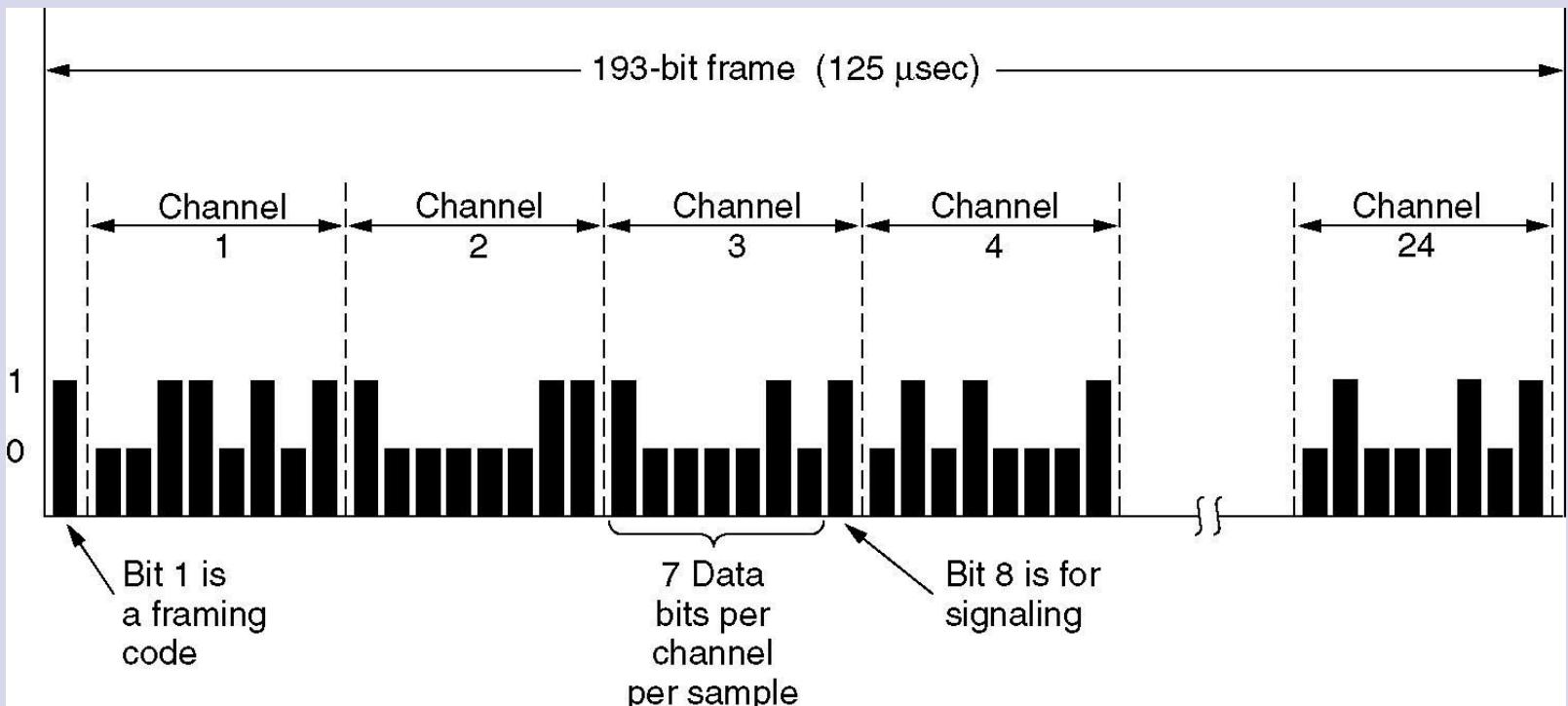


# Multiplexování podle délky vlny (Wavelength Division Multiplexing)

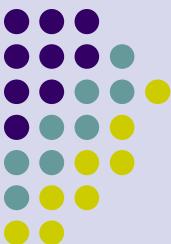




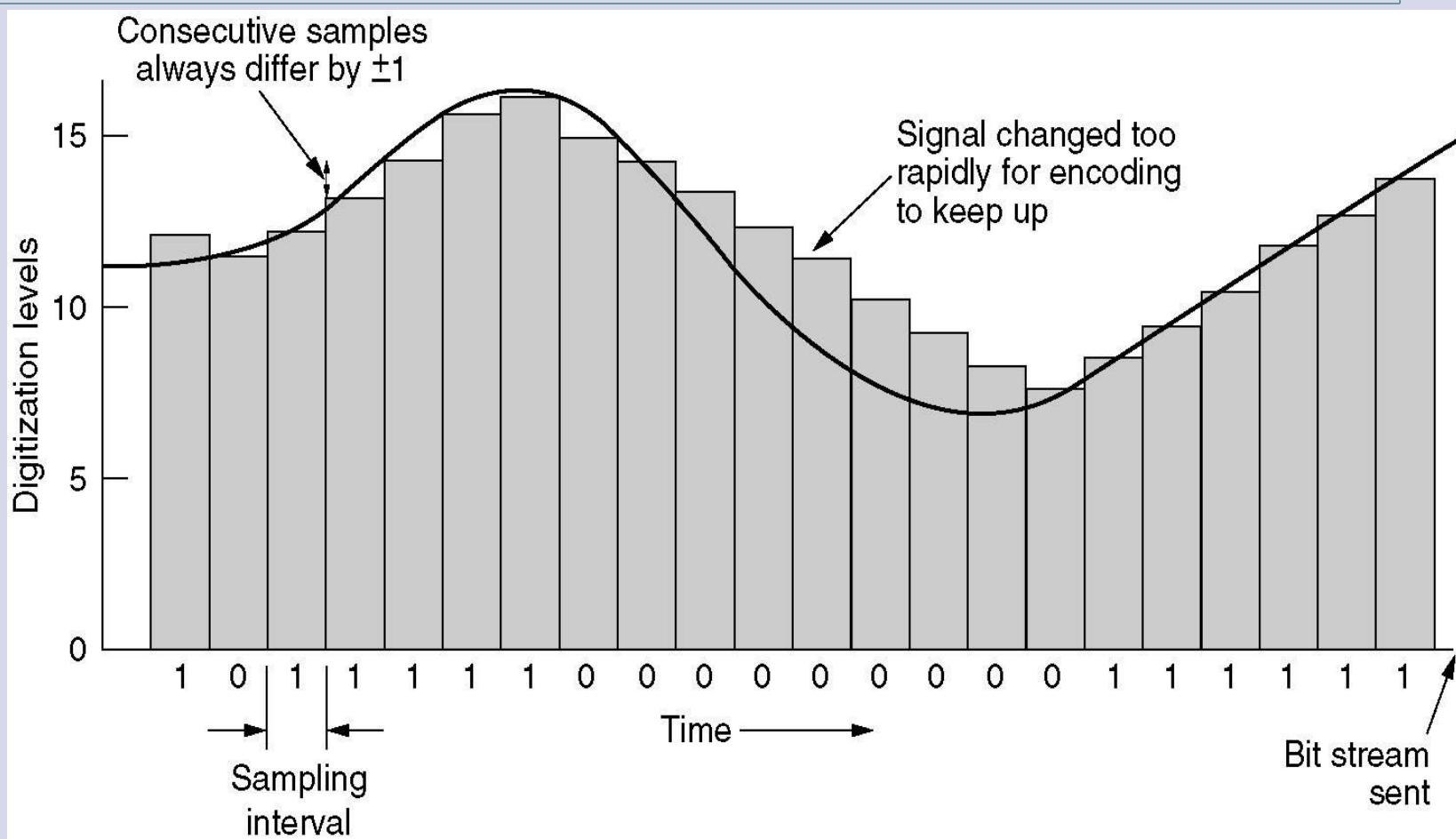
# Časové multiplexování - (Time Division Multiplexing)



Přenosový systém T1 (1.544 Mbps).

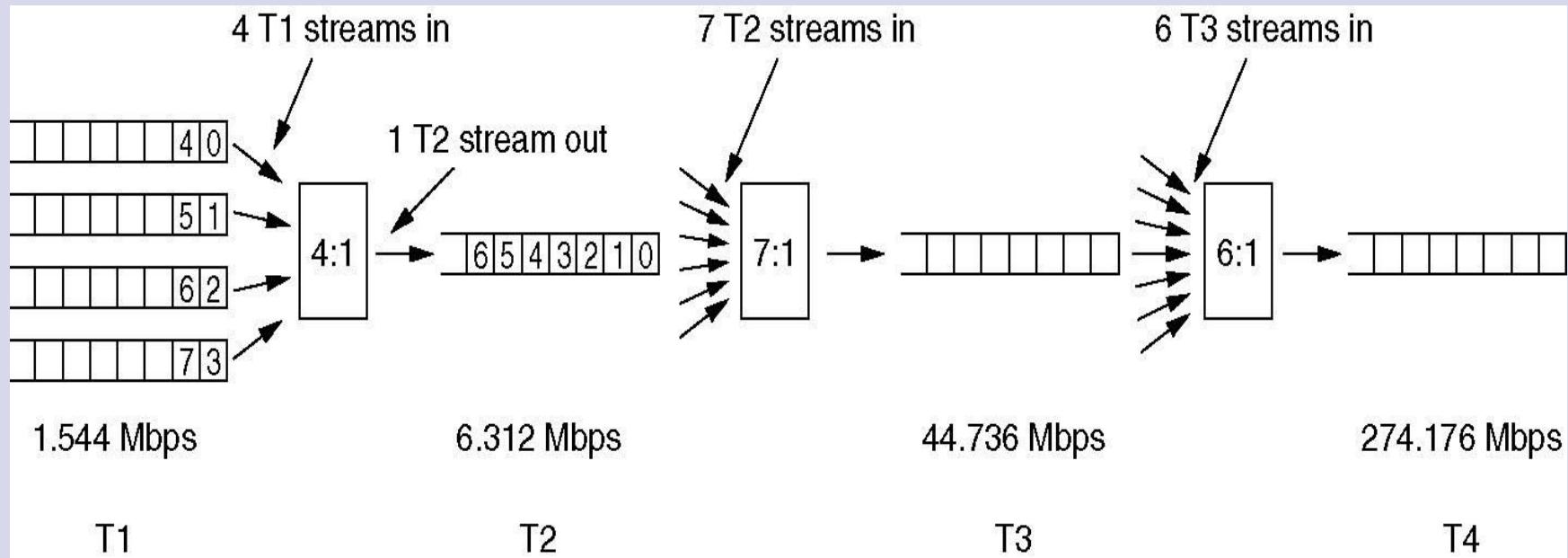


# Časové multiplexování (2)





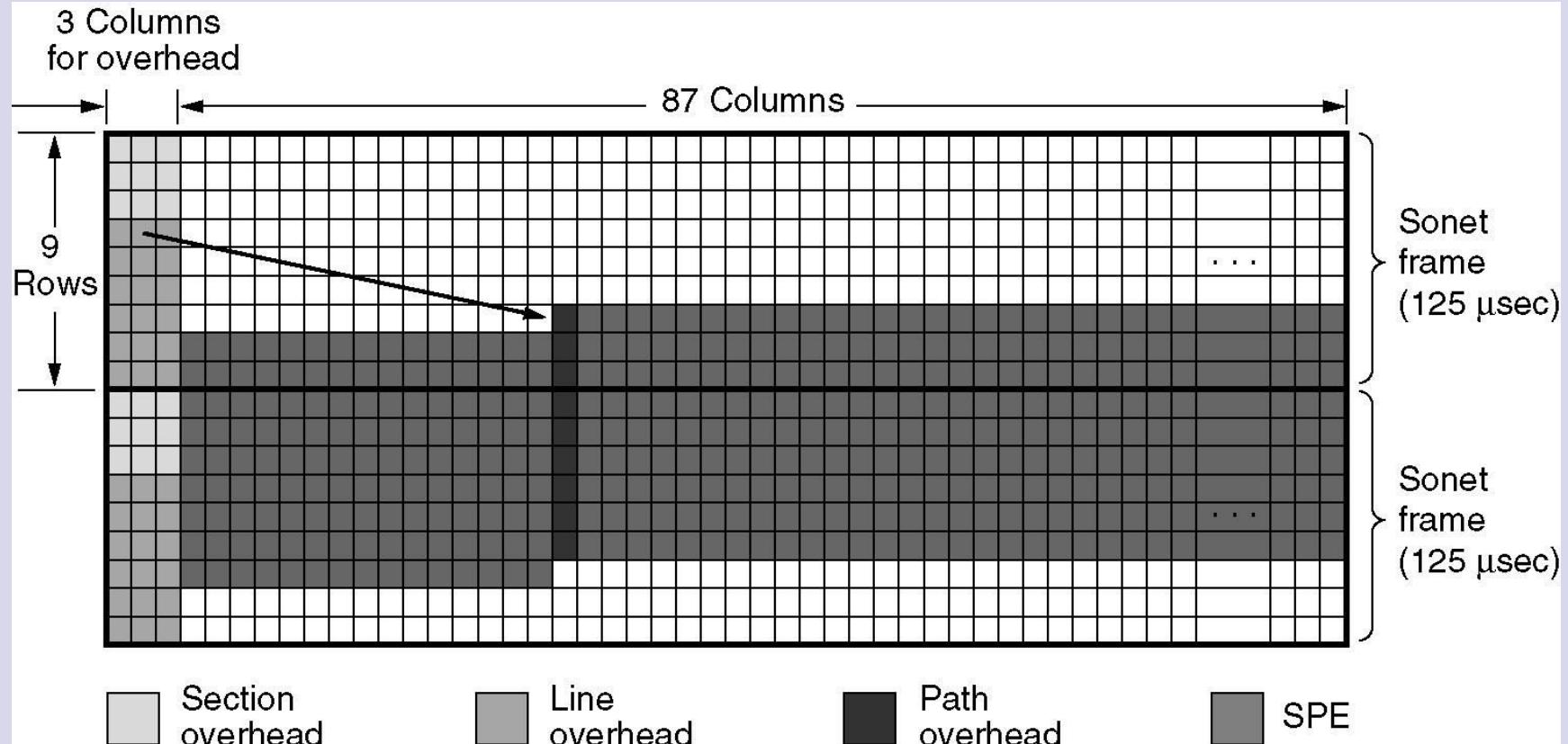
# Časové multiplexování (3)



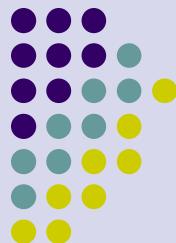
Multiplexování T1 do vyšších přenosových systémů (T2, T3, T4).



# Časové multiplexování (4)



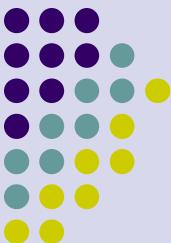
SONET Synchronous Optical NETwork) rámce.



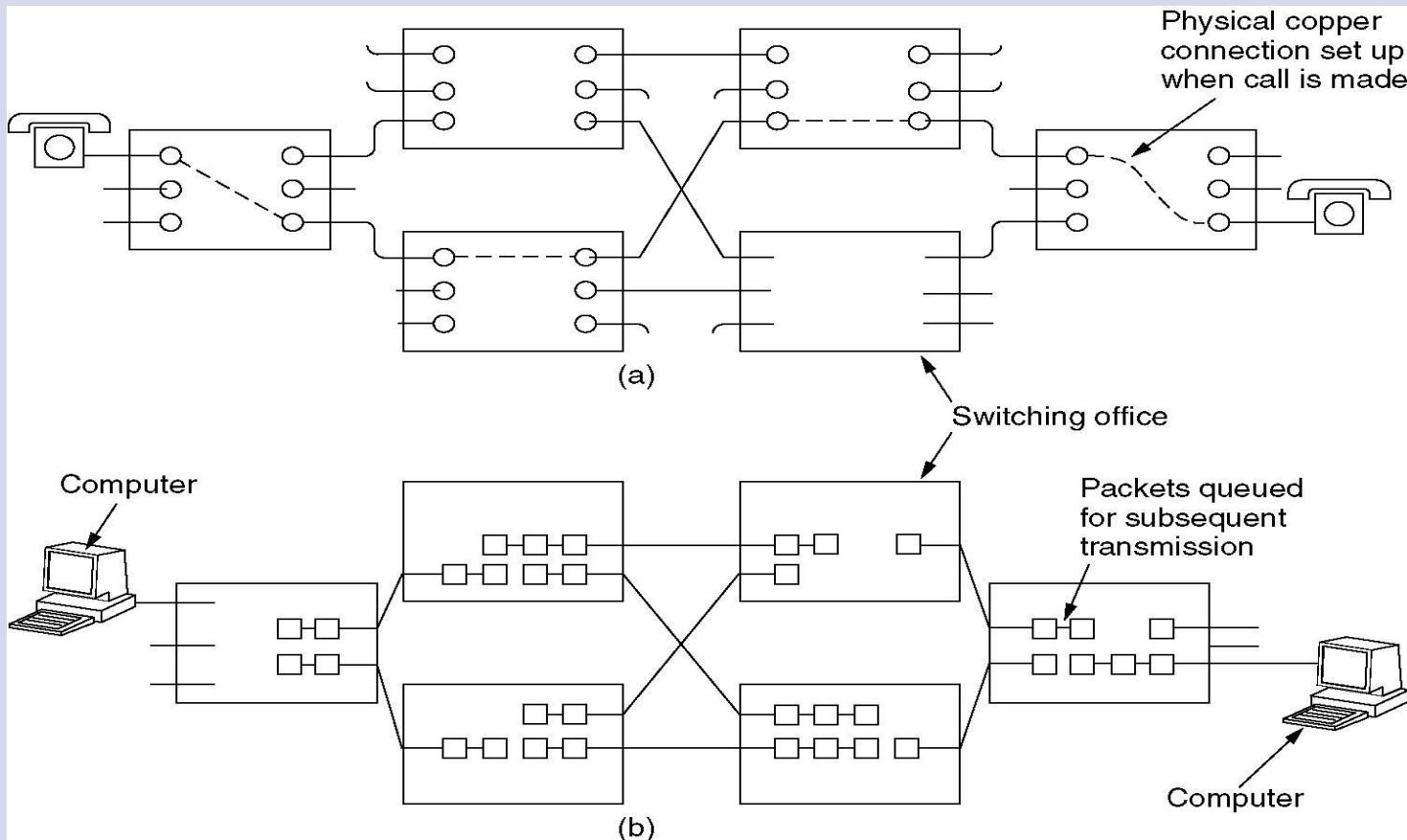
# Časové multiplexování (5)

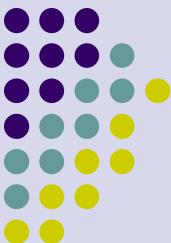
SONET		SDH	Data rate (Mbps)		
Electrical	Optical	Optical	Gross	SPE	User
STS-1	OC-1		51.84	50.112	49.536
STS-3	OC-3	STM-1	155.52	150.336	148.608
STS-9	OC-9	STM-3	466.56	451.008	445.824
STS-12	OC-12	STM-4	622.08	601.344	594.432
STS-18	OC-18	STM-6	933.12	902.016	891.648
STS-24	OC-24	STM-8	1244.16	1202.688	1188.864
STS-36	OC-36	STM-12	1866.24	1804.032	1783.296
STS-48	OC-48	STM-16	2488.32	2405.376	2377.728
STS-192	OC-192	STM-64	9953.28	9621.504	9510.912

Rychlosti multiplexování SONET and SDH (Synchronous Digital Hierarchy).

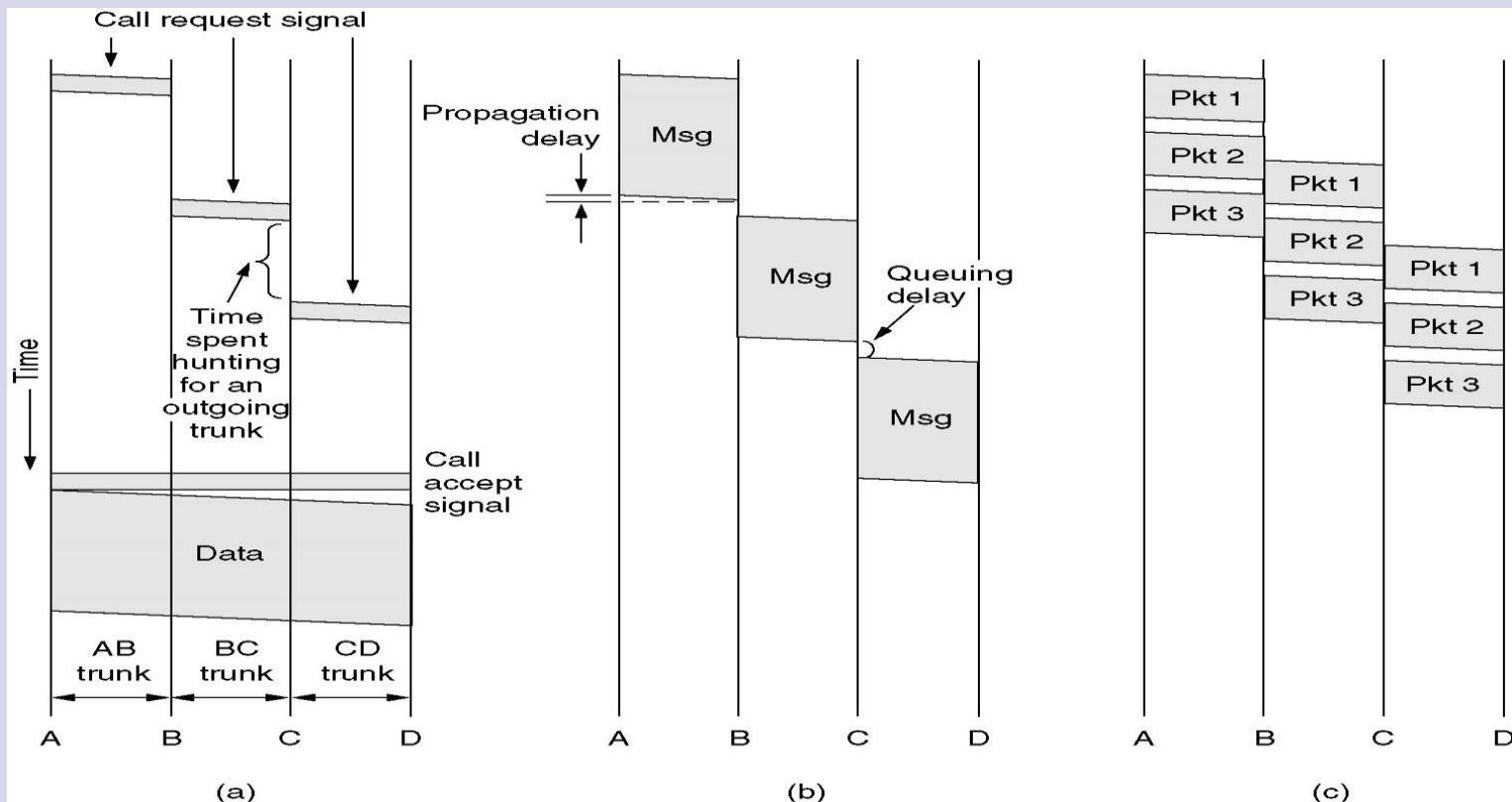


# Přepínání okruhů

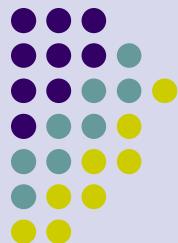




# Přepínání zpráv



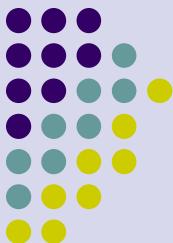
(a) Přepínání okruhů (b) přepínání zpráv (c) přepínání paketů



# Přepínání paketů

Item	Circuit-switched	Packet-switched
Call setup	Required	Not needed
Dedicated physical path	Yes	No
Each packet follows the same route	Yes	No
Packets arrive in order	Yes	No
Is a switch crash fatal	Yes	No
Bandwidth available	Fixed	Dynamic
When can congestion occur	At setup time	On every packet
Potentially wasted bandwidth	Yes	No
Store-and-forward transmission	No	Yes
Transparency	Yes	No
Charging	Per minute	Per packet

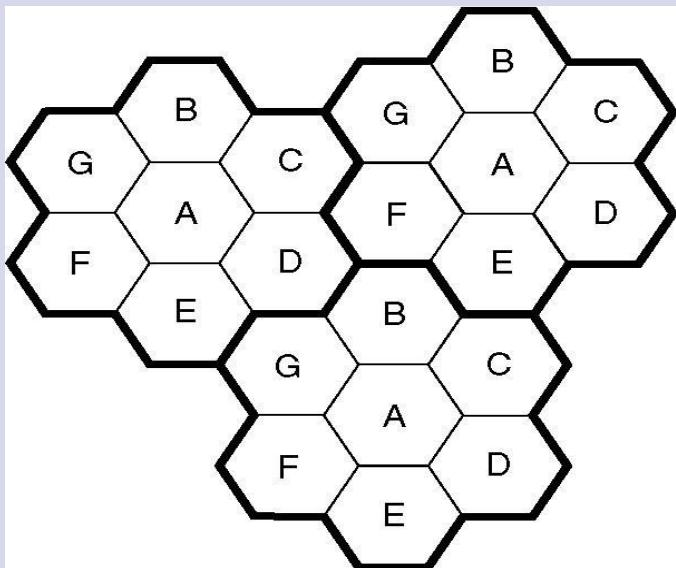
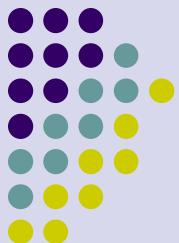
Porovnání sítí s přepínáním paketů a přepínáním okruhů.



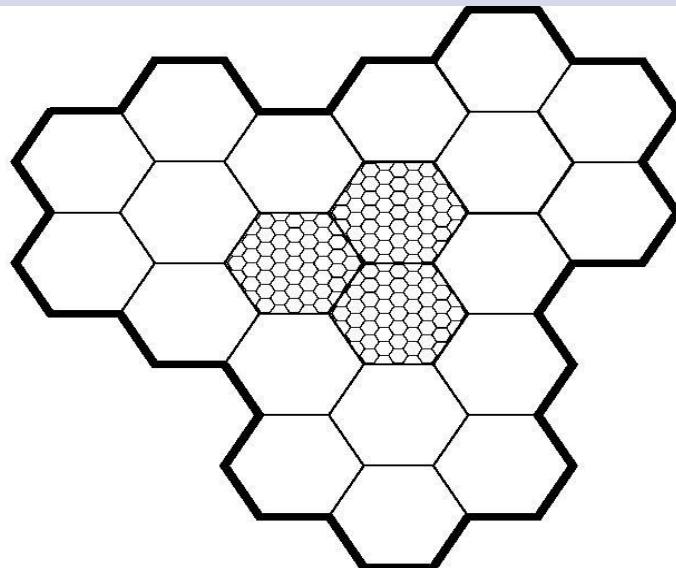
# Mobilní telefonní systém

- První generace mobilních telefonů:  
analogové přenosy hlasu
- Druhá generace mobilních telefonů:  
digitální přenosy hlasu
- Třetí generace mobilních telefonů:  
digitální přenosy hlasu i dat

# Zdokonalený mobilní telefonní systém

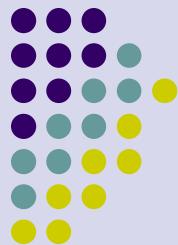


(a)



(b)

- (a) V sousedních buňkách se nemohou použít stejné frekvence.
- (b) Použití menších buňek dovoluje zvýšit počet uživatelů.



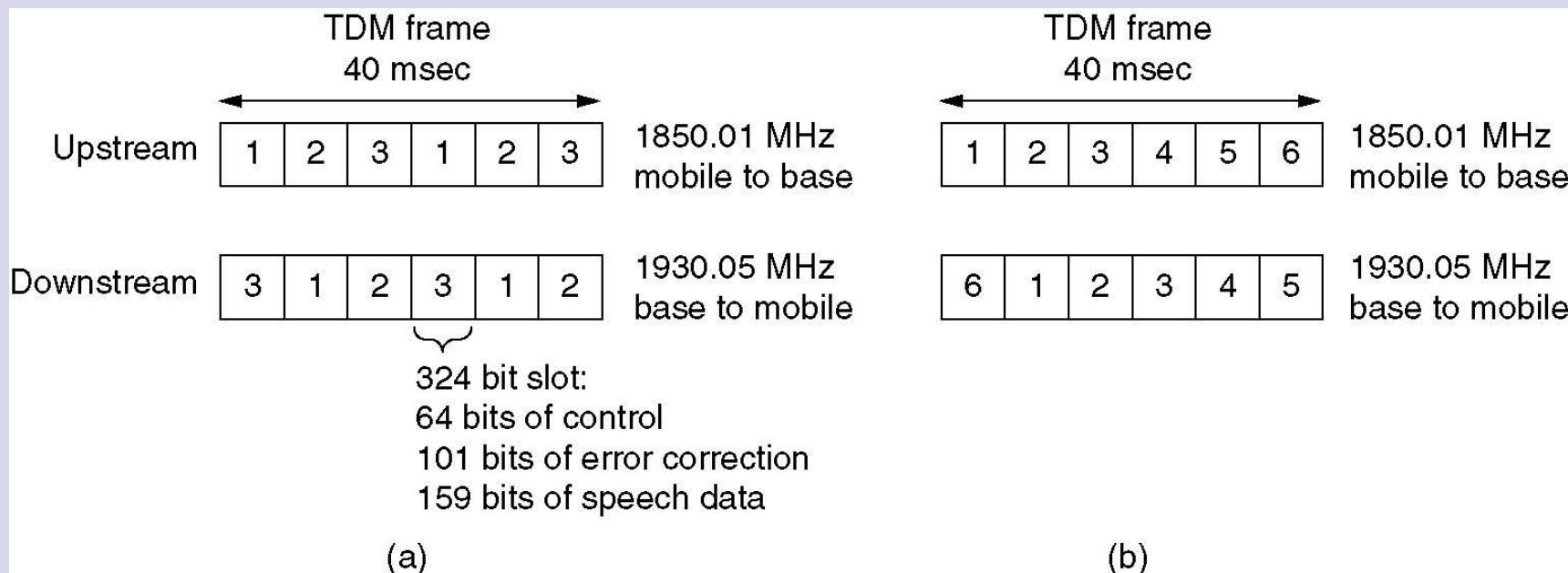
# Kategorie kanálů

832 kanálů rozděleno do 4 kategorií:

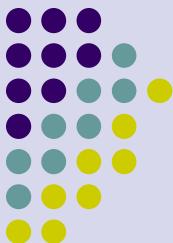
- Řízení (základna do mobilu) pro řízení systému
- Paging (základna do mobilu) upozornění uživatelů na volání
- Přístup (obousměrný) pro vytváření spojení a přidělení kanálu
- Data (obousměrný) pro hlas, fax a data

# D-AMPS (Digital Advanced Mobile Phone System)

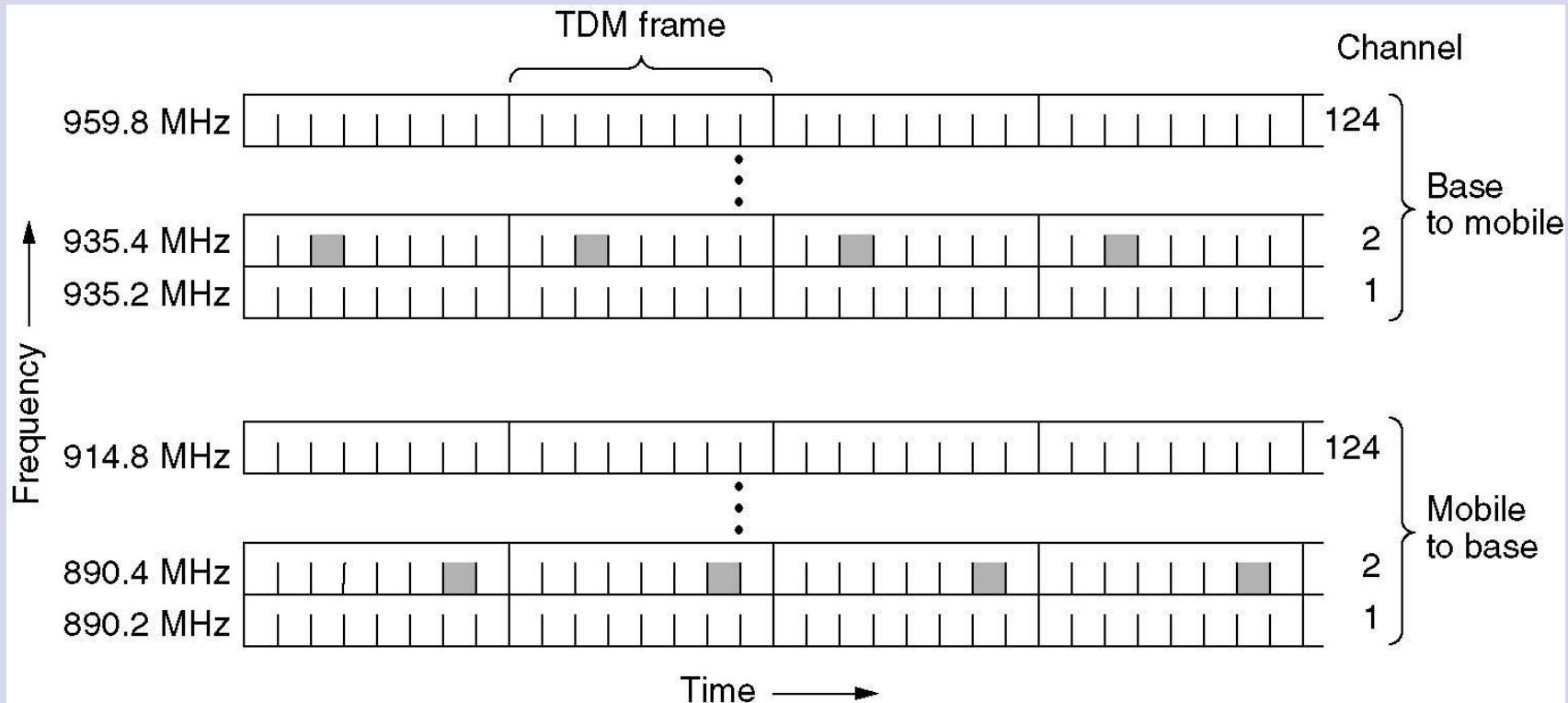
## Zdokonalený systém mobilních telefonů



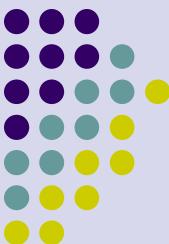
- (a) D-AMPS kanál se třemi uživateli.
- (b) D-AMPS kanál se šesti uživateli.



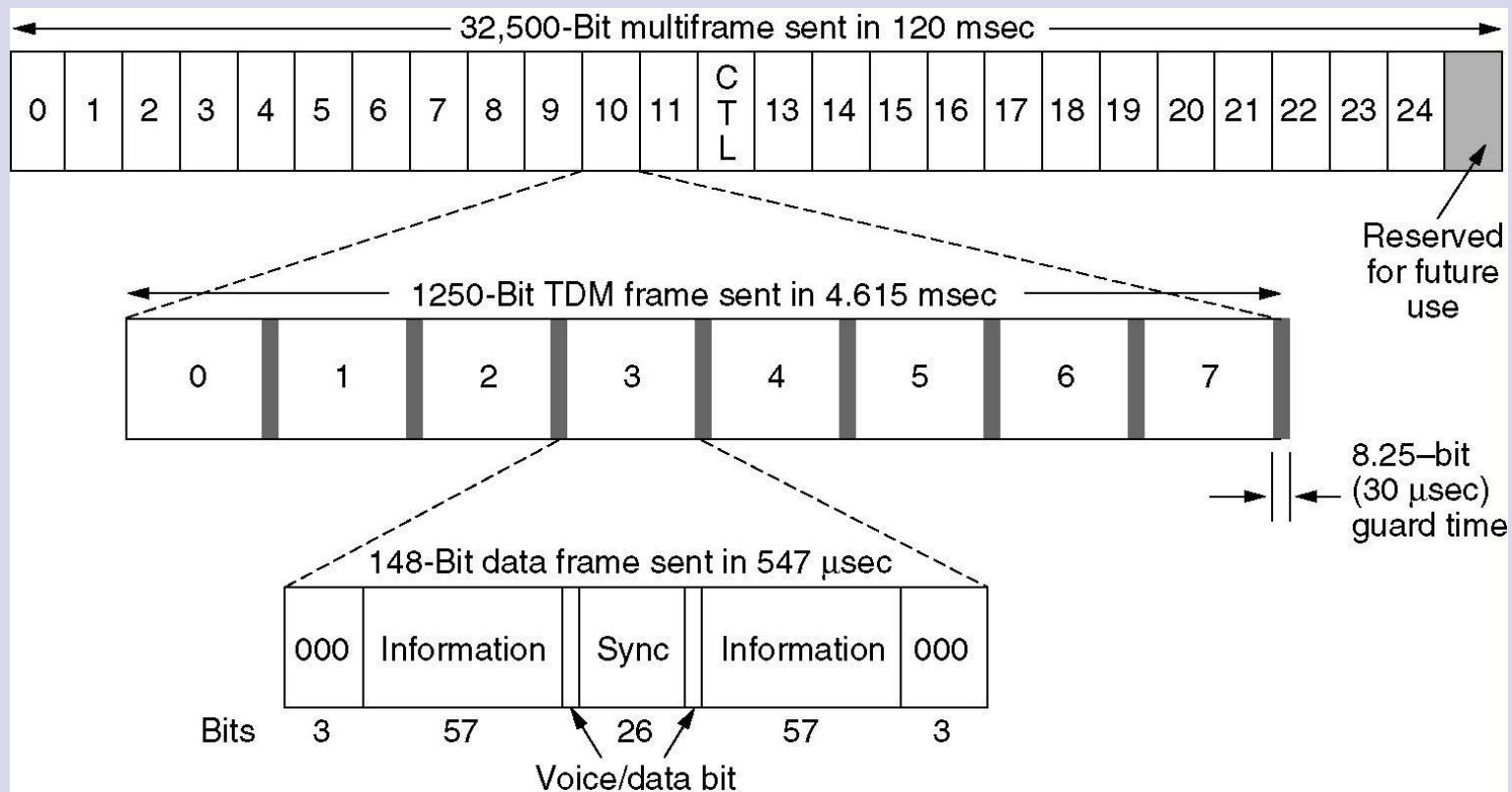
# Globální systém pro mobilní komunikace

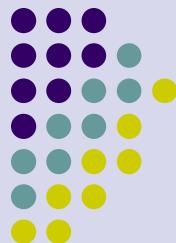


GSM používá 124 frekvenčních kanálů, každý z nich používá 8 časových slotů systému časového multiplexu (TDM)



# GSM (2)

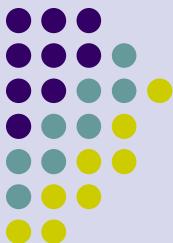




# Třetí generace mobilních telefonů: digitální zvuk a data

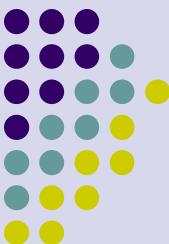
Základní služby sítě International Mobile Communications - 2000 (IMT-2000) zahrnují

- Přenos zvuku s velmi vysokou kvalitou
- Posílání zpráv (náhrada e-mail, fax, SMS, chat, atd.)
- Multimédia (hudba, video, film, TV, atd.)
- Přístup k Internetu (surfování, multimédia)

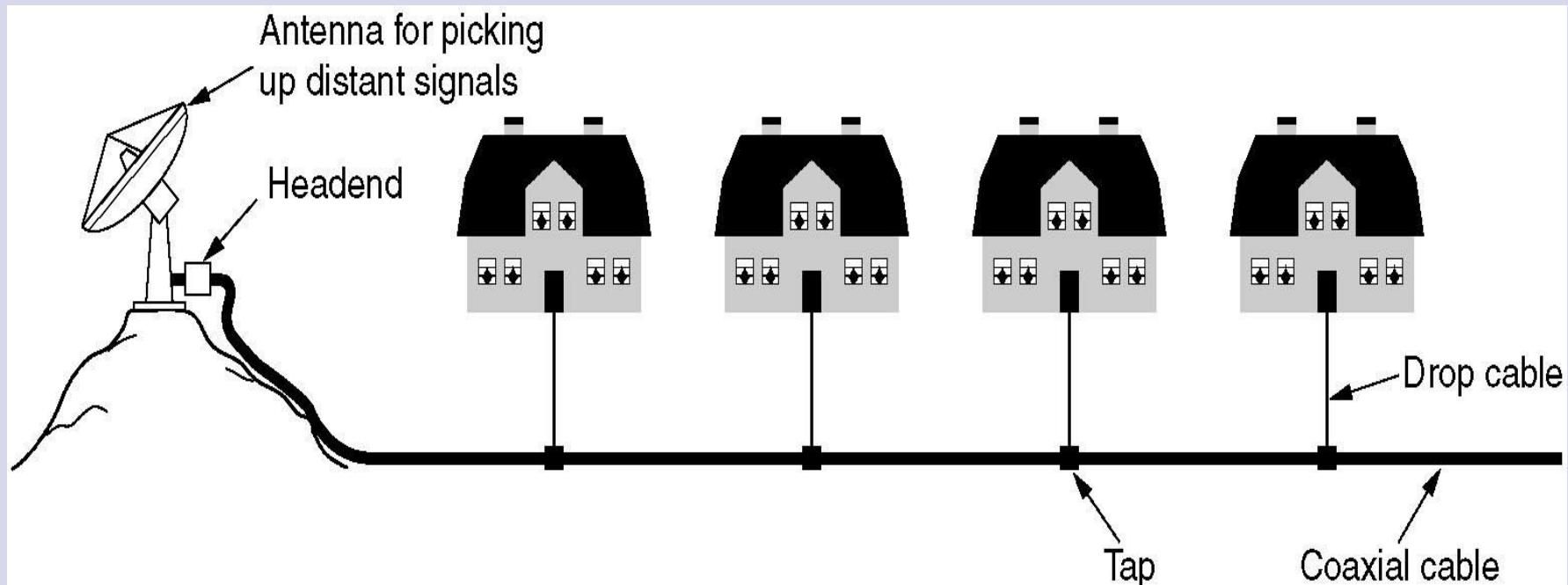


# Kabelová televize

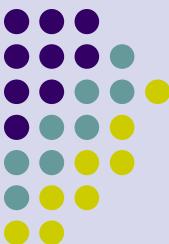
- Společná televizní anténa
- Přístup k Internetu prostřednictvím účastnického kabelu
- Rozdělení přenosového spektra
- Kabelové modemy
- ADSL kontra kabelové přenosy



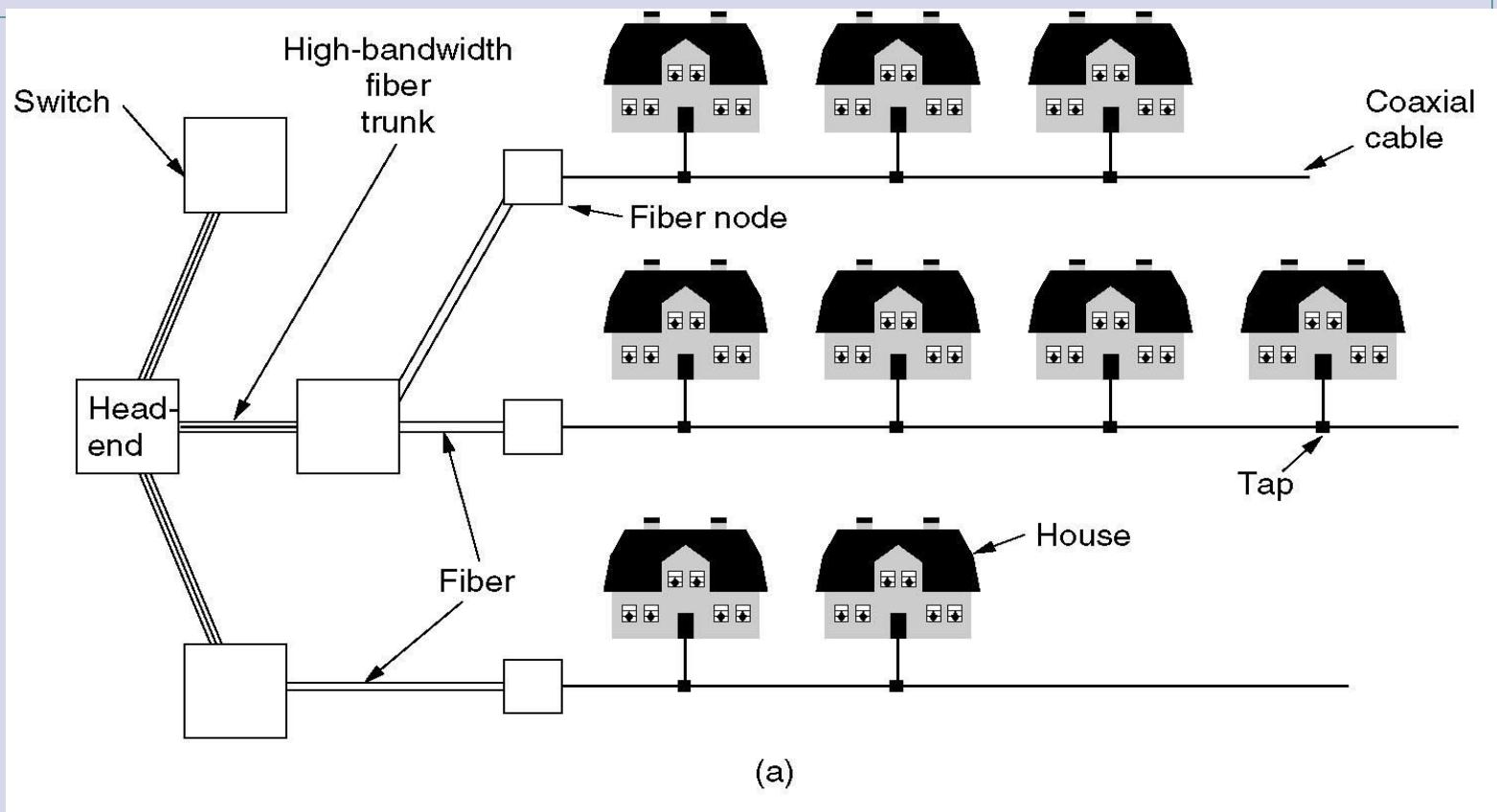
# Skupinová televizní anténa



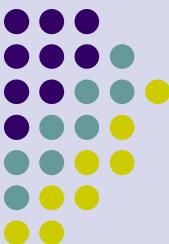
Původní systémy kabelové televize.



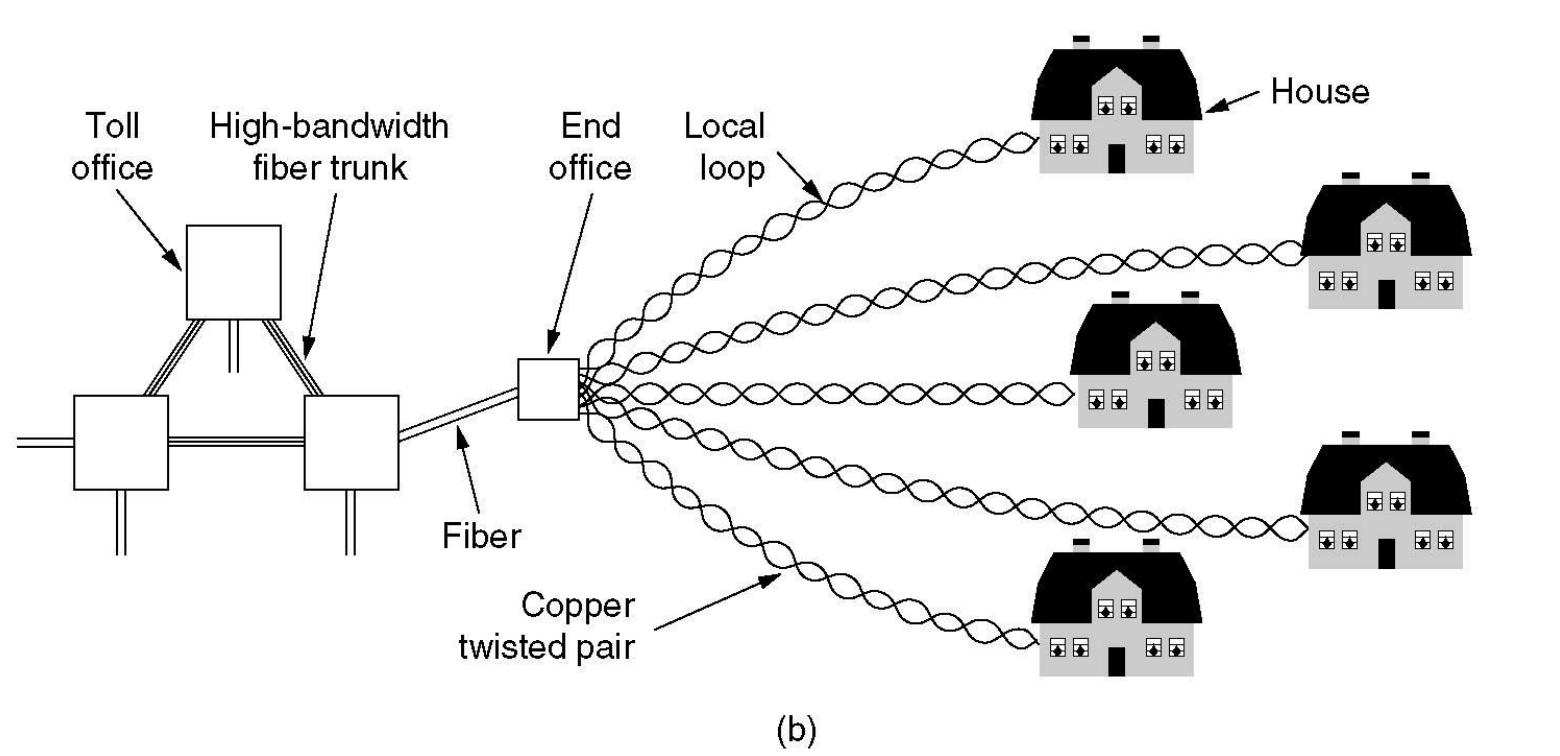
# Kabelový Internet



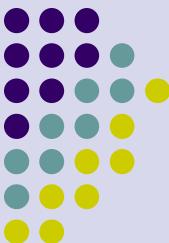
## Kabelová televize



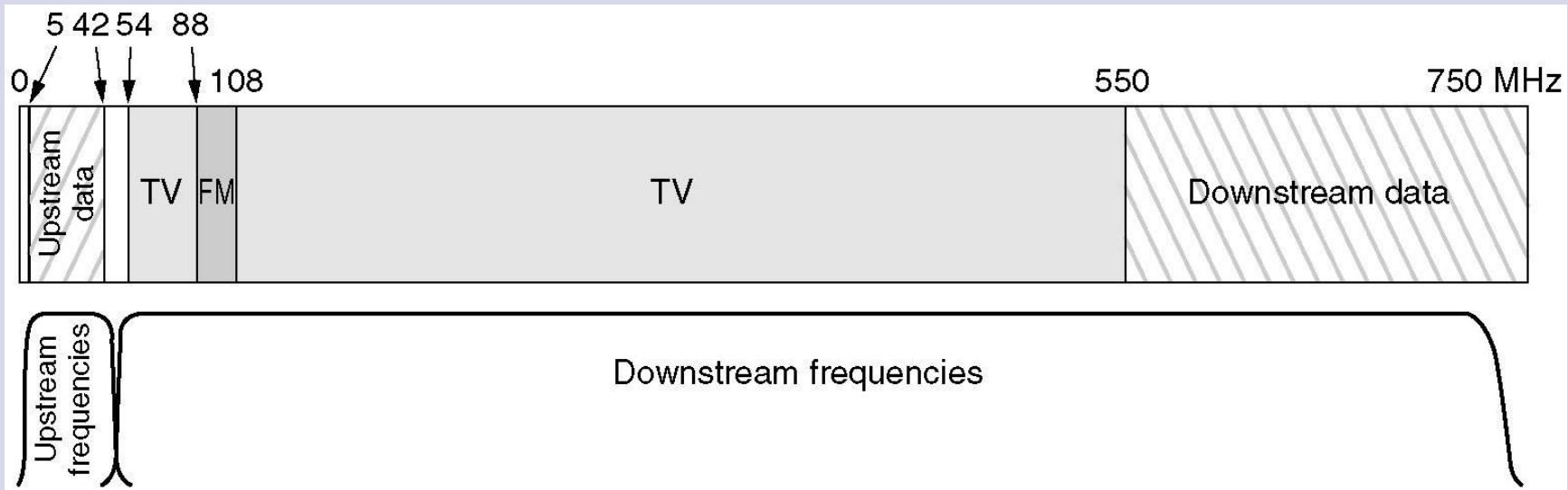
# Kabelový Internet (2)



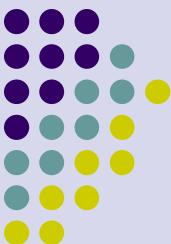
Fixní telefonní systém.



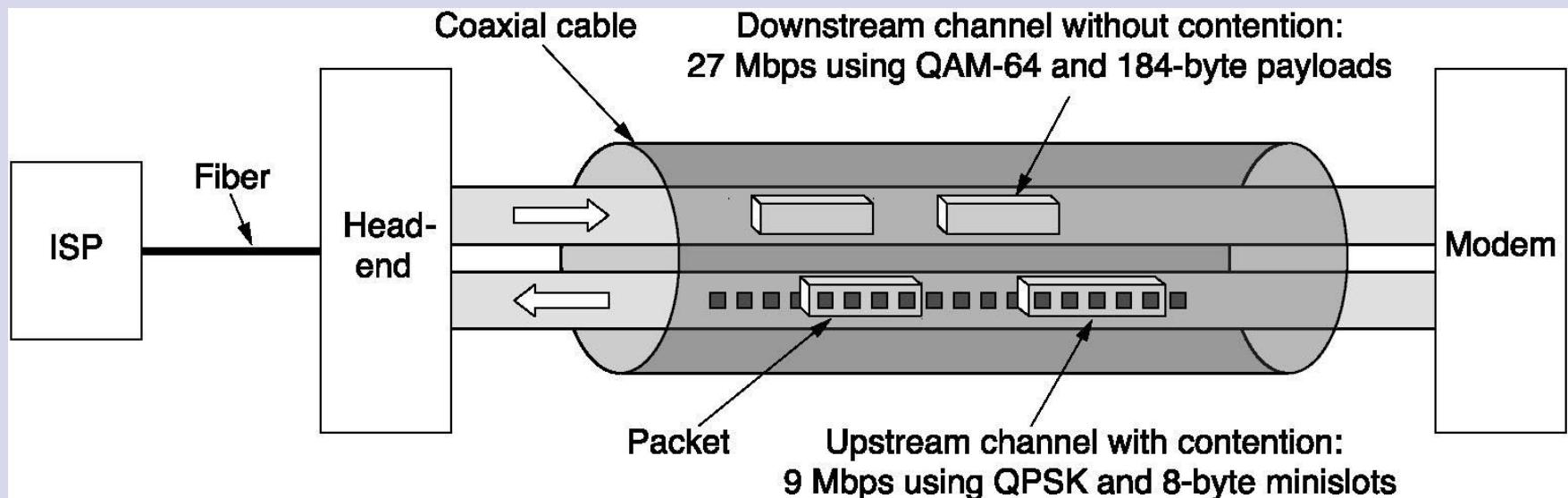
# Rozdělení spektra



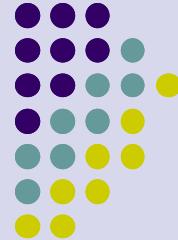
Rozdělení spektra v typickém TV kabelovém systému s možností přístupu k Internetu.



# Kabelové modemy



Upstream a downstream kabelové televize.

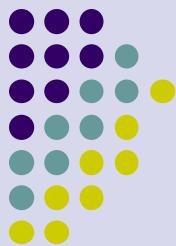


# Linková úroveň

Úvod do počítačových sítí

Lekce 05

Ing. Jiří Iedvina, CSc.



# Linková úroveň

- úroveň 2 protokolového zásobníku
  - fyzická úroveň – přenos bitů (Protokolové datové jednotky fyzické úrovně)
  - linková úroveň – přenos rámců (protokolové datové jednotky linkové úrovně)
- zajišťuje přenos rámců mezi sousedními uzly
- poskytuje služby vyšší úrovni (síťová, aplikační)



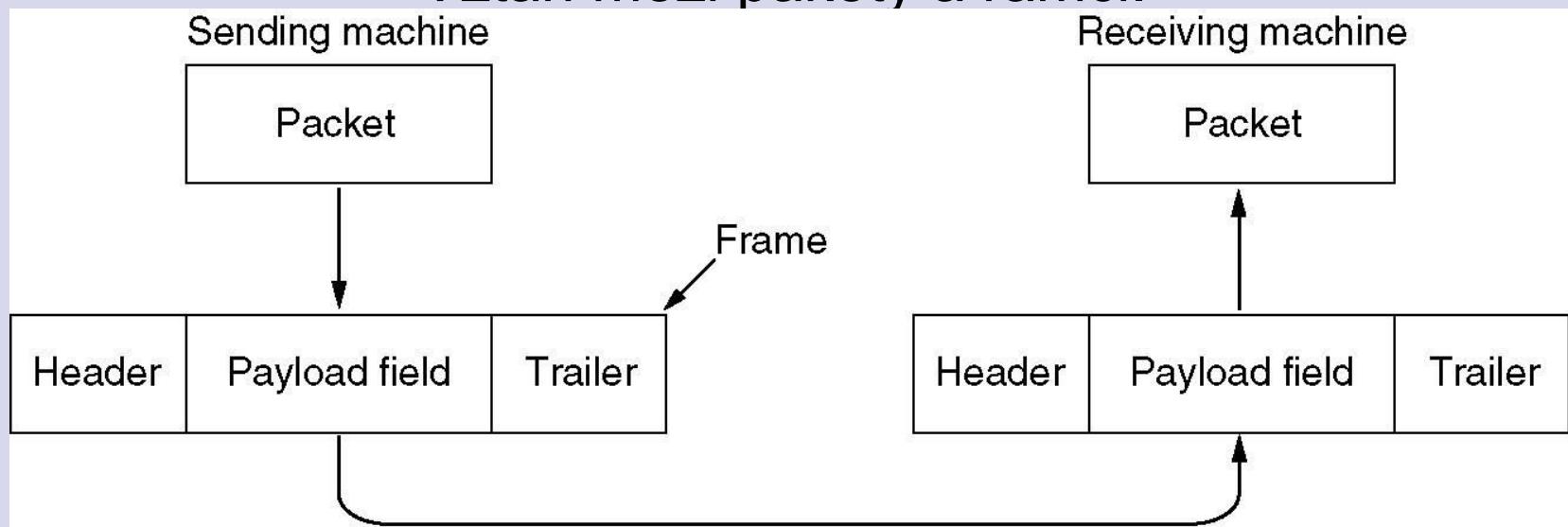
# Funkce linkové úrovně

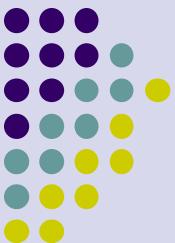
- Zajišťuje služby pro síťovou úroveň
  - Vysílání dat, příjem dat, nastavení parametrů přenosu
  - Hlášení neodstranitelných chyb
- Využívá služeb fyzické úrovně
  - Vysílání rámců, příjem rámců
- Určení hranice rámců
- Detekce a odstranění chyb přenosu
- Řízení toku dat
  - Pomalí příjemci nesmí být udolání rychlými vysílači
  - Příjemce nesmí zpracovat data, která nebyla odeslána.
  - Vysílač nesmí (?) odeslat data, která nemohou být přijata.



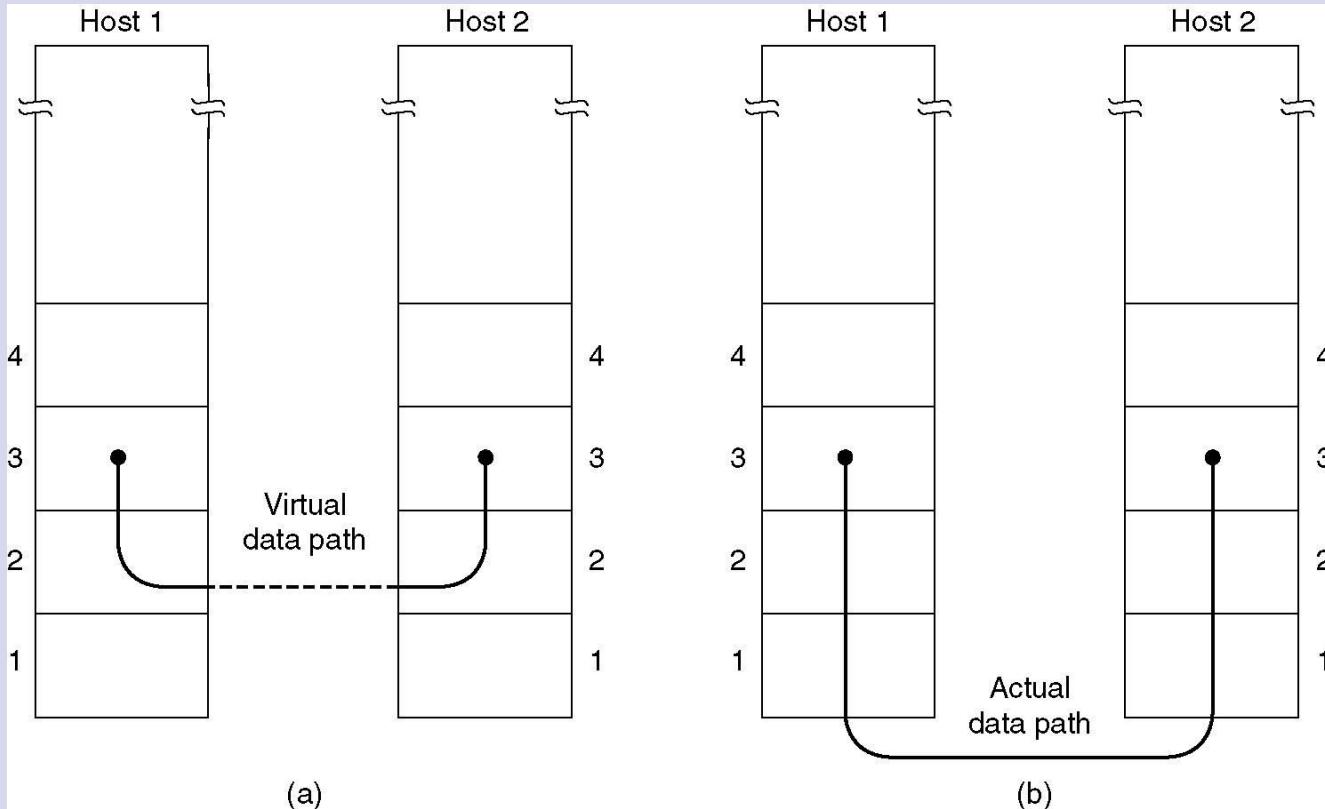
# Vytváření rámce

Vztah mezi pakety a rámci.



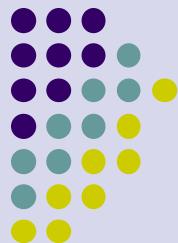


# Služby poskytované síťové úrovni

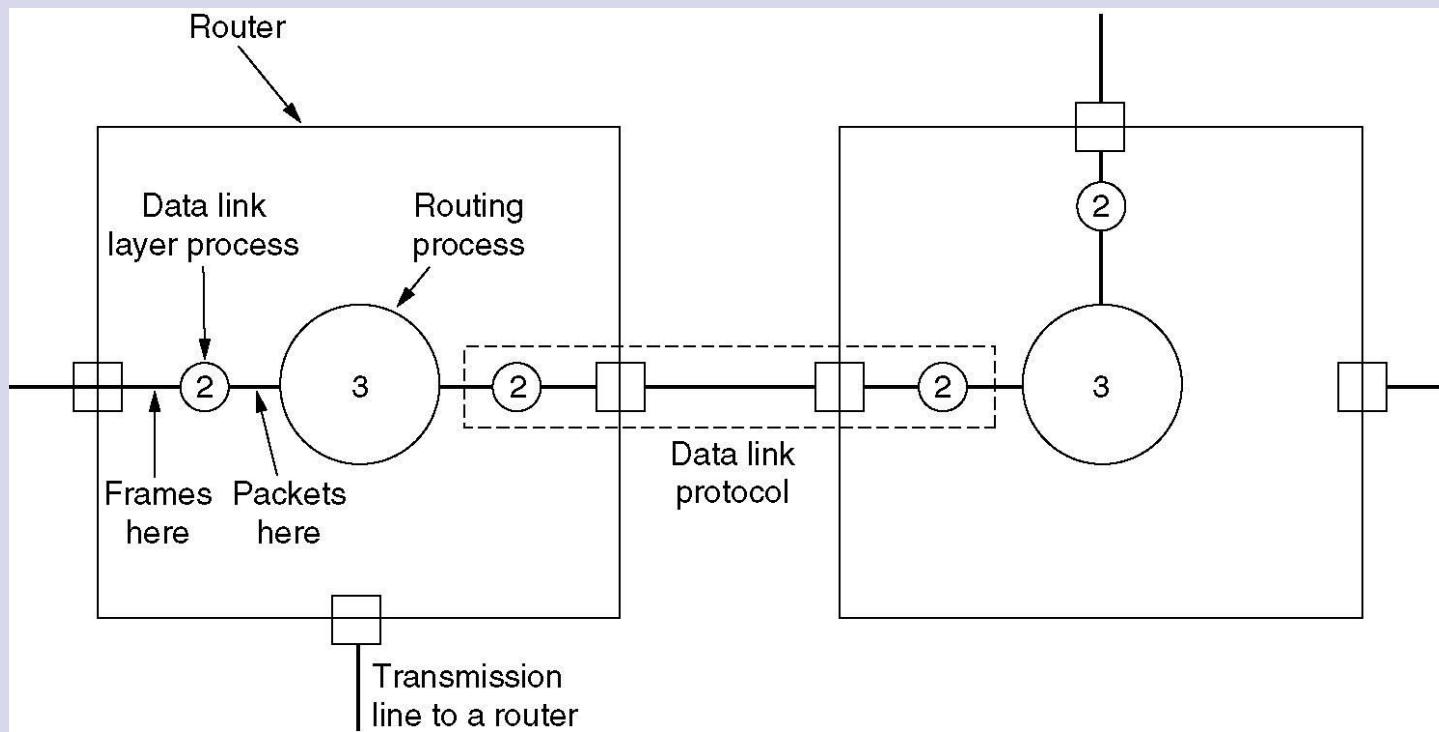


(a) Virtuální komunikace.

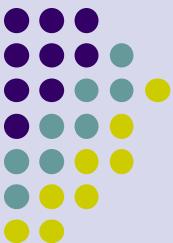
(b) Skutečná komunikace.



# Služby poskytované síťové úrovni (2)

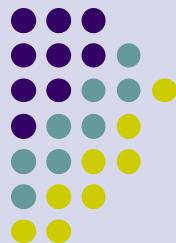


Umístění linkového protokolu v uzlu. Data přichází linkovou úrovni, předány síťové úrovni a po nalezení správné linky (rozhraní) předány další linkové úrovni ke zpracování.



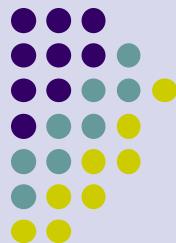
# Typy přenosů

- Simplexní
- Duplexní
- Poloduplexní



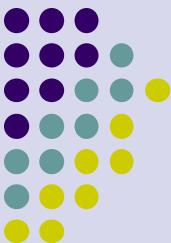
# Rozdělení přenosů do rámčů

- Určení začátku a konce rámce
  - délkově orientované
  - znakově orientované
  - bitově orientované
- Převod bitů na slabiky
- Oddělení dat od řídicí informace – transparentní přenos
  - znakově orientované
  - bitově orientované

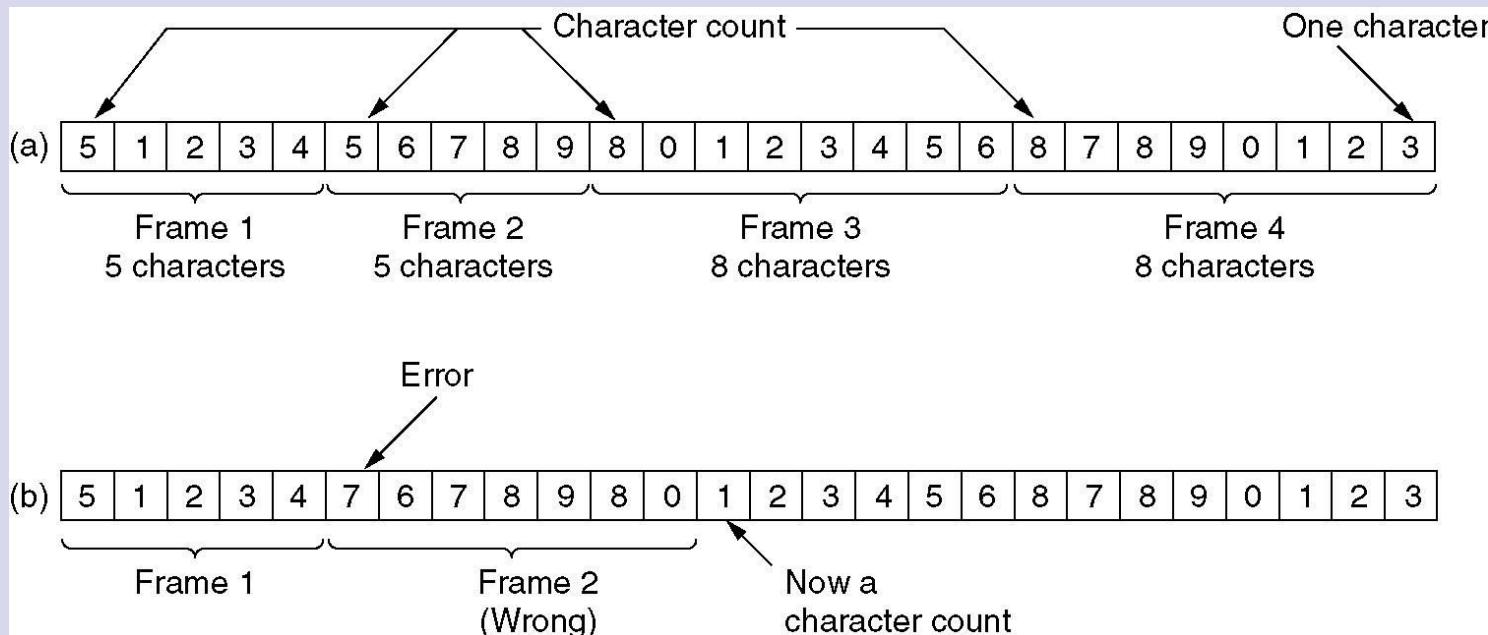


# Typy rámců linkové úrovнě

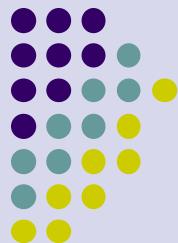
- V rámci je třeba určit jeho začátek a konec
  - Zadáním délky na začátku rámce – nepoužívá se
  - Vybraným znakem (STX – ETX, BOF – EOF, ...)
  - Nezáměnnou posloupností bitů (FLAG – 01111110)
- Typy rámců – podle způsobu chápání obsahu rámce
  - **Znakově orientované** (řídicí informace i data jsou disjunktní množiny znaků)
    - Např. kódy 0 až 31 a 255 jsou řídicí znaky, ostatní jsou datové
    - Problém s transparentností přenosu (co s daty s kódy 0 až 31)
  - **Bitově orientované** (řídicí informace má v rámci pevné místo)
    - data jsou posloupnost bitů, délka je celistvým násobkem počtu bitů ve slabice ( $n^*8$ ,  $n^*7$ ,  $n^*6$ , ...)
    - Řídicí informace na začátku a konci rámce (zabezpečení)



# Rámce s hranicemi danými délkou

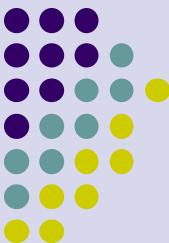


Problém s určením hranic rámce při chybě. Přenos proudu znaků. (a) bezchybný. (b) s chybami.

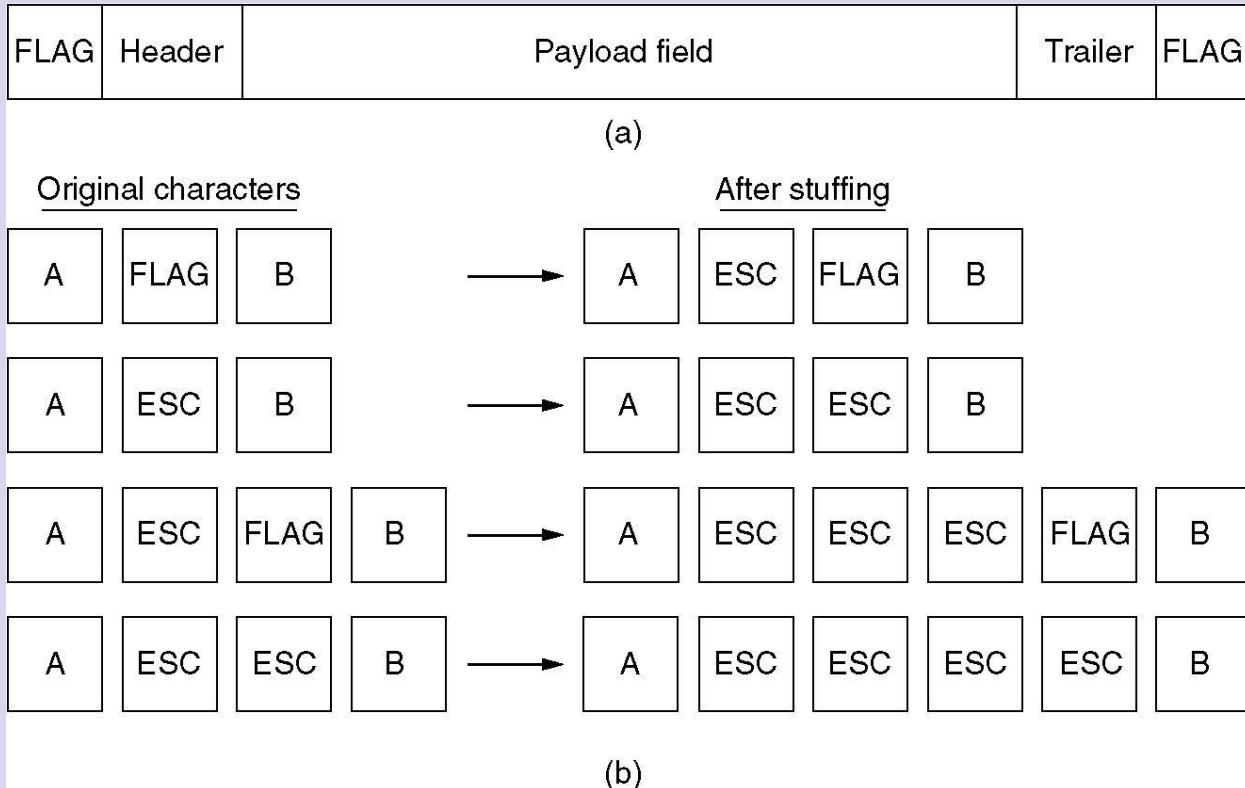


# Určení hranice rámce – znakově orientovaný protokol

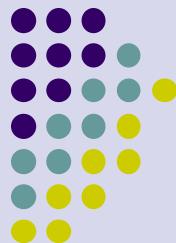
- Začátek rámce – STX, BOF (STX = 2, BOF = 0xC0)
- Konec rámce – ETX, EOF (ETX = 3, EOT = 0xC1)
- Problém s transparentností – náhrada řídicích znaků
  - STX → DLE STX,  
ETX → DLE ETX,  
DLE → DLE DLE
  - BOT → ESC (BOT xor 0x20),  
EOT → ESC (EOT xor 0x20),  
CE → CE (CE xor 0x20)
- Problém s transparentností – náhrada datových znaků
  - 0x02 → DLE 0x02,  
0x03 → DLE 0x03,  
DLE → DLE DLE



# Rámce ohraničené značkou



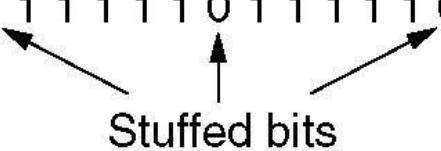
- (a) Rámcem ohrazený speciální jednoznačnou značkou.
- (b) Zajištění transparentnosti vkládáním znakových prefixů.



# Transparentní přenos dat

(a) 0 1 1 0 1 0 0 1 0

(b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0 0 1 0



(c) 0 1 1 0 1 0 0 1 0

Vkládání bitů – po 5 jedničkách vložíme vždy nulu

- (a) Původní data.
- (b) Data přenášená linkou.
- (c) Přijatá data zbavená vložených bitů.



# Detekce a korekce chyb

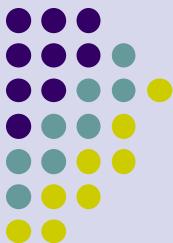
- Model kanálu
  - Symetrický binární kanál bez paměti.
- Typy šumu
  - Bílý šum
  - Impulsní šum
- Pravděpodobnostní výpočet chybovosti
  - $p$  – pravděpodobnost bezchybného přenosu jednoho bitu
  - $1 - p$  – pravděpodobnost chyby v jednom bitu
  - $P_N = (1 - p)^N$  - pravděpodobnost bezchybného přenosu  $N$  bitů

$$P_N^k = \binom{N}{k} p^{N-k} (1-p)^k$$



# Detekce a korekce chyb

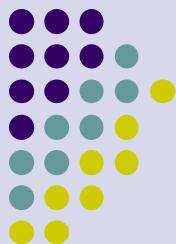
- Hammingova vzdálenost ( $d$ )
  - Určuje zda-li je kód detekční nebo samoopravný
  - Doplnění informace o další bity – redundance
  - Vyloučení některých kombinací bitů z informace → možnost detekce nebo opravení chyby
- Kódy pro detekci chyb
  - Paritní kódy (sudá parita, lichá parita, iterační kód)
  - CRC – Cyclic Redundancy Check
- Kódy pro korekci chyb
  - Hammingovy kódy
    - Generační matice, Hammingova matice (kontrolní), syndrom
  - BCH kódy (Bose, Ray-Chaudhuri, Hocquenghem code) - kombinace výpočtu CRC



# Detekce a korekce chyb

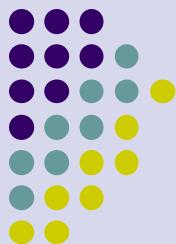
- Hammingovy kódy ( $n,k$ )
  - $2^r = r + k + 1$
  - $n = r + k$
  - $r$  - redundantní bity
  - $k$  - informační bity
  - Kódy (3,1), (7,4), (15,11), (31,26), (63,57)

$$v = uG \quad s = vH^T \quad GH^T = 0$$



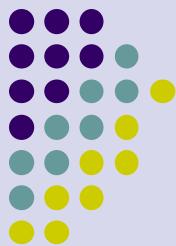
# Odstranění chyb přenosu

- Samoopravné kódy (redundantní přenos, metoda FEC)
- Detekční kódy (opakování přenosu, metoda ARQ)
- Redundantní přenos dat
- Samoopravné kódy
  - Hammingovy kódy
  - BCH kódy



# Odstranění chyb přenosu

- Opakování přenosu
- Rozhodovací zpětná vazba
  - kladné potvrzování
  - záporné potvrzování
  - kladné a záporné potvrzování
- Informační zpětná vazba
- Kombinovaná zpětná vazba



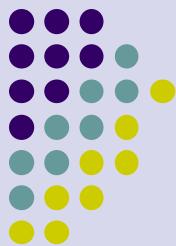
# Odstranění chyb přenosu

- Rozhodovací zpětná vazba
  - Rozhodovací zpětná vazba, kladné potvrzování
  - Rozhodovací zpětná vazba, záporné potvrzování
  - Rozhodovací zpětná vazba, kladné i záporné potvrzování



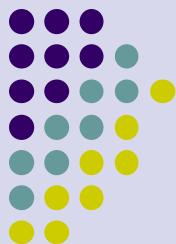
# Simplexní přenos dat

- Protokol Stop and Wait
- Protokol Ask and Go
- Další protokoly



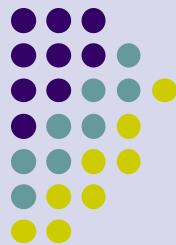
# Elementární protokol linkové úrovni

- Simplexní protokol bez omezení
- Simplexní Stop-and-Wait protokol
- Simplexní protokol pro kanál se šumem



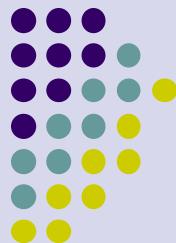
# Protokol Stop and Wait

- Simplexní protokol Stop and Wait s kladným potvrzováním
  - číslování rámců
  - využití přenosového kanálu
- Duplexní protokol Stop and Wait s kladným potvrzováním
  - číslování rámců
  - souběžný přenos
  - nesamostatné potvrzování (piggybacking)



# Protokoly s klouzajícím okénkem

- Protokoly s klouzajícím okénkem, sekvenční příjem
  - číslování rámců
  - velikost okénka
  - využití přenosového kanálu
- Protokoly s klouzajícím okénkem, nesekvenční příjem
  - číslování rámců
  - velikost okénka

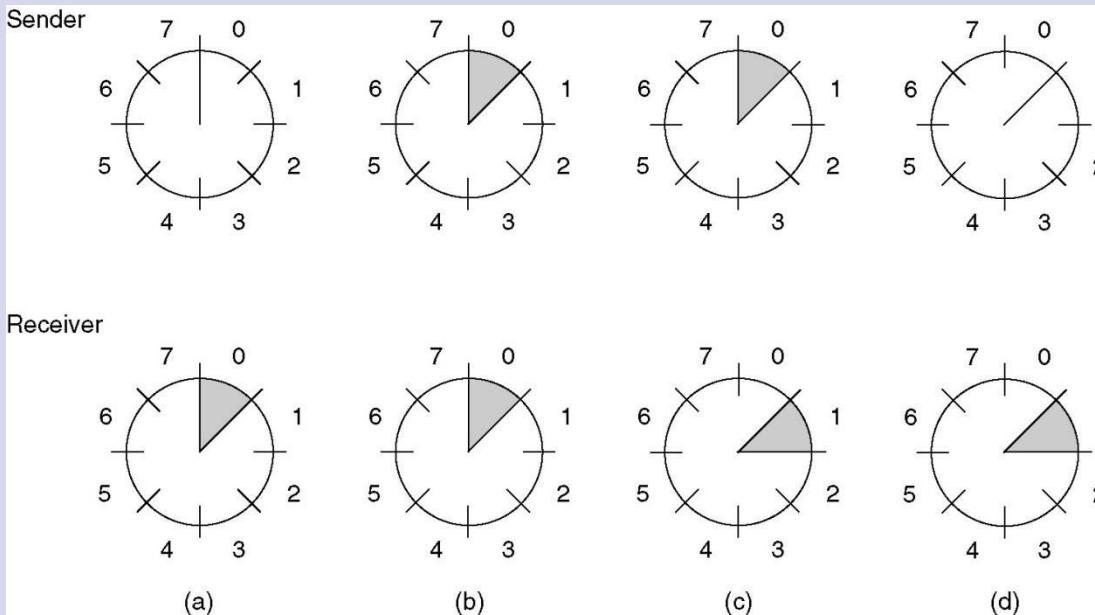


# Protokoly s klouzajícím okénkem

- Protokol s jednabitovým klouzajícím okénkem
- Protokol se sekvenčním příjemem ( Go Back N)
- Protokol s nesekvenčním příjemem (Selective Repeat)



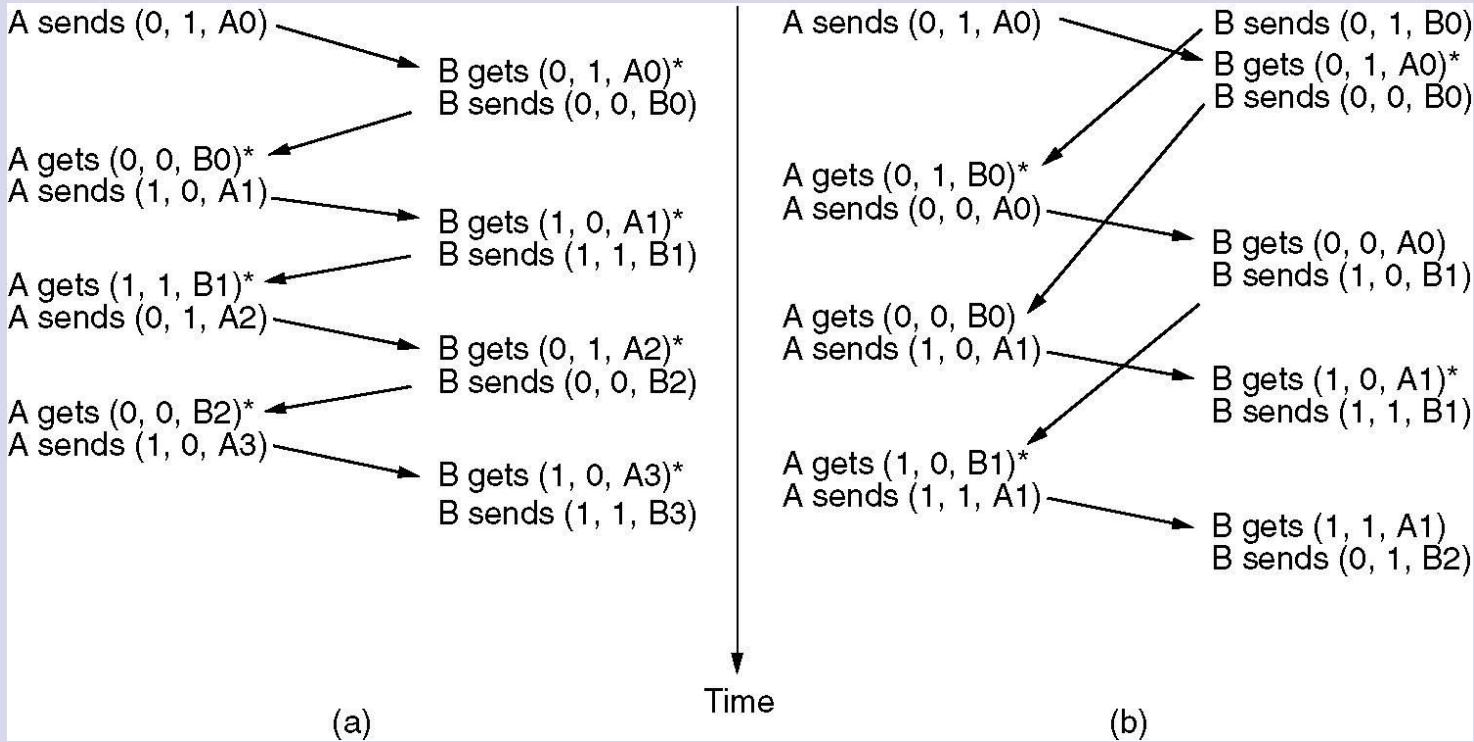
# Protokoly s klouzajícím okénkem (2)



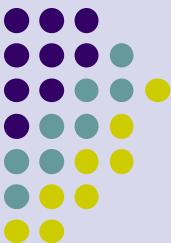
Klouzající okénko velikosti 1 s š bitovým sekvenčním číslem.

- (a) Počáteční nastavení.
- (b) Po odeslání prvního rámce.
- (c) Po přijetí prvního rámce.
- (d) Po přijetí potvrzení prvního rámce.

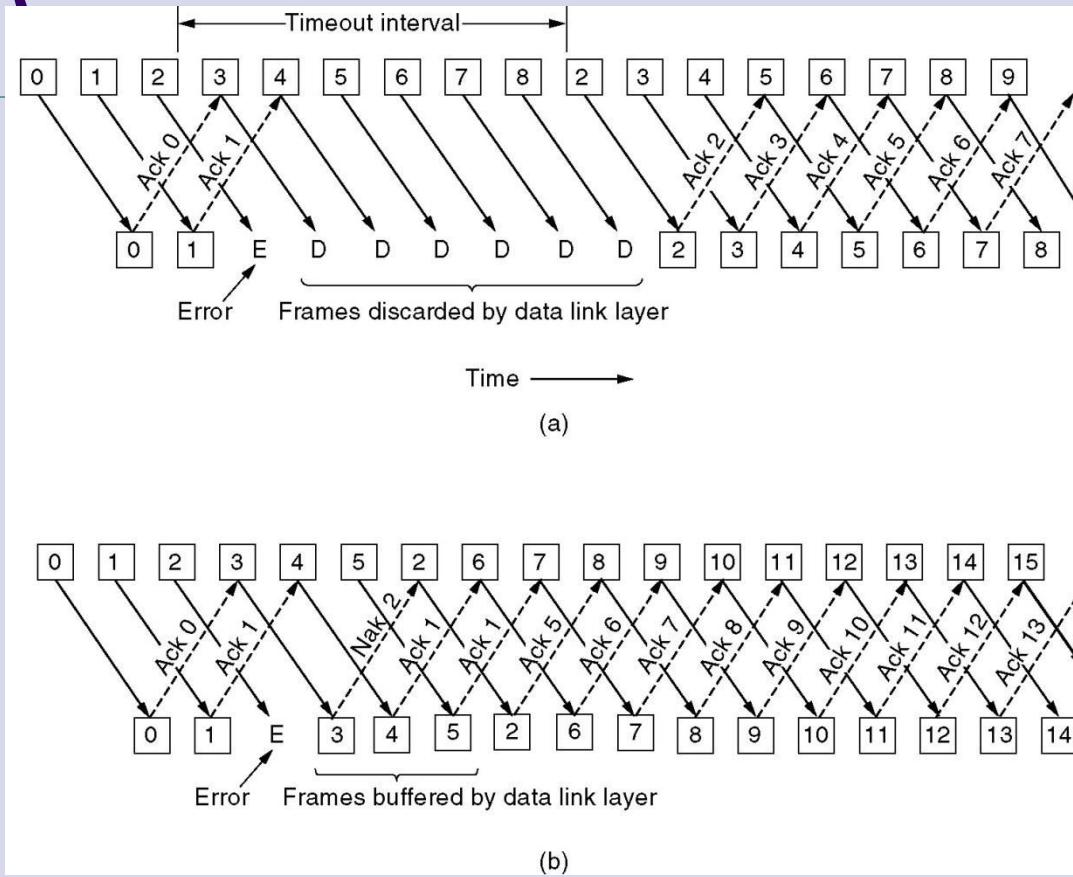
# Protokol s klouzajícím jednobitovým okénkem (2)



Dvě situace protokolu. (a) normální případ. (b) nenormální případ.  
V závorkách (seq, ack, č. paketu).  
Hvězdička znamená přijetí paketu síťovou úrovní.



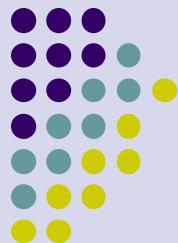
# Protokol se sekvenčním příjemem (Go Back N')



Proudové zpracování a obnova po chybě. Působení chyby při:

(a) Velikosti okna příjemce 1.

(b) Velikosti okna příjemce  $> 1$ .

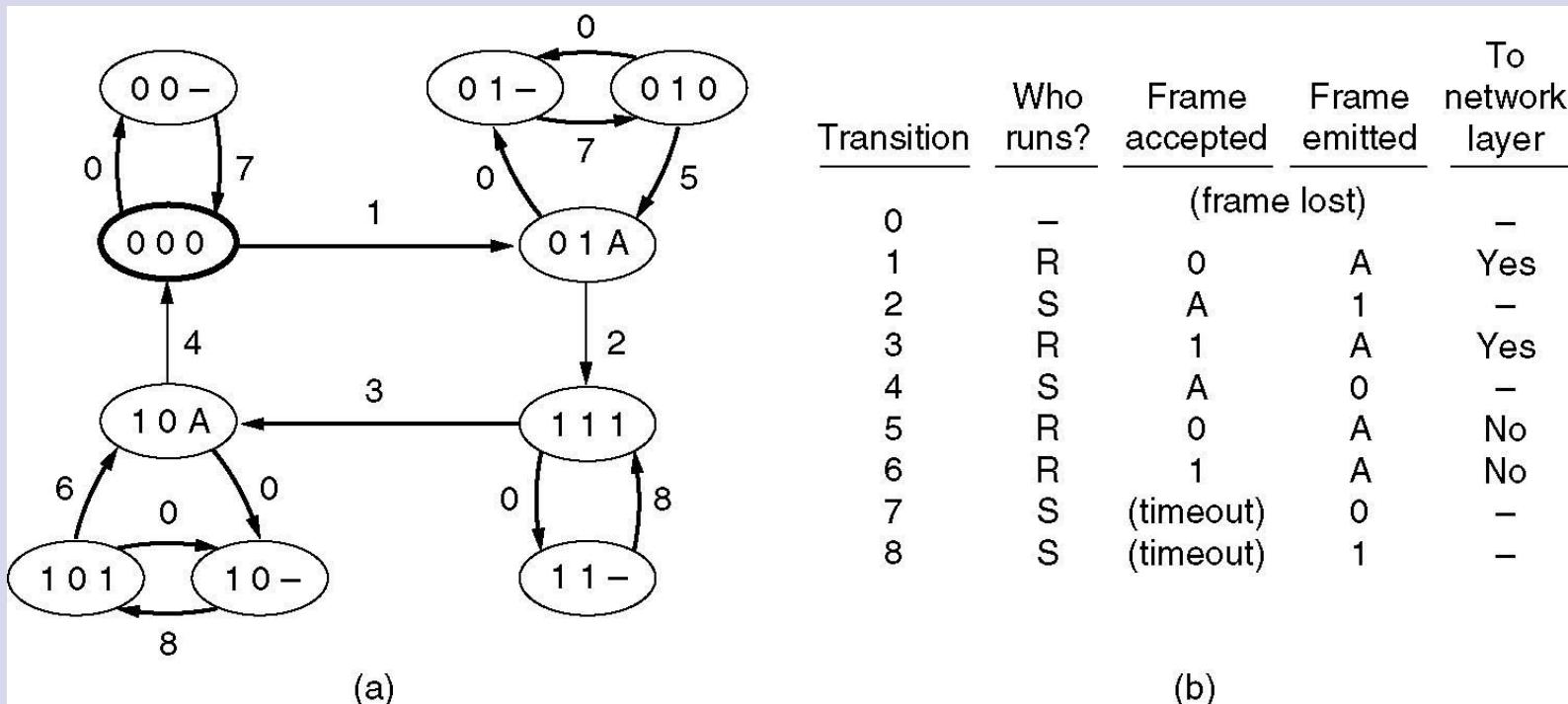


# Verifikace protokolů

- Modely založené na konečných automatech
- Modely založené na Petriho sítích



# Konečně automatový model

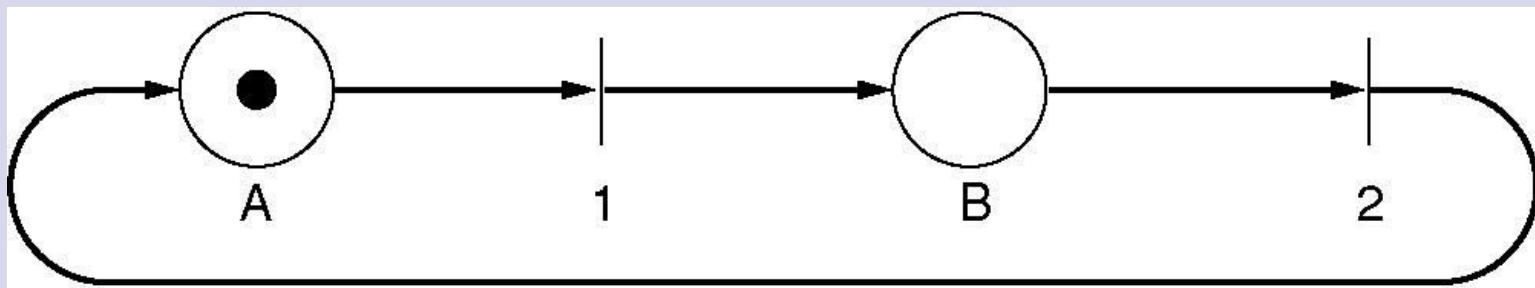


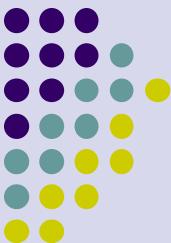
(a) Stavový diagram protokolu. (b) přechody.



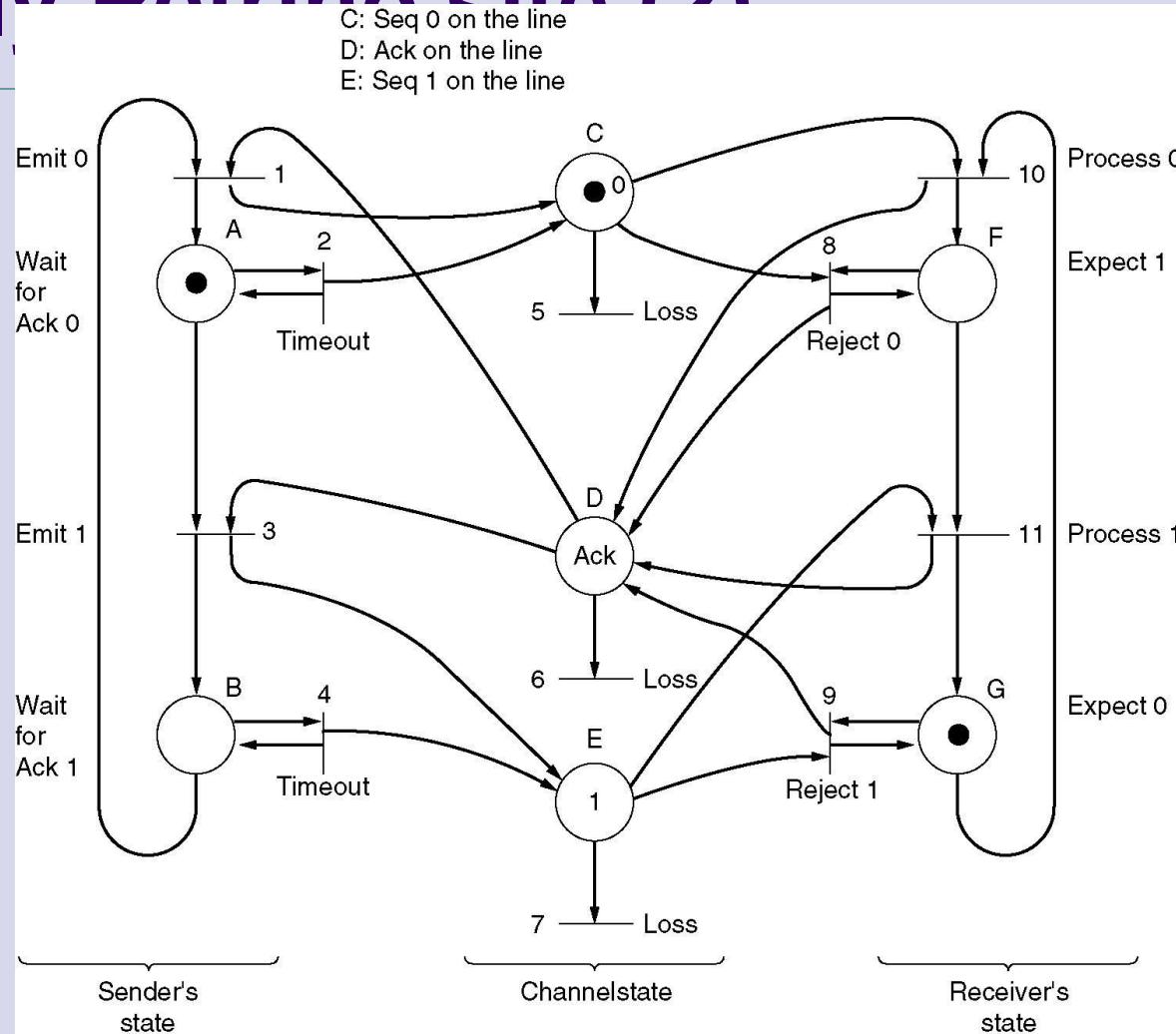
# Modely Petriho sítě

Petriho síť se dvěma místy a dvěma přechody.

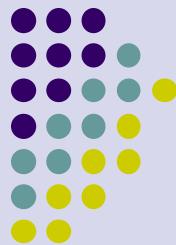




# Modely Petriho sítí (2)



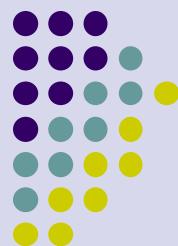
Model protokolu realizovaný Petriho sítí.



# Příklad linkových protokolů

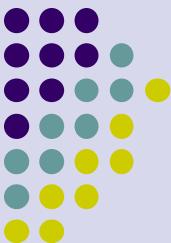
- HDLC – High-Level Data Link Control
- Linková úroveň Internetu

# High-Level Data Link Control (HDLC)



Formát rámce bitově orientovaného protokolu.

Bits	8	8	8	$\geq 0$	16	8
	0 1 1 1 1 1 1 0	Address	Control	Data	Checksum	0 1 1 1 1 1 1 0



# HDLC (2)

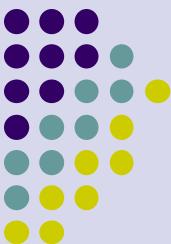
Bits	1	3	1	3
(a)	0	Seq	P/F	Next
(b)	1	0	Type	P/F
(c)	1	1	Type	Modifier

## Řídící pole

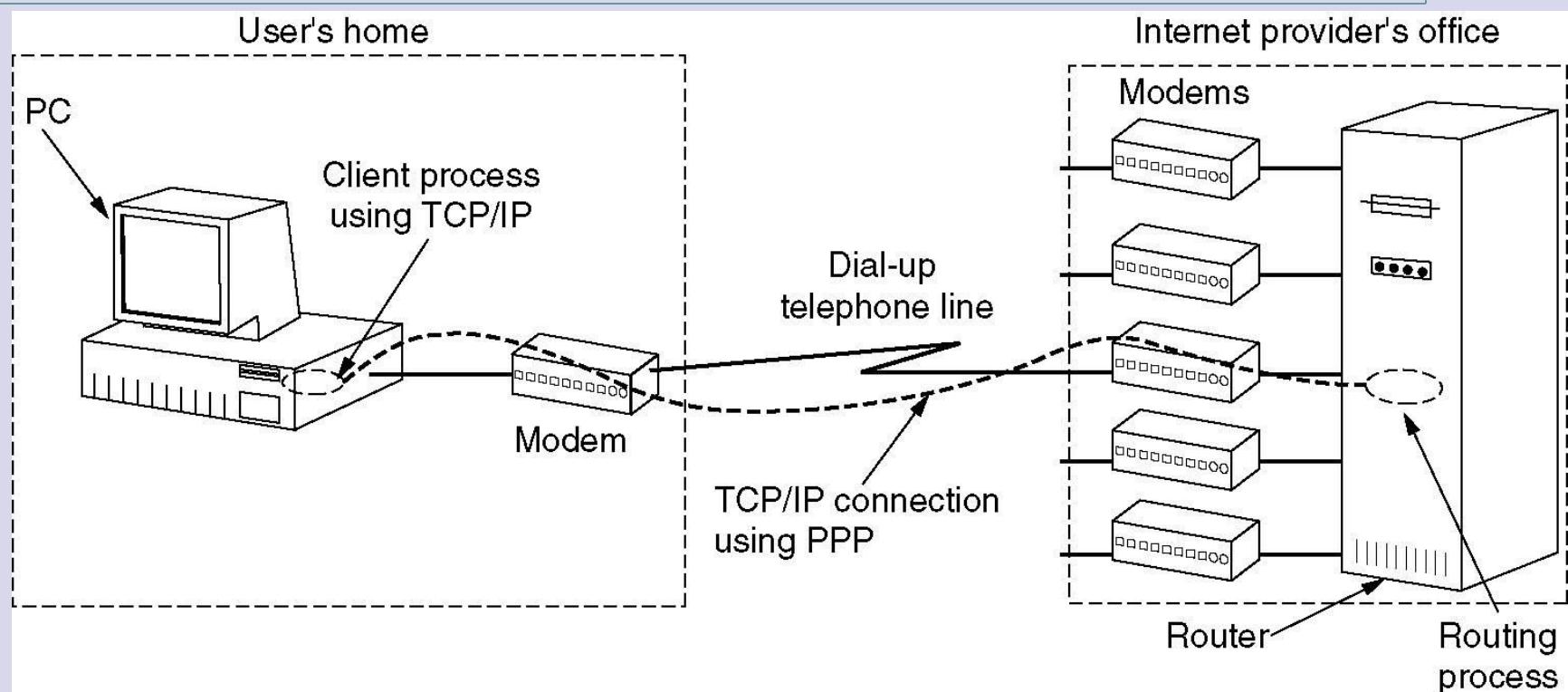
(a) Informačního rámce.

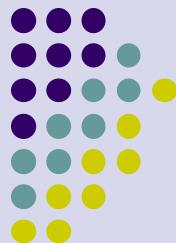
(b) Řídicího rámce.

(c) Nečíslovaného rámce.



# Linková úroveň v Internetu

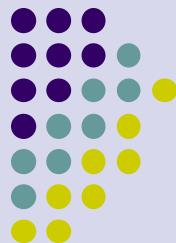




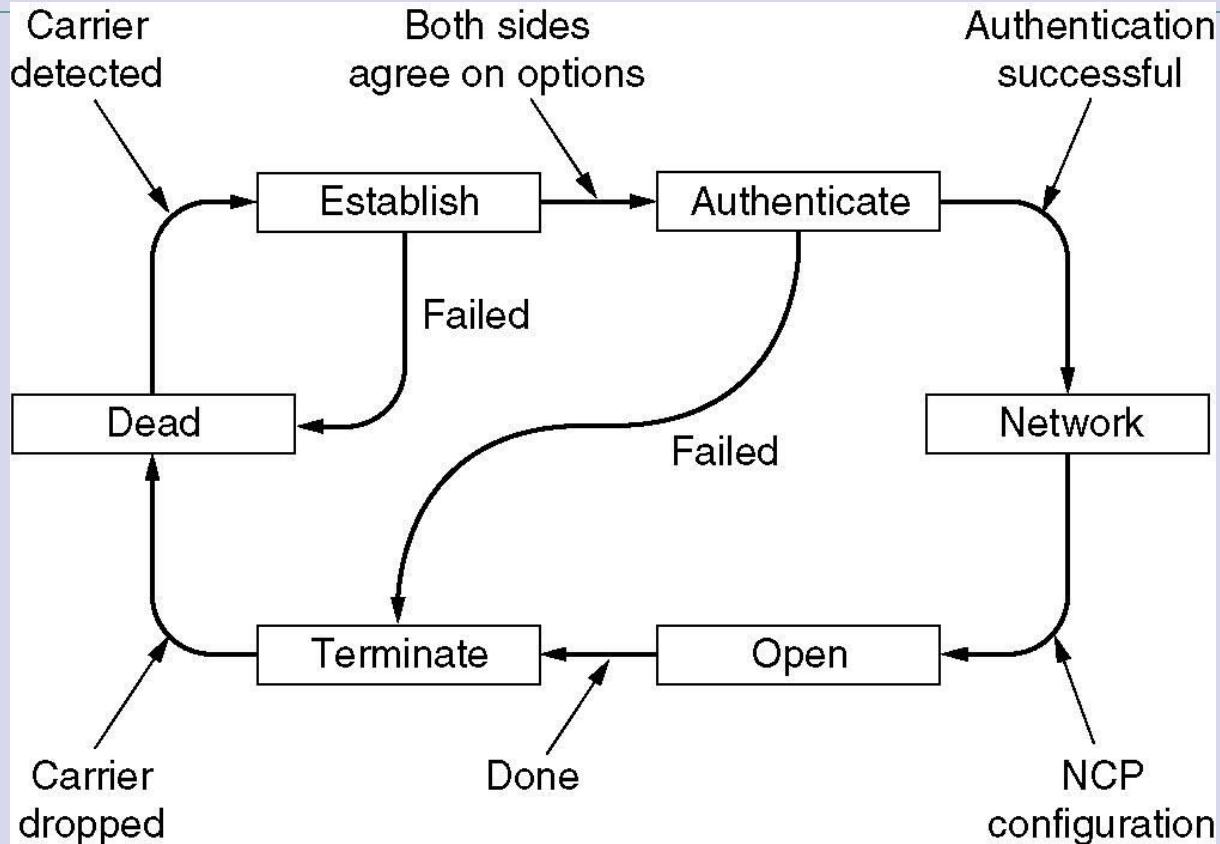
# PPP – Point to Point Protocol

Úplný rámec PPP pro nečíslované operace.

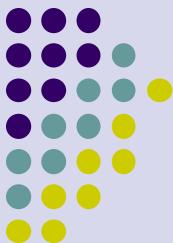
Bytes	1	1	1	1 or 2	Variable	2 or 4	1
	Flag 01111110	Address 11111111	Control 00000011	Protocol	Payload }} {{	Checksum	Flag 01111110



# PPP – Point to Point Protocol (2)

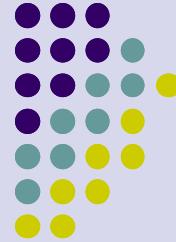


Zjednodušený diagram pro vytvoření a rušení PPP spojení.



# PPP – Point to Point Protocol (3)

Name	Direction	Description
Configure-request	I → R	List of proposed options and values
Configure-ack	I ← R	All options are accepted
Configure-nak	I ← R	Some options are not accepted
Configure-reject	I ← R	Some options are not negotiable
Terminate-request	I → R	Request to shut the line down
Terminate-ack	I ← R	OK, line shut down
Code-reject	I ← R	Unknown request received
Protocol-reject	I ← R	Unknown protocol requested
Echo-request	I → R	Please send this frame back
Echo-reply	I ← R	Here is the frame back
Discard-request	I → R	Just discard this frame (for testing)

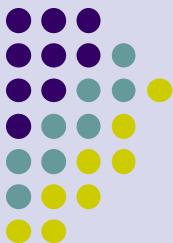


# Linková úroveň

Úvod do počítačových sítí

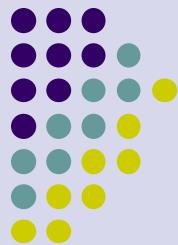
Lekce 05

Ing. Jiří Iedvina, CSc.



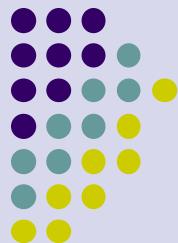
# Linková úroveň

- úroveň 2 protokolového zásobníku
  - fyzická úroveň – přenos bitů (Protokolové datové jednotky fyzické úrovně)
  - linková úroveň – přenos rámců (protokolové datové jednotky linkové úrovně)
- zajišťuje přenos rámců mezi sousedními uzly
- poskytuje služby vyšší úrovni (síťová, aplikační)



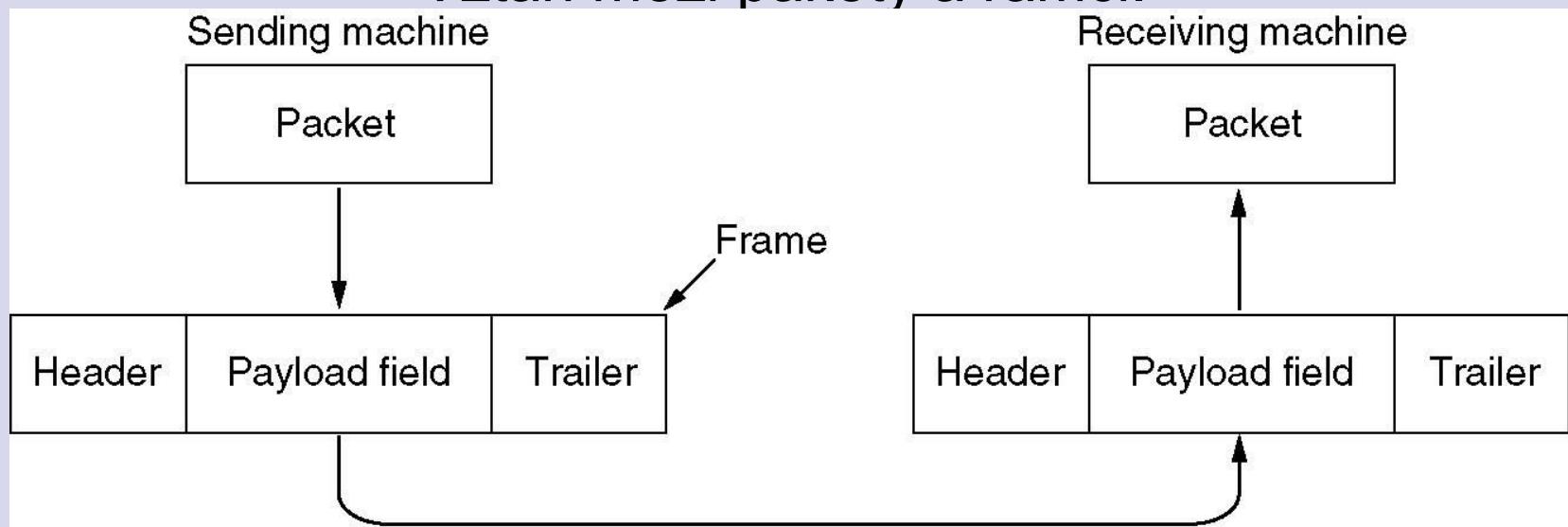
# Funkce linkové úrovně

- Zajišťuje služby pro síťovou úroveň
  - Vysílání dat, příjem dat, nastavení parametrů přenosu
  - Hlášení neodstranitelných chyb
- Využívá služeb fyzické úrovně
  - Vysílání rámců, příjem rámců
- Určení hranice rámců
- Detekce a odstranění chyb přenosu
- Řízení toku dat
  - Pomalí příjemci nesmí být udolání rychlými vysílači
  - Příjemce nesmí zpracovat data, která nebyla odeslána.
  - Vysílač nesmí (?) odeslat data, která nemohou být přijata.



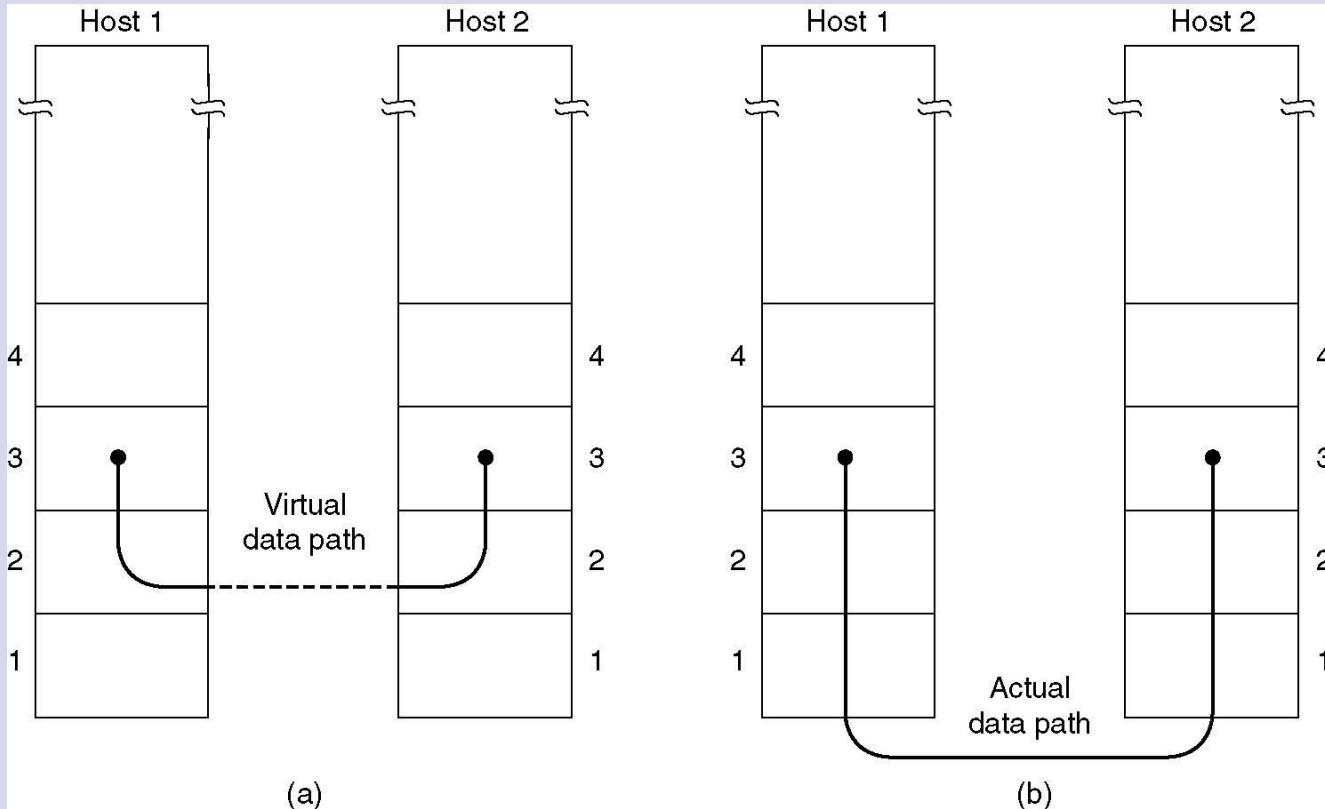
# Vytváření rámce

Vztah mezi pakety a rámci.





# Služby poskytované síťové úrovni

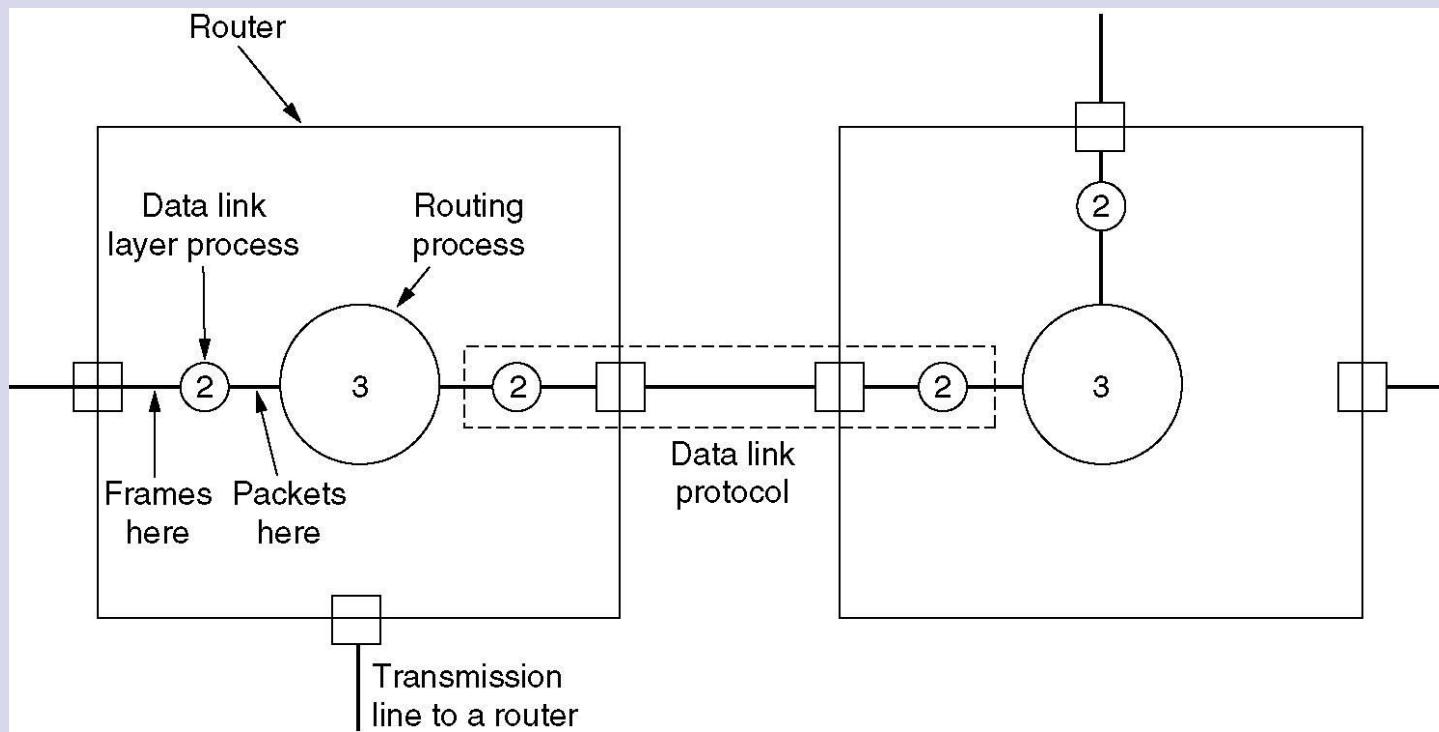


(a) Virtuální komunikace.

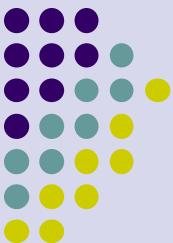
(b) Skutečná komunikace.



# Služby poskytované síťové úrovni (2)

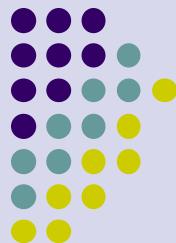


Umístění linkového protokolu v uzlu. Data přichází linkovou úrovni, předány síťové úrovni a po nalezení správné linky (rozhraní) předány další linkové úrovni ke zpracování.



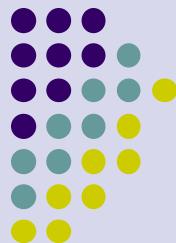
# Typy přenosů

- Simplexní
- Duplexní
- Poloduplexní



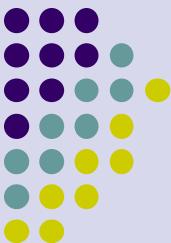
# Rozdělení přenosů do rámčů

- Určení začátku a konce rámce
  - délkově orientované
  - znakově orientované
  - bitově orientované
- Převod bitů na slabiky
- Oddělení dat od řídicí informace – transparentní přenos
  - znakově orientované
  - bitově orientované

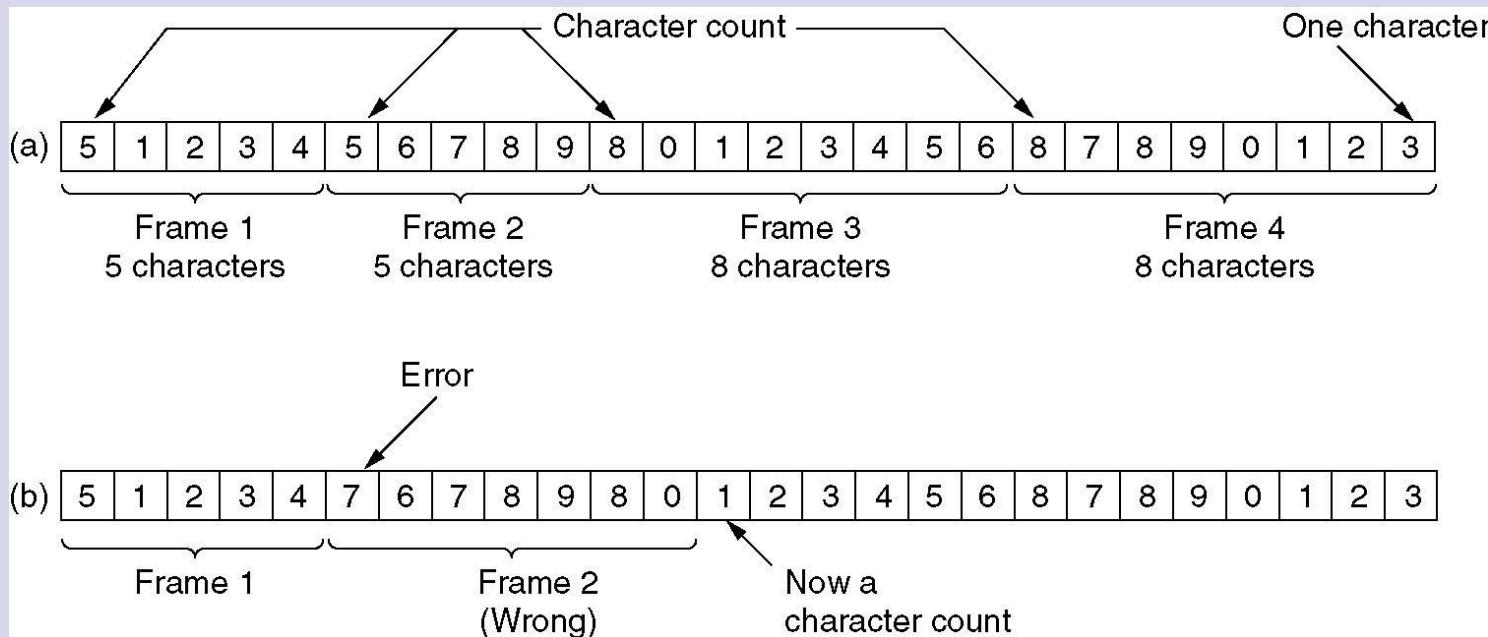


# Typy rámců linkové úrovнě

- V rámci je třeba určit jeho začátek a konec
  - Zadáním délky na začátku rámce – nepoužívá se
  - Vybraným znakem (STX – ETX, BOF – EOF, ...)
  - Nezáměnnou posloupností bitů (FLAG – 01111110)
- Typy rámců – podle způsobu chápání obsahu rámce
  - **Znakově orientované** (řídicí informace i data jsou disjunktní množiny znaků)
    - Např. kódy 0 až 31 a 255 jsou řídicí znaky, ostatní jsou datové
    - Problém s transparentností přenosu (co s daty s kódy 0 až 31)
  - **Bitově orientované** (řídicí informace má v rámci pevné místo)
    - data jsou posloupnost bitů, délka je celistvým násobkem počtu bitů ve slabice ( $n^*8$ ,  $n^*7$ ,  $n^*6$ , ...)
    - Řídicí informace na začátku a konci rámce (zabezpečení)



# Rámce s hranicemi danými délkou

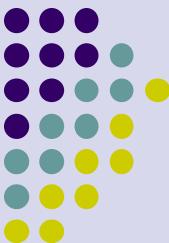


Problém s určením hranic rámce při chybě. Přenos proudu znaků. (a) bezchybný. (b) s chybami.

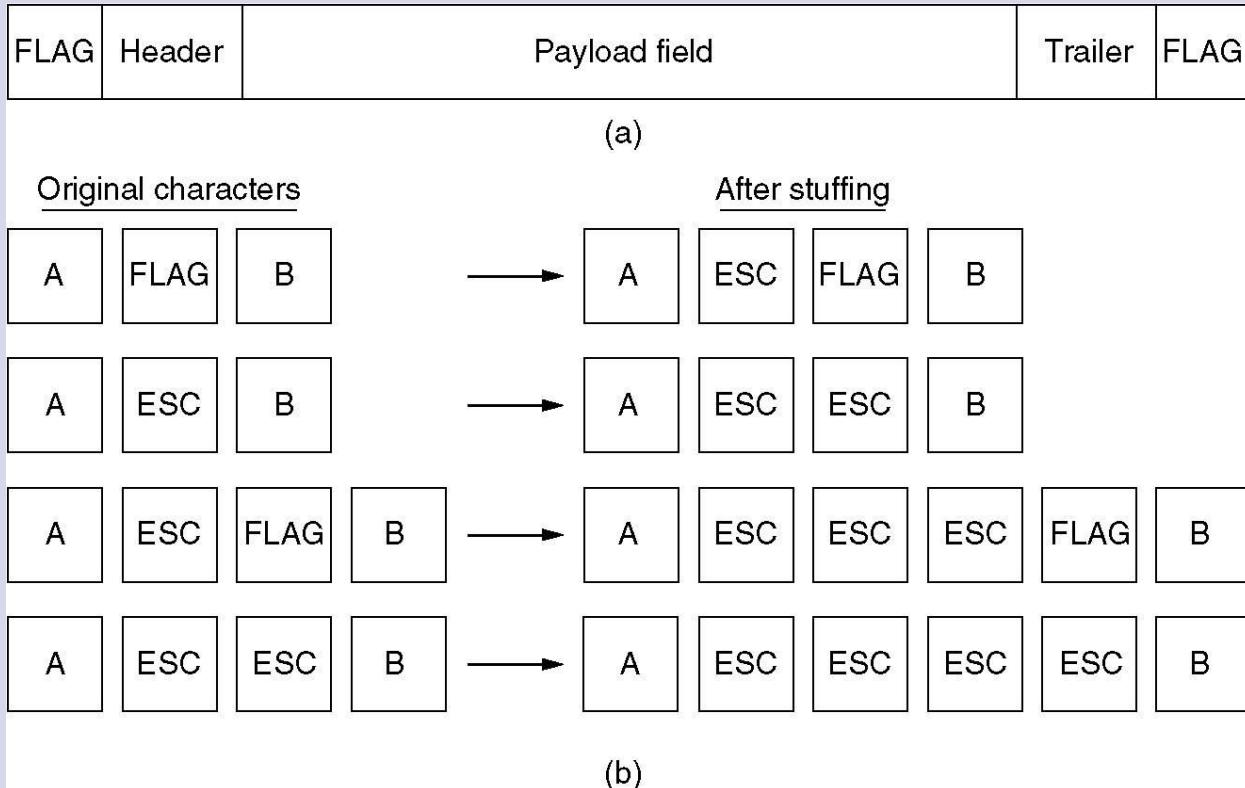


# Určení hranice rámce – znakově orientovaný protokol

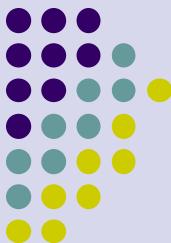
- Začátek rámce – STX, BOF (STX = 2, BOF = 0xC0)
- Konec rámce – ETX, EOF (ETX = 3, EOT = 0xC1)
- Problém s transparentností – náhrada řídicích znaků
  - STX → DLE STX,  
ETX → DLE ETX,  
DLE → DLE DLE
  - BOT → ESC (BOT xor 0x20),  
EOT → ESC (EOT xor 0x20),  
CE → CE (CE xor 0x20)
- Problém s transparentností – náhrada datových znaků
  - 0x02 → DLE 0x02,  
0x03 → DLE 0x03,  
DLE → DLE DLE



# Rámce ohraničené značkou



- (a) Rámcem ohrazený speciální jednoznačnou značkou.  
(b) Zajištění transparentnosti vkládáním znakových prefixů.



# Transparentní přenos dat

(a) 0 1 1 0 1 0 0 1 0

(b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 1 0 1 1 1 1 1 1 1 1 0 1 0 0 1 0

Stuffed bits

(c) 0 1 1 0 1 0 0 1 0

Vkládání bitů – po 5 jedničkách vložíme vždy nulu

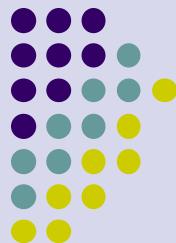
- (a) Původní data.
- (b) Data přenášená linkou.
- (c) Přijatá data zbavená vložených bitů.



# Detekce a korekce chyb

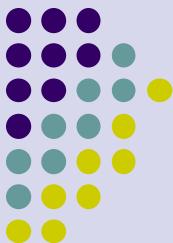
- Model kanálu
  - Symetrický binární kanál bez paměti.
- Typy šumu
  - Bílý šum
  - Impulsní šum
- Pravděpodobnostní výpočet chybovosti
  - $p$  – pravděpodobnost bezchybného přenosu jednoho bitu
  - $1 - p$  – pravděpodobnost chyby v jednom bitu
  - $P_N = (1 - p)^N$  - pravděpodobnost bezchybného přenosu  $N$  bitů

$$P_N^k = \binom{N}{k} p^{N-k} (1-p)^k$$



# Detekce a korekce chyb

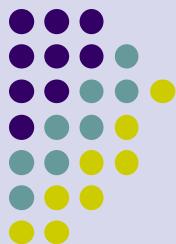
- Hammingova vzdálenost ( $d$ )
  - Určuje zda-li je kód detekční nebo samoopravný
  - Doplnění informace o další bity – redundance
  - Vyloučení některých kombinací bitů z informace → možnost detekce nebo opravení chyby
- Kódy pro detekci chyb
  - Paritní kódy (sudá parita, lichá parita, iterační kód)
  - CRC – Cyclic Redundancy Check
- Kódy pro korekci chyb
  - Hammingovy kódy
    - Generační matice, Hammingova matice (kontrolní), syndrom
  - BCH kódy (Bose, Ray-Chaudhuri, Hocquenghem code) - kombinace výpočtu CRC



# Detekce a korekce chyb

- Hammingovy kódy ( $n,k$ )
  - $2^r = r + k + 1$
  - $n = r + k$
  - $r$  - redundantní bity
  - $k$  - informační bity
  - Kódy (3,1), (7,4), (15,11), (31,26), (63,57)

$$v = uG \quad s = vH^T \quad GH^T = 0$$



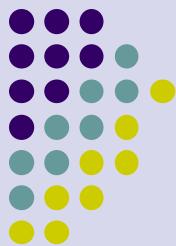
# Odstranění chyb přenosu

- Samoopravné kódy (redundantní přenos, metoda FEC)
- Detekční kódy (opakování přenosu, metoda ARQ)
- Redundantní přenos dat
- Samoopravné kódy
  - Hammingovy kódy
  - BCH kódy



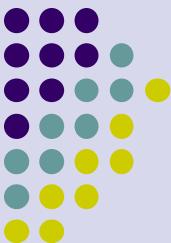
# Odstranění chyb přenosu

- Opakování přenosu
- Rozhodovací zpětná vazba
  - kladné potvrzování
  - záporné potvrzování
  - kladné a záporné potvrzování
- Informační zpětná vazba
- Kombinovaná zpětná vazba



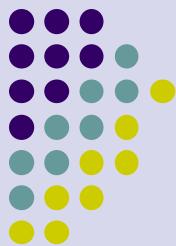
# Odstranění chyb přenosu

- Rozhodovací zpětná vazba
  - Rozhodovací zpětná vazba, kladné potvrzování
  - Rozhodovací zpětná vazba, záporné potvrzování
  - Rozhodovací zpětná vazba, kladné i záporné potvrzování



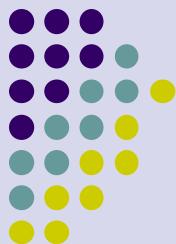
# Simplexní přenos dat

- Protokol Stop and Wait
- Protokol Ask and Go
- Další protokoly



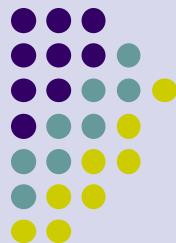
# Elementární protokol linkové úrovni

- Simplexní protokol bez omezení
- Simplexní Stop-and-Wait protokol
- Simplexní protokol pro kanál se šumem



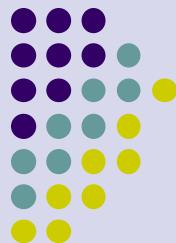
# Protokol Stop and Wait

- Simplexní protokol Stop and Wait s kladným potvrzováním
  - číslování rámců
  - využití přenosového kanálu
- Duplexní protokol Stop and Wait s kladným potvrzováním
  - číslování rámců
  - souběžný přenos
  - nesamostatné potvrzování (piggybacking)



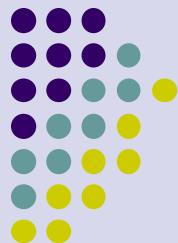
# Protokoly s klouzajícím okénkem

- Protokoly s klouzajícím okénkem, sekvenční příjem
  - číslování rámců
  - velikost okénka
  - využití přenosového kanálu
- Protokoly s klouzajícím okénkem, nesekvenční příjem
  - číslování rámců
  - velikost okénka

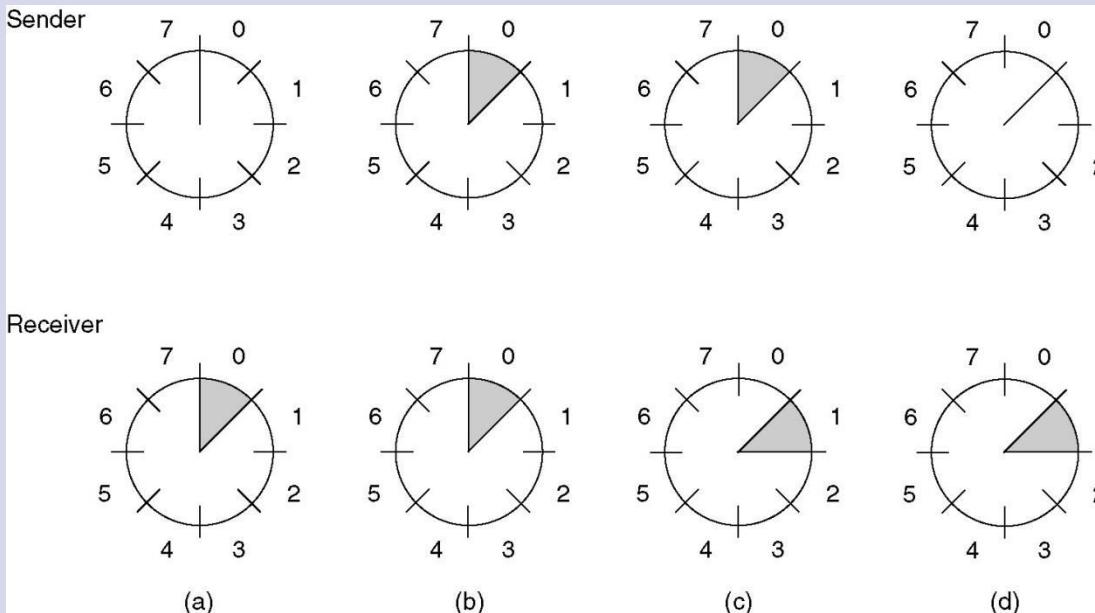


# Protokoly s klouzajícím okénkem

- Protokol s jednabitovým klouzajícím okénkem
- Protokol se sekvenčním příjemem ( Go Back N)
- Protokol s nesekvenčním příjemem (Selective Repeat)



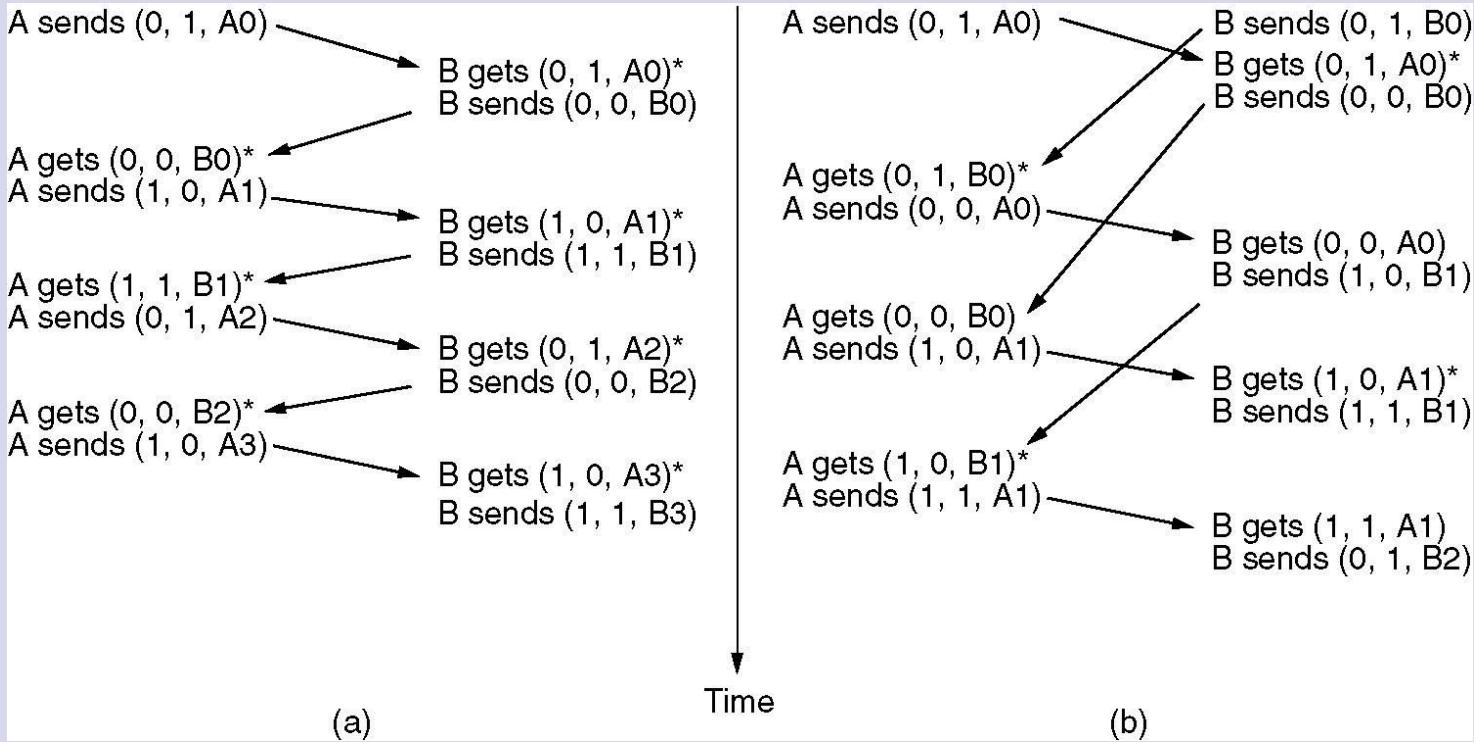
# Protokoly s klouzajícím okénkem (2)



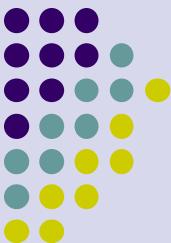
Klouzající okénko velikosti 1 s š bitovým sekvenčním číslem.

- (a) Počáteční nastavení.
- (b) Po odeslání prvního rámce.
- (c) Po přijetí prvního rámce.
- (d) Po přijetí potvrzení prvního rámce.

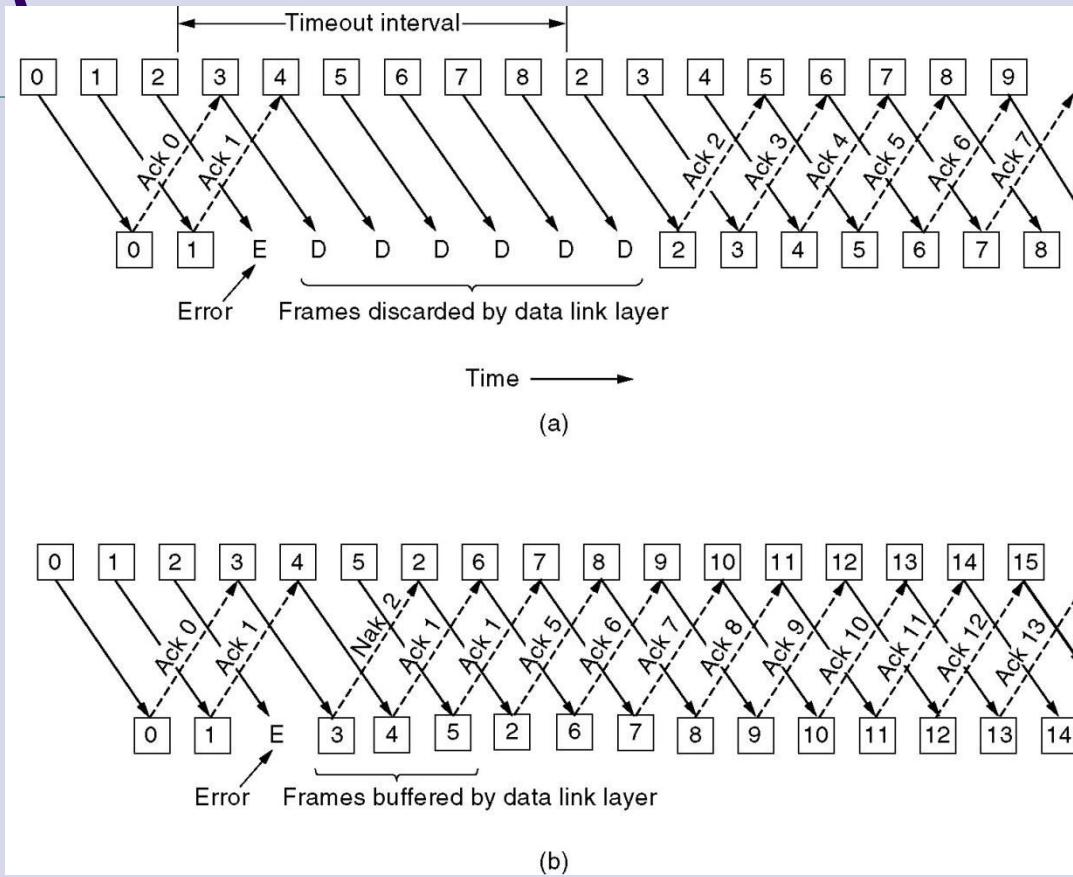
# Protokol s klouzajícím jednobitovým okénkem (2)



Dvě situace protokolu. (a) normální případ. (b) nenormální případ.  
V závorkách (seq, ack, č. paketu).  
Hvězdička znamená přijetí paketu síťovou úrovní.



# Protokol se sekvenčním příjemem (Go Back N')



Proudové zpracování a obnova po chybě. Působení chyby při:

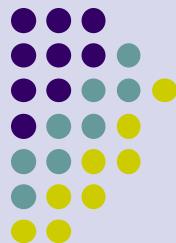
(a) Velikosti okna příjemce 1.

(b) Velikosti okna příjemce > 1.

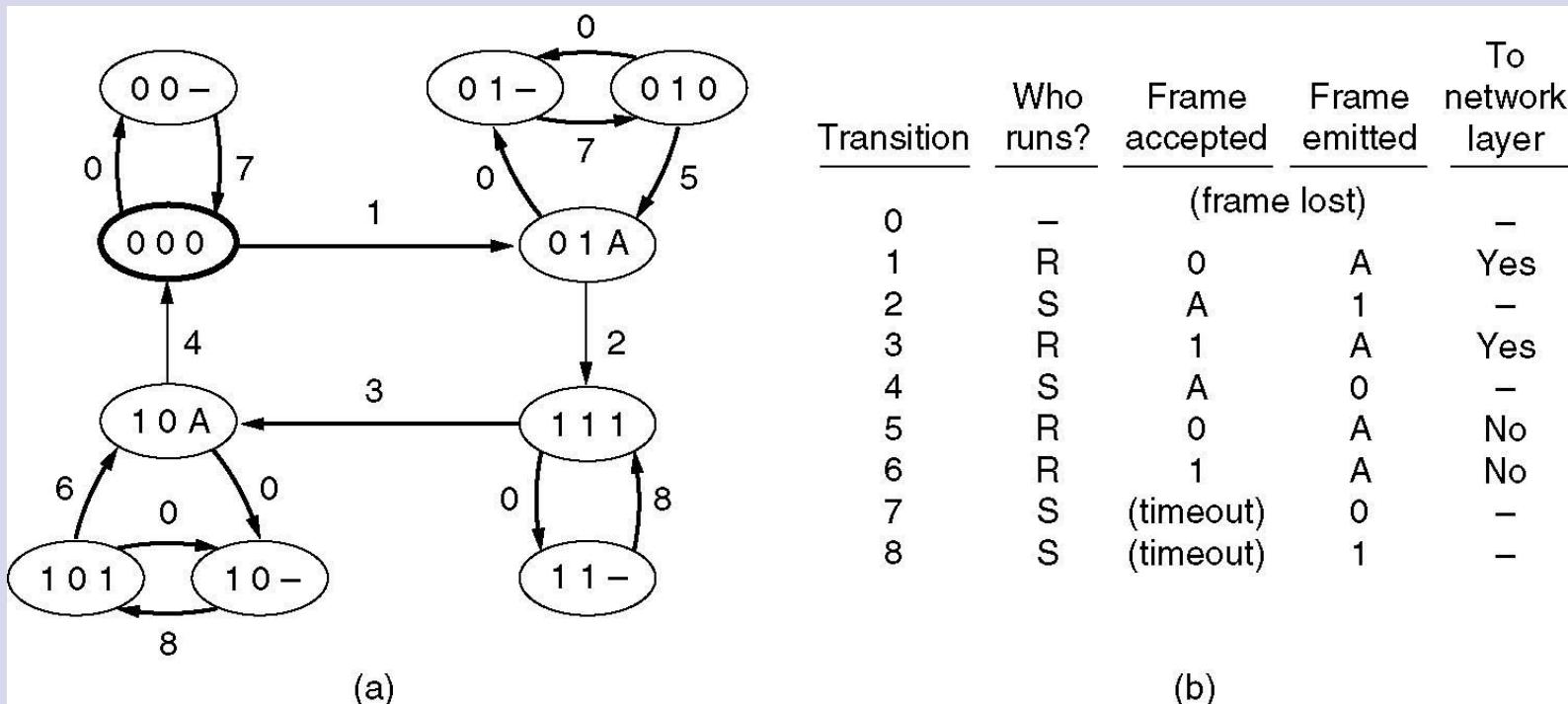


# Verifikace protokolů

- Modely založené na konečných automatech
- Modely založené na Petriho sítích



# Konečně automatový model

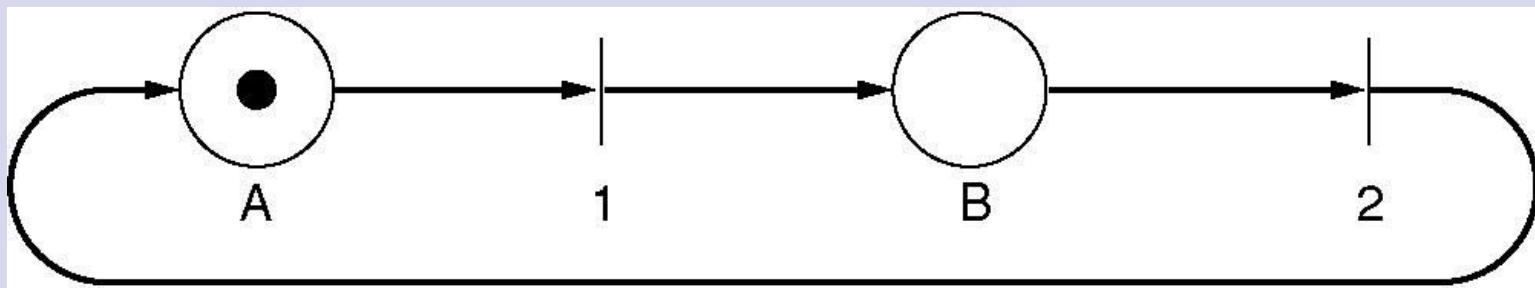


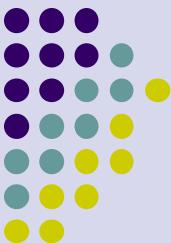
(a) Stavový diagram protokolu. (b) přechody.



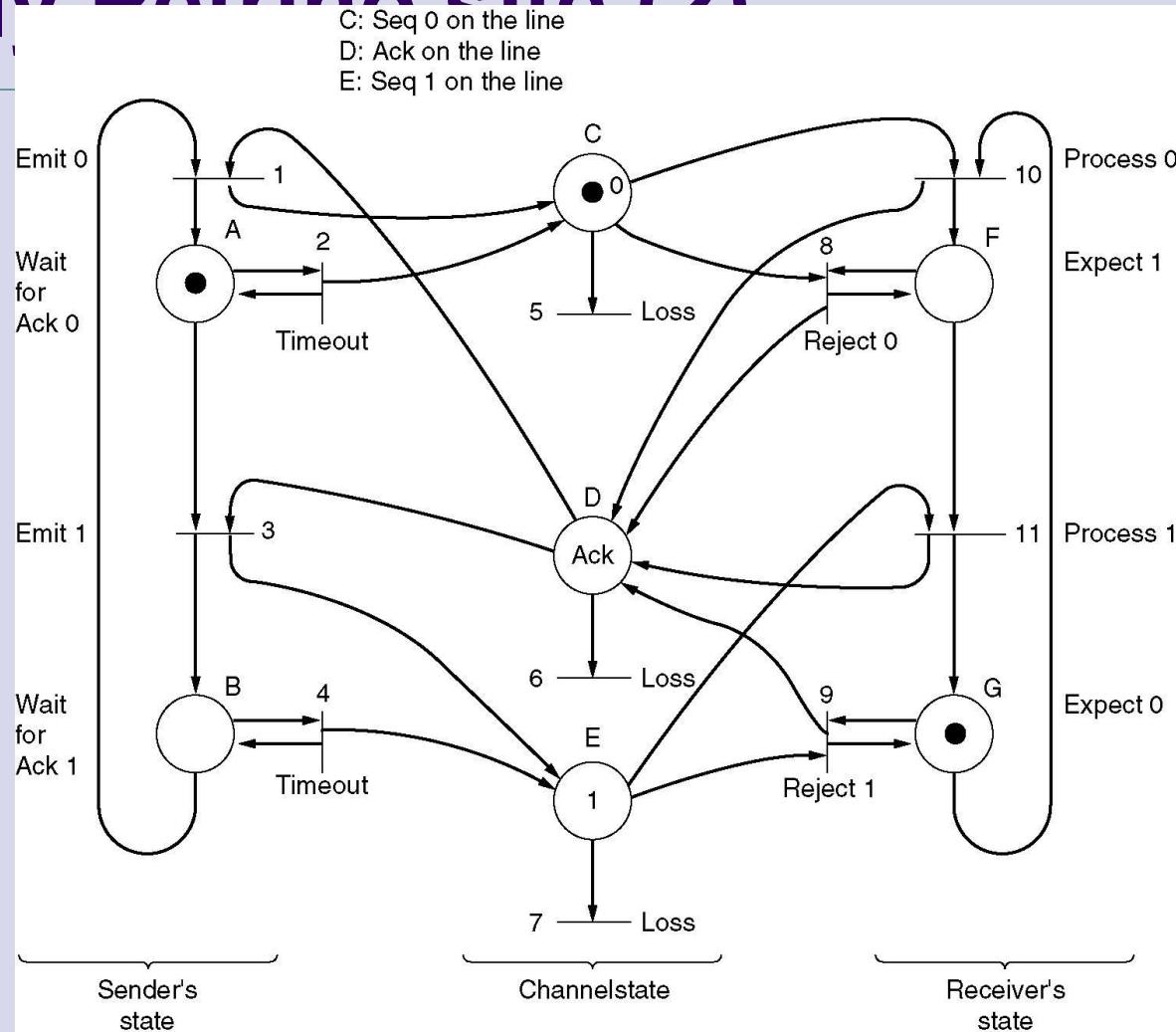
# Modely Petriho sítě

Petriho síť se dvěma místy a dvěma přechody.

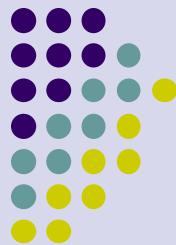




# Modely Petriho sítí (2)



Model protokolu realizovaný Petriho sítí.



# Příklad linkových protokolů

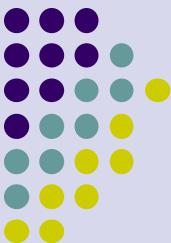
- HDLC – High-Level Data Link Control
- Linková úroveň Internetu

# High-Level Data Link Control (HDLC)



Formát rámce bitově orientovaného protokolu.

Bits	8	8	8	$\geq 0$	16	8
	0 1 1 1 1 1 1 0	Address	Control	Data	Checksum	0 1 1 1 1 1 1 0



# HDLC (2)

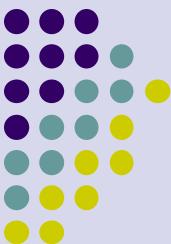
Bits	1	3	1	3
(a)	0	Seq	P/F	Next
(b)	1	0	Type	P/F
(c)	1	1	Type	Modifier

## Řídící pole

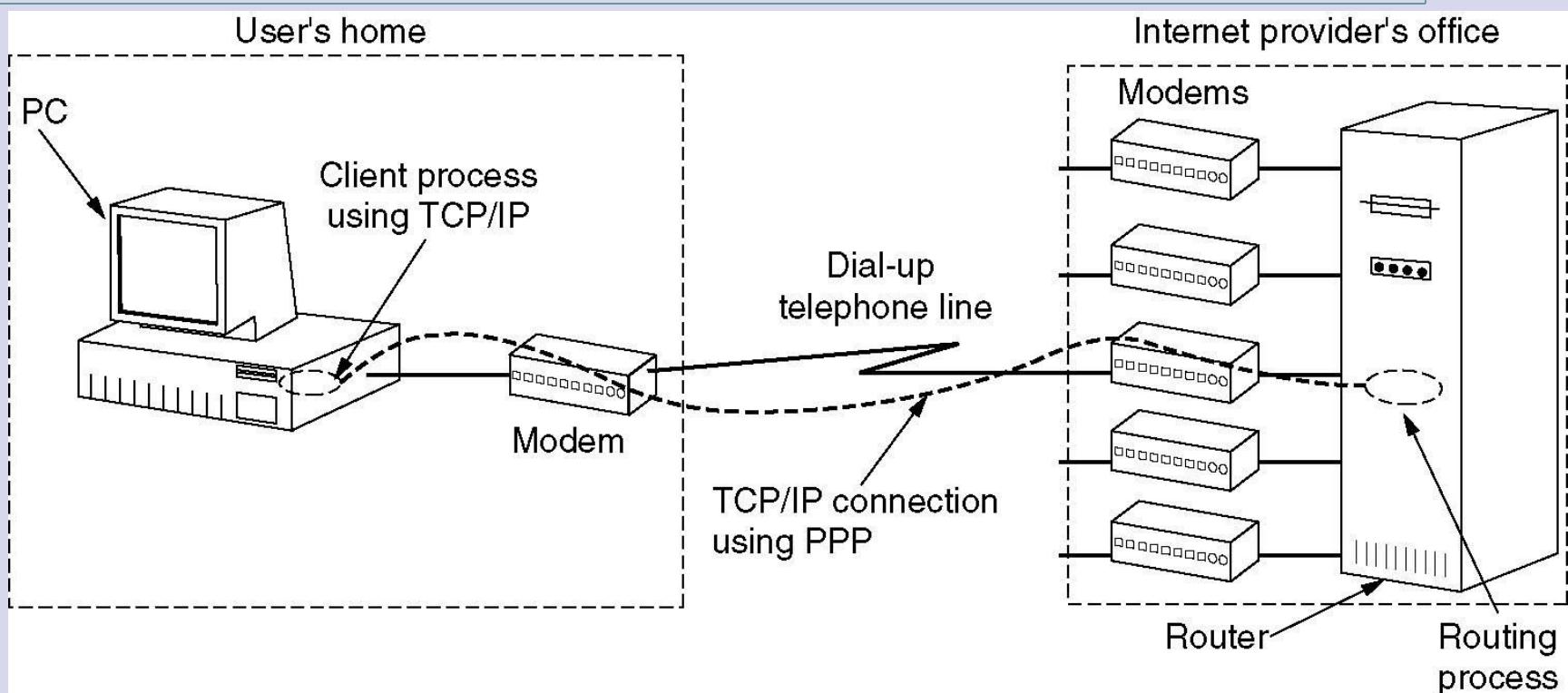
(a) Informačního rámce.

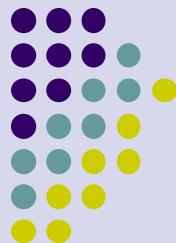
(b) Řídicího rámce.

(c) Nečíslovaného rámce.



# Linková úroveň v Internetu

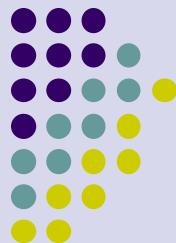




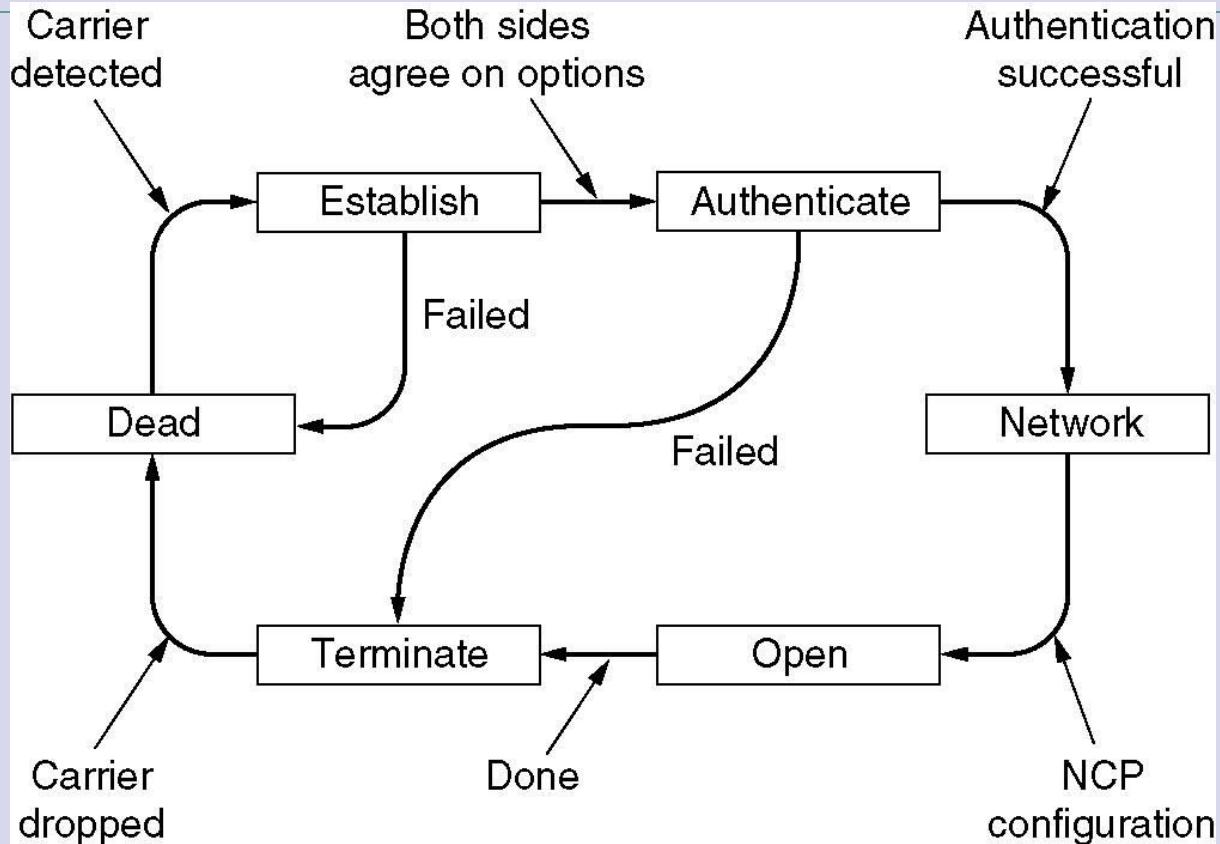
# PPP – Point to Point Protocol

Úplný rámec PPP pro nečíslované operace.

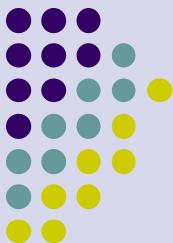
Bytes	1	1	1	1 or 2	Variable	2 or 4	1
	Flag 01111110	Address 11111111	Control 00000011	Protocol	Payload }} {{	Checksum	Flag 01111110



# PPP – Point to Point Protocol (2)



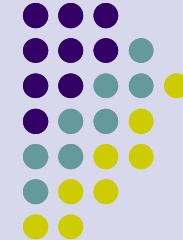
Zjednodušený diagram pro vytvoření a rušení PPP spojení.



# PPP – Point to Point Protocol (3)

Name	Direction	Description
Configure-request	I → R	List of proposed options and values
Configure-ack	I ← R	All options are accepted
Configure-nak	I ← R	Some options are not accepted
Configure-reject	I ← R	Some options are not negotiable
Terminate-request	I → R	Request to shut the line down
Terminate-ack	I ← R	OK, line shut down
Code-reject	I ← R	Unknown request received
Protocol-reject	I ← R	Unknown protocol requested
Echo-request	I → R	Please send this frame back
Echo-reply	I ← R	Here is the frame back
Discard-request	I → R	Just discard this frame (for testing)

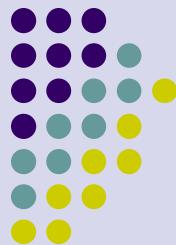
# Lokální počítačové sítě



Úvod do počítačových sítí

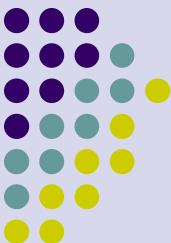
Lekce 07

Ing. Jiří lédvina, CSc.



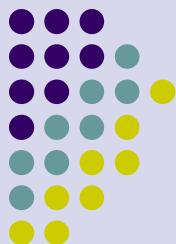
# Lokální počítačové sítě

- Protokoly náhodného přístupu
  - ALOHA, synchronizovaná ALOHA
  - CSMA, naléhající, nenaléhající, p-naléhající CSMA
  - CSMA/CD – CSMA s detekcí kolize
- Protokoly rovnoměrného přístupu
  - Protokol s bitovým okénkem
  - Protokol MLMA (Multi-Level-Multi-Access)
  - Token Ring – kruhová síť s předáváním pověření
  - Token Bus – sběrnicová síť s předáváním pověření



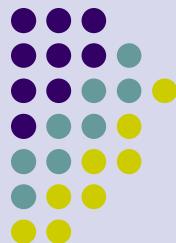
# Lokální počítačové sítě

- Protokoly s prioritním přístupem
- Problém monopolizace přístupu
  - Vícebitová priorita
  - Jednobitová priorita
- Způsoby zadávání priority
  - Priorita zadaná kódem
  - Priorita zadaná časem
  - Kombinované systémy



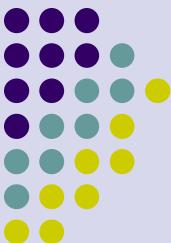
# Lokální počítačové sítě

- Ethernet
  - Metoda náhodného přístupu, sběrnicová nebo hvězdicová topologie, 10Mb/s až 1Gb/s, rozlehlosť stovky metrů až několik km, nejrozšírenější lokální síť.
- Typy sítě Ethernet:
  - IEEE 802.3, Ethernet II:
    - 10BASE-5, 10BASE-2, 10BASE-T
  - Fast Ethernet (IEEE 802.3u):
    - 100BASE-TX (100m, UTP 5)
    - 100BASE-FX (2000m, MMF)
  - Gigabit Ethernet (IEEE 802.3z):
    - 1000BASE-SX (550m, MMF 50µm, 62,5µm)
    - 1000BASE-LX (5000m, SMF 10µm, MMF)
    - 1000BASE-T (100m, 4 páry UTP 5)
    - 1000BASE-CX (25m, 2 páry STP)



# Lokální počítačové sítě

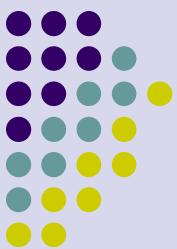
- Token Ring
  - Kruhová síť, kroucená dvojlinka, 4 nebo 16 Mb/s, metoda předávání pověření, 250 stanic v kruhu, odolnost proti poruchám.
  - Multiple access unit - MAU
  - Přenos dat – token a data
  - Priorita
  - Rekonstrukce kruhu – algoritmus výběru 1 z N
- FDDI
  - Optická síť, kruhová topologie (dvojitý kruh), metoda předávání pověření, 100Mb/s, 100km, páteřní sítě, propojení rychlých stanic.



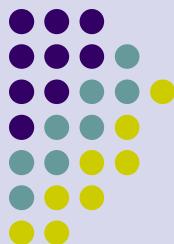
# Lokální počítačové sítě

- Token Bus
  - Sběrnicová síť s předáváním pověření
  - Typy rámců a operace
    - Přenos dat (Token, data)
    - Výpadek uzlu (Who follows)
    - Přidání uzlu (Solicit successor, Set successor)
    - Kolize při přidávání (Resolve contention)
    - Vytvoření sítě (Claim token)
  - Priority
    - Token Holding Time - THT
    - Token Rotation Time - TRT

# Asynchronous Transfer Mode - ATM

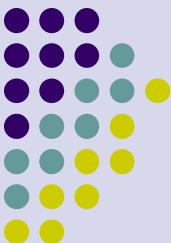


- Použití ve všech typech sítí (lokální, metropolitní, rozlehlé)
  - Přenos hlasu, videa a dat
  - Přenos optickými vlákny, rychlosť přenosu až jednotky Gb/s, dvoubodové spoje, přepínaná síť (používá přepínače).
  - Základní přenosová jednotka buňka (53 slabik, 5 řídicích, 48 datových).
  - Vytváří virtuální okruhy (vytvoření, přenos dat, rušení).
  - Pevné okruhy, přepínané okruhy, virtuální okruh, virtuální cesta.
  - Různé druhy přenosu – přenosy v reálném čase (zvuku, videa), přenos dat.
  - Původně zamýšlen jako náhrada ostatních přenosových technologií



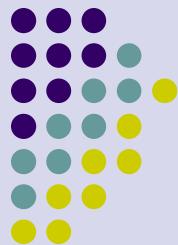
# Bezdrátové sítě

- Topologie bezdrátových sítí
  - Propojení dvou základních komponent.
    - PC karta s přijímačem, vysílačem a integrovanou anténou.
    - Přístupový bod (Access Point) pro propojení se sítí Ethernet.
  - Přístupový bod funguje jako most mezi drátovou a bezdrátovou sítí. Může obsahovat základní směrovací funkce.



# Bezdrátové sítě

- Standardy bezdrátových sítí
  - IEEE 802.11 (starší, 2 Mbps)
  - IEEE 802.11b (11 Mb/s, 2.4 GHz)
  - IEEE 802.11a (54 Mb/s, 5 GHz, v r.2002)
  - IEEE 802.11g (54 Mb/s, 2.4 GHz, v r.2002)
  - HiperLAN/2 (evropský standard, 54 Mb/s v pásmu 5 GHz)
  - IEEE 802.15 Personal Area Networks (Bluetooth)
  - IEEE 802.16 Bezdrátové širokopásmové sítě



# Přenosové technologie rozlehlých sítí

- ISDN – Integrated Services Digital Network
  - Digitální telefonní síť pro přenos hlasu i dat
  - Základní pásmo: 2B+1D
  - Primární pásmo: 23B+1D, 30B+1D
  - Multiplexování (T1, T2, T3, T4, E1, E2, E3, E4, E5)
- DSL – Digital Subscriber Line
  - Telefonní linka pronajatá uživatelem
  - Poskytování digitálních služeb
  - Poskytování DSL služeb prostřednictvím ISDN



# Přenosové technologie rozlehlých sítí

- ASDL – Asymmetric DSL
  - Není založeno na ISDN
  - Video-on-demand, 8Mb/s, 1MB/s
- VSDL – Very-high-speed DSL
  - Není založeno na ISDN
  - 20Mb/s symetricky
  - 52Mb/s+1.5Mb/s nesymetricky
- Kabelové televizní rozvody
  - Kabelové modemy
  - Přenos telefonu, dat, videa
- GSM sítě

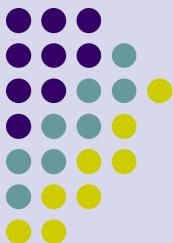
# **Hub, Bridge, Switch**



Úvod do počítačových sítí

Lekce 08

Ing. Jiří lédvina, CSc.

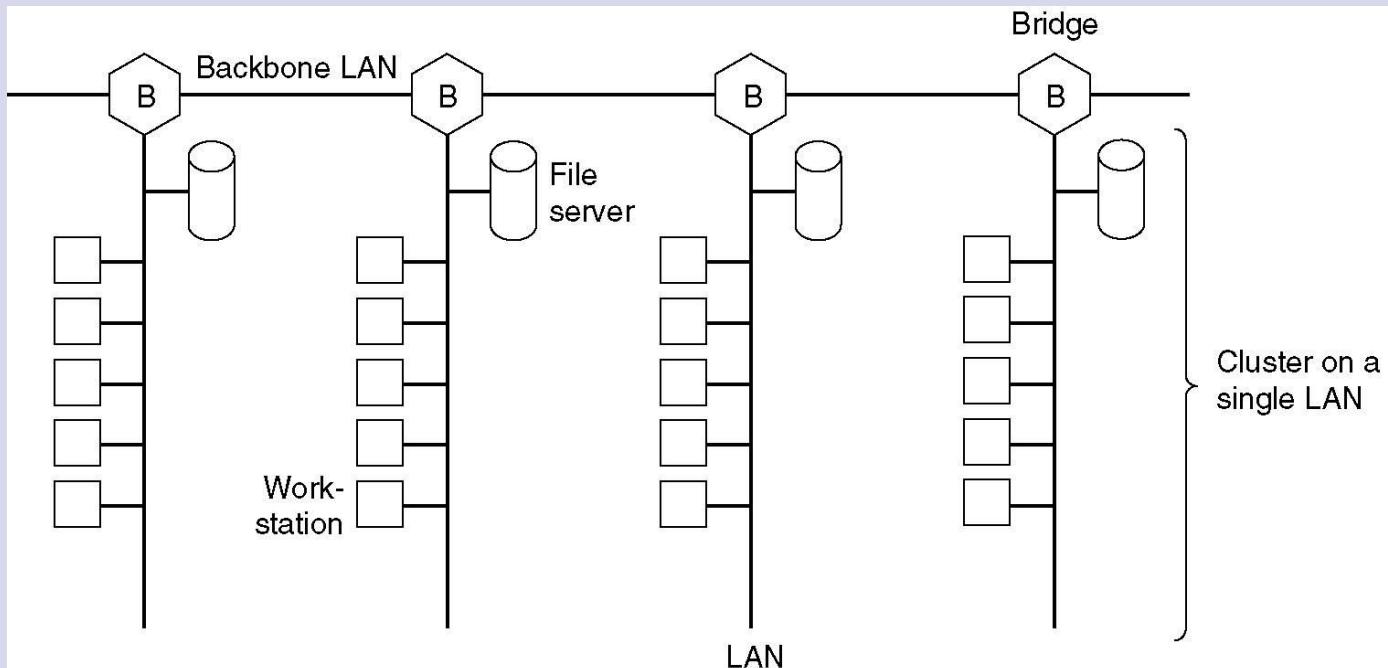


# Přepínání na linkové úrovni

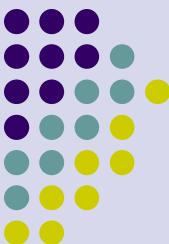
- Mosty mezi 802.x a 802.y
- Lokální Internetworking
- Mosty se spanning tree algoritmem (nalezení kostry grafu)
- Vzdálené mosty
- Opakovače, rozbočovače (Hubs), mosty, přepínače, směrovače, brány
- Virtuální lokální počítačové sítě



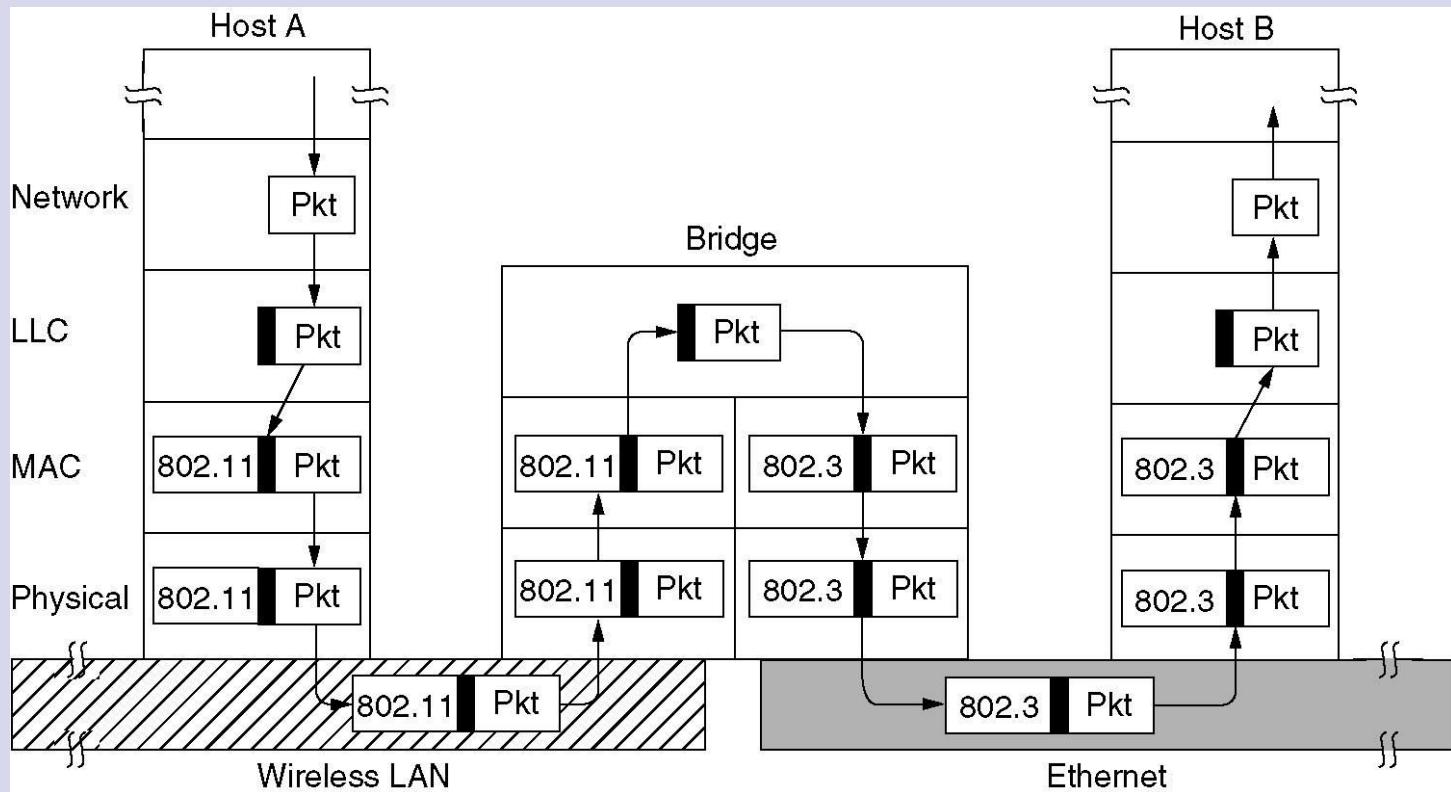
# Přepínání na linkové úrovni



Několik sítí LAN připojených do páteřní sítě s propustností větší než mají jednotlivé LAN..



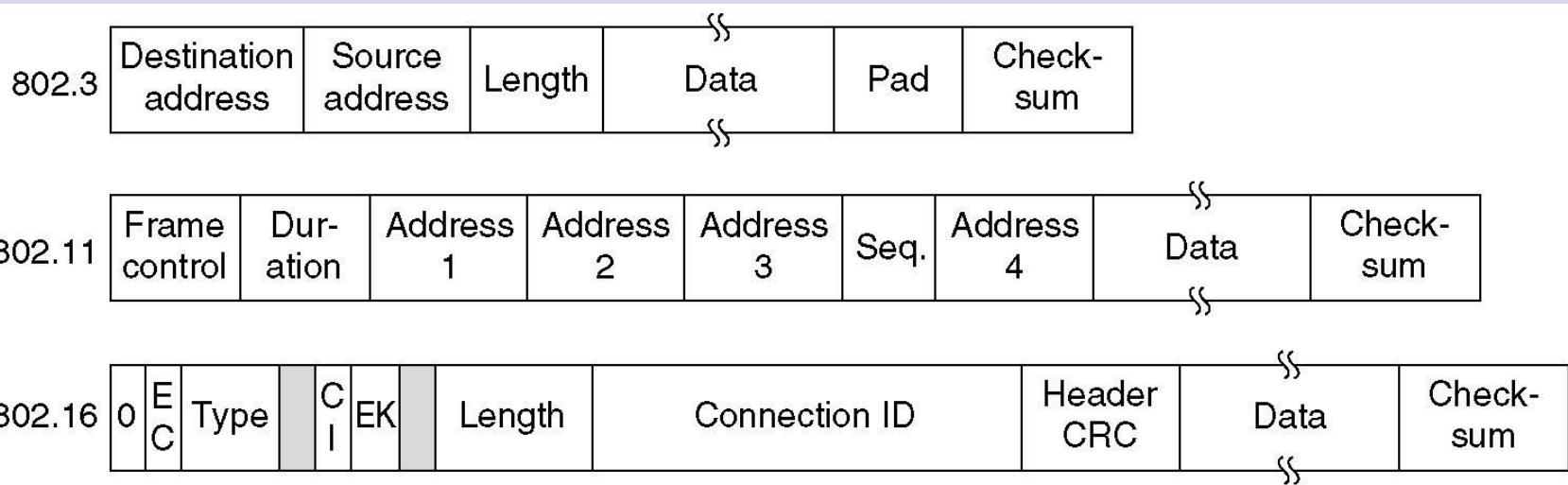
# Mosty mezi 802.x a 802.y



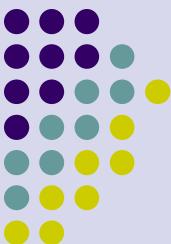
Znázornění mostu mezi dvěma sítěmi LAN (802.11 a 802.3).



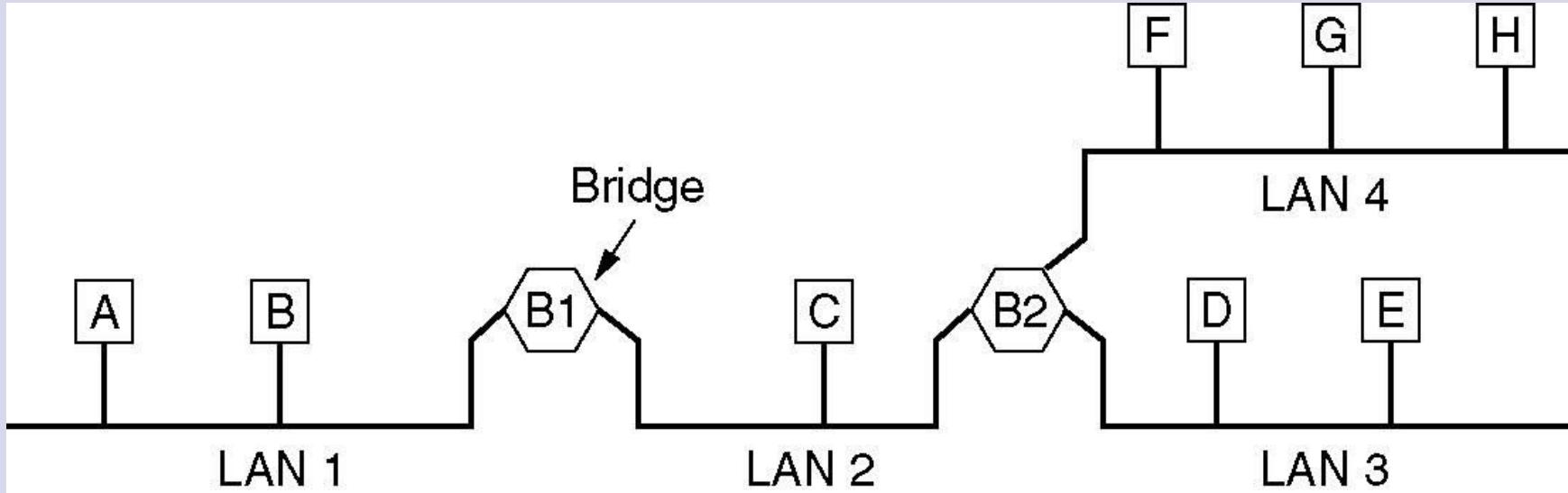
# Mosty mezi 802.x a 802.y (2)



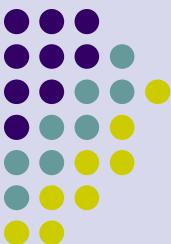
Různé formáty rámce IEEE 802.



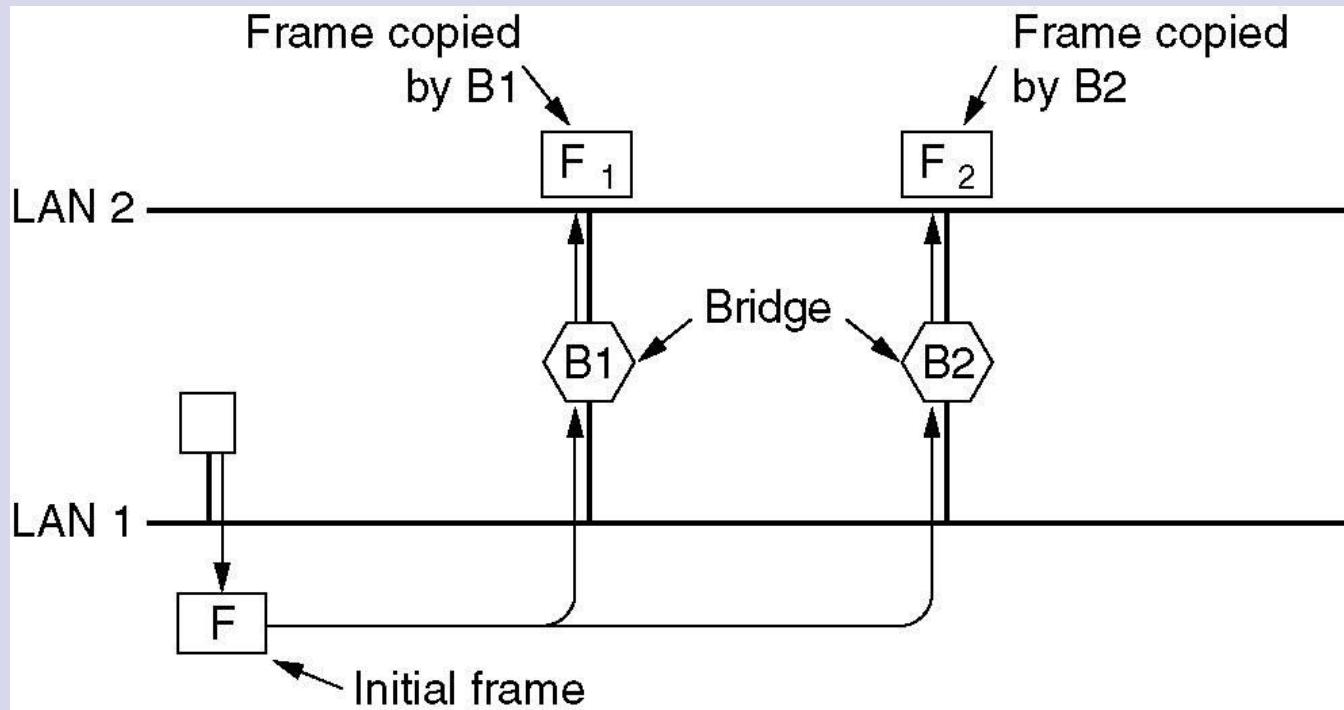
# Lokální Internetworking



Propojení 4 LAN a dvou mostů.

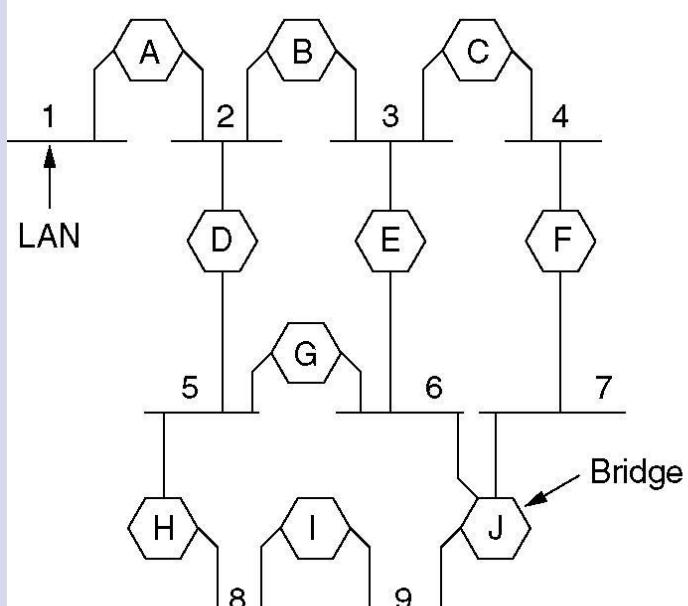
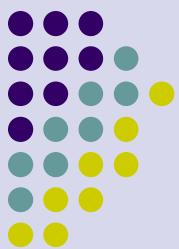


# Mosty se spanning tree algoritmem

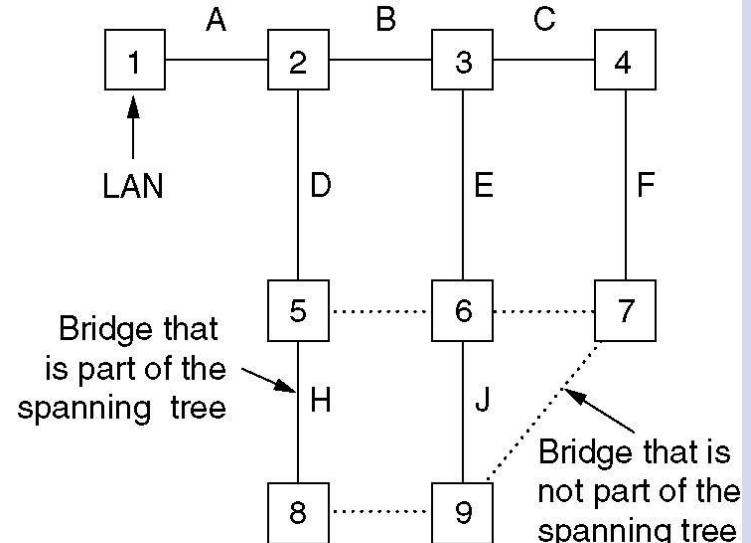


Dva paralelní transparentní mosty.

# Mosty se spanning tree algoritmem (2)

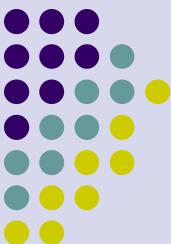


(a)

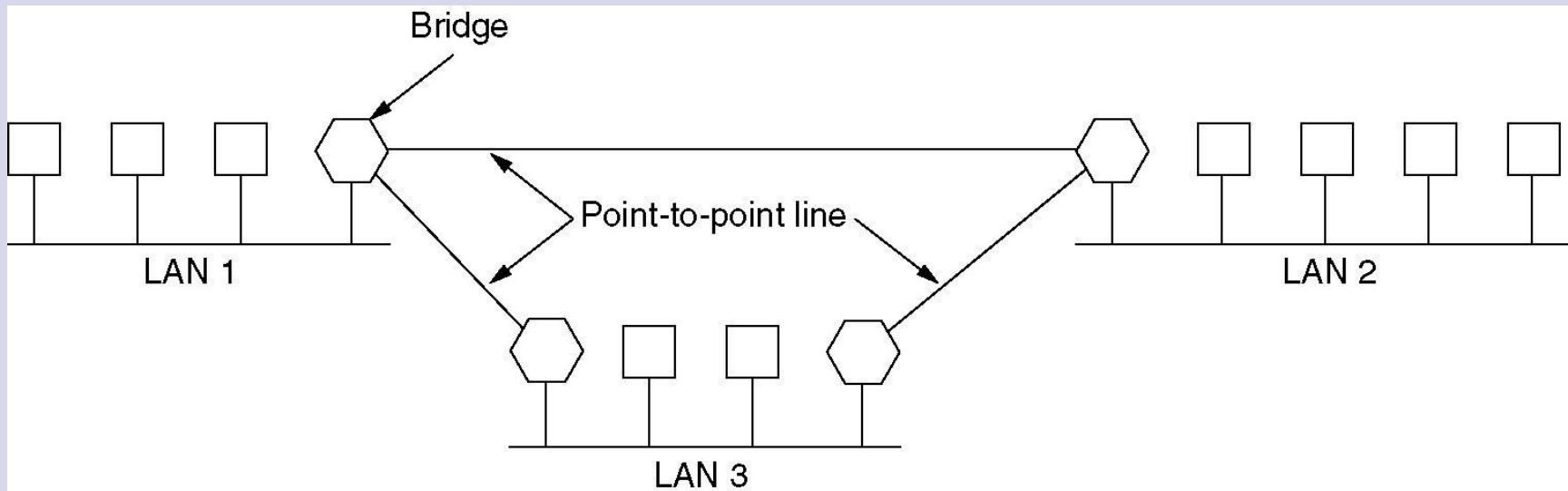


(b)

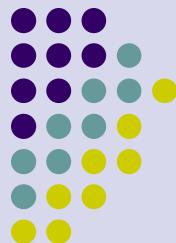
(a) Propojené LAN. (b) vytvoření kostry LAN. Tečkované čáry nejsou součástí kostry.



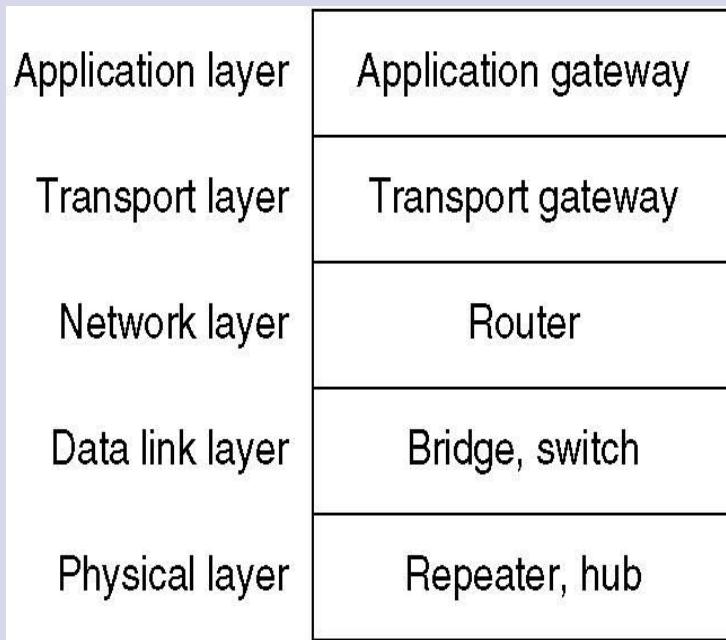
# Vzdálené mosty



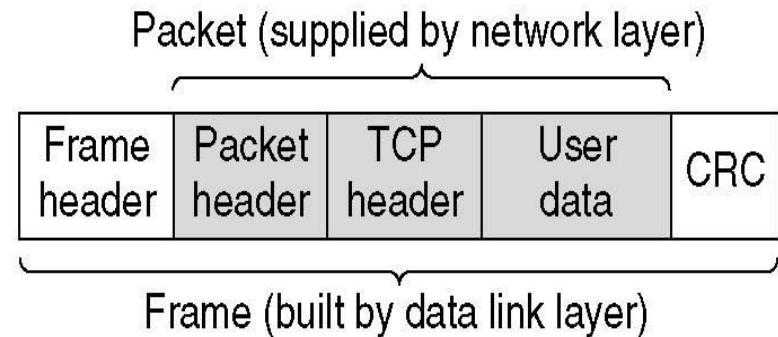
Vzdálené mosty mohou být použity pro propojení vzdálených LAN.



# Opakovače, rozbočovače (Hubs), mosty, přepínače, směrovače a brány

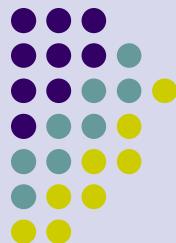


(a)

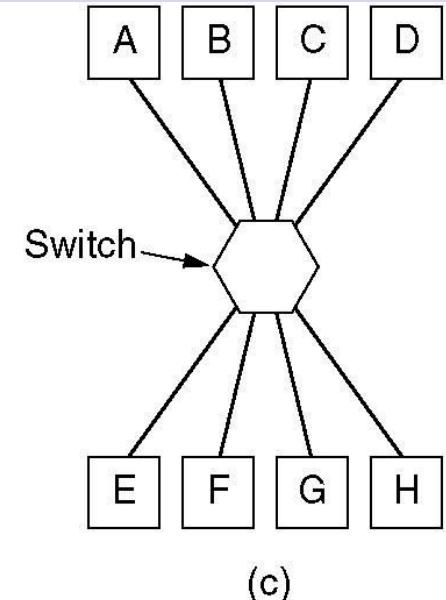
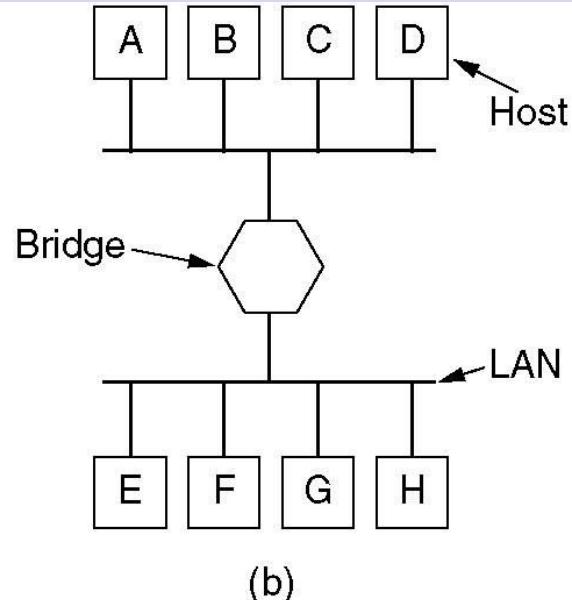
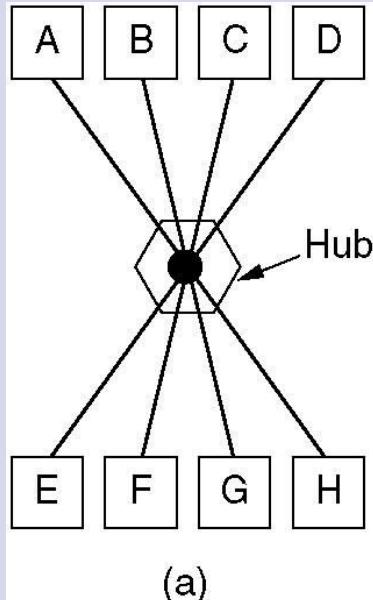


(b)

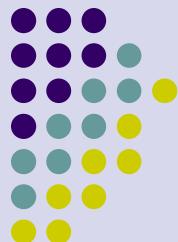
- (a) Zařízení na jednotlivých úrovních.
- (b) Rámce pakety a záhlaví.



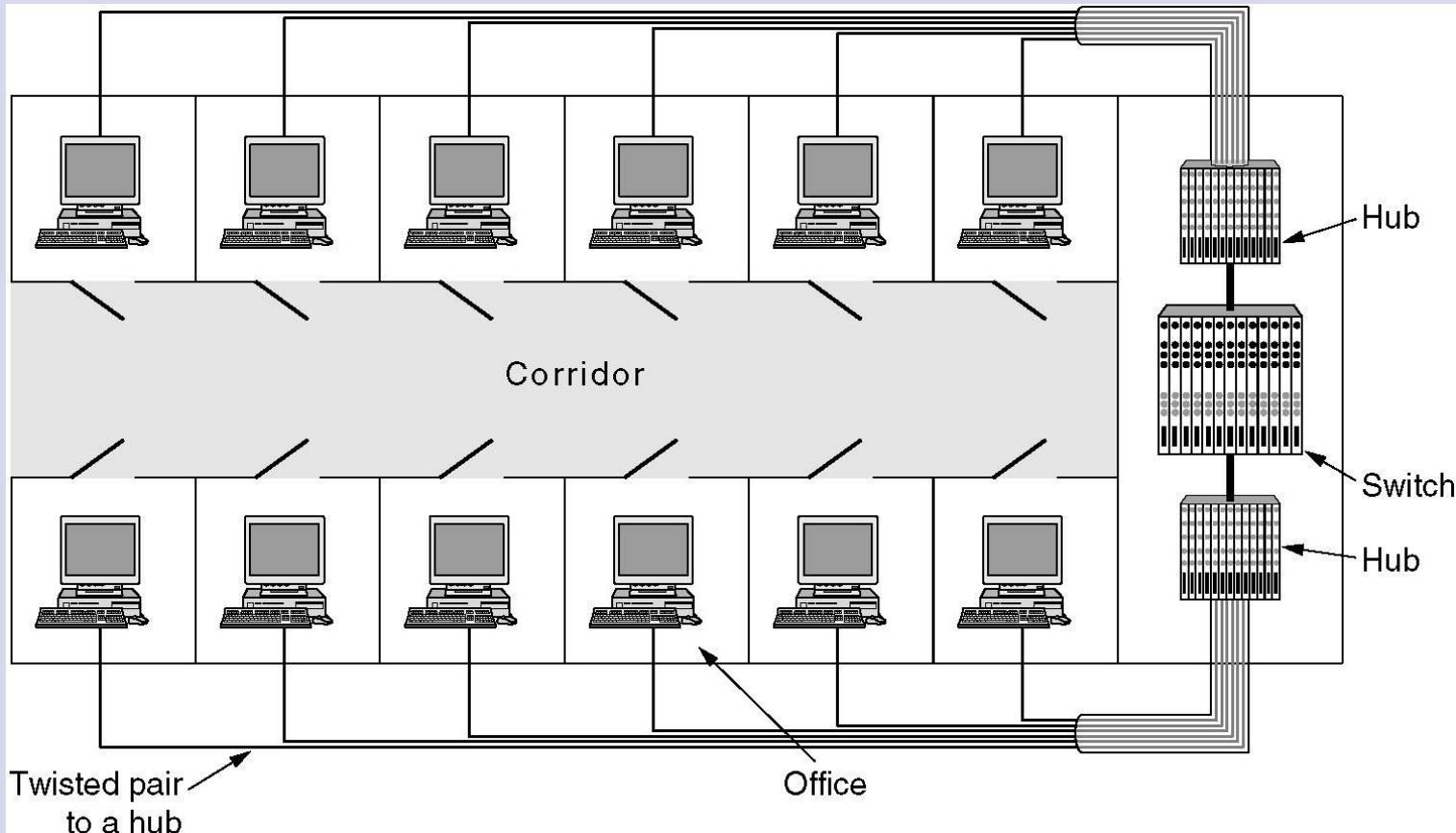
# Opakovače, rozbočovače (Hubs), mosty, přepínače, směrovače a brány (2)



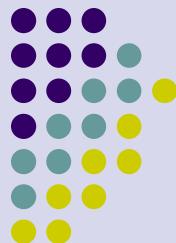
(a) Hub. (b) most. (c) přepínač.



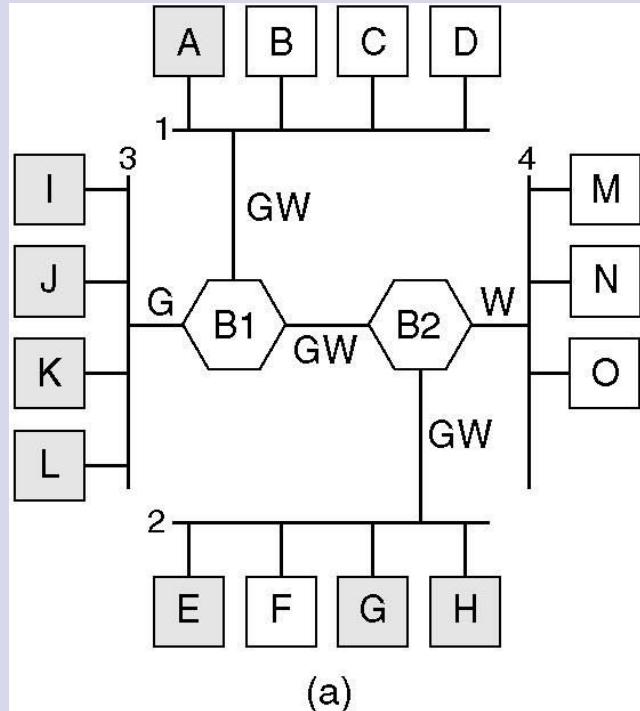
# Virtuální lokální počítačové sítě



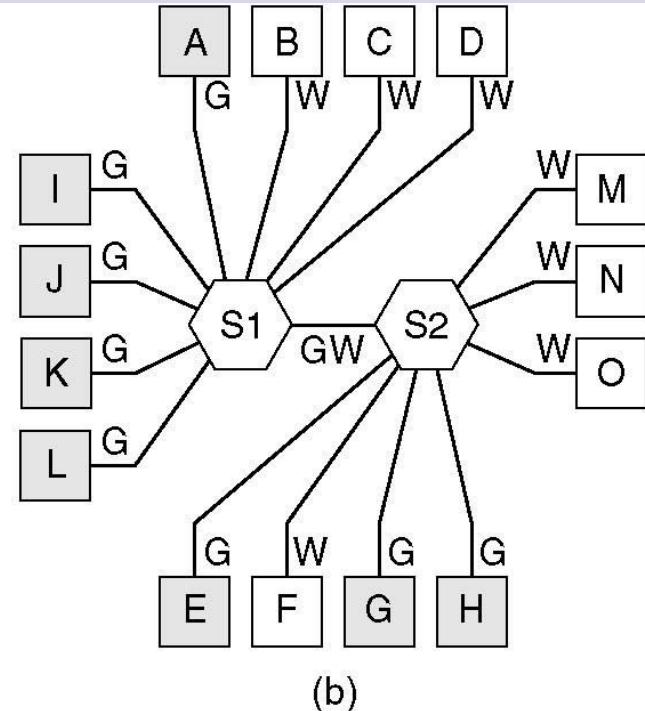
Strukturovaná kabeláž s použitím hubů a přepínače.



# Virtuální lokální počítačové sítě (2)

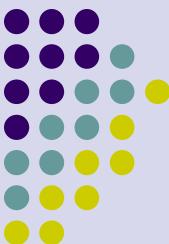


(a)

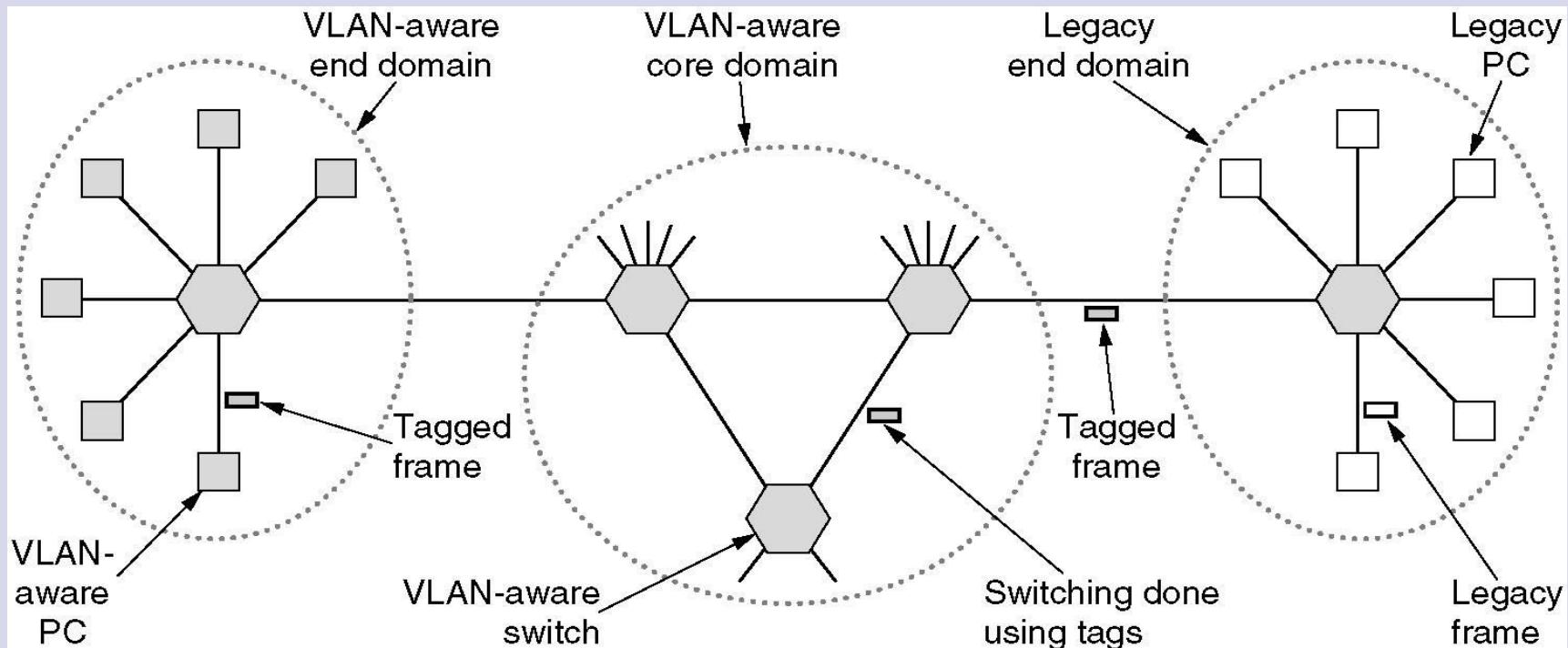


(b)

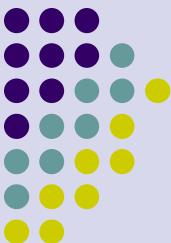
- (a) 4 fyzické LAN uspořádané do 2 VLAN (bílé a šedé) pomocí dvou mostů.
- (b) Totéž uspořádané do 2 VLAN pomocí dvou přepínačů.



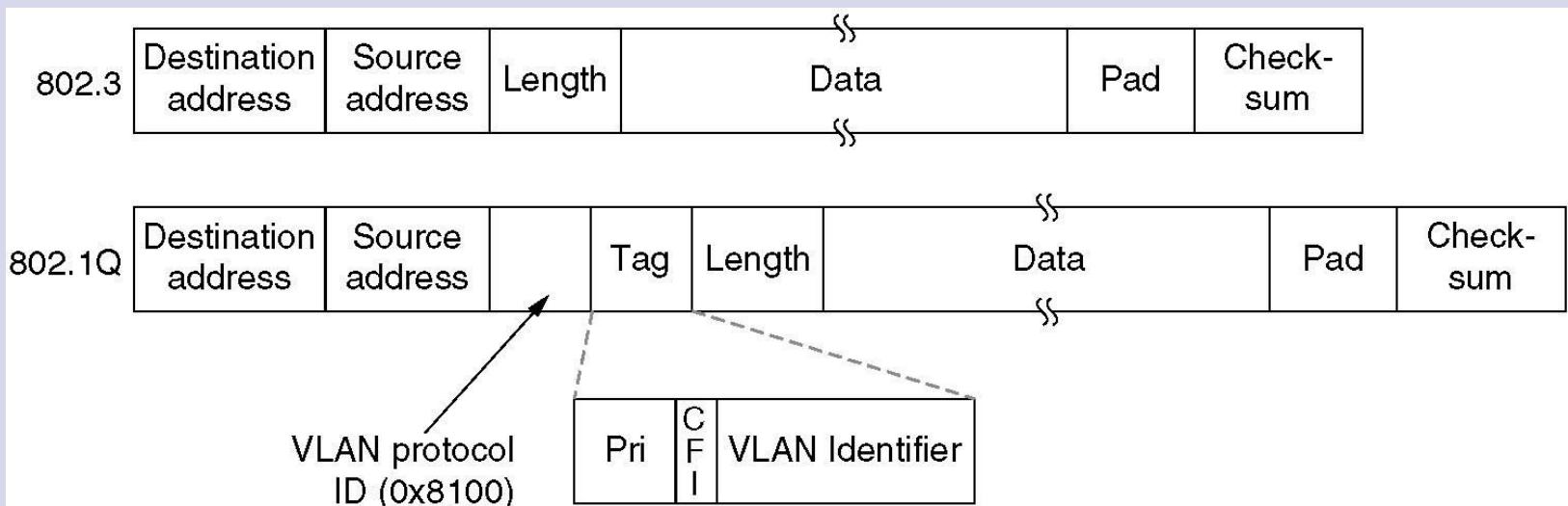
# Standard IEEE 802.1Q



Přechod z tradičního Ethernetu do přepínaného Ethernetu. Šedé komponenty jsou VLAN-ové, prázdné ne.

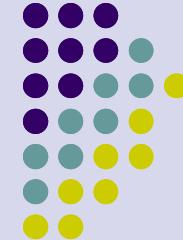


# Standard IEEE 802.1Q (2)



Porovnání klasického formátu 802.3 rámce s 802.1Q rámcem.

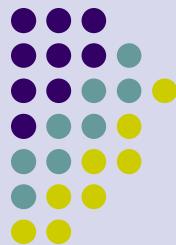
# Lokální počítačové sítě



Úvod do počítačových sítí

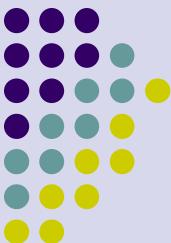
Lekce 07

Ing. Jiří lédvina, CSc.



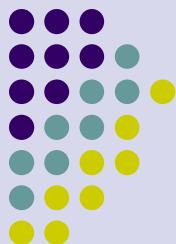
# Lokální počítačové sítě

- Protokoly náhodného přístupu
  - ALOHA, synchronizovaná ALOHA
  - CSMA, naléhající, nenaléhající, p-naléhající CSMA
  - CSMA/CD – CSMA s detekcí kolize
- Protokoly rovnoměrného přístupu
  - Protokol s bitovým okénkem
  - Protokol MLMA (Multi-Level-Multi-Access)
  - Token Ring – kruhová síť s předáváním pověření
  - Token Bus – sběrnicová síť s předáváním pověření



# Lokální počítačové sítě

- Protokoly s prioritním přístupem
- Problém monopolizace přístupu
  - Vícebitová priorita
  - Jednobitová priorita
- Způsoby zadávání priority
  - Priorita zadaná kódem
  - Priorita zadaná časem
  - Kombinované systémy



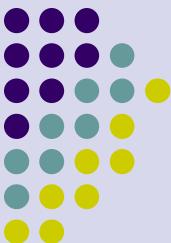
# Lokální počítačové sítě

- Ethernet
  - Metoda náhodného přístupu, sběrnicová nebo hvězdicová topologie, 10Mb/s až 1Gb/s, rozlehlosť stovky metrů až několik km, nejrozšírenější lokální síť.
- Typy sítě Ethernet:
  - IEEE 802.3, Ethernet II:
    - 10BASE-5, 10BASE-2, 10BASE-T
  - Fast Ethernet (IEEE 802.3u):
    - 100BASE-TX (100m, UTP 5)
    - 100BASE-FX (2000m, MMF)
  - Gigabit Ethernet (IEEE 802.3z):
    - 1000BASE-SX (550m, MMF 50µm, 62,5µm)
    - 1000BASE-LX (5000m, SMF 10µm, MMF)
    - 1000BASE-T (100m, 4 páry UTP 5)
    - 1000BASE-CX (25m, 2 páry STP)



# Lokální počítačové sítě

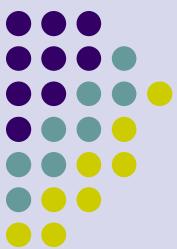
- Token Ring
  - Kruhová síť, kroucená dvojlinka, 4 nebo 16 Mb/s, metoda předávání pověření, 250 stanic v kruhu, odolnost proti poruchám.
  - Multiple access unit - MAU
  - Přenos dat – token a data
  - Priorita
  - Rekonstrukce kruhu – algoritmus výběru 1 z N
- FDDI
  - Optická síť, kruhová topologie (dvojitý kruh), metoda předávání pověření, 100Mb/s, 100km, páteřní sítě, propojení rychlých stanic.



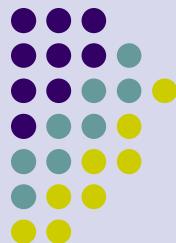
# Lokální počítačové sítě

- Token Bus
  - Sběrnicová síť s předáváním pověření
  - Typy rámců a operace
    - Přenos dat (Token, data)
    - Výpadek uzlu (Who follows)
    - Přidání uzlu (Solicit successor, Set successor)
    - Kolize při přidávání (Resolve contention)
    - Vytvoření sítě (Claim token)
  - Priority
    - Token Holding Time - THT
    - Token Rotation Time - TRT

# Asynchronous Transfer Mode - ATM

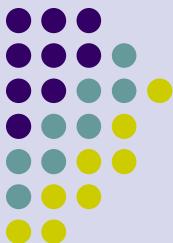


- Použití ve všech typech sítí (lokální, metropolitní, rozlehlé)
  - Přenos hlasu, videa a dat
  - Přenos optickými vlákny, rychlosť přenosu až jednotky Gb/s, dvoubodové spoje, přepínaná síť (používá přepínače).
  - Základní přenosová jednotka buňka (53 slabik, 5 řídicích, 48 datových).
  - Vytváří virtuální okruhy (vytvoření, přenos dat, rušení).
  - Pevné okruhy, přepínané okruhy, virtuální okruh, virtuální cesta.
  - Různé druhy přenosu – přenosy v reálném čase (zvuku, videa), přenos dat.
  - Původně zamýšlen jako náhrada ostatních přenosových technologií



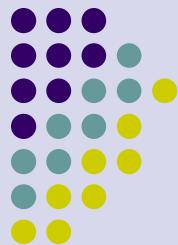
# Bezdrátové sítě

- Topologie bezdrátových sítí
  - Propojení dvou základních komponent.
    - PC karta s přijímačem, vysílačem a integrovanou anténou.
    - Přístupový bod (Access Point) pro propojení se sítí Ethernet.
  - Přístupový bod funguje jako most mezi drátovou a bezdrátovou sítí. Může obsahovat základní směrovací funkce.



# Bezdrátové sítě

- Standardy bezdrátových sítí
  - IEEE 802.11 (starší, 2 Mbps)
  - IEEE 802.11b (11 Mb/s, 2.4 GHz)
  - IEEE 802.11a (54 Mb/s, 5 GHz, v r.2002)
  - IEEE 802.11g (54 Mb/s, 2.4 GHz, v r.2002)
  - HiperLAN/2 (evropský standard, 54 Mb/s v pásmu 5 GHz)
  - IEEE 802.15 Personal Area Networks (Bluetooth)
  - IEEE 802.16 Bezdrátové širokopásmové sítě



# Přenosové technologie rozlehlých sítí

- ISDN – Integrated Services Digital Network
  - Digitální telefonní síť pro přenos hlasu i dat
  - Základní pásmo: 2B+1D
  - Primární pásmo: 23B+1D, 30B+1D
  - Multiplexování (T1, T2, T3, T4, E1, E2, E3, E4, E5)
- DSL – Digital Subscriber Line
  - Telefonní linka pronajatá uživatelem
  - Poskytování digitálních služeb
  - Poskytování DSL služeb prostřednictvím ISDN



# Přenosové technologie rozlehlých sítí

- ASDL – Asymmetric DSL
  - Není založeno na ISDN
  - Video-on-demand, 8Mb/s, 1MB/s
- VSDL – Very-high-speed DSL
  - Není založeno na ISDN
  - 20Mb/s symetricky
  - 52Mb/s+1.5Mb/s nesymetricky
- Kabelové televizní rozvody
  - Kabelové modemy
  - Přenos telefonu, dat, videa
- GSM sítě

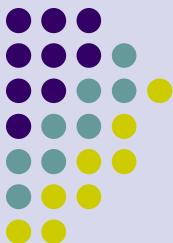
# **Hub, Bridge, Switch**



Úvod do počítačových sítí

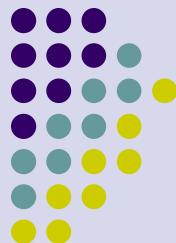
Lekce 08

Ing. Jiří lédvina, CSc.

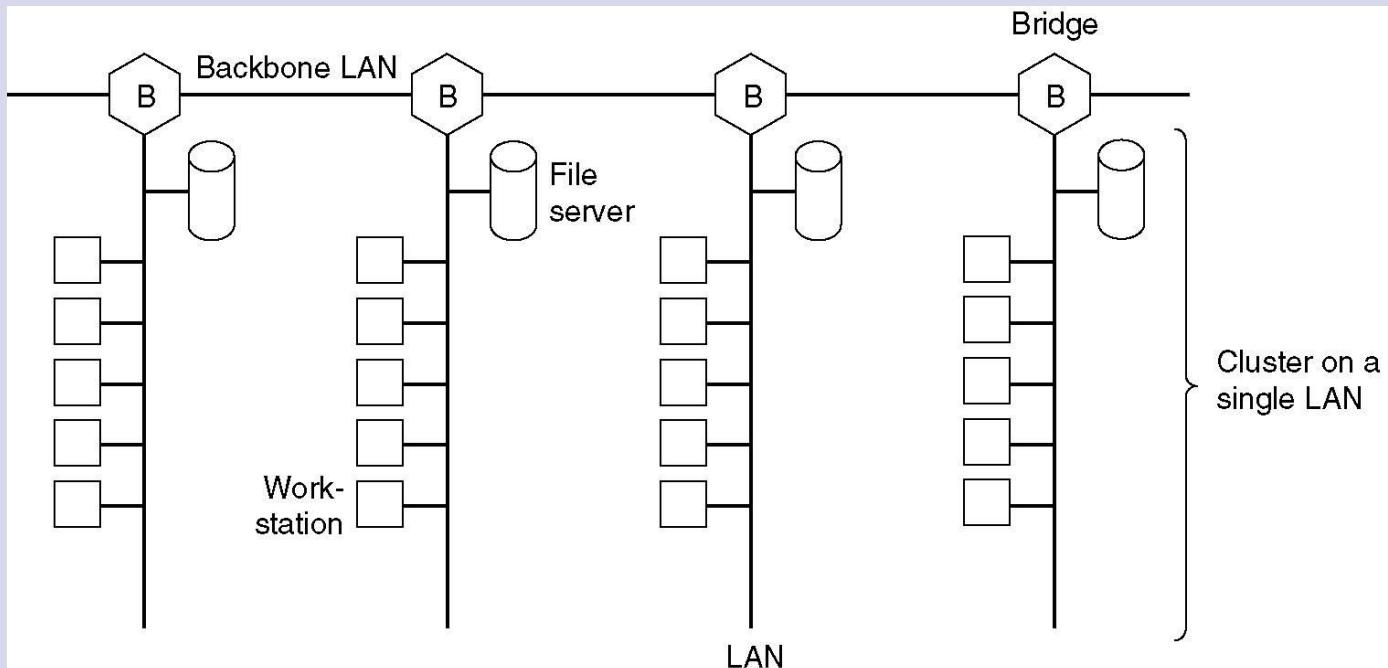


# Přepínání na linkové úrovni

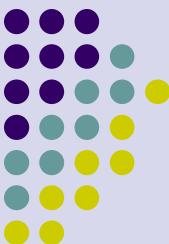
- Mosty mezi 802.x a 802.y
- Lokální Internetworking
- Mosty se spanning tree algoritmem (nalezení kostry grafu)
- Vzdálené mosty
- Opakovače, rozbočovače (Hubs), mosty, přepínače, směrovače, brány
- Virtuální lokální počítačové sítě



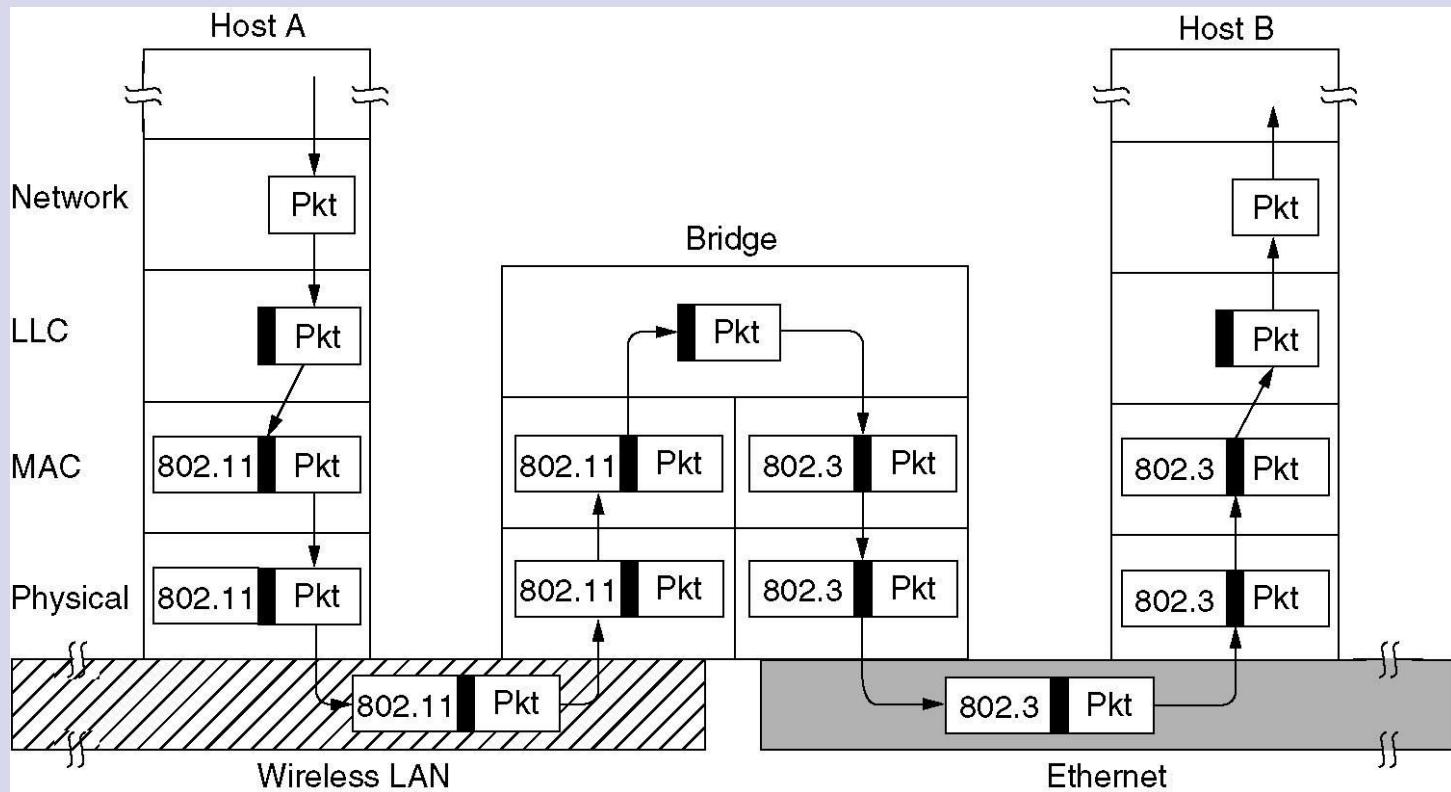
# Přepínání na linkové úrovni



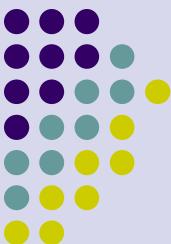
Několik sítí LAN připojených do páteřní sítě s propustností větší než mají jednotlivé LAN..



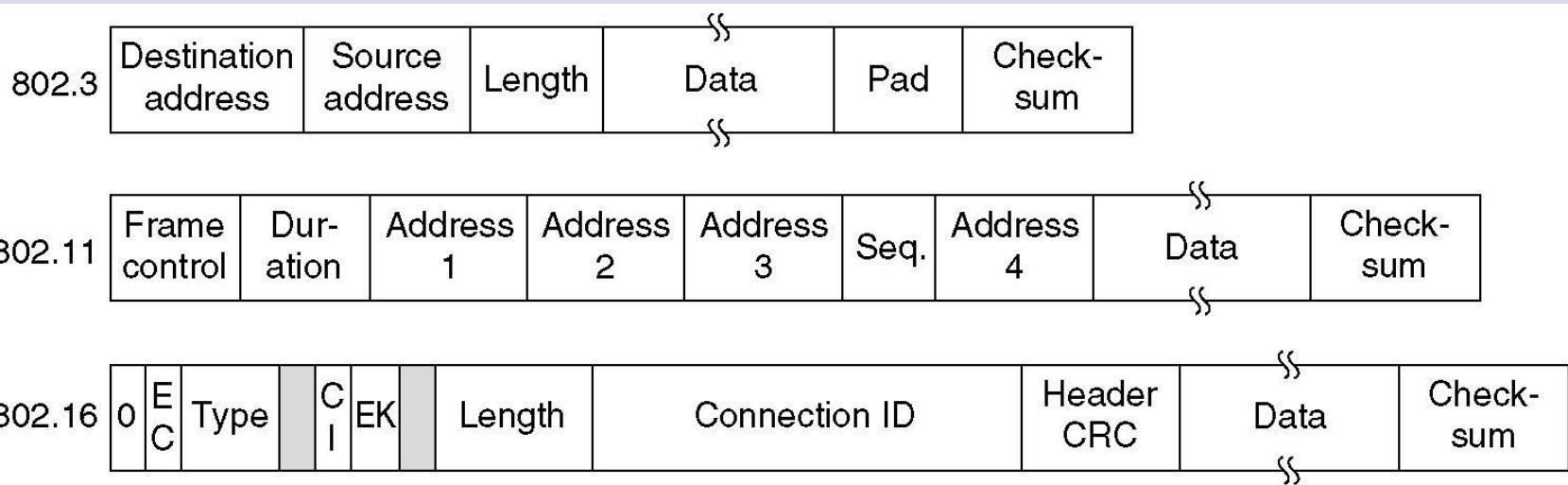
# Mosty mezi 802.x a 802.y



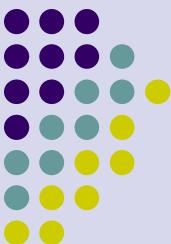
Znázornění mostu mezi dvěma sítěmi LAN (802.11 a 802.3).



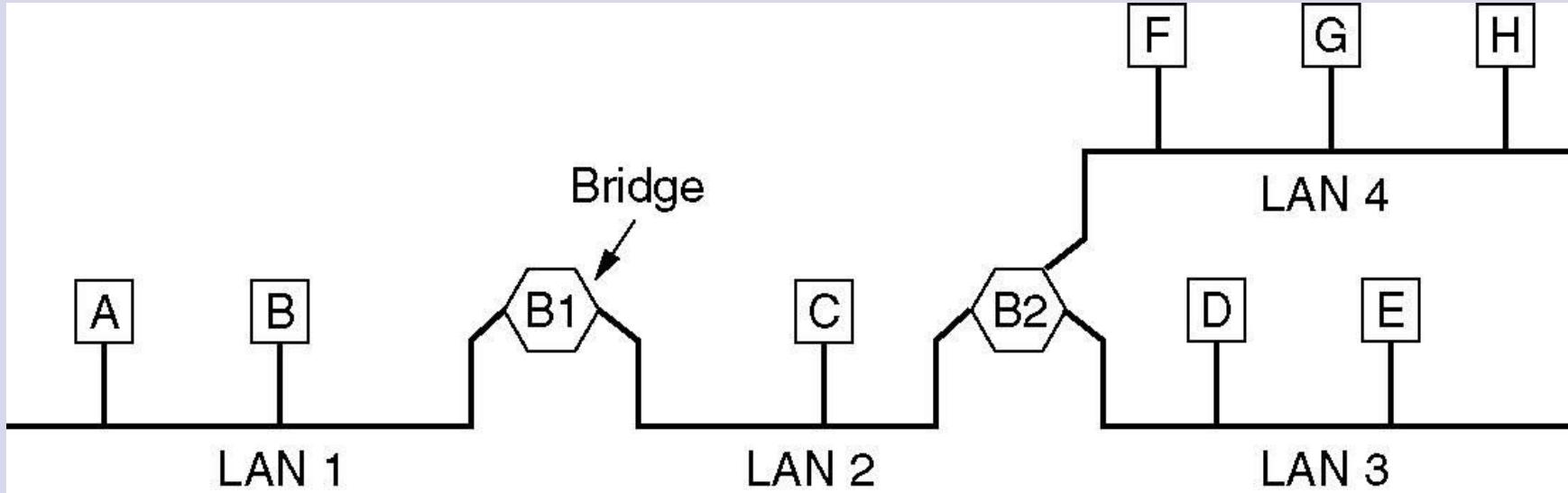
# Mosty mezi 802.x a 802.y (2)



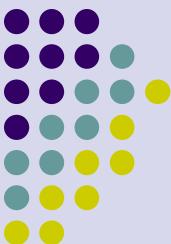
Různé formáty rámce IEEE 802.



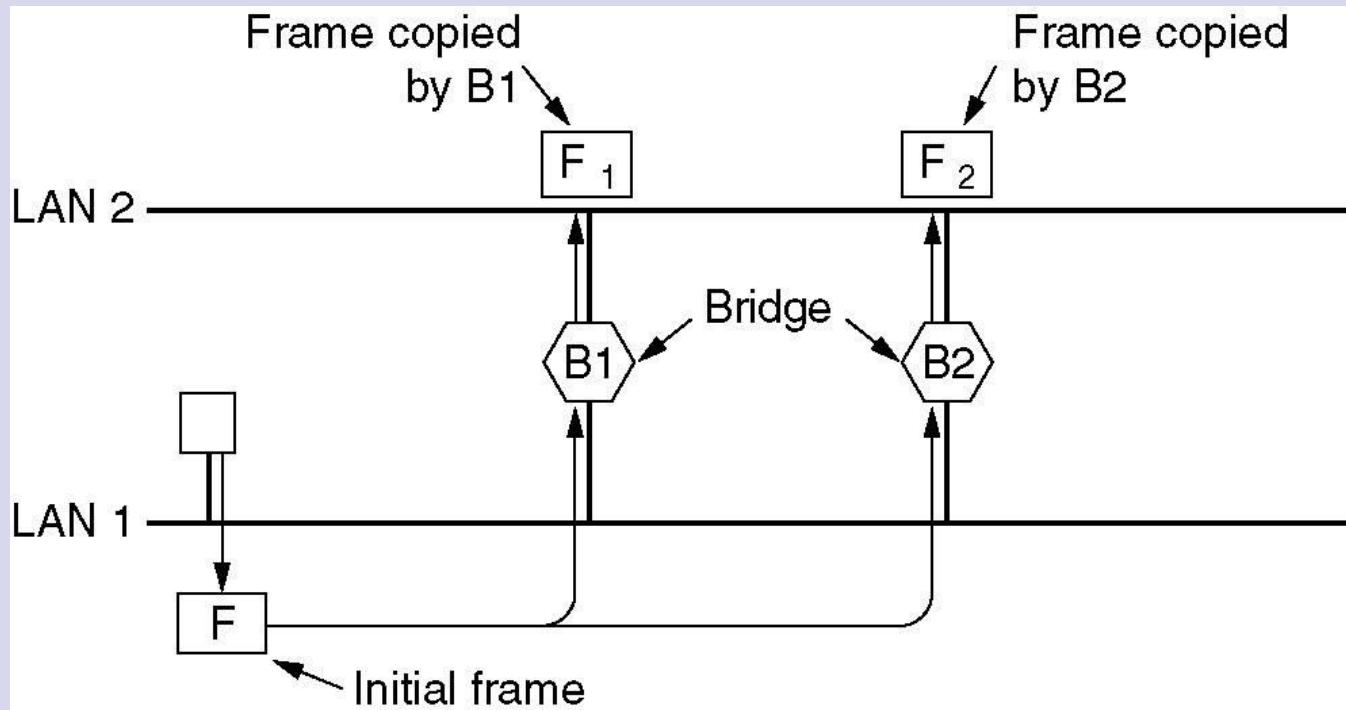
# Lokální Internetworking



Propojení 4 LAN a dvou mostů.

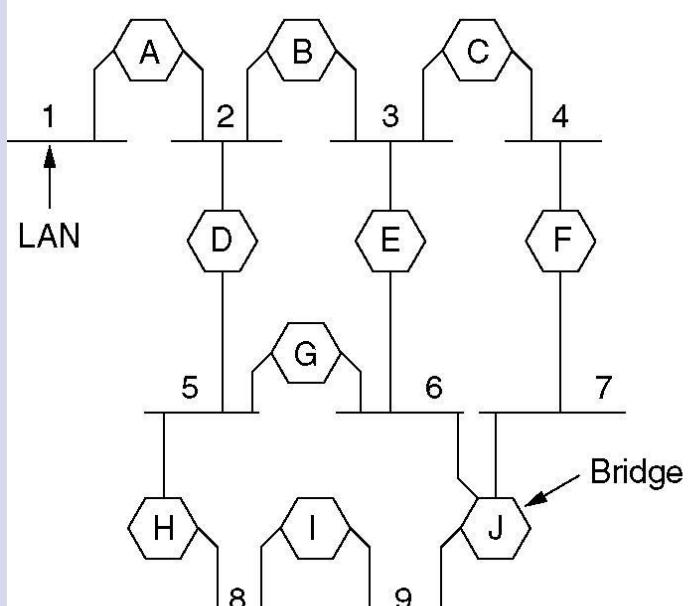
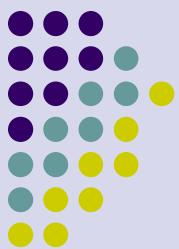


# Mosty se spanning tree algoritmem

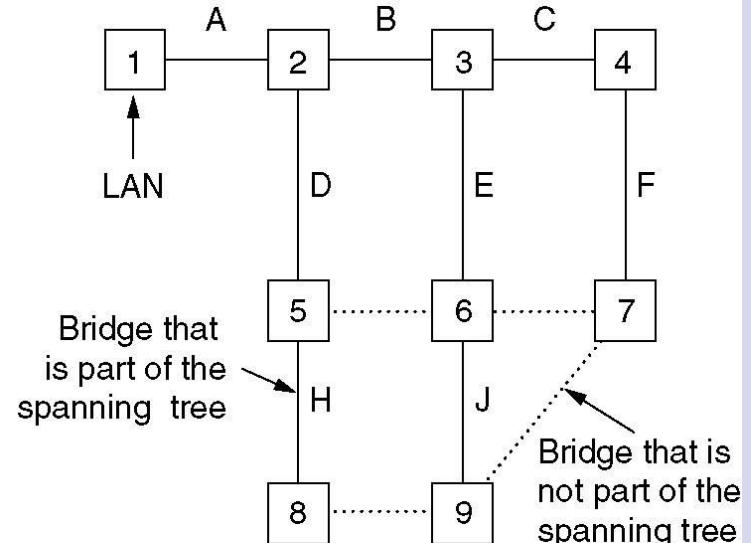


Dva paralelní transparentní mosty.

# Mosty se spanning tree algoritmem (2)

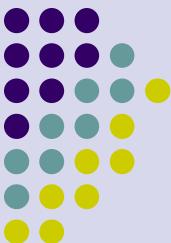


(a)

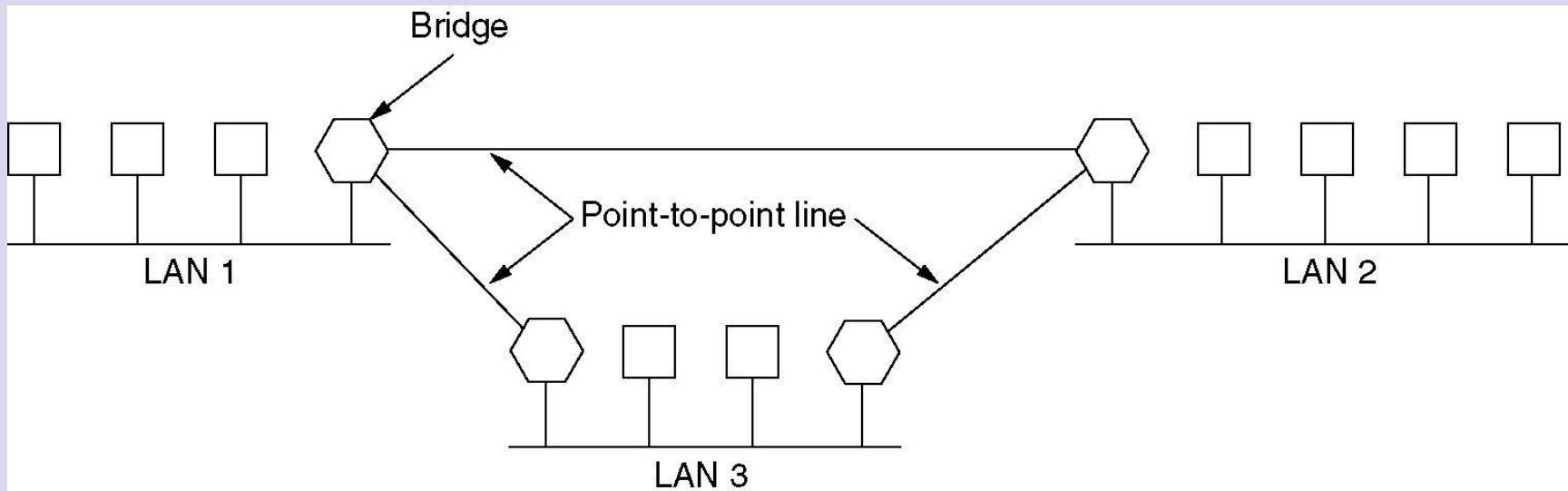


(b)

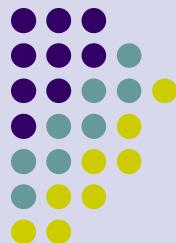
(a) Propojené LAN. (b) vytvoření kostry LAN. Tečkované čáry nejsou součástí kostry.



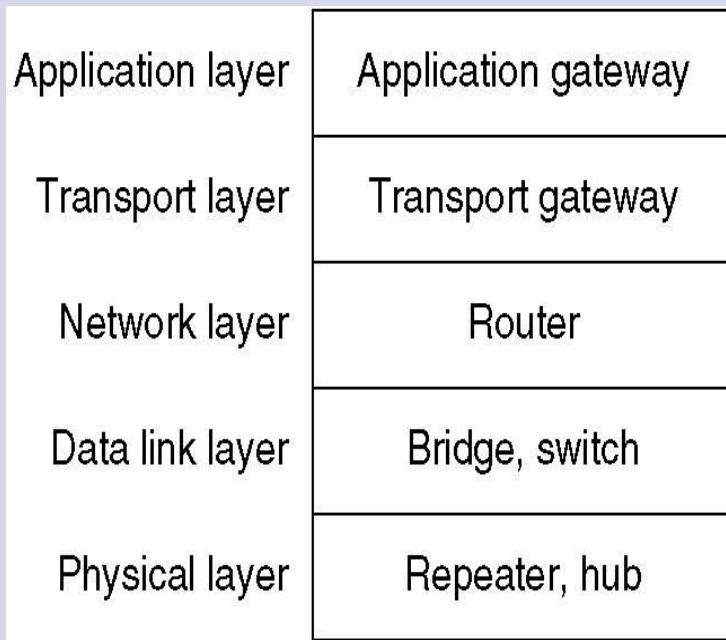
# Vzdálené mosty



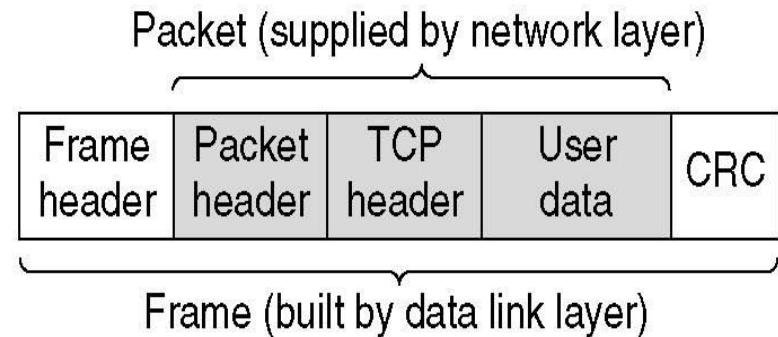
Vzdálené mosty mohou být použity pro propojení vzdálených LAN.



# Opakovače, rozbočovače (Hubs), mosty, přepínače, směrovače a brány

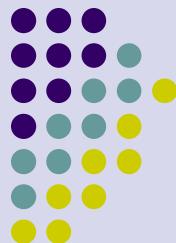


(a)

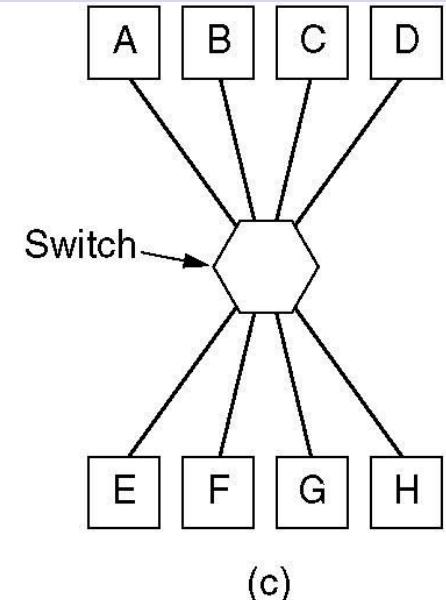
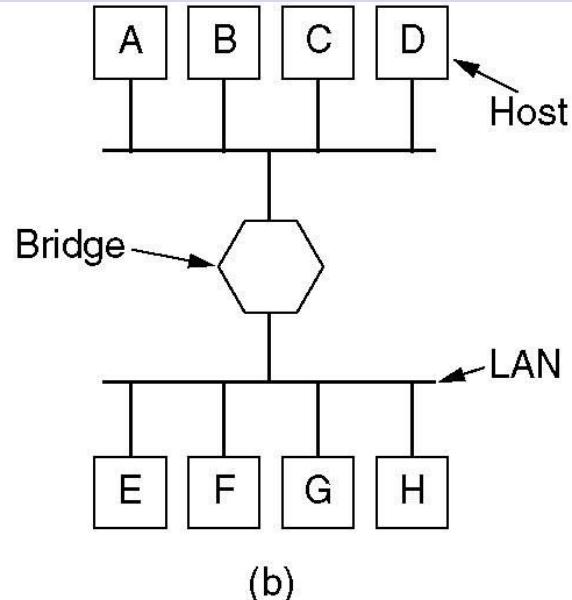
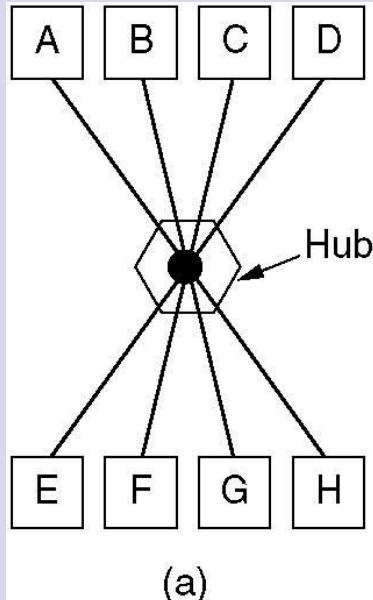


(b)

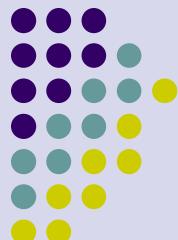
- (a) Zařízení na jednotlivých úrovních.
- (b) Rámce pakety a záhlaví.



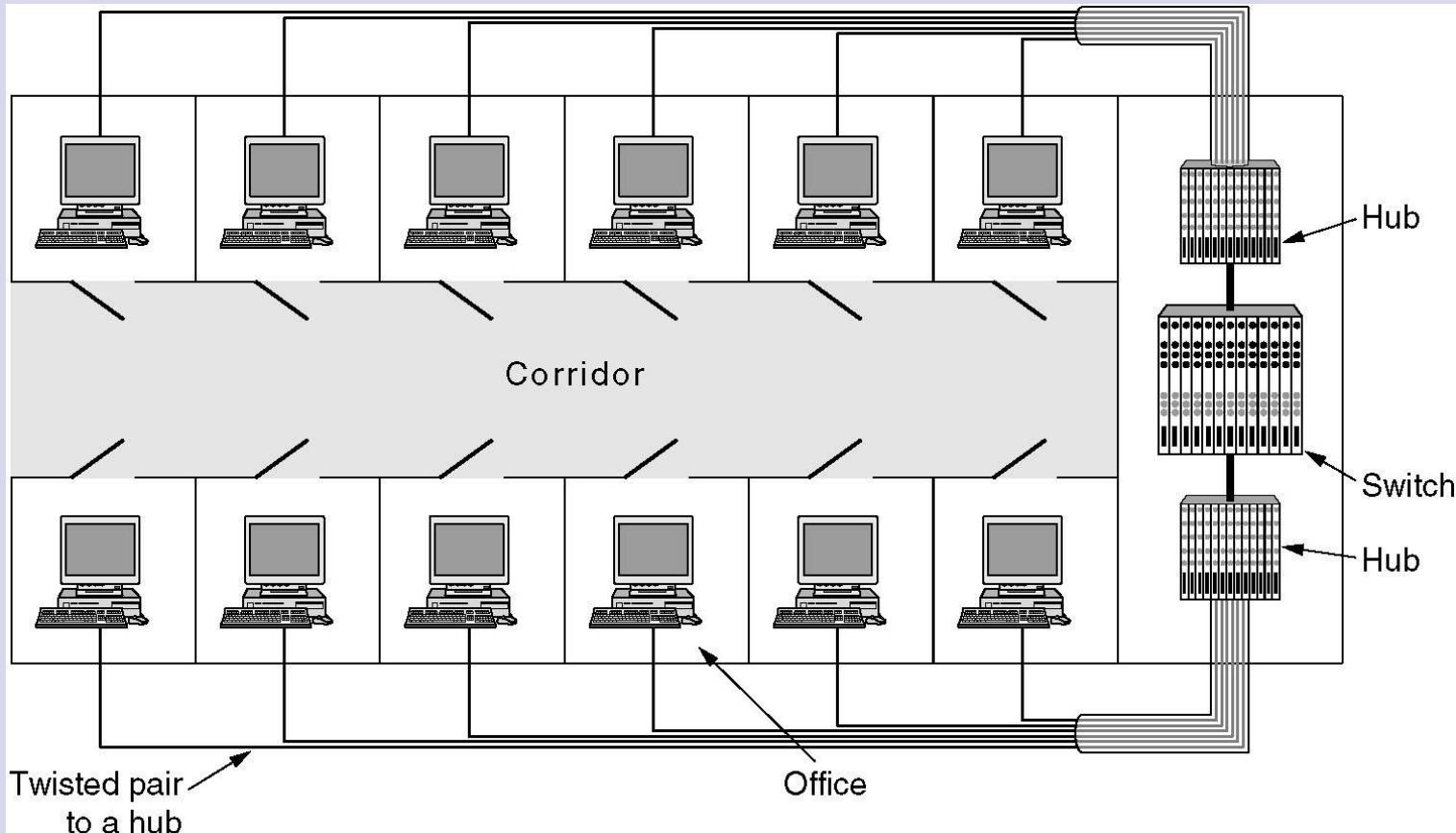
# Opakovače, rozbočovače (Hubs), mosty, přepínače, směrovače a brány (2)



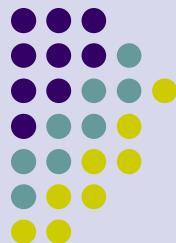
(a) Hub. (b) most. (c) přepínač.



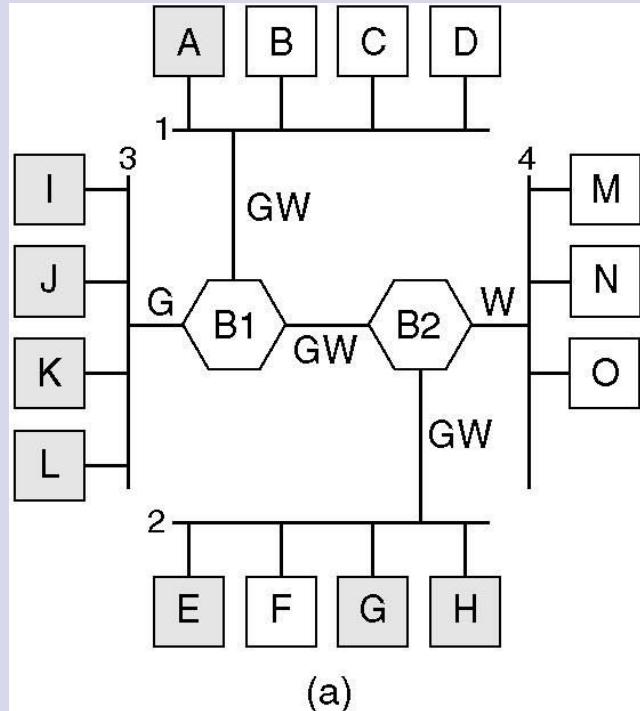
# Virtuální lokální počítačové sítě



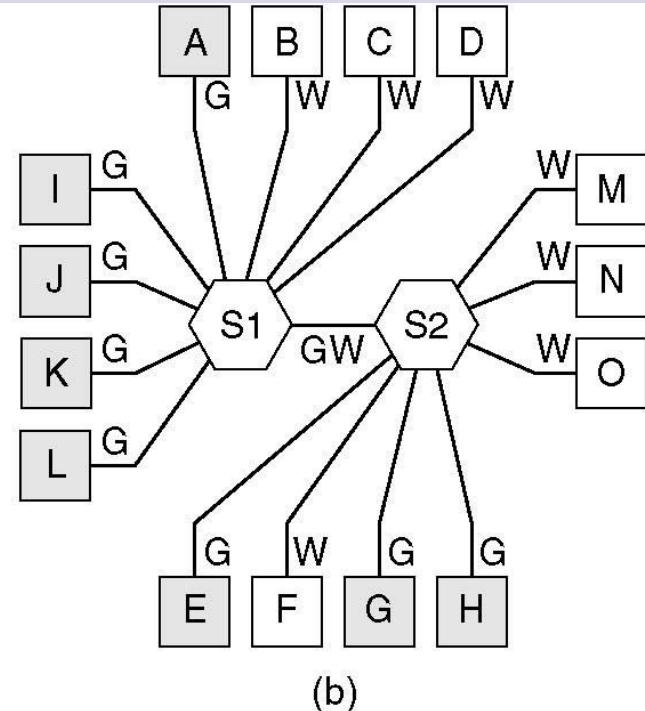
Strukturovaná kabeláž s použitím hubů a přepínače.



# Virtuální lokální počítačové sítě (2)

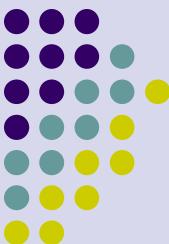


(a)

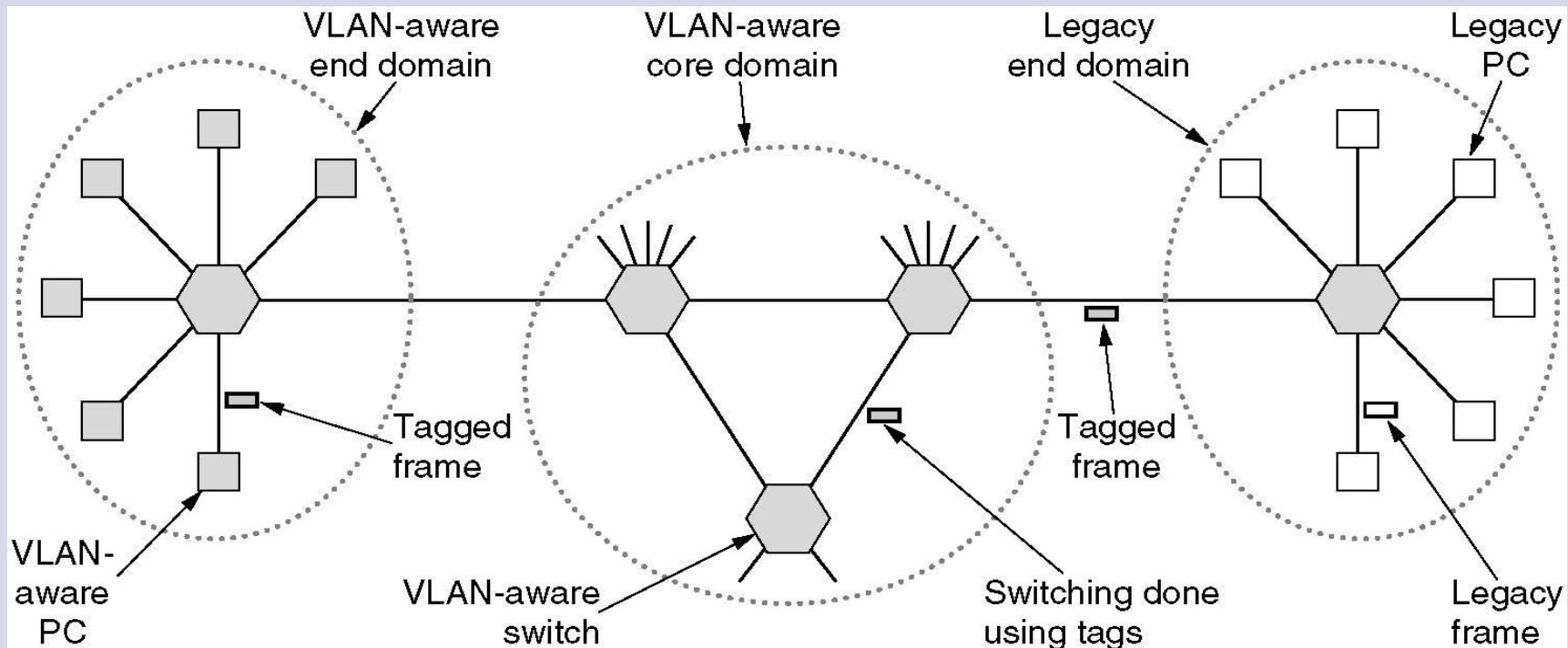


(b)

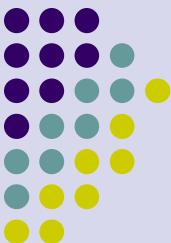
- (a) 4 fyzické LAN uspořádané do 2 VLAN (bílé a šedé) pomocí dvou mostů.
- (b) Totéž uspořádané do 2 VLAN pomocí dvou přepínačů.



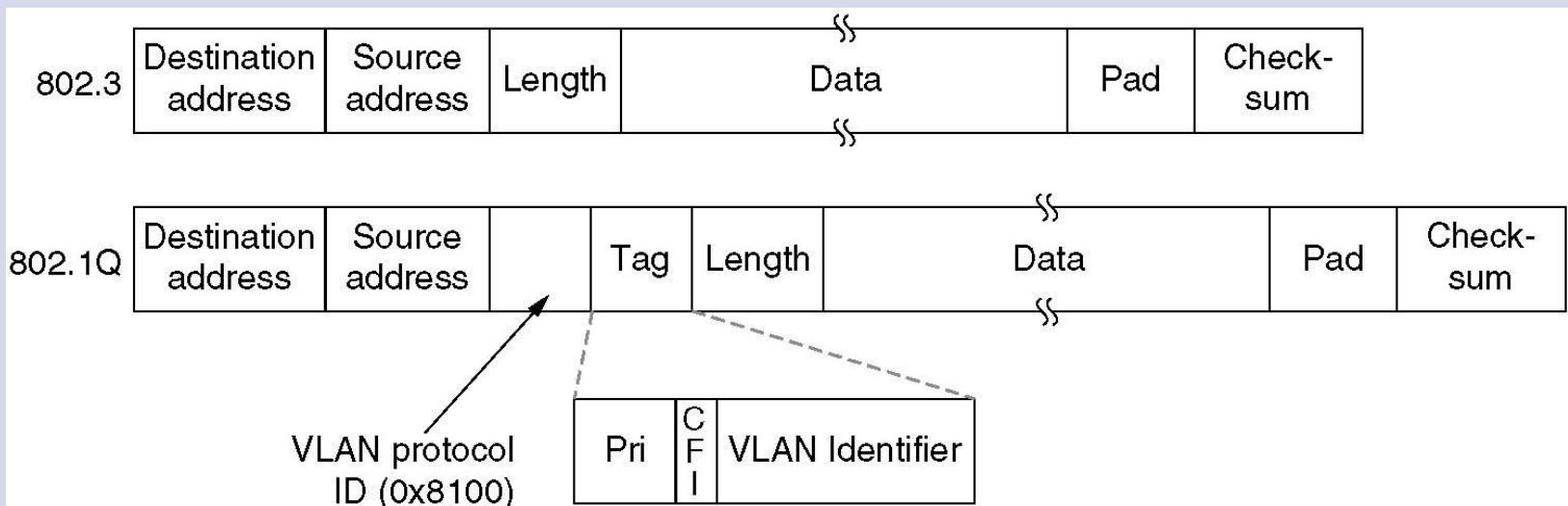
# Standard IEEE 802.1Q



Přechod z tradičního Ethernetu do přepínaného Ethernetu. Šedé komponenty jsou VLAN-ové, prázdné ne.

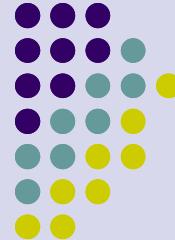


# Standard IEEE 802.1Q (2)



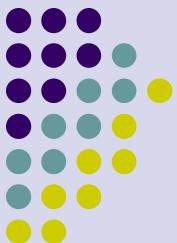
Porovnání klasického formátu 802.3 rámce s 802.1Q rámcem.

# Sítová úroveň



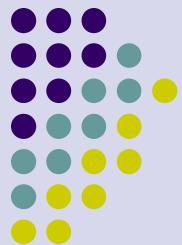
---

**Úvod do počítačových sítí**  
**Lekce 08**  
**Ing. Jiří ledvina, CSc.**

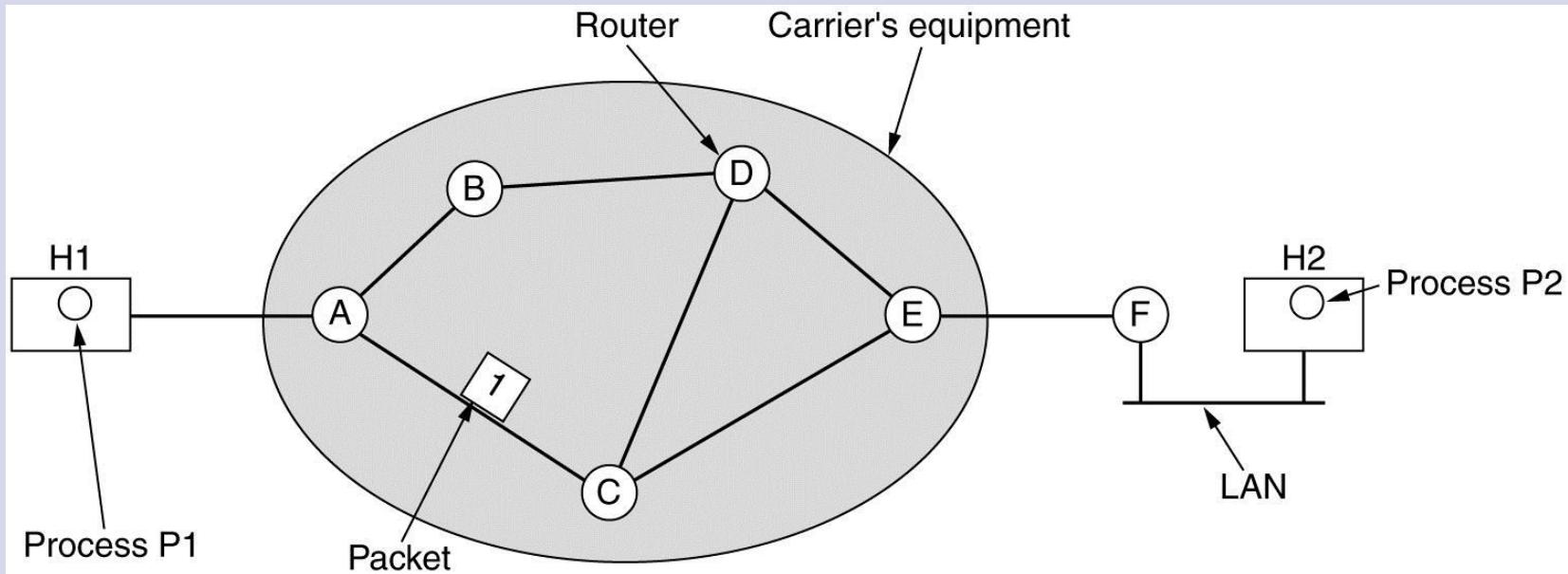


# Problémy návrhu sítové úrovně

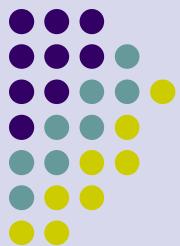
- Přepínání paketů metodou store and forward (ulož a pošli)
- Služby podporované na transportní úrovni
- Realizace nespojovaných služeb
- Realizace spojově orientovaných služeb
- Porovnání virtuálních okruhů a datagramových sítí



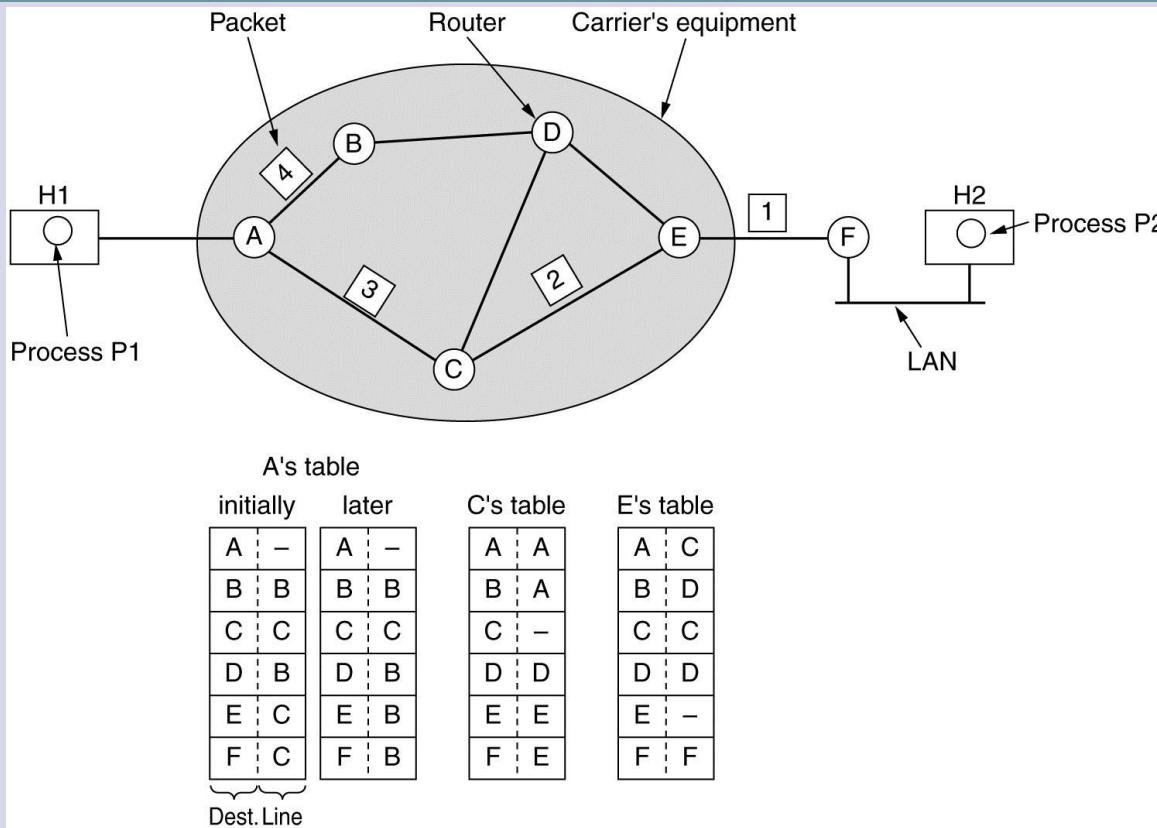
# Přepínání paketů metodou store and forward



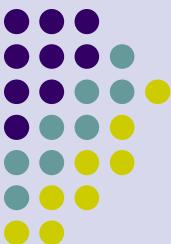
Prostředí protokolů sítové úrovně.



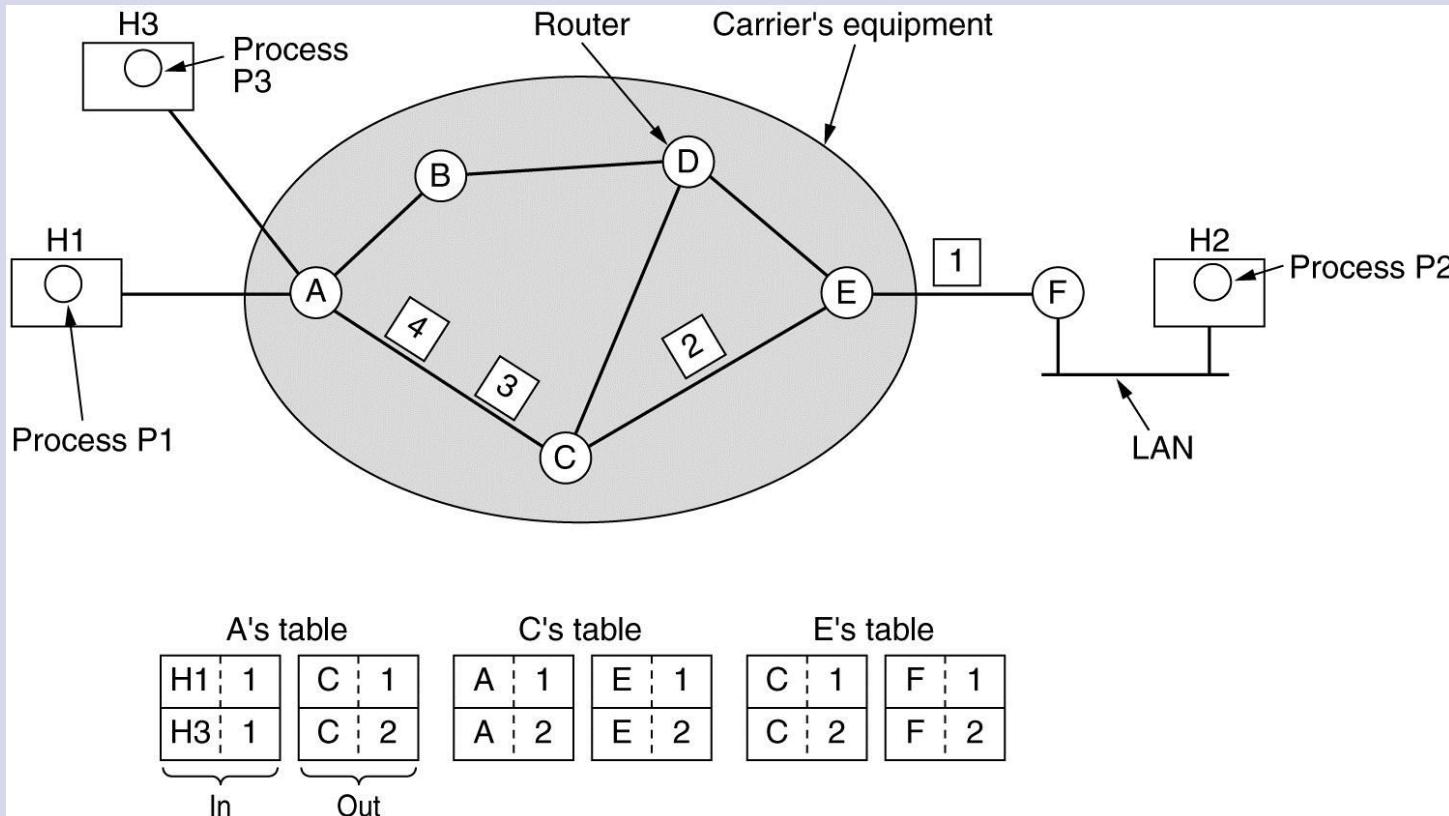
# Realizace nespojovaných služeb



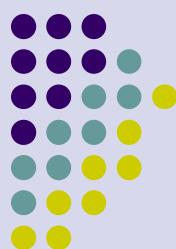
Směrování mezi datagramovými subsítěmi.



# Realizace spojově orientovaných služeb

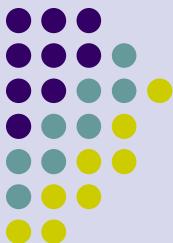


Směrování v sítích s virtuálními okruhy.



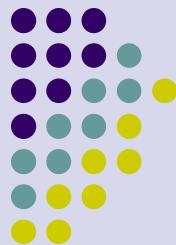
# Porovnání virtuálních okruhů a datagramových subsítí

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC



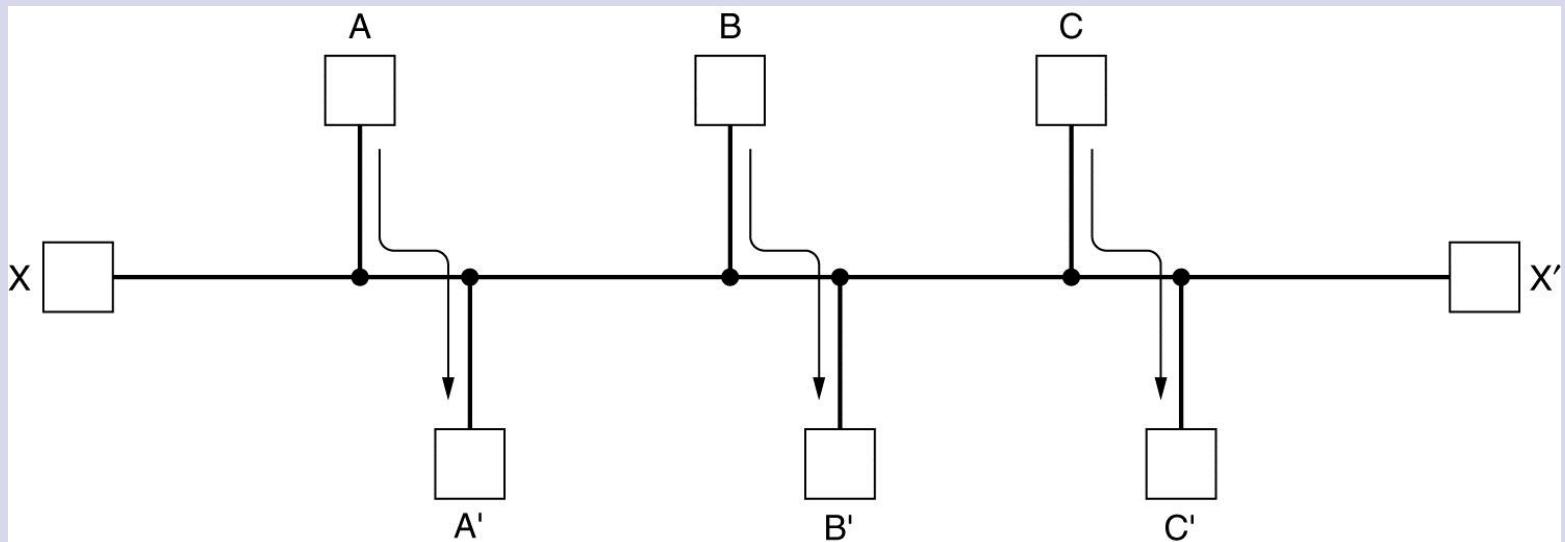
# Algoritmy směrování

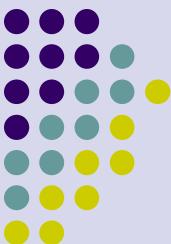
- Principy optimálnosti
- Směrování nalezením nejkratší cesty
- Záplavové směrování
- Směrování podle vektoru vzdáleností
- Směrování podle stavu linek
- Hierarchické směrování
- Směrování pomocí broadcastu (všeobecné vysílání)
- Skupinové směrování



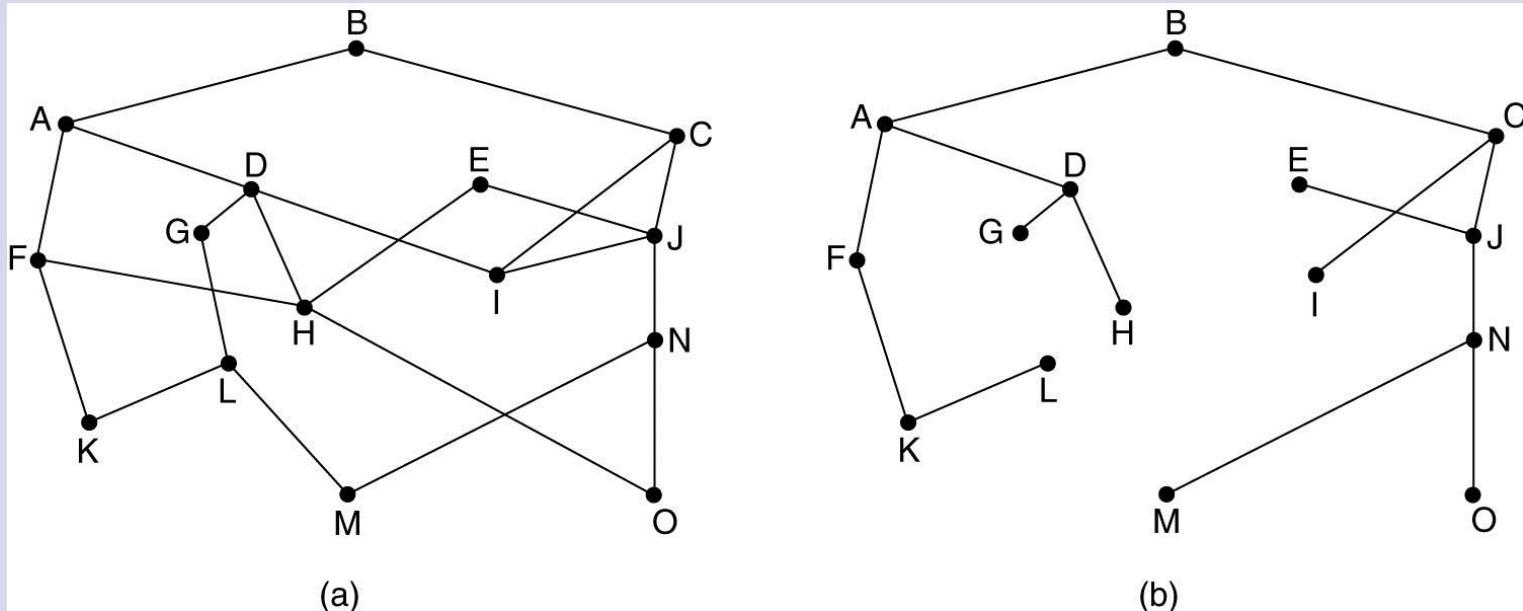
# Algoritmy směrování (2)

Konflikt mezi spravedlností a optimálností.

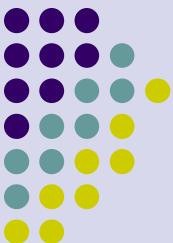




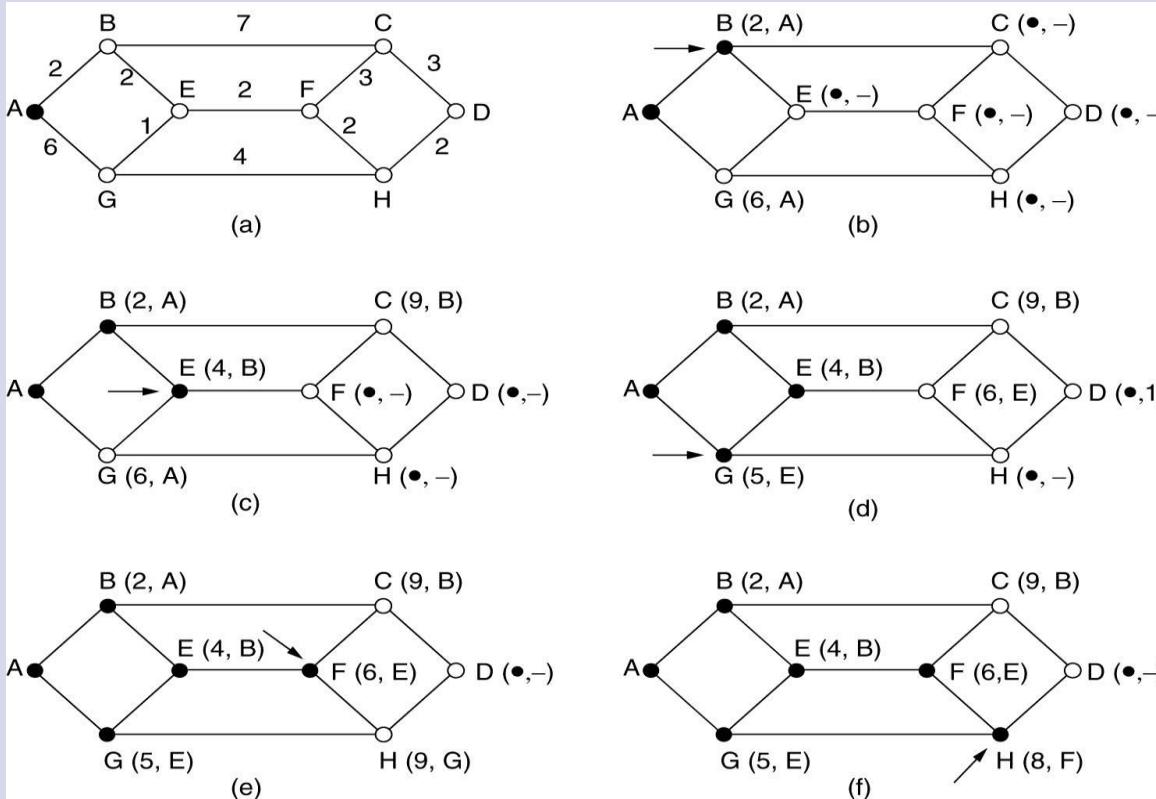
# Princip optimálnosti



(a) Pod síť. (b) minimální strom pro uzel B.



# Směrování podle nejkratší cesty



Prvních 5 kroků použitých při výpočtu nejkratší cesty z A do D (Dijkstrův algoritmus). Šipkou je označen pracovní uzel.



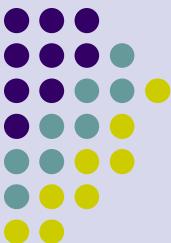
# Záplavové směrování

```
#define MAX_NODES 1024           /* maximum number of nodes */
#define INFINITY 1000000000        /* a number larger than every maximum path */
int n, dist[MAX_NODES][MAX_NODES];/* dist[i][j] is the distance from i to j */

void shortest_path(int s, int t, int path[])
{ struct state {
    int predecessor;           /* the path being worked on */
    int length;                /* previous node */
    /* length from source to this node */
    enum {permanent, tentative} label; /* label state */
} state[MAX_NODES];

int i, k, min;
struct state *p;

for (p = &state[0]; p < &state[n]; p++) { /* initialize state */
    p->predecessor = -1;
    p->length = INFINITY;
    p->label = tentative;
}
state[t].length = 0; state[t].label = permanent;
k = t;                                /* k is the initial working node */
```



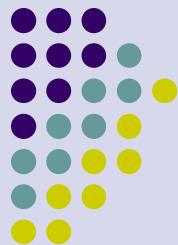
# Záplavové směrování (2)

```
do {                                     /* Is there a better path from k? */
    for (i = 0; i < n; i++)             /* this graph has n nodes */
        if (dist[k][i] != 0 && state[i].label == tentative) {
            if (state[k].length + dist[k][i] < state[i].length) {
                state[i].predecessor = k;
                state[i].length = state[k].length + dist[k][i];
            }
        }
    }

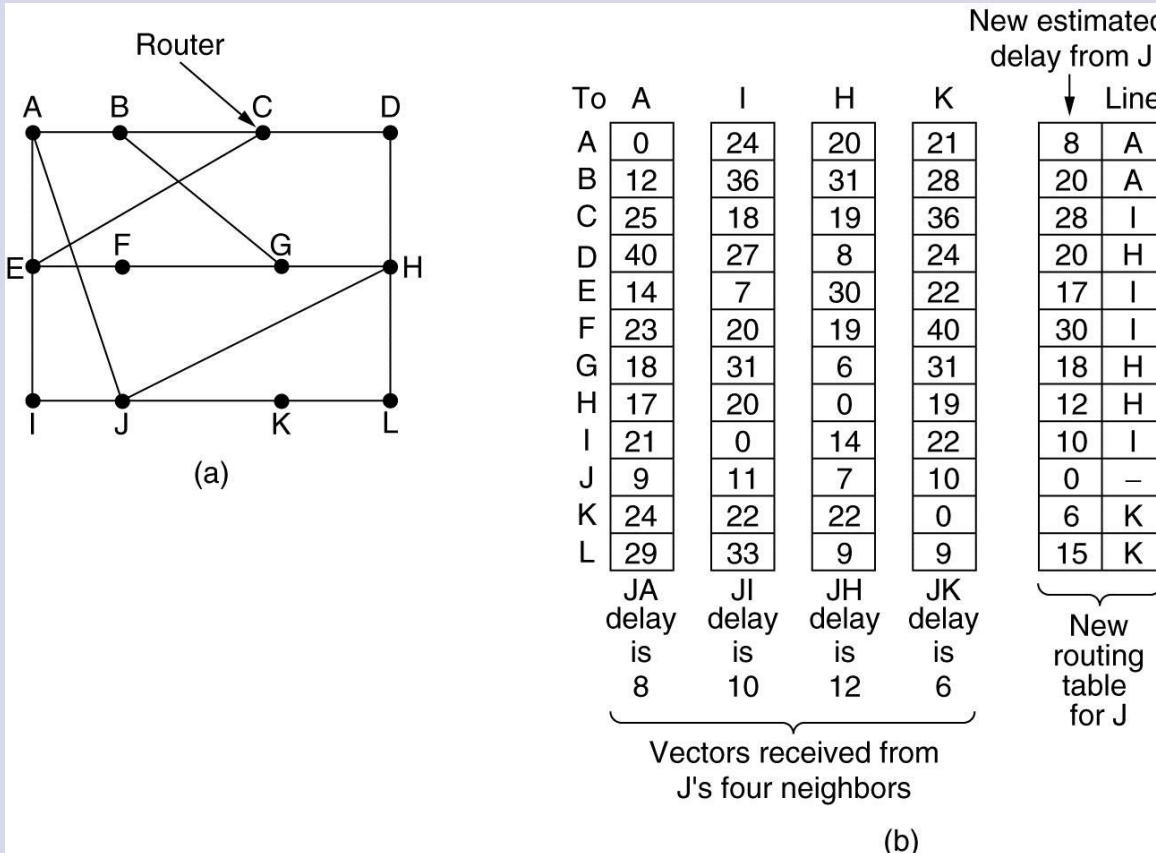
/* Find the tentatively labeled node with the smallest label. */
k = 0; min = INFINITY;
for (i = 0; i < n; i++)
    if (state[i].label == tentative && state[i].length < min) {
        min = state[i].length;
        k = i;
    }
state[k].label = permanent;
} while (k != s);

/* Copy the path into the output array. */
i = 0; k = s;
do {path[i++] = k; k = state[k].predecessor;} while (k >= 0);
}
```

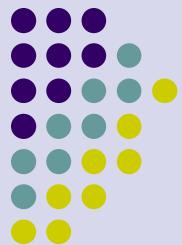
Dijkstruv algoritmus pro výpočet nejkratší cesty v grafu.



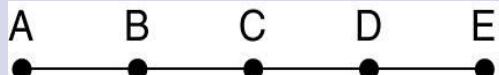
# Směrování podle vektoru vzdáleností



(a) Subsít. (b) Vstup od A, I, H, K a nová směrovací tabulka.



# Směrování podle vektoru vzdáleností (2)



•	•	•	•	Initially
1	•	•	•	After 1 exchange
1	2	•	•	After 2 exchanges
1	2	3	•	After 3 exchanges
1	2	3	4	After 4 exchanges

(a)



1	2	3	4	Initially
3	2	3	4	After 1 exchange
3	4	3	4	After 2 exchanges
5	4	5	4	After 3 exchanges
5	6	5	6	After 4 exchanges
7	6	7	6	After 5 exchanges
7	8	7	8	After 6 exchanges
⋮				
•	•	•	•	

(b)

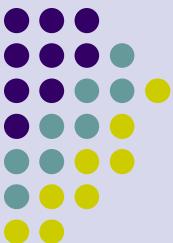
Problém počítání do nekonečna.

# Směrování podle stavu linek (spojení)



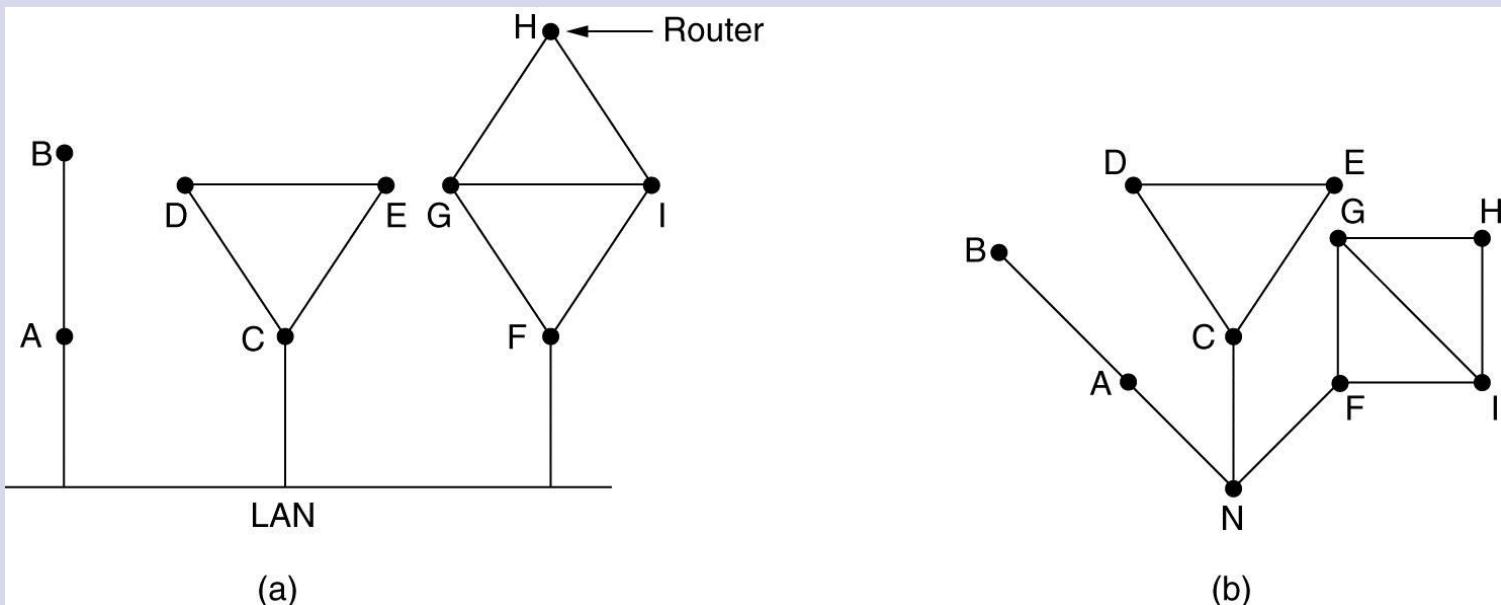
Každý uzel musí dělat následující:

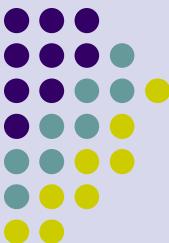
- Vyhledávat sousedy a znát jejich síťové adresy.
- Měřit zpoždění nebo cenu ke každému sousedovi.
- Vytvořit paket s informací, kterou se uzel naučil od sousedních směrovačů.
- Poslat paket ostatním směrovačům.
- Vypočítat nejkratší cestu k ostatním směrovačům.



# Učení se o sousedech

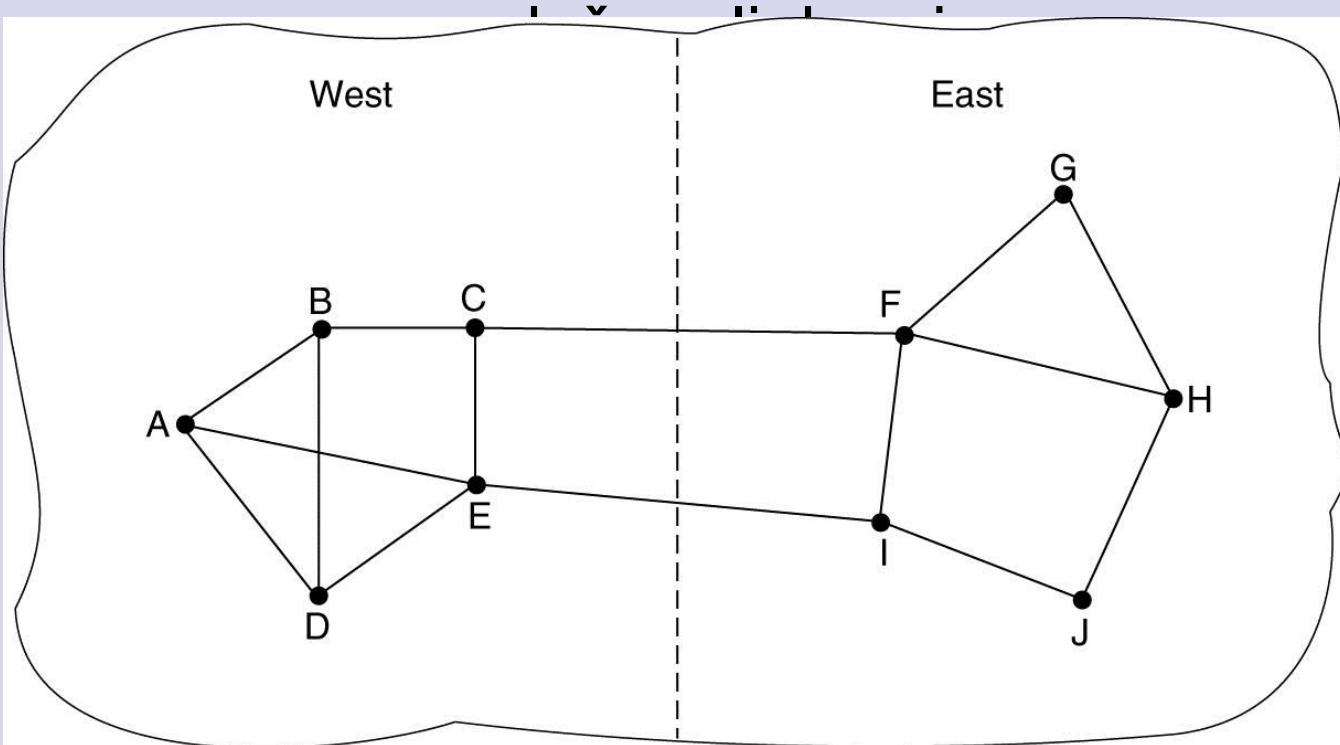
(a) Devět směrovačů a LAN. (b) model grafu ad (a).

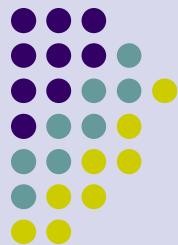




# Měření ceny linky

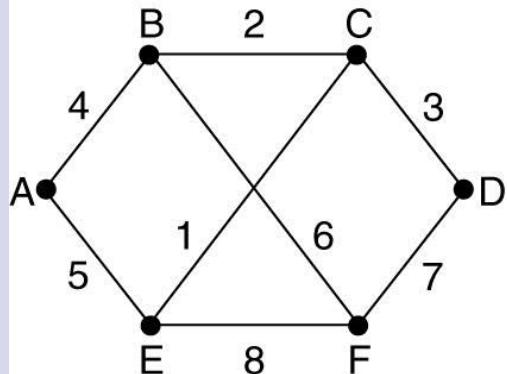
Podsíť, ve které jsou levá s pravou částí propojeny





# Vytváření paketů stavu linky

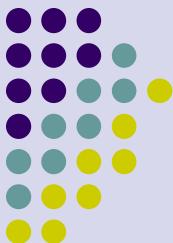
(a) podsíť (b) pakety stavu linek pro  
tuto podsíť



(a)

Link	State	Packets	F
A	B	E	Seq.
	C		Seq.
Seq.	Age		Age
Age	B   4	A   5	B   6
B   4	A   4	B   6	D   7
A   4	C   2	C   1	E   8
C   2	D   3	F   7	
D   3	F   7		
F   7	E   1		
E   1			

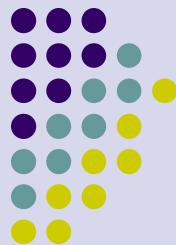
(b)



# Distribuce paketů stavu linky

Soubor paketů pro směrovač B z předchozího příkladu.

Source	Seq.	Age	Send flags			ACK flags			Data
			A	C	F	A	C	F	
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	



# Hierarchické směrování

## Hierarchické směrování

(a)

Full table for 1A

Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

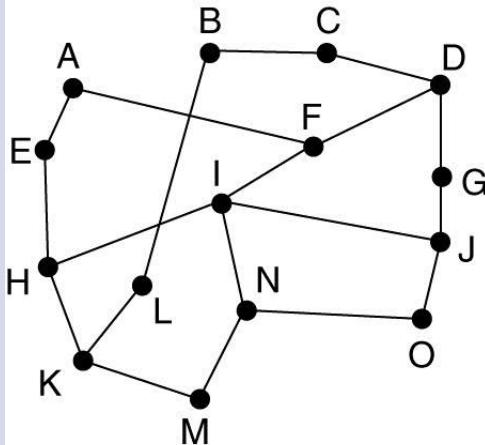
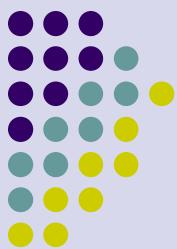
Hierarchical table for 1A

Dest.	Line	Hops
1A	-	-
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

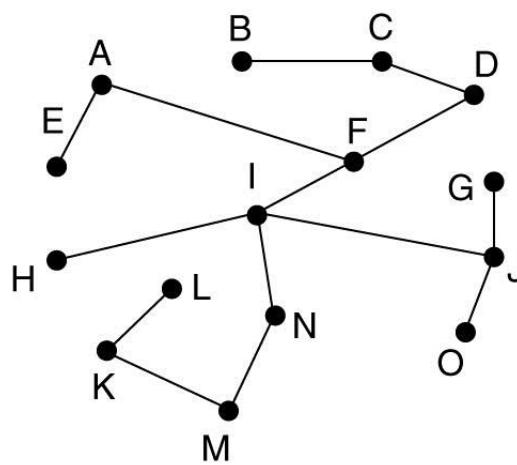
(c)

Úvod do počítačových sítí, lekce 7

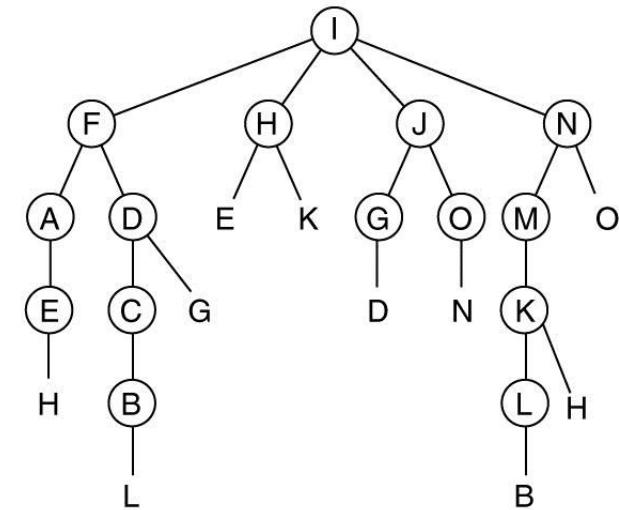
# Celoplošné (broadcast) směrování



(a)



(b)

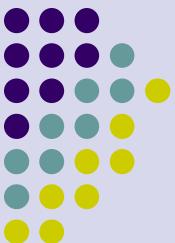


(c)

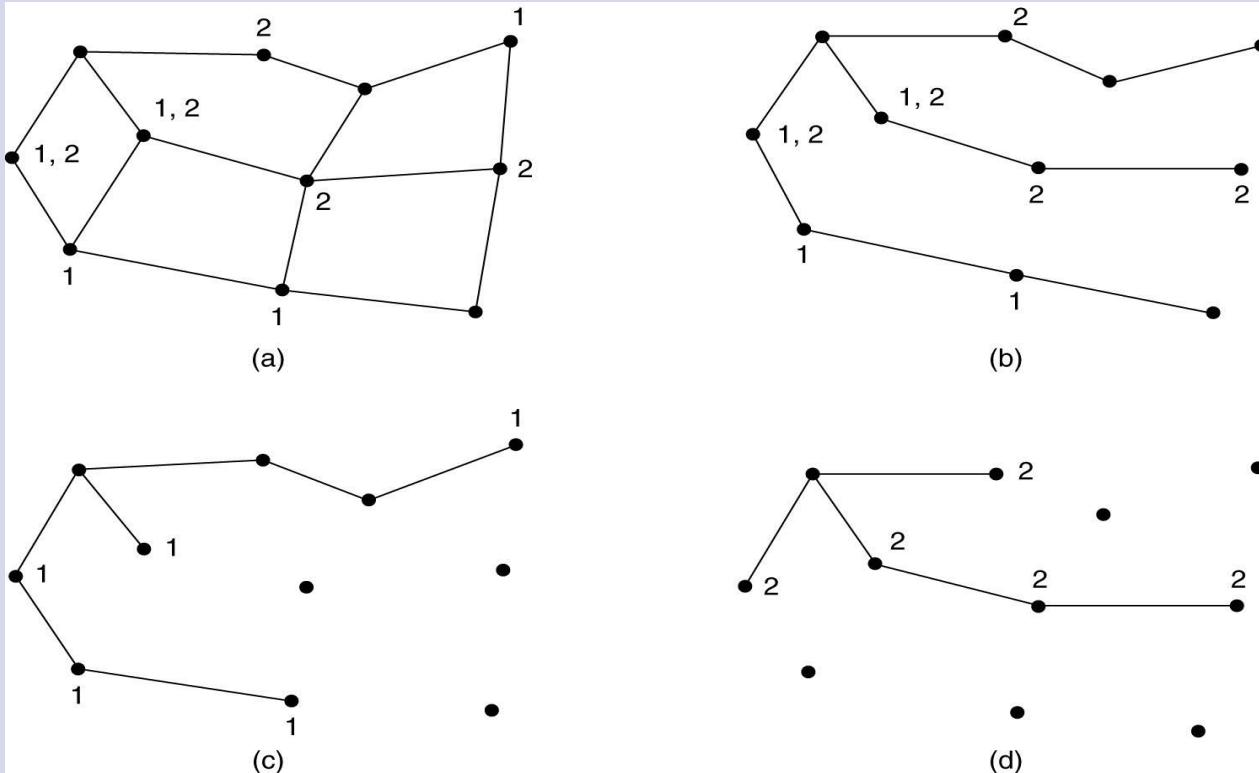
Zasílání (forwardování) paketů podle zpětné cesty.

(a) Podsíť. (b) Minimální strom.

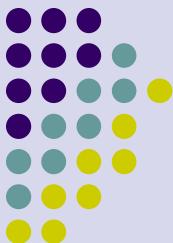
(c) Strom vytvořený zasíláním podle zpětné cesty.



# Skupinové (multicast) směrování

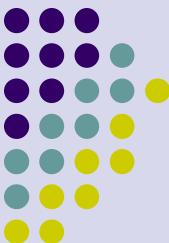


- (a) Síť. (b) Minimální strom pro nejlevější směrovač.  
(c) Doručovací strom pro skup. 1. (d) Doručovací strom pro skup. 2.

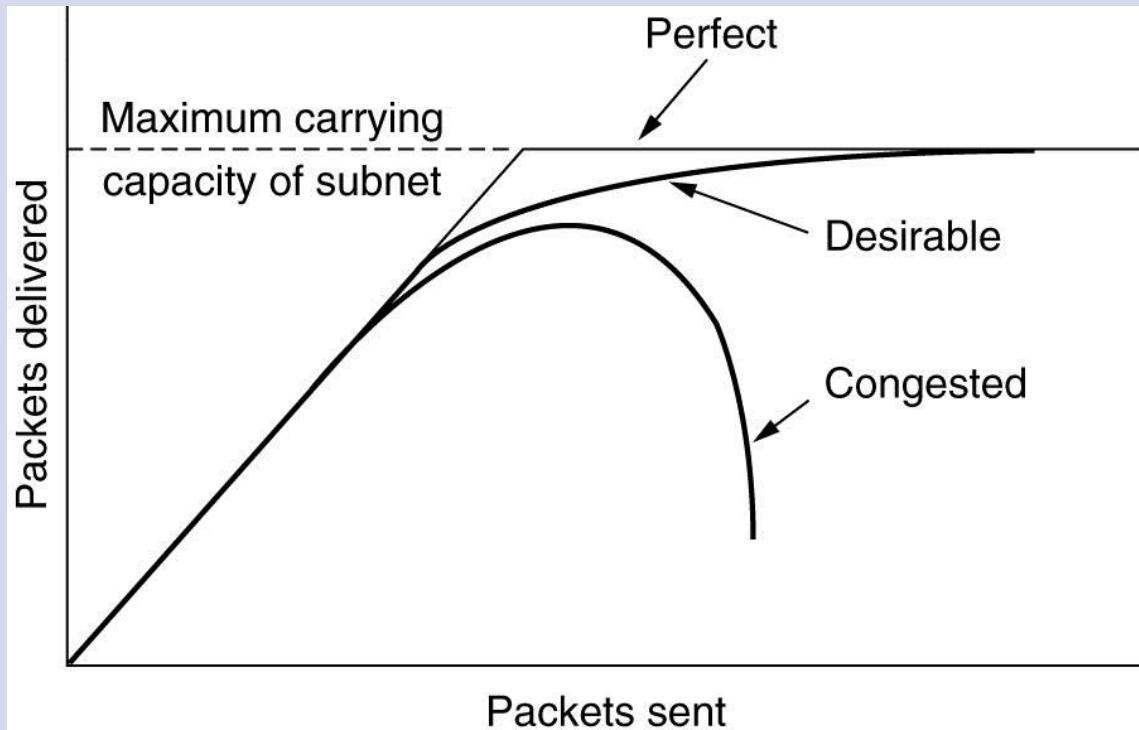


# Algoritmus řízení zahlcení

- Obecné principy řízení zahlcení
- Zásady prevence zahlcení
- Řízení zahlcení v podsítích s virtuálními okruhy
- Řízení zahlcení v datagramových sítích
- Uvolnění zatížení
- Ovládání rozptylu zpoždění

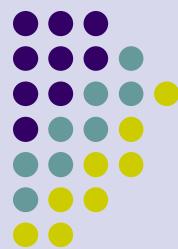


# Zahlcení

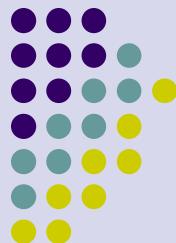


Při velkém zatížení dochází k zahlcení a propustnost prudce klesá.

# Obecné principy řízení zahlcení



- Monitorování systému .
  - Detekce kdy a kde se objevilo zahlcení.
- Poslání informace tam, kde může být provedena nějaké akce.
- Provedení operací, které zahlcení pomohou odstranit.

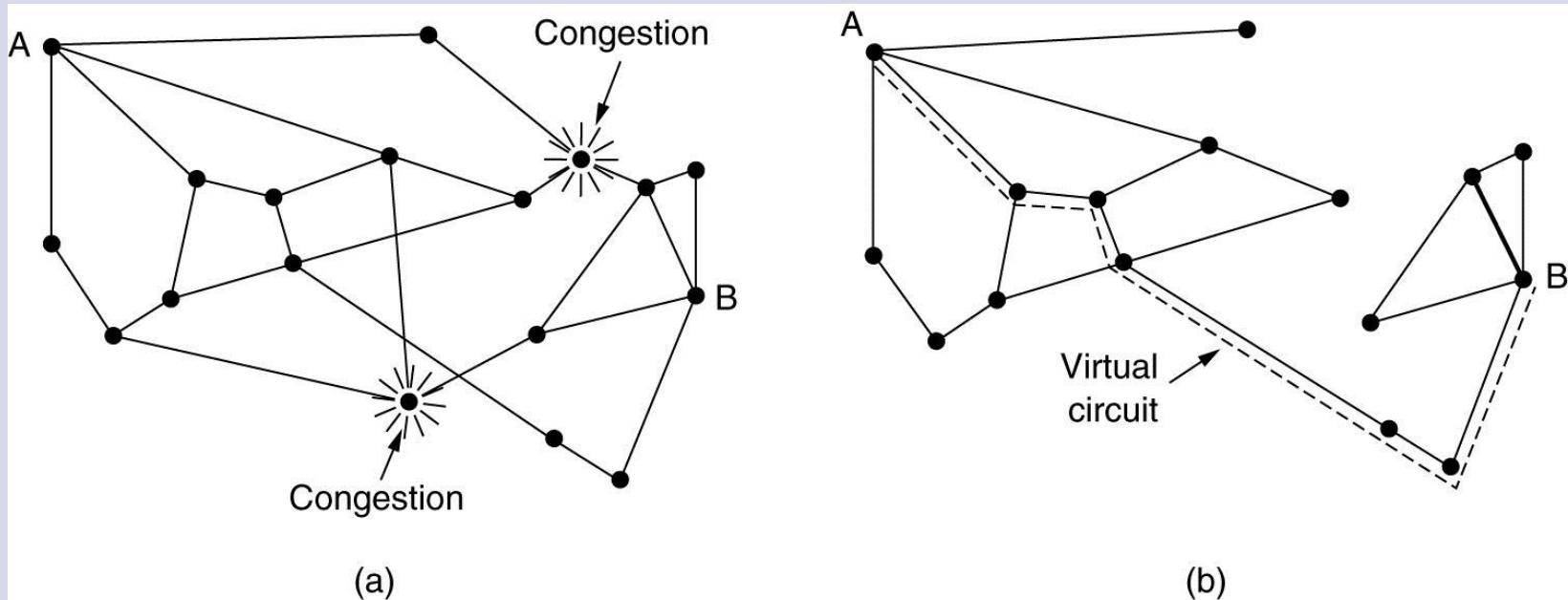


# Zásady prevence zahlcení

Layer	Policies
Transport	<ul style="list-style-type: none"><li>• Retransmission policy</li><li>• Out-of-order caching policy</li><li>• Acknowledgement policy</li><li>• Flow control policy</li><li>• Timeout determination</li></ul>
Network	<ul style="list-style-type: none"><li>• Virtual circuits versus datagram inside the subnet</li><li>• Packet queueing and service policy</li><li>• Packet discard policy</li><li>• Routing algorithm</li><li>• Packet lifetime management</li></ul>
Data link	<ul style="list-style-type: none"><li>• Retransmission policy</li><li>• Out-of-order caching policy</li><li>• Acknowledgement policy</li><li>• Flow control policy</li></ul>



# Řízení zahlcení v subsítích s virtuálními okruhy

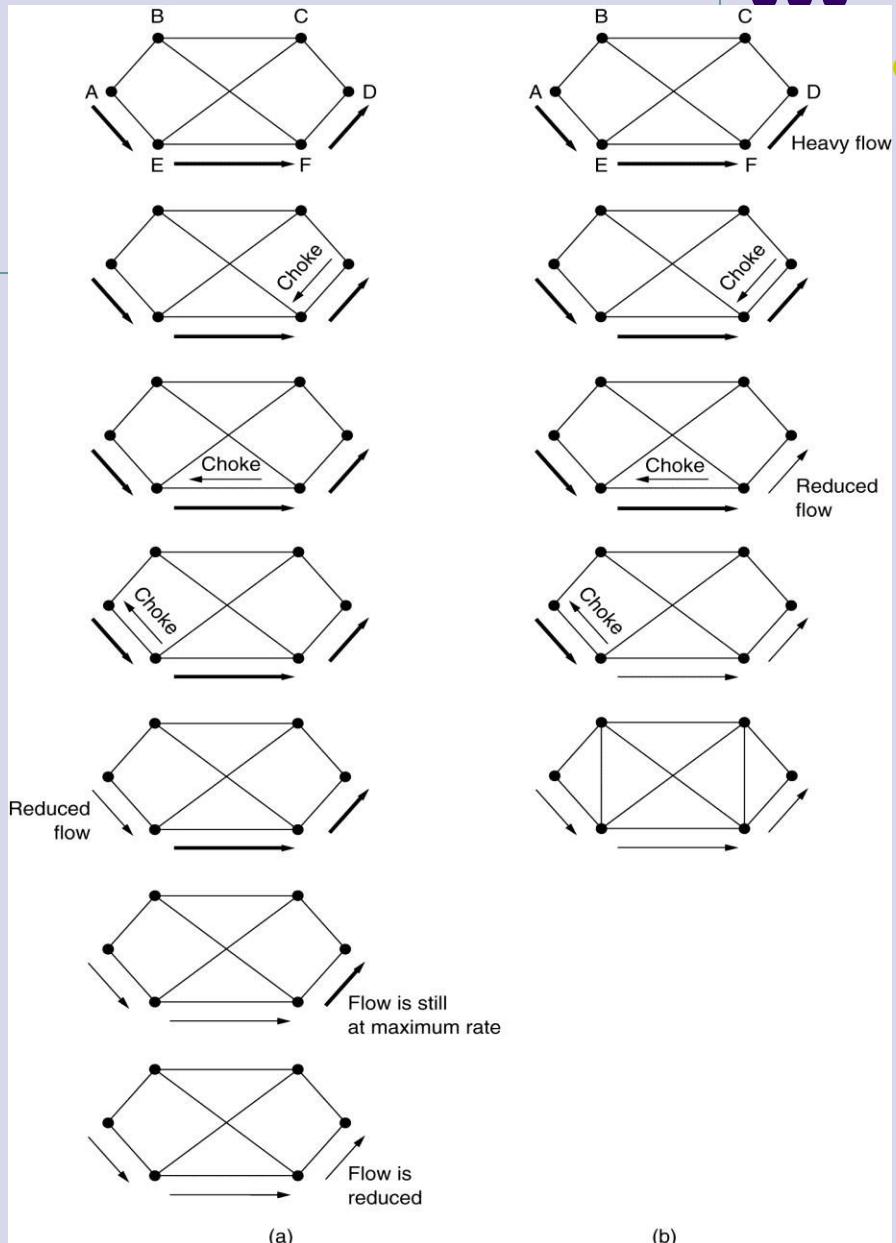


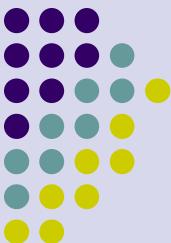
(a) Zahlcená subsít'. (b) Subsít' s odstraněnými místy zahlcení, virtuální spojení A a B

# Metoda škrtících paketů

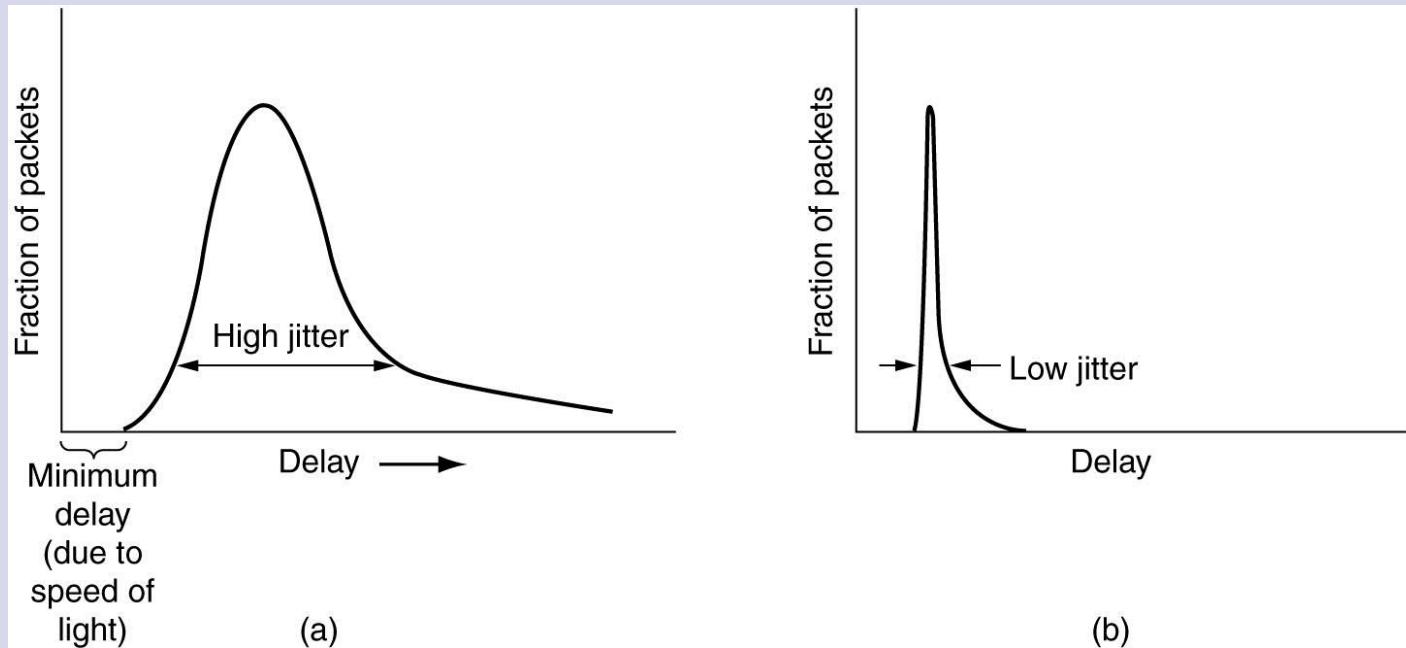
(a) Škrtící paket ovlivňující pouze zdroj.

(b) Škrtící paket ovlivňující každý uzel, přes který je přenášen.



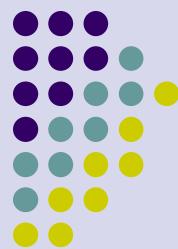


# Řízení rozptylu zpoždění

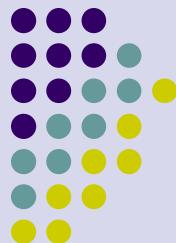


V digitální technice se termínem jitter (rozptyl hodnot) označuje obecná chyba časování signálu, která je všudypřítomná, protože žádný signál není ideálně pravoúhlý a žádný obvod nemá ideální vlastnosti.

# Kvalita služeb (Quality of Service)



- Požadavky
- Techniky pro dosažení požadované QoS
- Integrované (jednotné, sdružené) služby
- Odlišované (diferencované) služby
- Label Switching and MPLS (multiprotocol label switching)



# Kvalita služeb (2)

Požadavky na služby sítě – požadovaná kvalita služeb

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

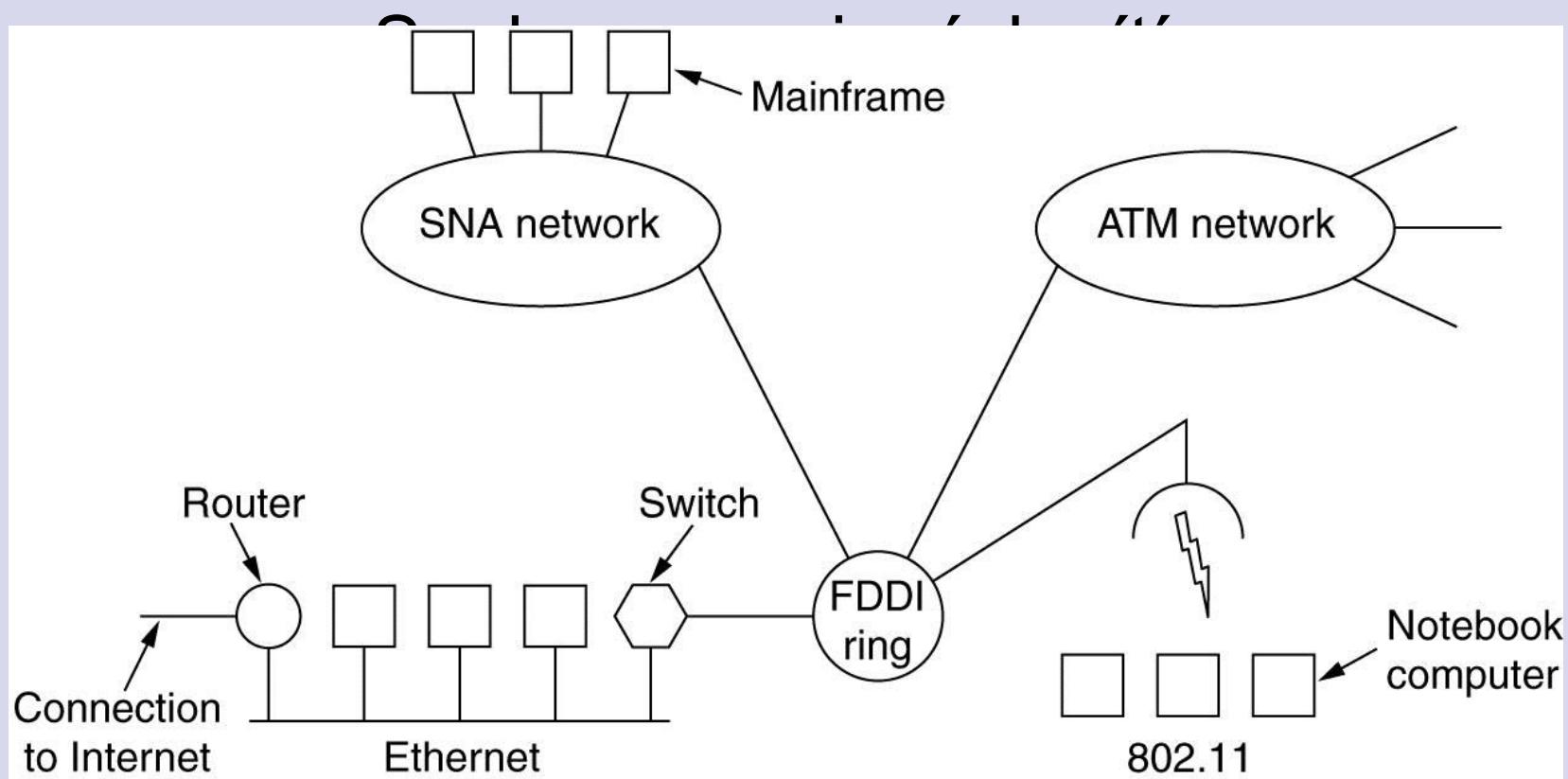


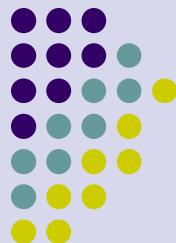
# Internetworking

- Čím se liší sítě
- Jak mohou být sítě propojeny
- Propojované virtuální okruhy
- Propojení sítí nespojovanými službami
- Tunelování
- Směrování mezi sítěmi
- Fragmentace



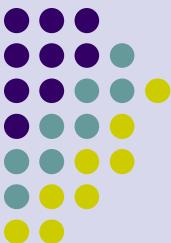
# Propojování sítí



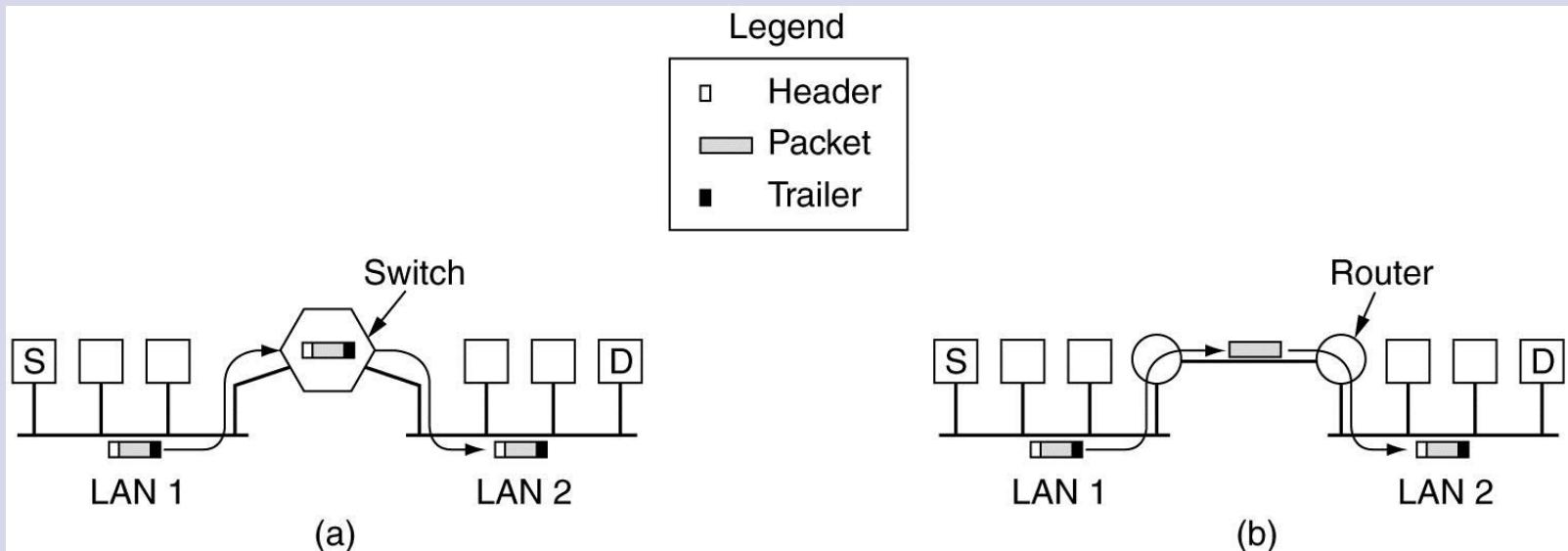


# Čím se sítě liší

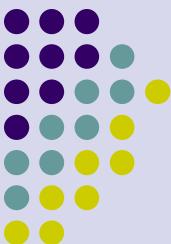
Item	Some Possibilities
Service offered	Connection oriented versus connectionless
Protocols	IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.
Addressing	Flat (802) versus hierarchical (IP)
Multicasting	Present or absent (also broadcasting)
Packet size	Every network has its own maximum
Quality of service	Present or absent; many different kinds
Error handling	Reliable, ordered, and unordered delivery
Flow control	Sliding window, rate control, other, or none
Congestion control	Leaky bucket, token bucket, RED, choke packets, etc.
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, by packet, by byte, or not at all



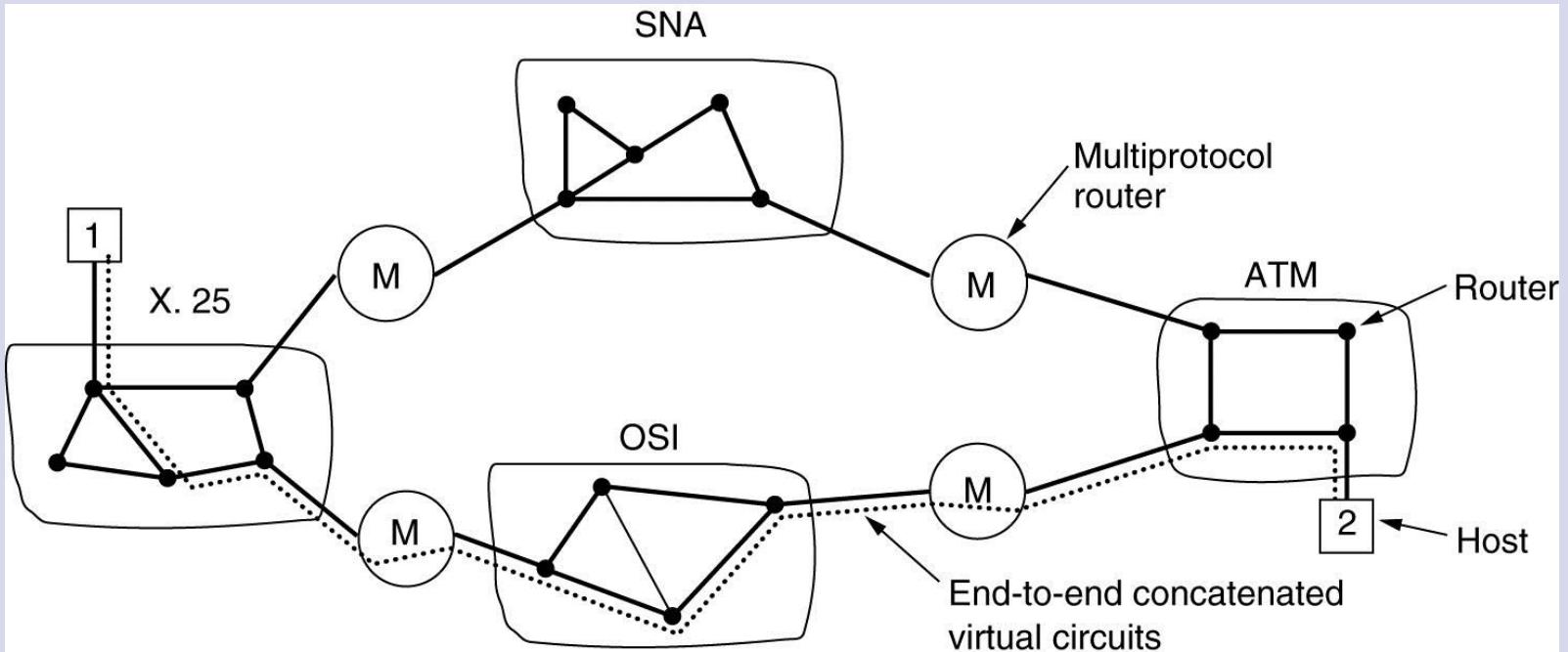
# Způsoby propojení sítí



- (a) Propojení sítí typu Ethernet přepínači.
- (b) Propojení sítí typu Ethernet směrovači.

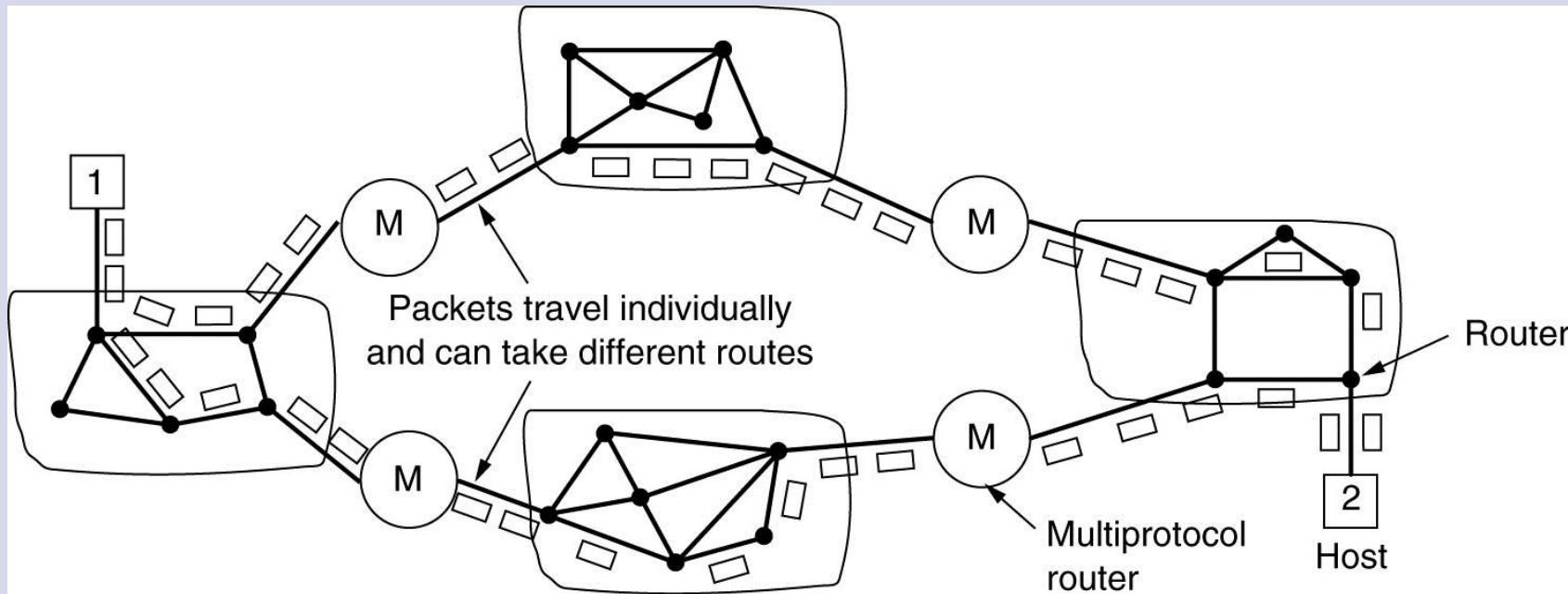


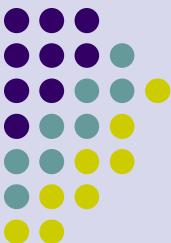
# Propojené virtuální okruhy



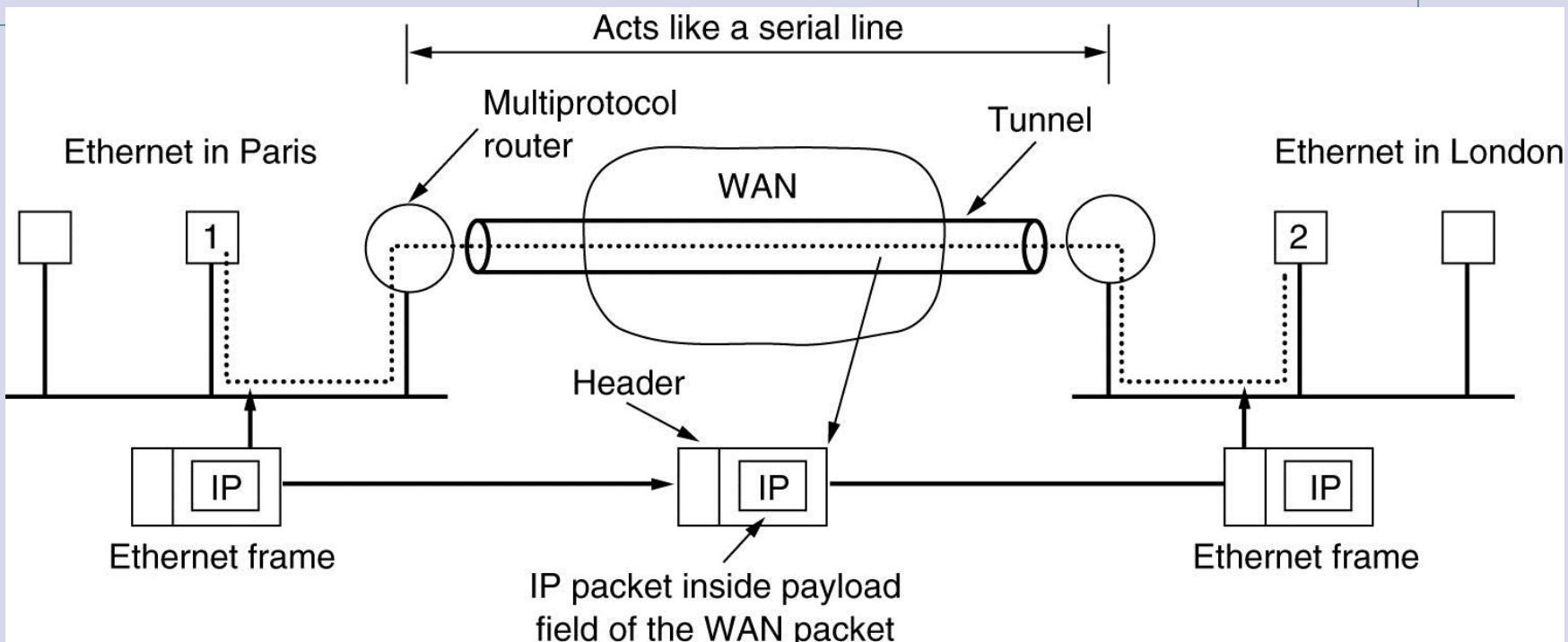


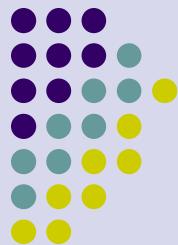
# Propojení sítí nespojovanými službami





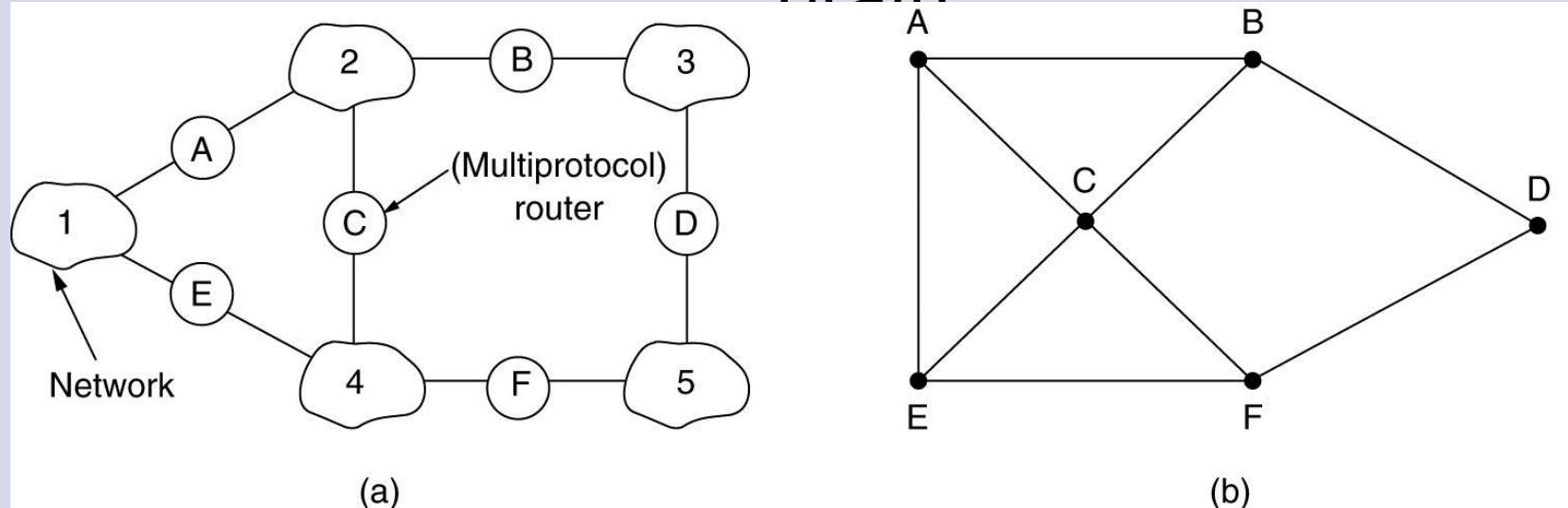
# Tunelování

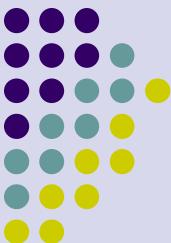




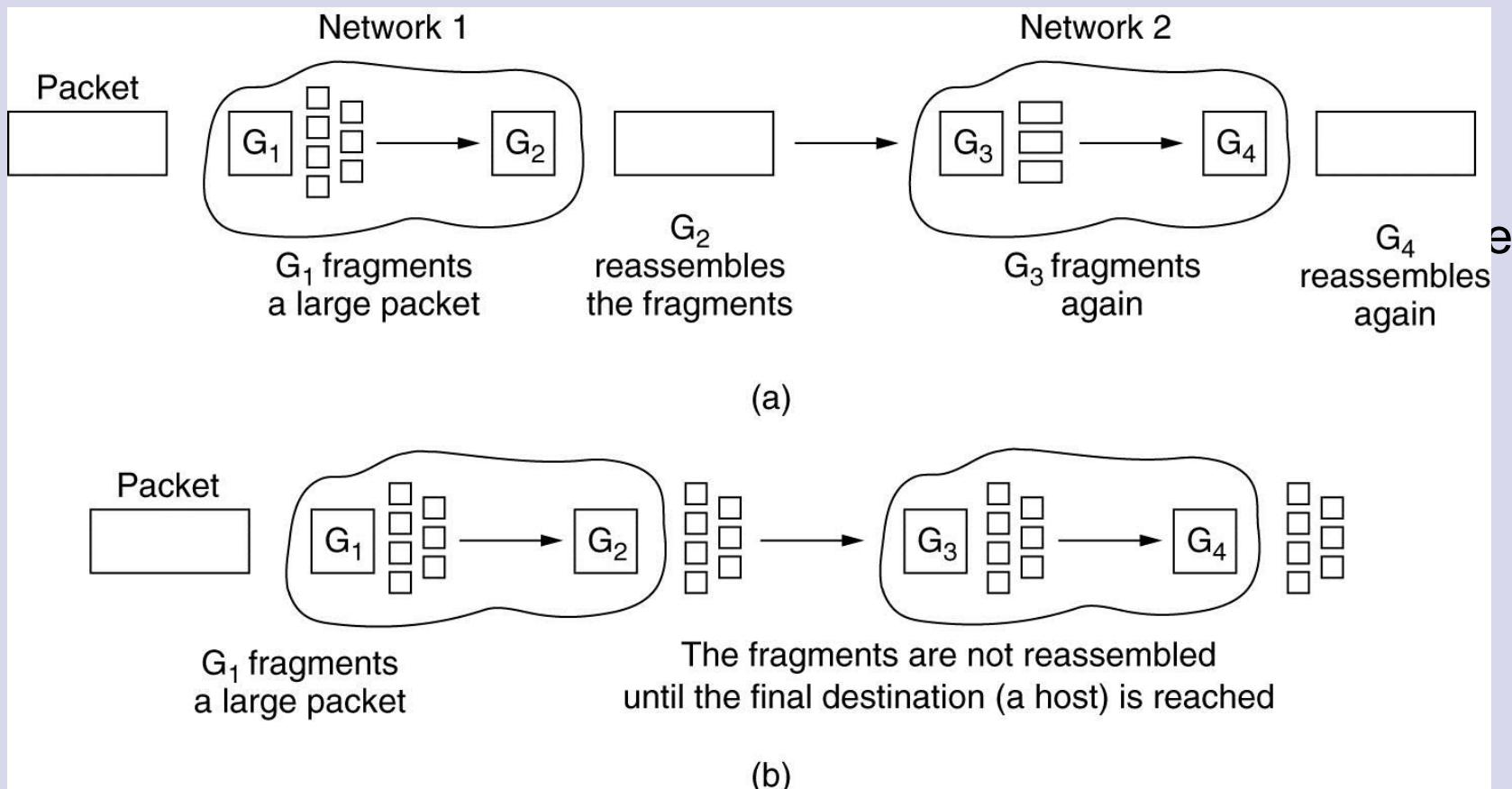
# Směrování mezi sítěmi

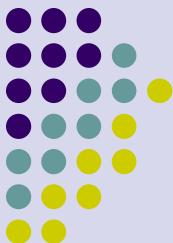
(a) Propojení sítí. (b) Znázornění v podobě grafu.



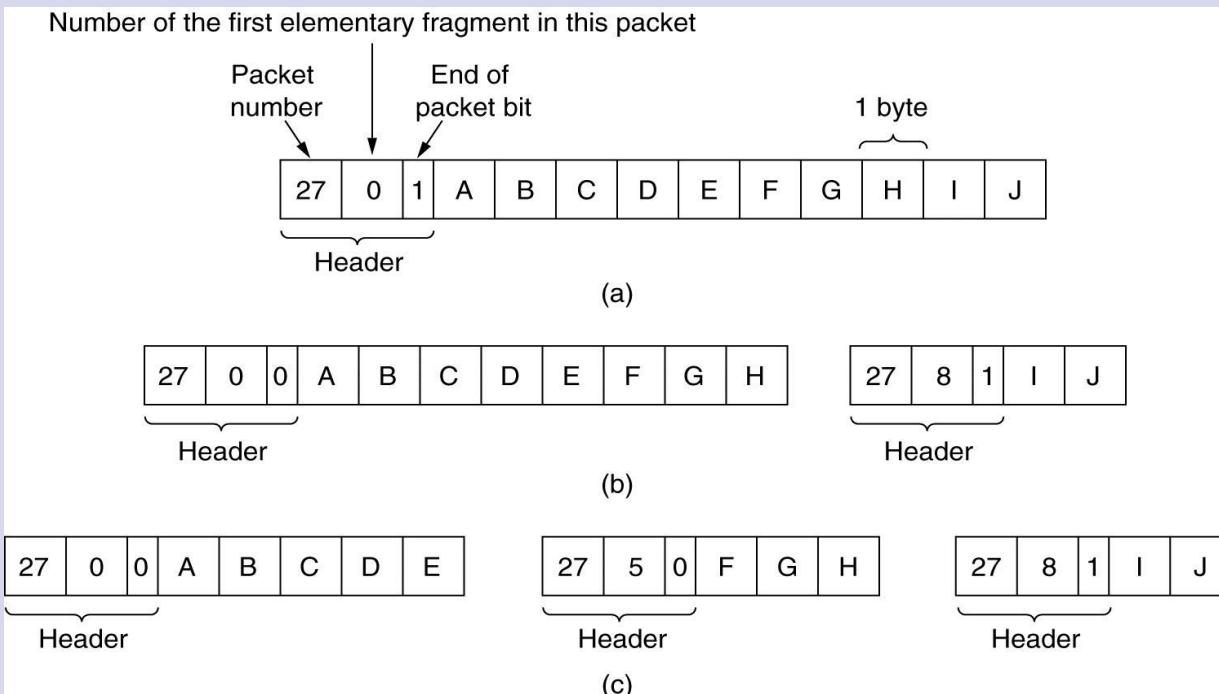


# Fragmentace





# Fragmentace (2)

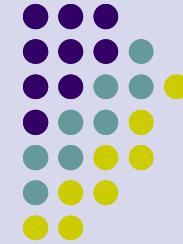


Fragmentace v případě, kdy je délka fragmentu 1.

- (a) Původní paket délky 10.
- (b) Fragmenty po přenosu sítí s maximální délkou paketu 8 (plus délka záhlaví).
- (c) Situace po průchodu směrovačem s délkou paketu 5.

# Úvod do počítačových sítí

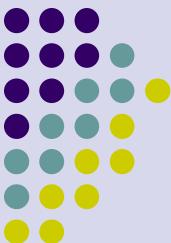
## Protokoly směrování



Úvod do počítačových sítí

Lekce 09

Ing. Jiří Iedvina, CSc.



# Protokoly směrování

- RIP – Routing Internet protocol
- OSPF – Open Shortest Path First
- BGP – Border Gateway Protocol



# Základy směrování

- Předpoklady:
  - Mějme směrovač X
  - Směrovač nemůže znát topologii celé sítě
  - X potřebuje určit směrovač pro přístup k ostatním subsítím v Internetu
  - Tato informace je uložena do směrovací tabulky směrovače
- Hlavní problémy směrování
  - Změny topologie ovlivňují rychlosť konvergence a stabilitu
  - Rozšiřitelnost (škálovatelnost) velkého množství propojených sítí, směrovačů a linek
  - Která cesta je nejlepší?
    - Minimální počet mezilehlých uzlů
    - Minimální zpoždění
    - Maximální propustnost

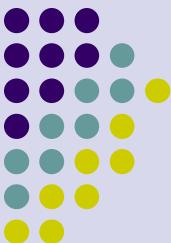


# Směrování kontra posílání

- Směrování( routing): proces vytváření směrovacích tabulek v každém směrovači
- Posílání (forwardování): zjištění cílové adresy paketu a poslání paketu na vybrané rozhraní směrovače
- Posílání vyžaduje přístup k lokální směrovací tabulce
- Někdy se vytváří tabulka pro forwardování, která se pak liší od směrovací tabulky
  - Forwardovací tabulka: optimalizovaná pro vyhledání cíle a posílání
  - Směrovací tabulka: optimalizovaná pro změny směrování, změny topologie

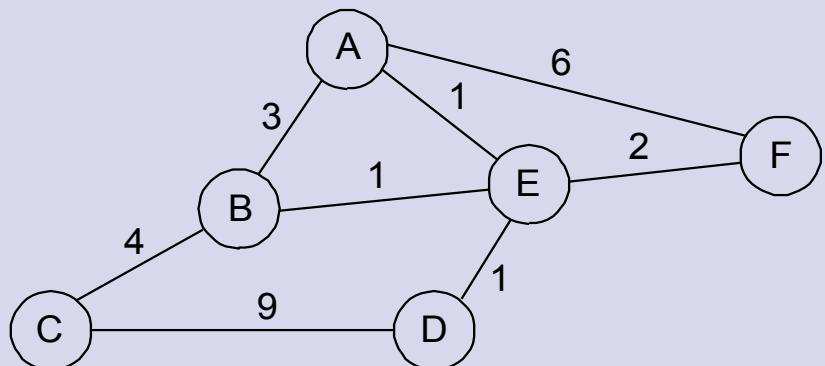
Net #	Next hop	Link Cost
10	171.69.245.10	2

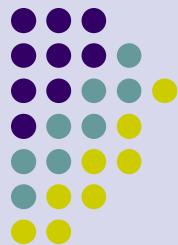
Net #	Interface	MAC Address
10	if1	00:8:0:2b:e4:b :1:2



# Směrování jako problém teorie grafů

- Uzly: směrovače jedné administrativní domény (vnitřní směrování), nebo různých sítí (vnější směrování)
- Hrany: vzájemné propojení směrovačů
- Ohodnocení hran: podle vzdálenosti, kapacity, zpoždění, ...
- Cíl: nalezení minimální cesty mezi libovolnými dvěma uzly
- Problém: nalezení minimální cesty decentralizovanou (nebo centralizovanou) metodou
- Rychlé a robustní reakce na změnu topologie



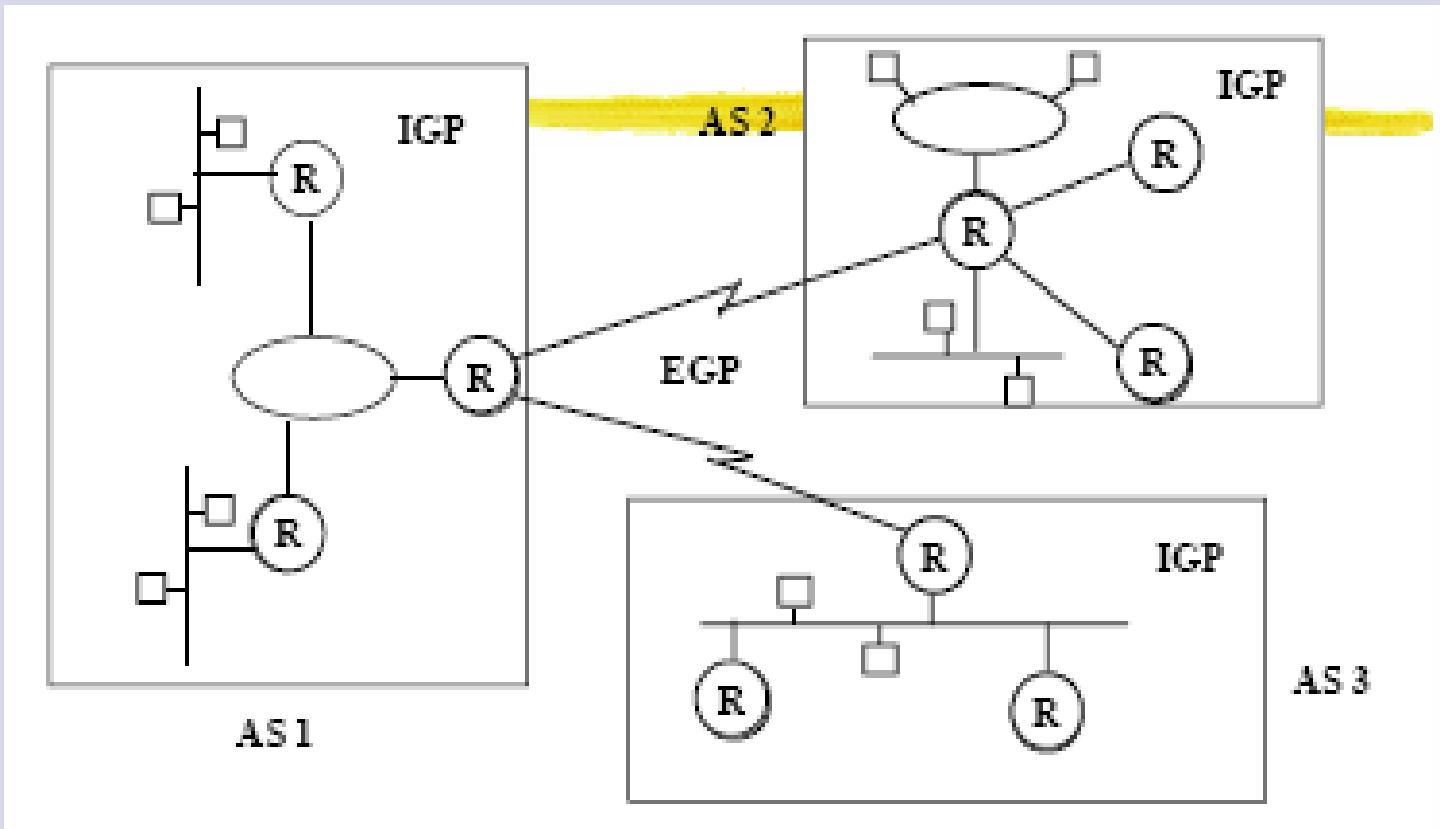


# Typy algoritmů směrování

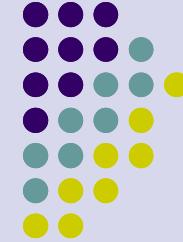
- „Statické“ směrování
  - Ruční nastavení směrovací tabulky
- „Dynamické“ směrování
  - Adaptivní algoritmy nastavení směrovací tabulky
  - Interní směrování (RIP, OSPF)
  - Externí směrování (BGP)
- Směrování podle vektoru vzdáleností (Distance Vector Algorithm)
  - Šíření obsahu směrovací tabulky sousedním směrovačům
- Směrování podle stavu linek (Link State Algorithm)
  - Šíření informace o stavu linek (hran grafu) sousedním směrovačům
- Hybridní směrování



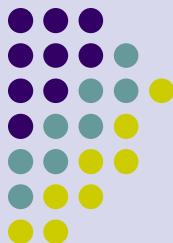
# Propojení tří autonomních oblastí



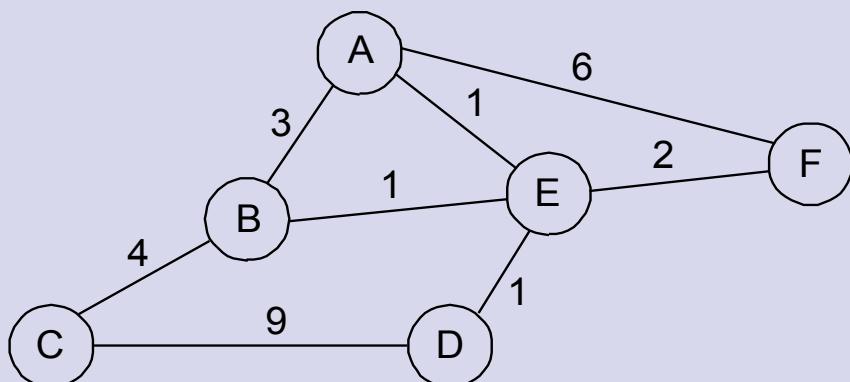
# Routing Internet Protocol



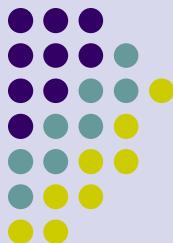
# Směrování podle vektoru vzdáleností



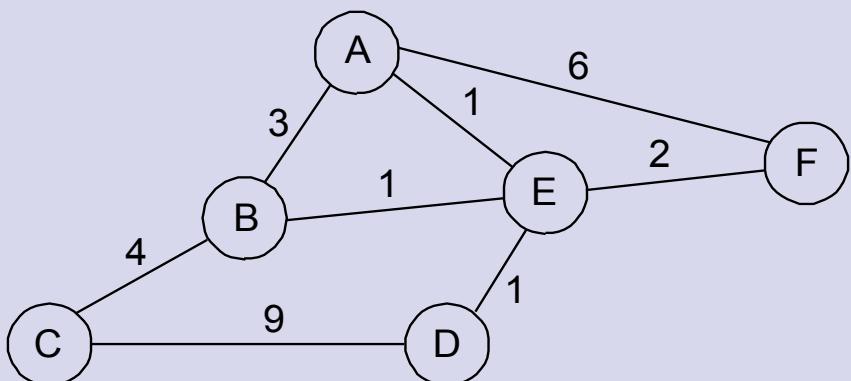
- Používá Bellman-Fordův algoritmus (dynamické programování)
- Vektor vzdáleností pro uzel X: minimální vzdálenost z uzlu X do všech ostatních uzlů
  - Např. pro uzel A je to  $\{2,6,2,1,3\}$
- Každý uzel provádí následující 3 operace souběžně
  - Posílá vektor vzdáleností svým sousedům
  - Přijímá vektor vzdáleností od svých sousedů
  - Počítá nové vzdálenosti na základě přijatých vektorů
    - $\text{distance}(X,Z) = \min \{\text{distance}(X,Y) + \text{distance}(Y, Z)\} \text{ pro všechny sousední uzly } Y$



# Směrování podle vektoru vzdáleností

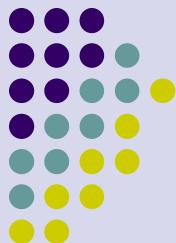


- Počáteční vektor vzdáleností vychází pouze ze znalosti vzdáleností k sousedním uzelům
  - Např. pro uzel A {3,∞,∞,1,6}

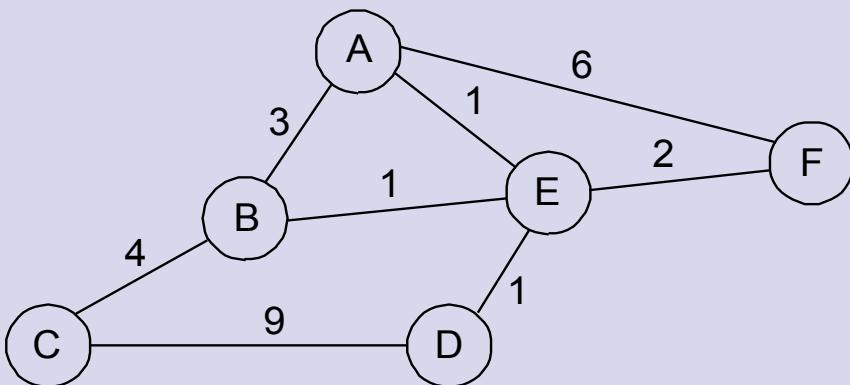


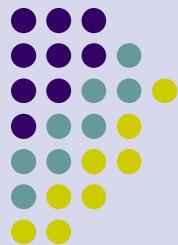
- Lokální výměna globální informace o dostupnosti
- Vektory vzdáleností jsou posílány
  - Periodicky (30s)
  - Při změně položky ve směrovací tabulce
- Uzel detekuje chyby uzelů a linek periodickou výměnou „Hello“ paketů nebo výměnou směrovací informace

# Počáteční nastavení směrování



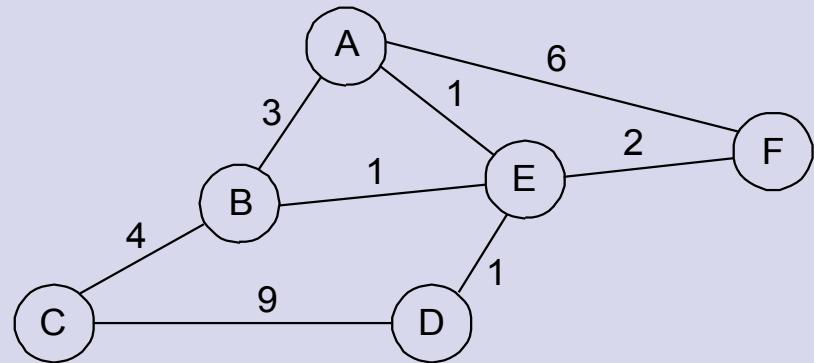
uzel	A	B	C	D	E	F
A	0	3	$\infty$	$\infty$	1	6
B	3	0	4	$\infty$	1	$\infty$
C	$\infty$	4	0	9	$\infty$	$\infty$
D	$\infty$	$\infty$	9	0	1	$\infty$
E	1	1	$\infty$	1	0	2
F	6	$\infty$	$\infty$	$\infty$	2	0

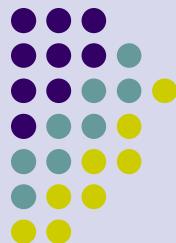




# Počáteční a finální směrovací tabulka uzlu A

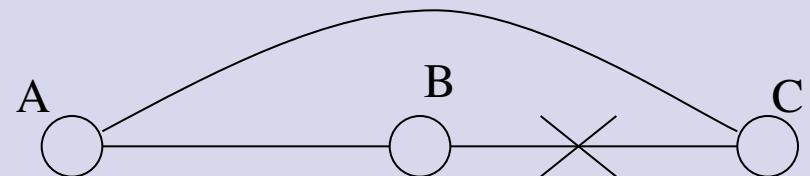
Cíl (od A)	cena	Násl. uzel
B	3	B
C	$\infty$	-
D	$\infty$	-
E	1	E
F	6	F
Cíl (od A)	cena	Násl. uzel
B	2	E
C	6	E
D	2	E
E	1	E
F	3	E

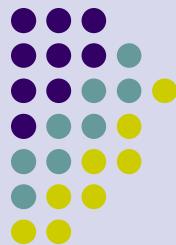




# Změny topologie

- Problém „čítání do nekonečna“
- Možná řešení
  - Omezení horní meze pro čítání (maximální vzdálenost)
  - Split horizon (rozštěpený obzor)
    - X nesmí poslat do uzlu Y svou vzdálenost k uzlu Z, je-li uzel Y ve směru z X do Z.
  - Split horizon with poisoned reverse (rozštěpený obzor s otráveným zpětným směrem)
    - X posílá do uzlu že jeho vzdálenost k uzlu Z je  $\infty$ , je-li uzel Y ve směru z X do Z.

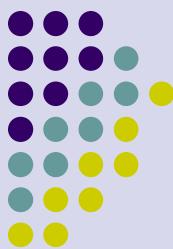




# Změny topologie

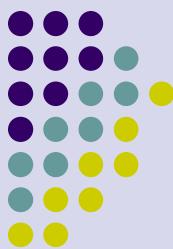
- Bohužel, žádné z těchto řešení nezabrání cyklům
- Možné řešení: Před generováním a posíláním vektoru vzdáleností, který upravuje konektivitu k jinému uzlu, počkat nějakou dobu na informace o konektivitě k tomuto uzlu od jiných uzel
  - Může významně prodloužit dobu konvergence.
- Příčinou potíží je asynchronní výměna stavových informací
- Není zaručeno, že je ve všech uzlech konzistentní směrovací informace
- Urychlení konvergence: triggered update (okamžité spuštění opravy)

# Routing Information Protocol (RIP)

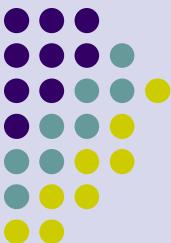


- Implementace algoritmu „směrování podle vektoru vzdáleností“
- RFC 1058, UDP port 520
- Všechny ohodnocení linek jsou nastaveny na 1 (počet mezilehlých uzlů)
- Vektory vzdáleností vyměňovány každých 30 s
- Maximální možné ohodnocení je 15, 16 je nekonečno

# Routing Information Protocol (RIP)



- Omezení cyklů pomocí algoritmu „Split horizon with poisoned reverse“ (rozštěpený obzor s otráveným zpětným směrem)
- Urychlení konvergence pomocí „Triggered update“ (okamžitá oprava)
- Někdy se používá také „Hold down“ (pozdržení odeslání informace o výpadku uzlu nebo linky)
- Detekce výpadku uzlu nebo linky po 180 s
- Výmaz z nedostupnosti ze směrovací tabulky po 120 s
- Max. velikost datagramu 512 slabik – 25 cest



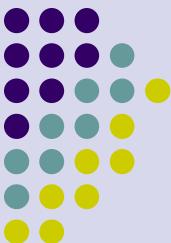
# Záhlaví RIP

0	8	16	31
Command	Version	Must be zero	
Family of net 1		Address of net 1	
Address of net 1			
Distance to net 1			
Family of net 2		Address of net 2	
Address of net 2			
Distance to net 2			



# Algoritmus opravy směrovací tabulky

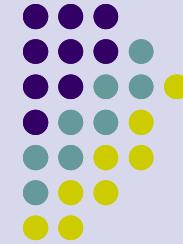
- Pokud je nově vypočtená vzdálenost
  - Menší – opravit
  - Stejná – nic neměnit
  - Horší
    - Na základě zprávy ze směrovače, který je sousední pro původní směrování – opravit (zhoršení ocenění)
    - Na základě zprávy z jiného směrovače – nic neměnit
- Aktivní režim (směrovač)
- Pasivní režim (hostitelský systém)



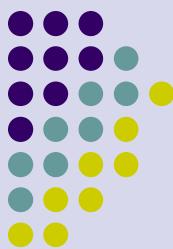
# RIP - 2

- Nástupce RIP
- Již se neprosadil – využívá se OSPF
- Úpravy odstraňující některé nevýhody RIP
  - Posílání subsítové masky a adresy následujícího uzlu
  - Podpora skupinového doručování – snížení zátěže
  - Podpora ověřování pravosti - heslo

# Open Shortest Path First

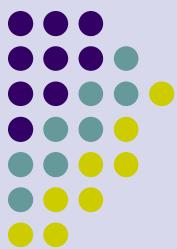


# Směrování podle stavu linek (LSA)



- Link State Algorithm (LSA) – směrování podle stavu linek
- Každý uzel ví jak dosáhnout přímo spojené sousedy: lokální link-state (stav linek)
- Přerušené linky nebo nefungující sousední směrovače jsou detekovány periodickou výměnou „hello“ zpráv
- Každý směrovač šíří vlastní stav linek do všech ostatních uzlů sítě pomocí spolehlivého záplavového doručování
- Znalost stavu linek ze všech uzlů je dostatečná pro konstrukci grafu propojení celé sítě
- Každý uzel vypočte minimální vzdálenost k ostatním uzlům pomocí Dijkstrova algoritmu

# Spolehlivé záplavové doručování

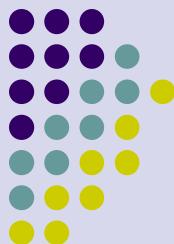


- Každý uzel generuje periodicky nebo při změně stavu lokální linky Link State pakety (LSP)
- LSP obsahuje:
  - ID uzlu, který LSP generuje
  - Seznam přímo propojených sousedů s cenami přidružených linek
  - Sekvenční číslo tohoto LSP
  - TTL pro toto LSP
- Uzel, který LSP přijme, pošle jej všem svým sousedům, kromě toho, od kterého ji obdržel
- Sekvenční číslo LSP musí být větší, než posledně uloženého LSP od tohoto uzlu
- Přenos LSP musí být spolehlivý
  - Používá se potvrzení, timeouty a opakování přenosu

# Spolehlivé záplavové doručování

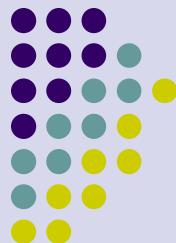


- Před posláním LSP sousedům snižuje hodnotu TTL
  - Jestliže TTL LSP dosáhlo nuly, posílá je uzel dál s tím, že je to signál pro vyřazení tohoto LSP ze všech uzlů
  - Pomocí TTL se měří stáří lokálně uložených LSP
- Co se stane, když sekvenční číslo LSP dosáhne maxima?
- Co se stane když se uzel rychle vypne a zase zapne bez toho, že sousedé detekují výpadek?
  - Uzel si může od souseda vyžádat poslední uložené LSP



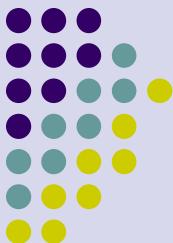
# Klady a zápory LSA

- Rychlé ustálení po změně topologie
- Více robustní než RIP
  - Předchází problému čítání do nekonečna
- Vyžaduje ukládání LPS v každém uzlu (týká se rozšiřitelnosti)
  - OSPF se proto používá pouze pro interní směrování (omezení z důvodu škálovatelnosti – rozšiřitelnosti)



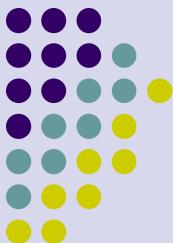
# Protokol OSPF

- Open Shortest Path First (OSPF) – RFC 2328
- Nejvýznamnější směrovací protokol pro interní směrování
- Používá zprávy:
  - Hello – vyhledání souseda
  - Database Description – přenos databáze sousedovi
  - Link State Request – požadavek na zaslání databáze (synchronizace)
  - Link State Update – oprava topologie (router, network, network summary, ASBR summary, AS external LSA)
  - Link State Acknowledgement – potvrzení opravy topologie

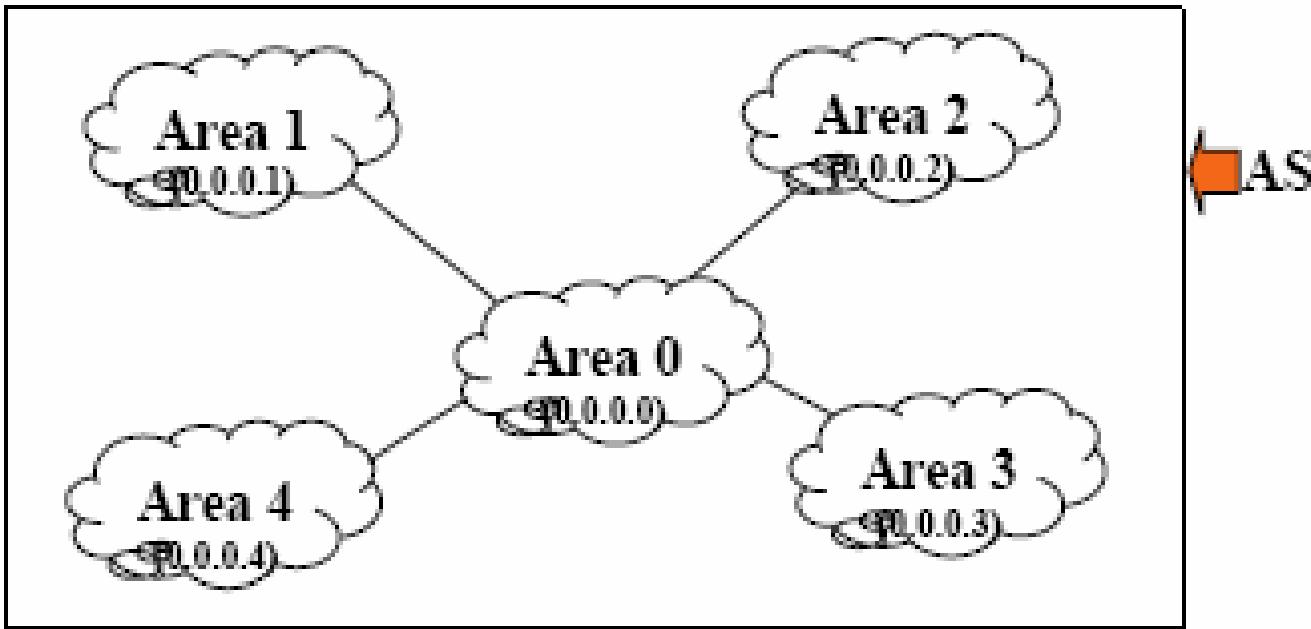


# Protokol OSPF

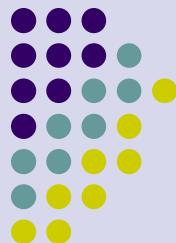
- Další vlastnosti:
  - Ověřování pravosti přenášených zpráv
  - Zavedení směrovacích oblastí – řešení problému rozšiřitelnosti
  - Vyrovnávání zátěže – využívání více cest se stejným ohodnocením mezi dvěma uzly
  - Směrování podle TOS (Type of Service)
  - Adresování pomocí skupinového adresování (multicast)
  - Přímé použití IP (protokol 69)
  - Import RIP a EGP cest do své databáze
  - Rozsáhlé směrovací tabulky



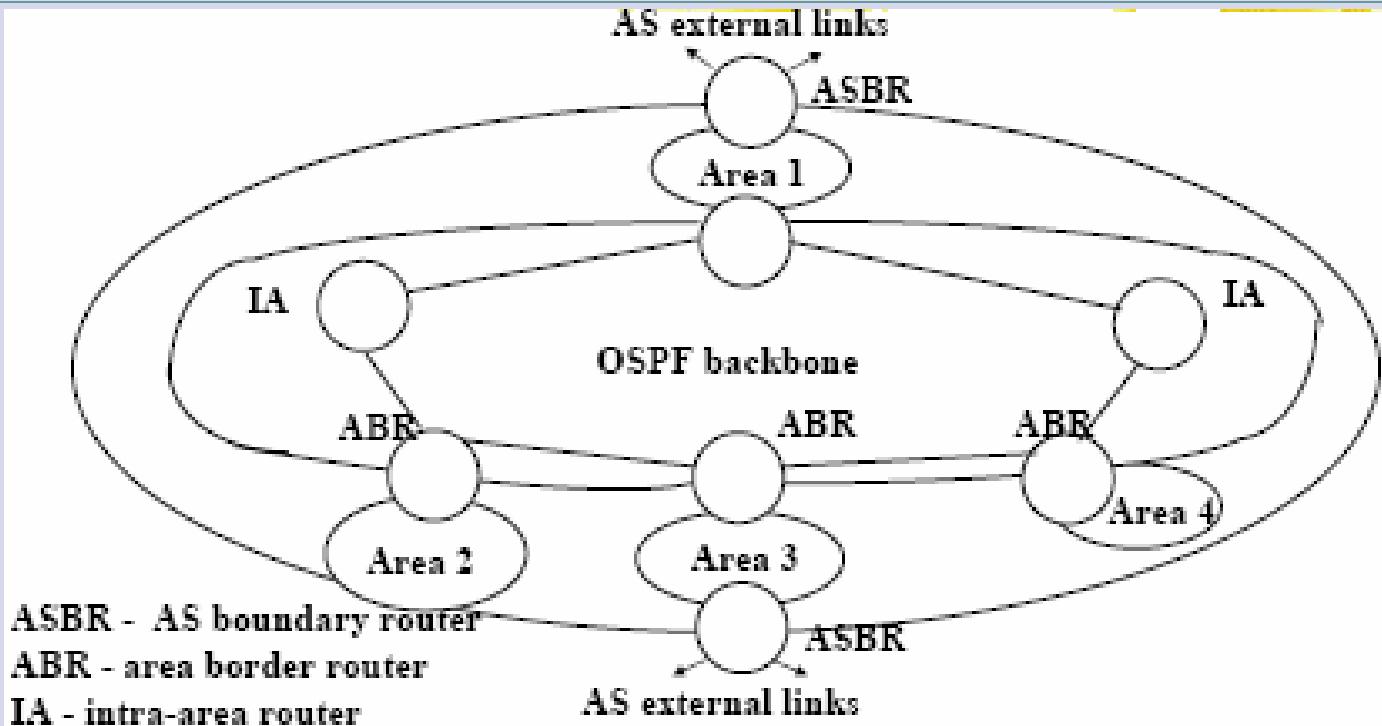
# OSPF oblasti



- Autonomní oblast rozdělena do několika oblastí – hierarchické směrování – škálovatelnost
- Každá oblast má přiřazeno číslo (32 bitů – a.b.c.d)
  - Páteřní oblast (oblast 0) je 0.0.0.0



# OSPF typy směrovačů

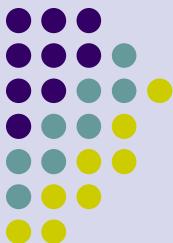


- ASBR – AS Boundary Router
- ABR – Area Border Router
- IA – Intra Area router
- Všechny směrovače mají tutéž topologickou databázi
- Znají topologii uvnitř oblasti



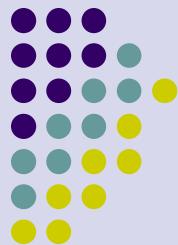
# Typy OSPF zpráv

- Hello – vyhledání souseda
- Database Description – přenos databáze sousedovi
- Link State Request – požadavek na zaslání databáze (synchronizace)
- Link State Update – oprava topologie
  - Route LSA
  - Network LSA
  - Network Summary LSA
  - ASBR Summary LSA
  - AS External LSA
- Link State Acknowledgement – potvrzení opravy topologie



# Určení ceny (ohodnocení) linky

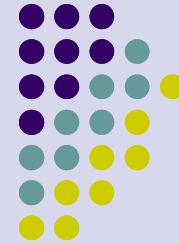
- Nejjednodušší (často používané)
  - Všechny linky mají stejnou cenu – směrování s minimálním ohodnocením
- Cena linky – převrácená hodnota kapacity
  - 10Mb linka má 100 krát vyšší cenu než 1Gb linka
- Cena linky – zpoždění linky
  - 250ms satelitní spojení má 10 krát větší cenu než 25ms pozemní linka
- Cena linky – využití linky
  - Linka s 90% využitím má 10 krát vyšší cenu než linka s 9% využitím
  - Může způsobit oscilace
- Žádný z těchto způsobů není optimální pro všechny sítě



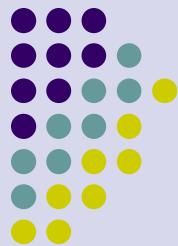
# Vyhledávání sousedství

- Používají se zprávy typu Hello
- Jsou generovány pro všechna rozhraní, obsahují
  - IP adresu a masku pro toto rozhraní
  - Hello interval (platnost)
  - Seznam sousedů jejichž Hello pakety vysílač již slyšel
- Posílány na IP adresu 224.0.0.5 každých 10s
- Nepřijme-li se Hello zpráva od souseda 40s – zrušení sousedství

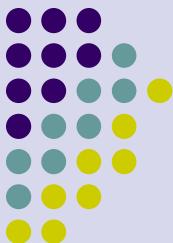
# **Směrování - BGP**



# Border Gateway Protocol (BGP)



- Protokol pro směrování mezi autonomními oblastmi
- Rozdíly Inter-AS a Intra-AS směrování
  - rozhodování
    - Intra-AS: jeden administrátor, není třeba rozhodovací strategie
    - Inter-AS: administrátor chce kontrolovat kudy je přenos směrován, kdo je směrován přes jeho síť
  - Rozsah
    - Hierarchické směrování redukuje velikost tabulek i přenos oprávek
  - Výkonnost
    - Intra-AS: může se soustředit na výkon
    - Inter-AS: rozhodovací strategie může vítězit nad výkonností



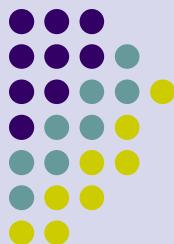
# AS - Autonomous System

- Soubor IP sítí a směrovačů pod kontrolou jedné entity, prezentovaná společnou směrovací politikou do Internetu
- K AS musí být přiřazeno ASN (AS number), které je použito při směrování pomocí BGP
- ASN jednoznačně identifikuje AS v Internetu (16 bitů)
- ASN 64512 až 65534 mohou být použity privátně
- ASN 0 a 65535 jsou rezervované
- Cesnet ASN 2852 (16 bitů)
- 1/2006 – cca 40000 obsazených (3500 za rok)
- RFC 4893 – 32 bitů ASN (číslo.číslo RIPE 3.0 až 3.1023)
- Nová verze BGP
- Multihomed (více AS), stub (jedna AS), transit (přenosová AS)



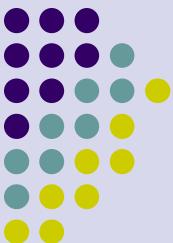
# BGP přenáší TCP

- TCP port 179
- Dvoubodové spoje, spojované služby, unicast
- TCP zachycuje mnoho problémů s chybami, BGP může být jednodušší
- BGP nepotřebuje vlastní spolehlivý protokol
- Může přenášet přes více uzlů, pokud je to třeba
- Přenáší tok dat



# BGP základní operace

- BGP udržuje směrovací tabulky, šíří opravy směrování a rozhodnutí o směrování zakladá na směrovací metrice
  - Vyměňuje informaci o dosažitelnosti sítě (reachability)
  - Vytváří graf propojitelnosti AS (AS connectivity)
  - Odstraňuje směrovací smyčky a prosazuje rozhodnutí o strategii
- BGP používá jednu metriku k určení nejlepší cesty
  - Linková metrika je hodnota preference přiřazená administrátorem
  - Je to multikriteriální funkce: počet procházených AS, strategie směrování, stability, rychlosti, zpoždění, ceny, ...
- Vybírá nejlepší cestu a instaluje IP forwardovací tabulku

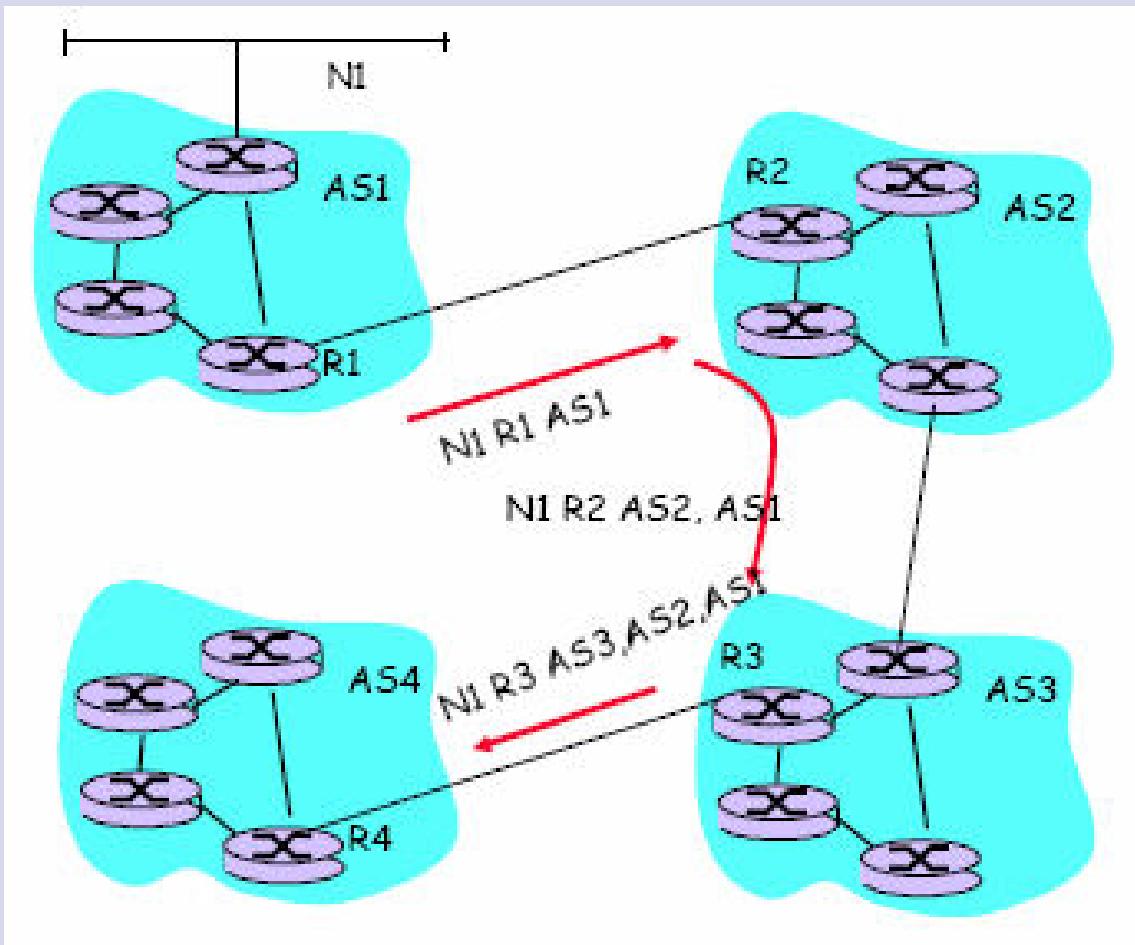
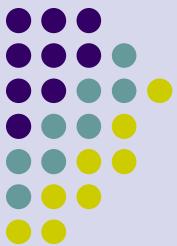


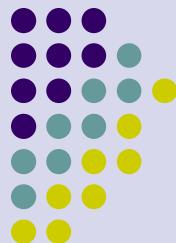
# Border Gateway Protocol (BGP)

- Path Vector protocol
  - Podobný Distance Vector Protocol
  - Každý BGP směrovač posílá pomocí broadcastu sousedům celou cestu (posloupnost AS) do cíle
  - BGP směruje do sítí (AS), ne do individuálních hostů
  - Př. Směrovač X posílá cestu do cílové sítě Z

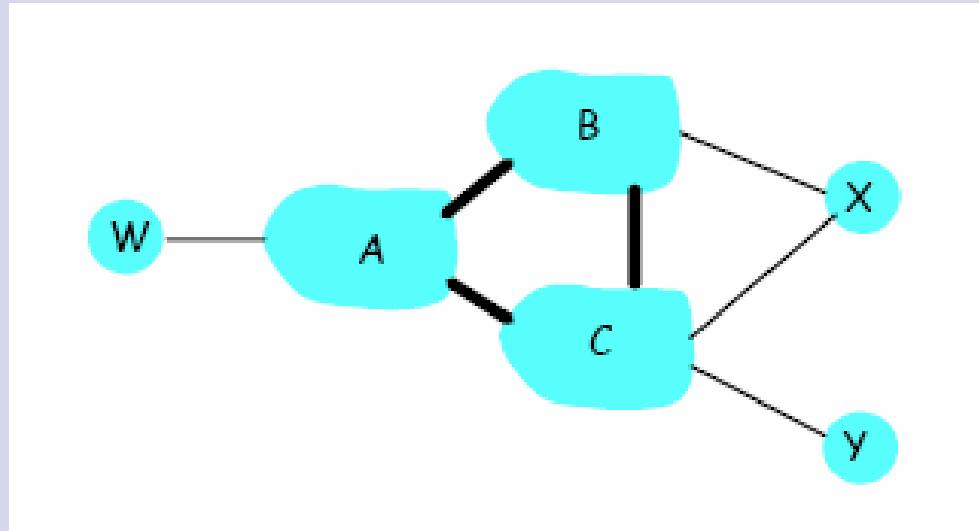
$$\text{Path}(X, Z) = X, Y_1, Y_2, \dots, Y_n, Z$$

# Border Gateway Protocol (BGP)

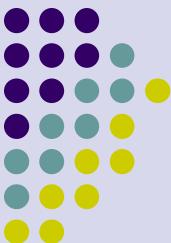




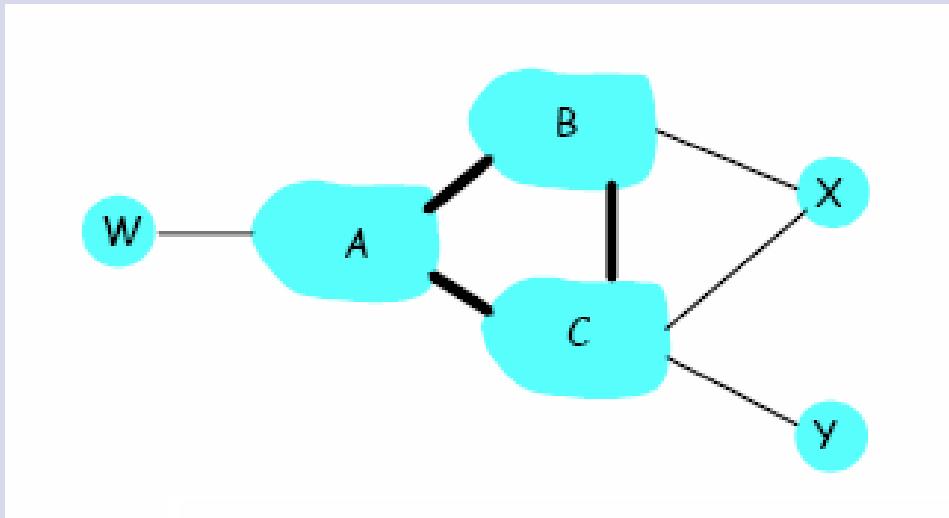
# BGP: řízení směrování



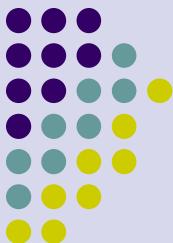
- A, B, C jsou sítě poskytovatele
- X, W, Y jsou uživatelé sítí poskytovatelů
- X je dual homed, připojený ke dvěma sítím
  - X nechce směrovat z B do C přes X
  - Proto X nebude nabízet (inzerovat) pro síť B cestu do C



# BGP: řízení směrování



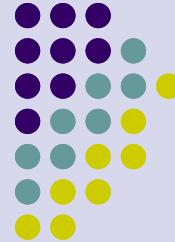
- A inzeruje do B cestu AW
- B inzeruje do X cestu BAW
- Může B inzerovat do C cestu BAW?
  - Ne, B nechce, aby přes B byly směrovány z W do C (CBAW), protože ani C, ani W není zákazníkem B
  - B chce, aby C komunikovalo s W přes A
  - B chce směrovat pouze pro své zákazníky



# BGP zprávy

- BGP zprávy jsou přenášeny pomocí TCP (port 179) – spolehlivý přenos dat
- BGP zprávy
  - OPEN: otevření spojení k protějšku a ověřování vysílače
  - UPDATE: nabízí novou cestu (nebo odstraňuje starou)
  - KEEPALIVE: udržuje spojení při životě pokud nechodí zprávy UPDATE. Také potvrzení požadavky OPEN
  - NOTIFICATION: oznamuje chyby předcházející zprávy, také použita pro uzavření spojení

# Internet multicast



Úvod do počítačových sítí

Lekce 9

Ing. Jiří Šedivina, CSc.

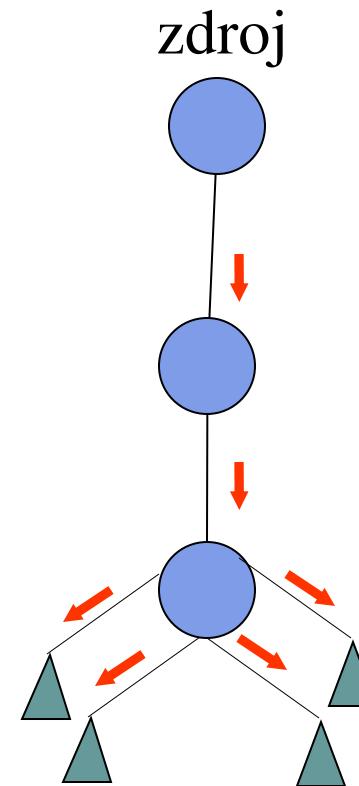
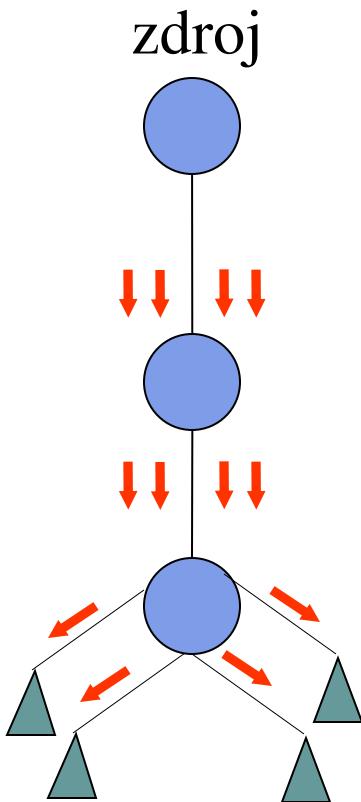


# Broadcast, multicast, unicast

- Broadcast
  - Posílání kopie všem
  - Jednoduché ale neefektivní
  - Zprávu musí zpracovat všichni, i když je to nezajímá
  - Zbytečné zatěžování CPU
  - Zbytečné zatěžování sítě
- Replikovaný unicast
  - Vysílač postupně posílá kopii každému příjemci
  - Příjemci musí být registrováni u vysílače
  - Vysílač je středem pro řízení
  - Spolehlivost – pro každý přijímač oddělený proces nebo stav ve vysílači



# Multicast – Efektivní distribuce dat





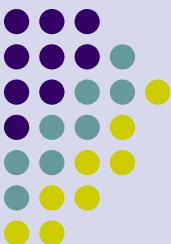
# Aplikace multicastu

- Obnova textových informací (noviny, sport, počasí, ...)
- Distance learning
- Konfigurace skupin zařízení
- Telekonferencing (zvuk, video, sdílená tabule, textový editor, ...)
- Distribuované interaktivní hry a simulace
- Doručování el.pošty
- Distribuce programového vybavení
- Obnova vyrovnávacích pamětí (cache)
- Replikace databází



# Metody skupinového směrování

- Záplavové směrování
- Sdílená kostra grafu
- Vytváření kostry grafu
  - Směrování typu „reverse path“
    - Pro všechny přenosy (broadcasting)
    - Pro skupiny (multicasting)
  - Ořezávání větví grafu
- „Core based tree“ – stromy se společným základem

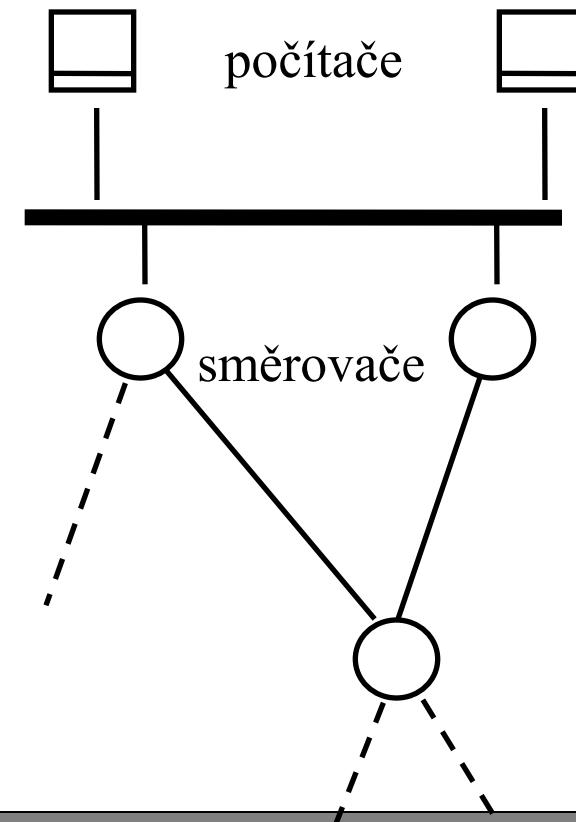


# Architektura IP multicastu

**Servisní model  
(adresování, zpracování dat)**

**Protokol pro registraci hostů  
(IGMP)**

**Protokoly pro směrování  
- interní, externí  
(PIM, MOSPF, DVMRP,  
BGMP)**





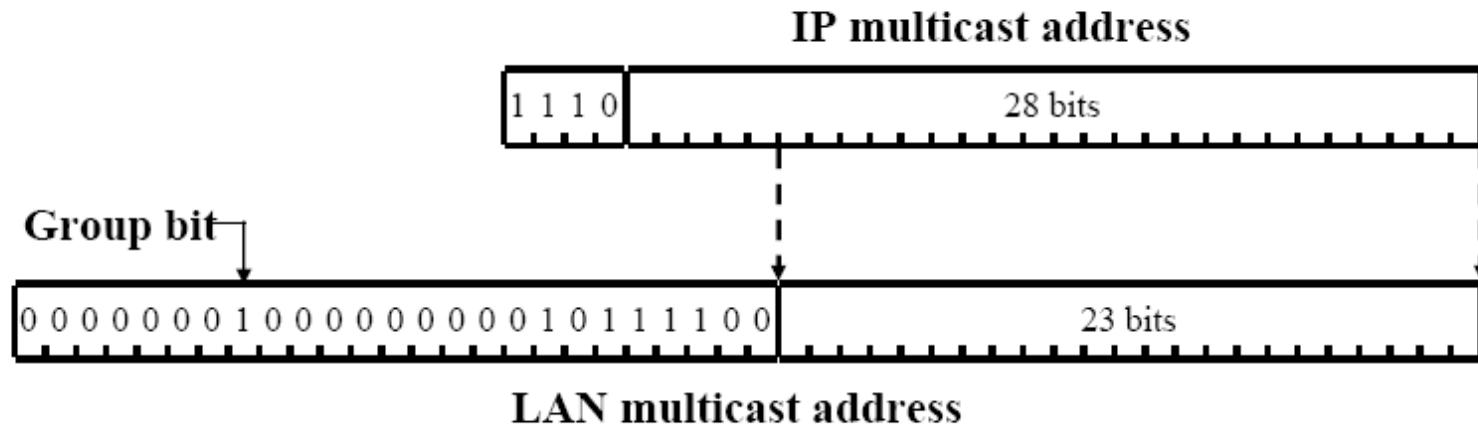
# Architektura IP multicastu

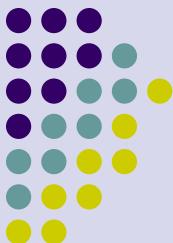
- Organizace hostitelského systému
  - Povolení přijímat multicast, definice multicast adresy na MAC úrovni
- Organizace lokální směrovač – hostitelský systém
  - Protokoly pro organizaci skupin
  - IGMP (Internet Group Management Protocol)
    - Verze 1 – pouze registrace/uvolnění (RFC 1112)
    - Verze 2 – připojení/odpojení zprávou (RFC 2236)
    - Verze 3 – podpora SSM (RFC3376)
- Skupinové směrování
  - Protokoly pro skupinové směrování (PIM-DM, PIM-SM, BGMP)



# Mapování IP síťových adres na MAC multicast adresy

- RFC 1112 definuje
  - Pro Ethernet a FDDI adresní prefix 01:00:5E
  - Mapuje nižších 23 bitů skupinové IP adresy přímo na MAC adresu
  - Token Ring používá funkční adresu c000.4000.0000





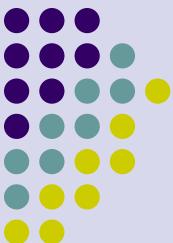
# Určení rozsahu doručování

- Implicitní
  - Použití link-local adresy
  - Neopustí podsít'
- Omezení rozsahu založené na TTL
  - Multicast směrovače mají nastaven práh (TTL práh)
  - Jestliže je  $\text{TTL} \leq \text{TTL práh}$ , je datagram zahozen
- Administrativní omezení
  - Použití skupiny adres 239.0.0.0 až 239.255.255.255
  - Omezení na administrativní doménu
  - V IPv6 je rozsah součástí atributu uvedeného v adrese



# Rozdělení skupinových adres (RFC3171)

224.0.0.0 - 224.0.0.255 (224.0.0/24)	Local Network Control Block
224.0.1.0 - 224.0.1.255 (224.0.1/24)	Internetwork Control Block
224.0.2.0 - 224.0.255.0	AD-HOC Block
224.1.0.0 - 224.1.255.255 (224.1/16)	ST Multicast Groups
224.2.0.0 - 224.2.255.255 (224.2/16)	SDP/SAP Block
224.252.0.0 - 224.255.255.255	DIS Transient Block
225.0.0.0 - 231.255.255.255	RESERVED
232.0.0.0 - 232.255.255.255 (232/8)	Source Specific Multicast Block
233.0.0.0 - 233.255.255.255 (233/8)	GLOP Block (233.X.Y.0)
234.0.0.0 - 238.255.255.255	RESERVED
239.0.0.0 - 239.255.255.255 (239/8)	Administratively Scoped Block



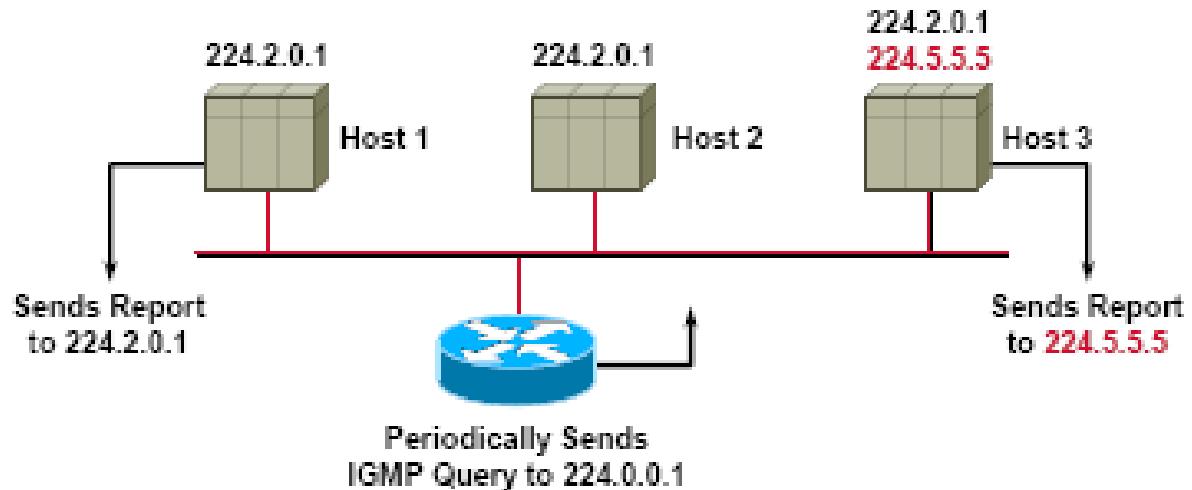
# IGMPv1

- Dotazování
  - Na subsíti je vybrán jeden směrovač pro údržbu skupin
  - Výzva je posílána na adresu 224.0.0.1 s TTL=1
  - Výzva se posílá v intervalu 60 až 120s (60 až 90s)
- Odpověď
  - IGMP report posílá pro každou skupinu pouze jeden host - ostatní se odpovědi zdrží, když za ně odpovídá jiný
  - Zajištěno tak, že odpověď není okamžitá, ale zpožděná o cca 5 až 10s
  - Odpověď je posílána na skupinovou adresu.
  - Při přistoupení ke skupině posílá host odpověď bez vyzvání
- Detekce existence skupiny
  - Pokud se nikdo neozve, skupina asi neexistuje

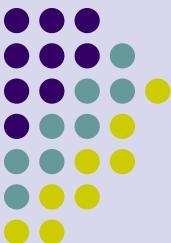


# IGMPv1

- Připojení se ke skupině

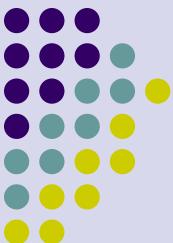


- Formát IGMP packetu
  - Version (4)
  - Typ (4)
  - Unused (8)
  - IGMP checksum (16)
  - Group address (32)
- Typ
  - Host Membership Query (1)
  - Host membership Report (2)
  - DVMRP (3)



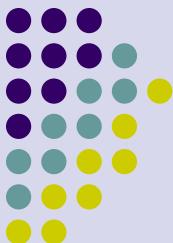
# IGMPv2

- Hostitelský systém posílá zprávu o opuštění skupiny
  - Leave message na adresu „all routers“ 224.0.0.2
  - Zkrátí se doba pro detekci prázdné skupiny
- Směrovač reaguje specifickou výzvou (specifická skupinová adresa) aby se ujistil, není-li skupina prázdná
  - Je-li skupina prázdná, přestává do subsítě posílat další multicast zprávy



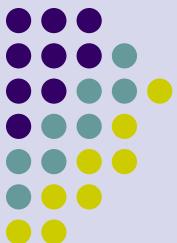
# IGMPv2

- Formát IGMP packetu
  - Typ (8)
  - MaxResponseTime (8)
    - Max čas pro odpověď v násobcích 0.1s
  - IGMP checksum (16)
  - Group address (32)
- Type
  - GroupMembershipQuery (0x11)
    - General
    - group-specific
  - Membership Report ver.1 (0x12)
  - Membership Report ver.2 (0x16)
  - Leave Group (0x17)
  - Multicast Router Advertisement (0x24)
  - Multicast Router Solicitation (0x25)
  - Multicast Router Termination (0x26)



# IGMPv3

- Dovoluje od sebe odlišit vysílače ve skupině
- Formát rámce MembershipQuery
  - General Query (GroupAddress = 0.0.0.0, N=0)
  - GroupSpecificQuery (GroupAddress = addr, N=0)
  - Group and Source Specific Query (GroupAddress = addr, SourceAddress = SourceAddrs)



# Multicast modely

- ASM – Any Source Multicast
  - Může být více zdrojů, které se nerozlišují
  - Jeden nebo více zdrojů, jedna skupina
- SSM – Source Specific Multicast
  - Může být více zdrojů, které se však při doručování rozlišují



# Protokoly pro skupinové směrování

- DVMRP – Distance Vector Multicast Routing protocol
  - Jeden z prvních protokolů pro skupinové doručování
  - Pouze pro „hustý režim“ – dense mode
  - Používá záplavové doručování a ořezávání hran
  - Explicitní připojení subsítě
  - Používá source-based distribuční stromy



# Protokoly pro skupinové směrování

- MOSPF – Multicast OSPF
  - Opět „hustý“ dense mode
  - Připojování pomocí zpráv Join
  - Není třeba neustále šířit data záplavou (flood) od každého zdroje do každé podsítě
  - Používá source-based distribuční stromy



# Protokoly pro skupinové směrování

- PIM-DM – Protocol Independent Multicast – Dense Mode
  - Hustý režim znamená, že se implicitně doručuje vše do všech subsítí
  - Nemůže se používat společně se PIM-SM – Sparse mode (řídký režim), ale existuje kombinace SM-DM
  - Může použít libovolný směrovací protokol k zjišťování RPF (Reverse Path Forwarding) – zjišťování nejkratší cesty ke zdroji
  - Používá source-based distribuční stromy
  - Směrovače používají záplavové směrování s odřezáváním (flood-and-prune)
  - Existuje i explicitní Join zpráva



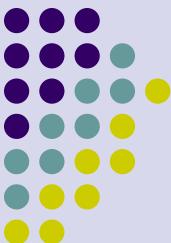
# Protokoly pro skupinové směrování

- PIM-SM – Protocol Independent Multicast – Sparse Mode
  - Řídký režim znamená, že protokol používá explicitní Join zprávu pro připojení toku do subsítě
  - RPF je nezávislé na konkrétním směrovacím protokolu
  - Doručovací stromy se budují mezi příjemcem a RP (Randevous Point) – univerzální (ASM – Any Source Multicast) strom
  - Pokud je cesta ke konkrétnímu zdroji kratší, přechází PIM-SM od ASM ke SSM (Source Specific Multicast)



# Protokoly pro skupinové směrování

- CBT – Core Based Tree
  - Přebírá charakteristiky PIM-SM
    - Řídký režim, explicitní připojení, sdílené doručovací stromy
  - Efektivnější při vyhledávání zdrojů než PIM-SM
  - Vytváří infrastrukturu (páteř) pro doručování multicast zpráv
  - Není komerčně používán



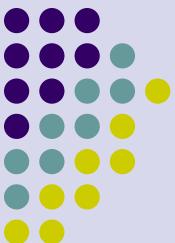
# Porovnání protokolů pro skupinové směrování

Protocol	Dense Mode?	Sparse Mode?	Implicit Join?	Explicit Join?	(S,G) SBT?	(*,G) shared tree?
DVMRP	Yes	No	Yes	No	Yes	No
MOSPF	Yes	No	No	Yes	Yes	No
PIM-DM	Yes	No	Yes	No	Yes	No
PIM-SM	No	Yes	No	Yes	Yes, maybe	Yes, initially
CBT	No	Yes	No	Yes	No	Yes



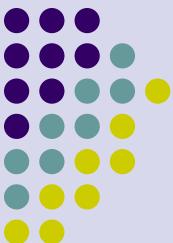
# PIM – Protocol Independent Multicast

- Existuje ve dvou verzích, lišících se formátem rámců
  - PIM-DM v1 – používá IGMP rámce (nemá RFC)
  - PIM-DM v2 – vlastní rámce (IP protokol 103) (RFC 3973)
  - Mohou koexistovat na tomtéž směrovači nebo tomtéž rozhraní
- **PIM-SM (RFC 2362, RFC 4601)**
  - Zavádí RP (Randevous Points)
  - Více RP – zvýšení odolnosti proti chybám
  - Provádí se RP-to-group mapping
    - Host požaduje připojení ke skupině prostřednictvím multicast směrovače podsítě
    - Multicast směrovač podsítě hledá RP
    - Řízeno BSR (Broadcast Router), PIM bootstrap protocol



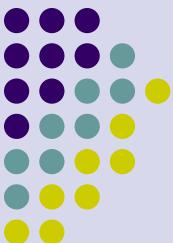
# Režimy PIM

- Dva základní režimy
  - Sparse mode
  - Dense mode
- Může pracovat také v sparse-dense mode
  - Nějaká skupina konfigurována pro sparse mode (flood-and-prune), (S,G) stavy
  - Jiné konfigurovány pro sparse mode (explicitní připojení k RP), (\*,G) stavy
- PIM source-specific mode (PIM-SSM)
  - Pouze jeden zdroj pro multicast v dané doméně



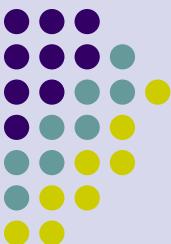
# PIM-DM

- Použitelný pro LAN skupinové aplikace
- Používá tentýž flood-and-prune mechanizmus jako DVMRP
- Rozdíl je v tom, že PIM nemá vlastní směrovací protokol
- PIM používá tabulky směrovacího protokolu pro individuální směrování
- Dat využívá pro realizaci RPF (Reverse Path Forwarding) mechanizmu

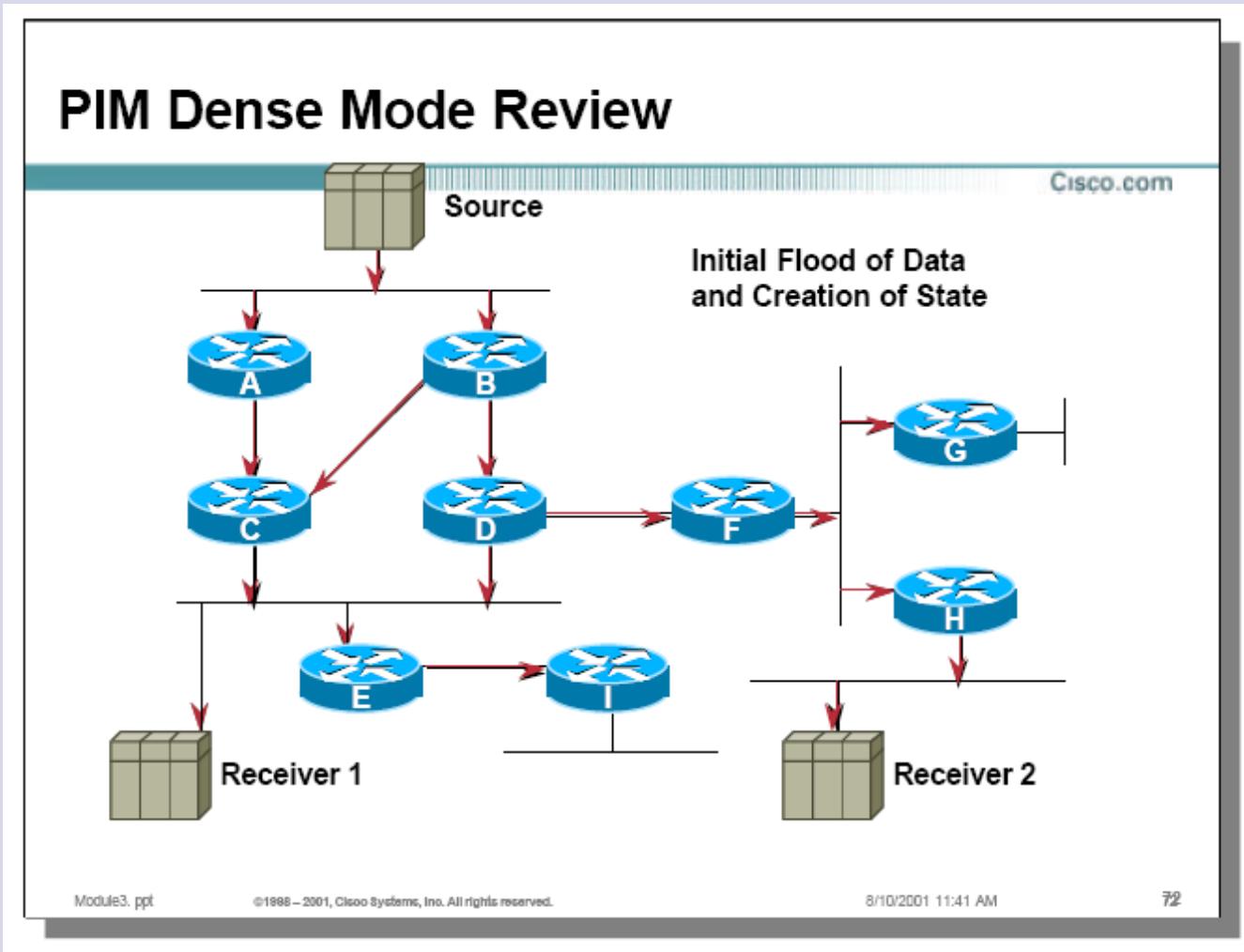


# PIM zprávy

- Hello
  - Vytvoření sousedství multicast směrovačů
  - Vysílají se periodicky (Hold time – doba dosažitelnosti, DR priority – výběr DR, Generation ID – náhodné číslo – detekce reaktivace)
- Join/Prune
  - Seznam připojovaných a odpojovaných adres pro dané skupiny
  - Záplavově se připojuje po 3min.
- Graft/GraftACK
  - Mnohabodové sítě, znovupřipojení po jedné po odpojení (prune) druhé (3s)
- Assert
  - Po detekci duplicitních cest do společné sítě posílají směrovače zprávu assert – výběr jednoho z nich. Následuje jakoby prune (3min)



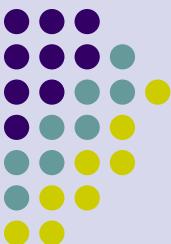
# Příklad PIM-DM





# PIM-SM

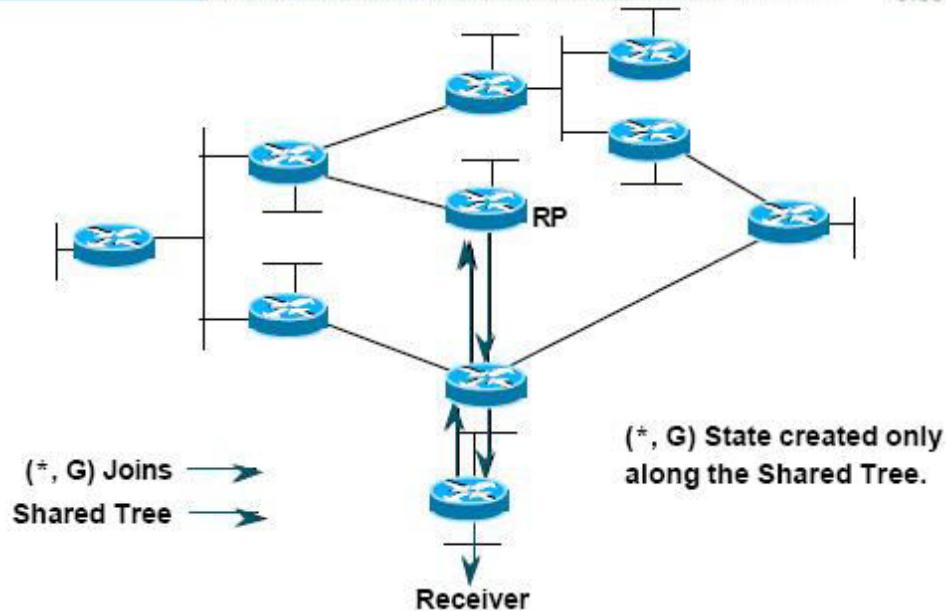
- Směrovače na straně přijímačů se připojují k PIM-SM stromu s pomocí explicitních zpráv JOIN
- PIM-SM RP jsou směrovače, kde se lze připojit na zdroje vysílání
- Vysílače se registrují u jednoho nebo více RP, přijímače hledají na RP vysílání
- V prvou chvíli se příjemce připojí přes další směrovače k RP
- Poslední směrovač u příjemce může připojení ke zdroji optimalizovat (sdílený strom – source-based strom)
- Prevence přetížení RP

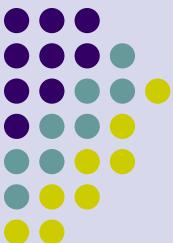


# PIM-SM

## PIM-SM Shared Tree Joins

Cisco.com





# PIM-SSM

- Předpokládá jeden zdroj vysílání pro skupinu (SSM)
  - Např. videokonference, vysílání televize, rozhlasu
- Jednodušší než PIM-SM
- Může budovat jeden optimální doručovací strom od zdroje vysílání

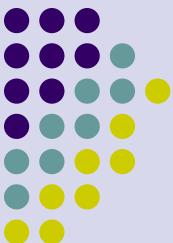
# Transportní úroveň



Úvod do počítačových sítí

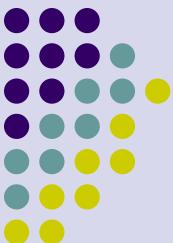
Lekce 10

Ing. Jiří Ledvina, CSc.

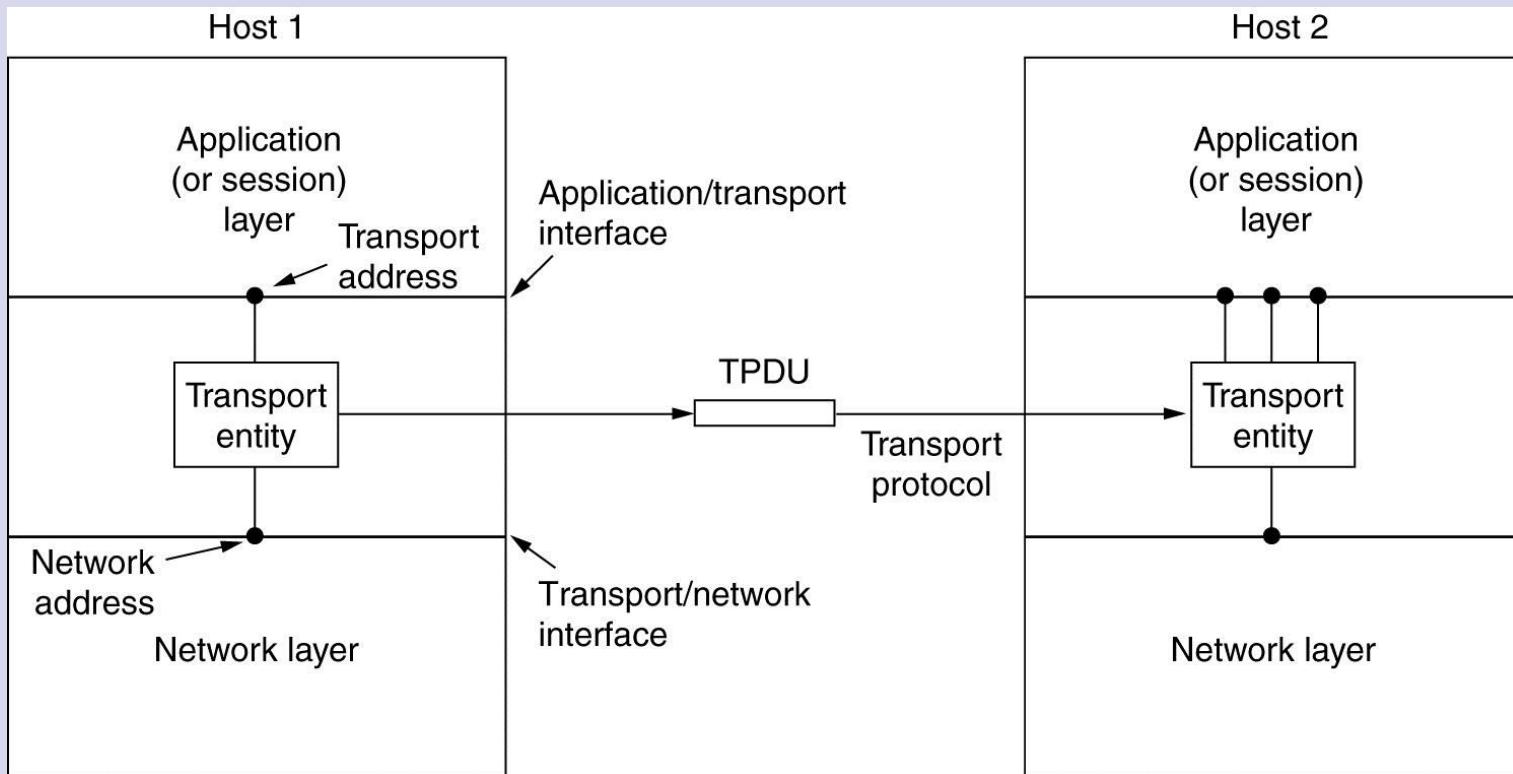


# Transportní služby

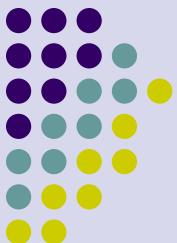
- Služby prováděné pro vyšší úrovně
- Primitivní transportní služby
- Berkeley Sockety



# Služby prováděné na nejvyšší úrovni



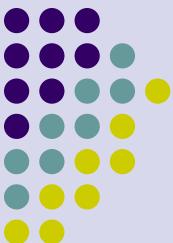
Síťová, transportní a aplikační úroveň



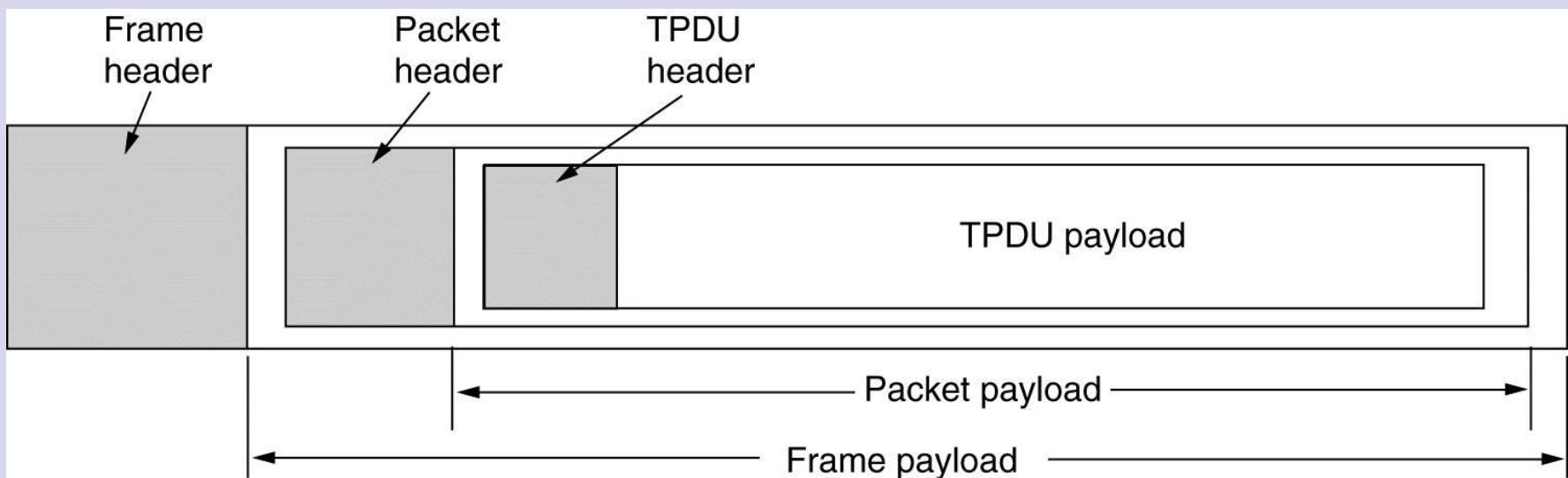
# Primitivní služby transportní úrovni

Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	This side wants to release the connection

Primitivní funkce pro jednoduché transportní služby.



# Primitivní služby transportní úrovni (2)

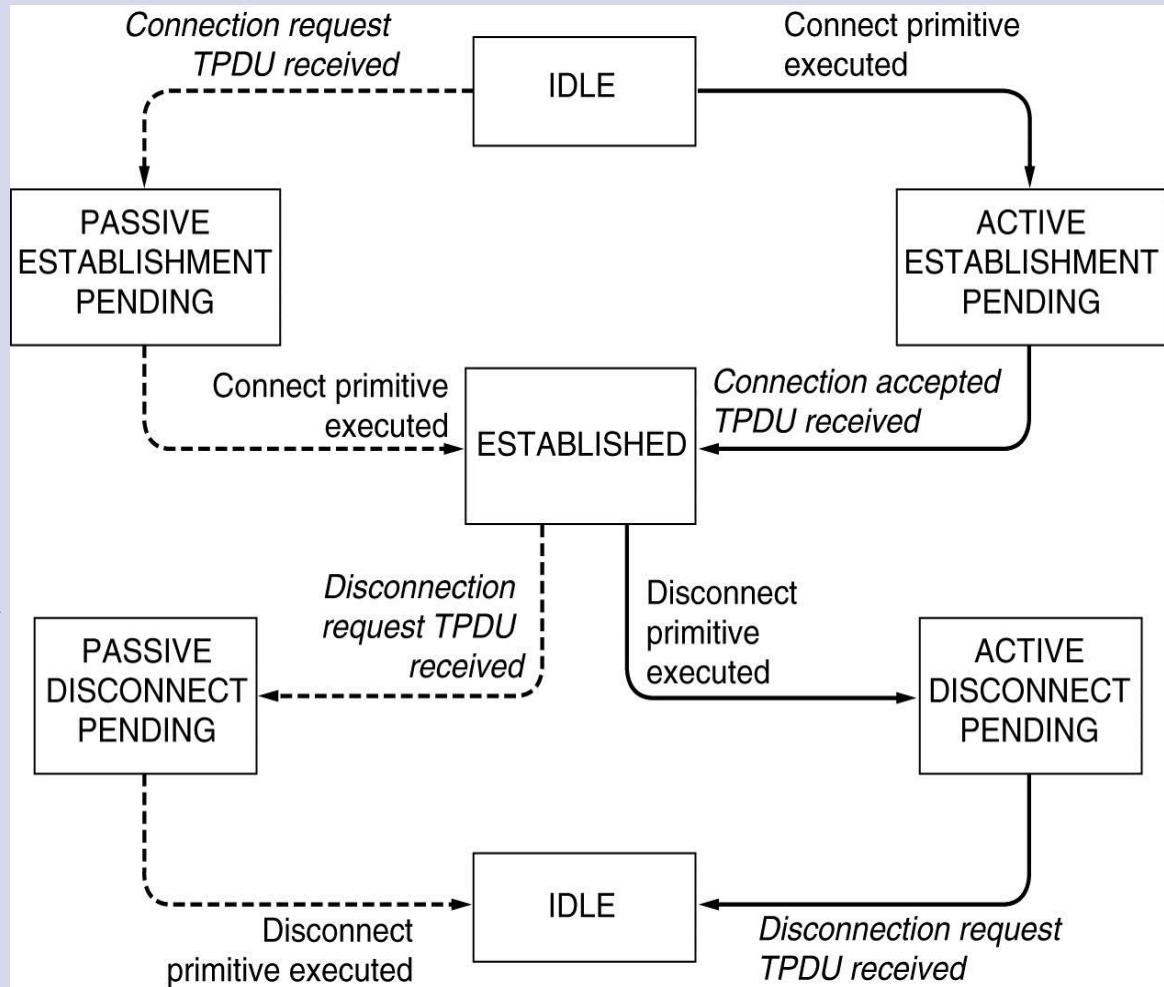


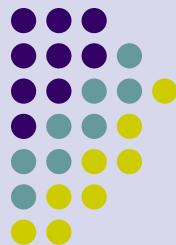
Zapouzdření TPDU, paketů a rámců.

# Primitivní služby transportní úrovni (3)



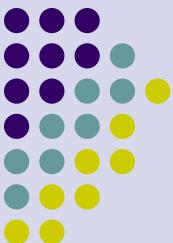
Stavový diagram pro jednoduchý transportní protokol. Plné čáry představují přechody klienta, tečkované přechody serveru. Přechody popsané skloněným písmem jsou způsobeny příjemem paketů.



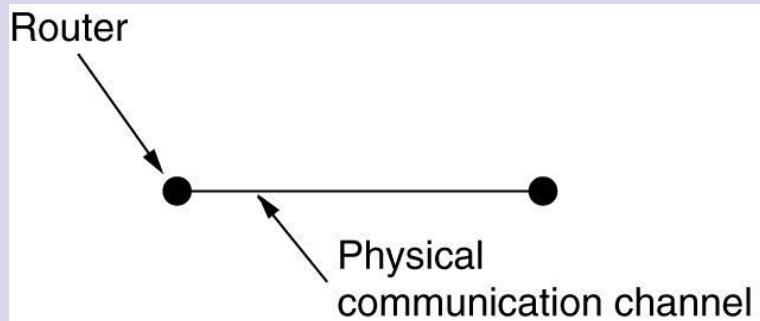


# Základy transportních protokolů

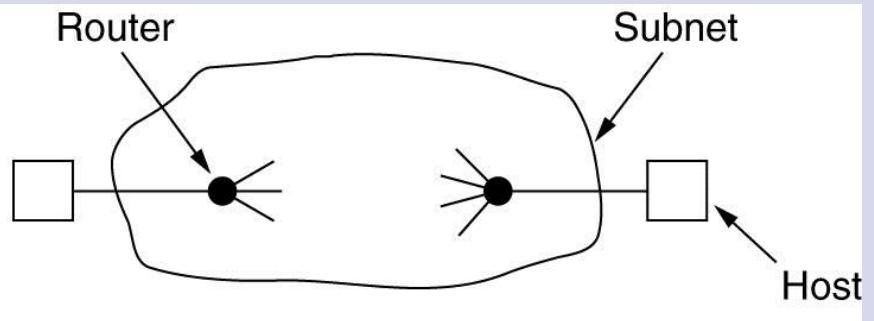
- Adresování
- Vytváření spojení
- Uvolnění spojení
- Řízení toku dat a vyrovnávací paměti
- Multiplexování
- Obnova po chybě



# Transportní protokol



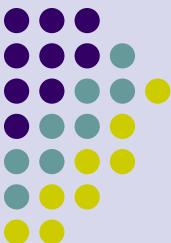
(a)



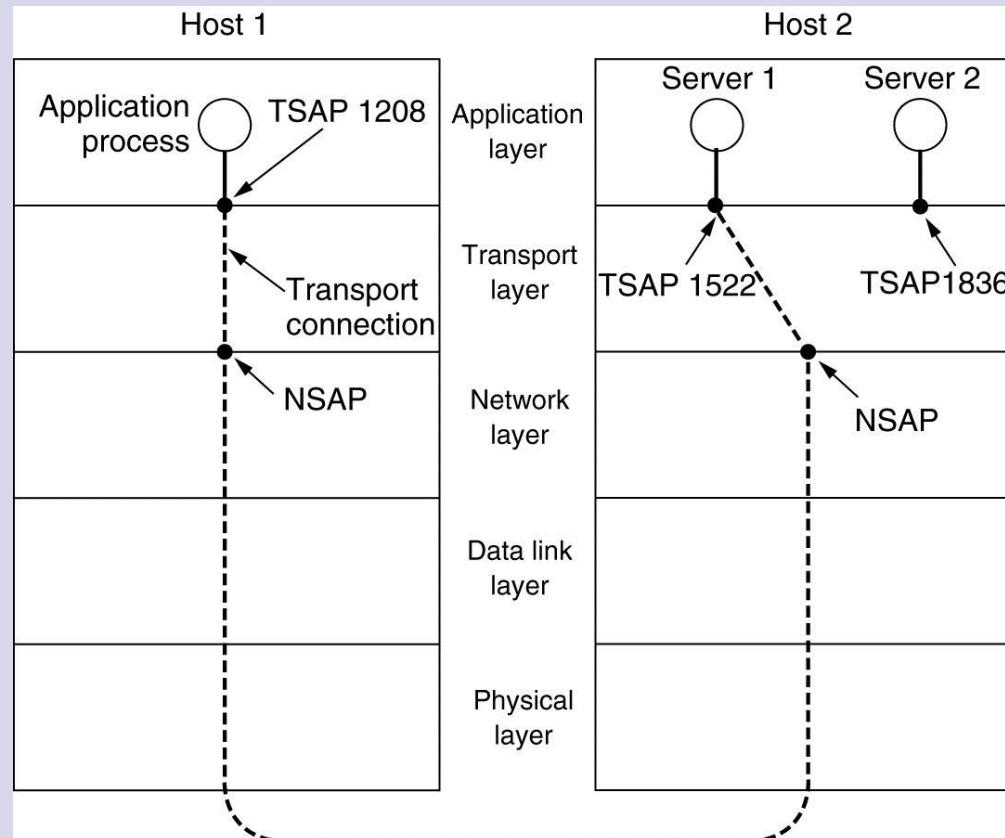
(b)

(a) Prostředí linkové úrovně.

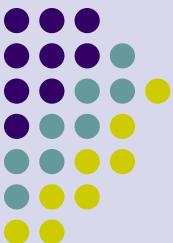
(b) Prostředí transportní úrovně.



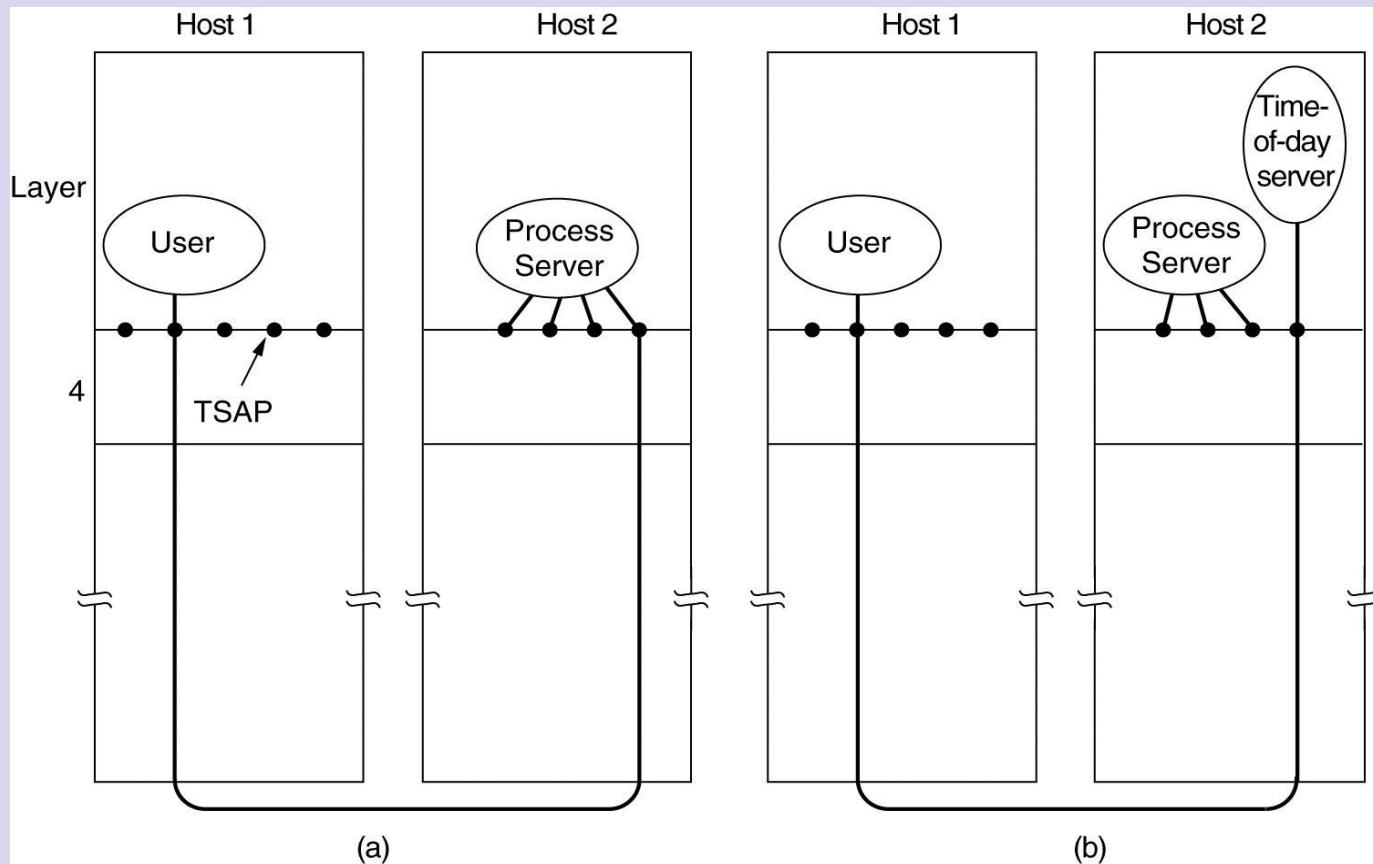
# Adresování



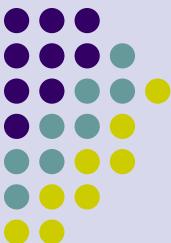
TSAP, NSAP a transportní spojení.



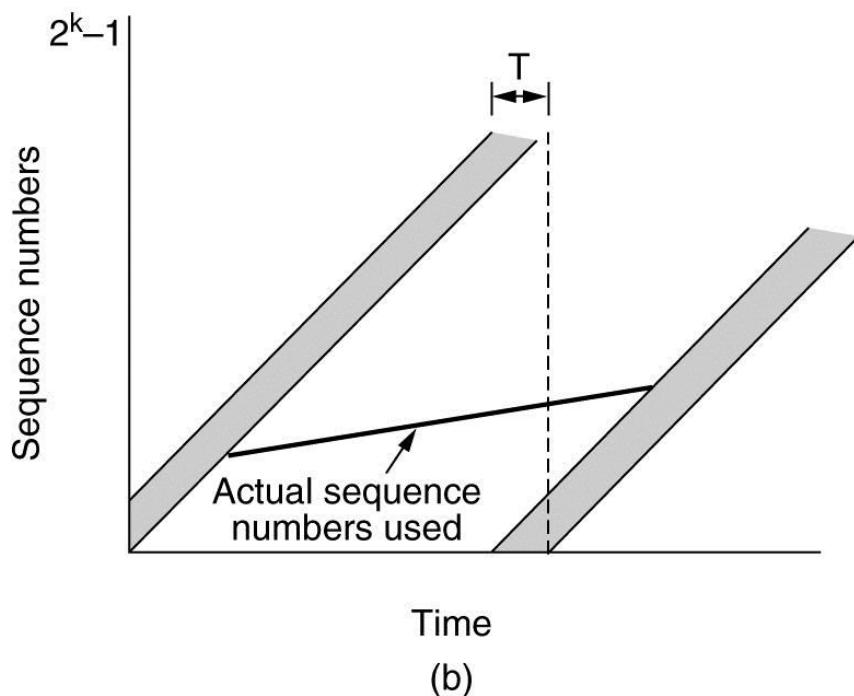
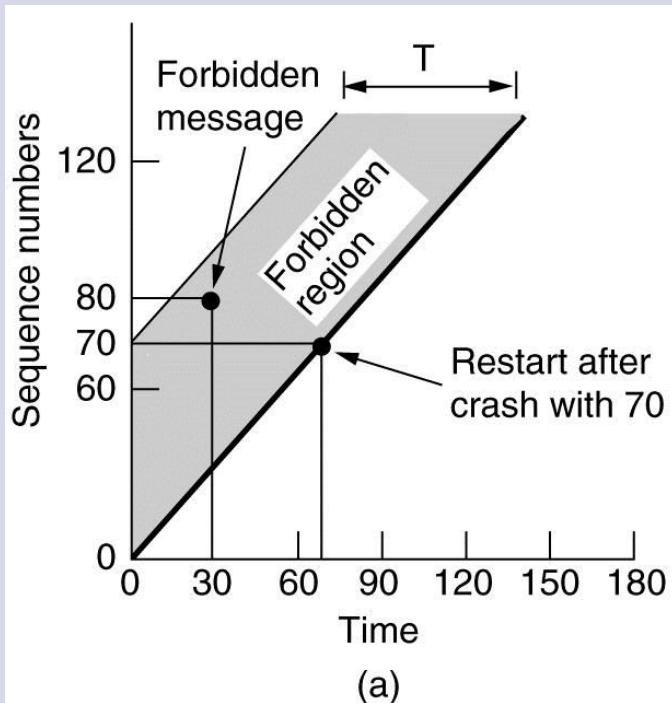
# Vytváření spojení



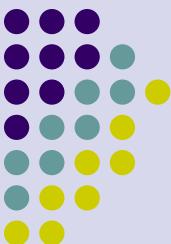
Postup vytváření spojení mezi host 1 a host 2.



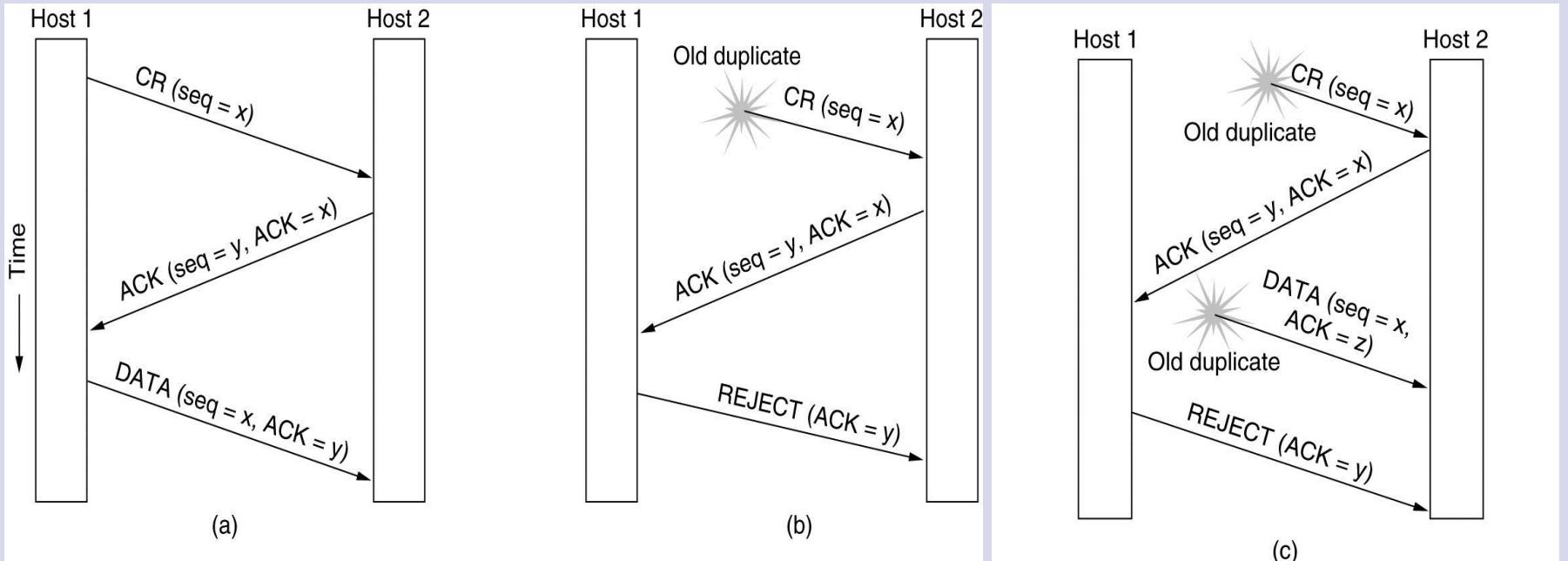
# Vytváření spojení (2)



- (a) TPDU nemohou vstoupit do zakázané oblasti.
- (b) Problém resynchronizace.



# Vytváření spojení (3)

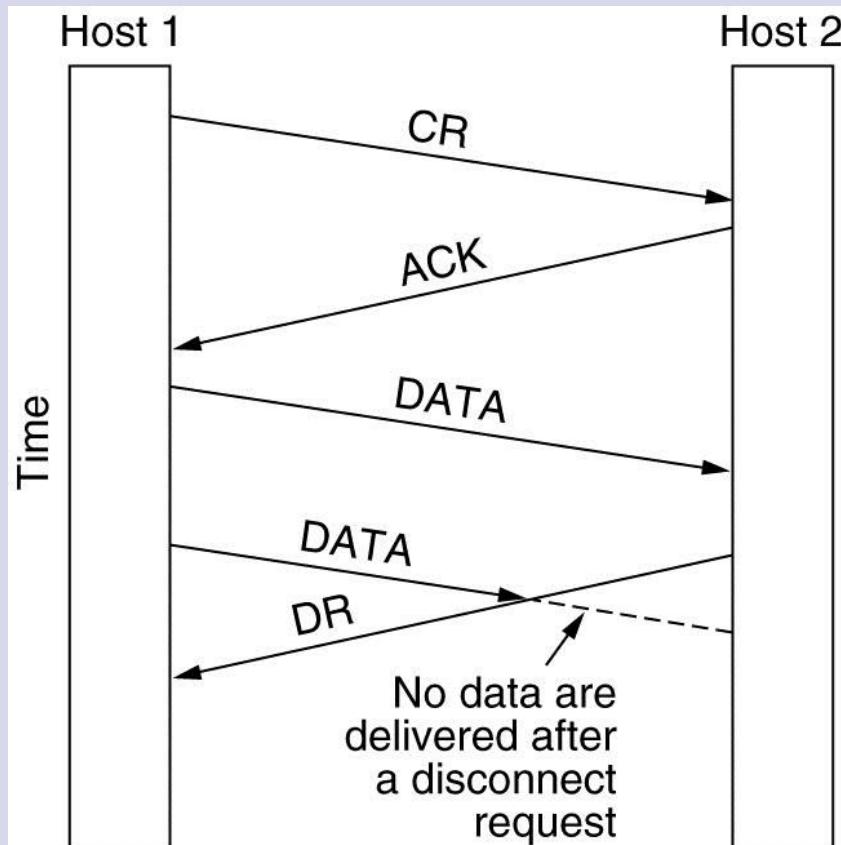


Tři případy vytváření spojení s využitím třífázového navazování spojení. CR znamená Connection Request.

- (a) Normální operace,
- (b) Staré CR, nikam nezapadá.
- (c) duplicitní CR a duplicitní ACK.



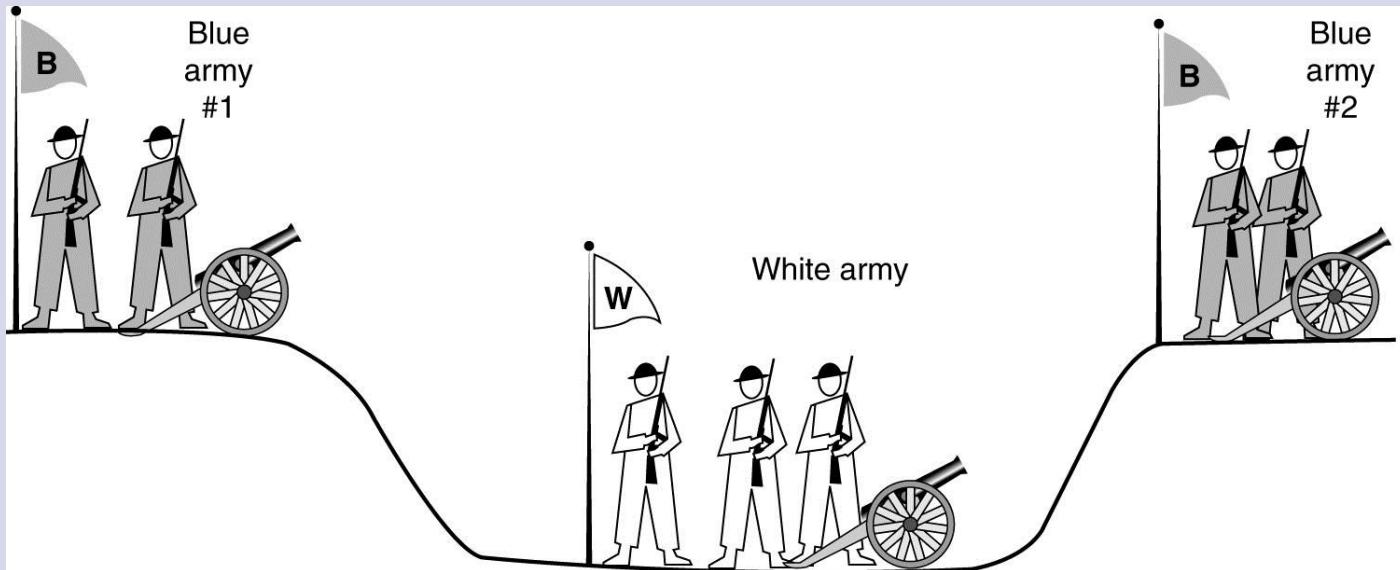
# Uvolnění spojení



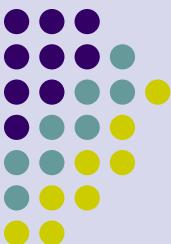
Náhlé přerušení spojení se ztrátou dat.



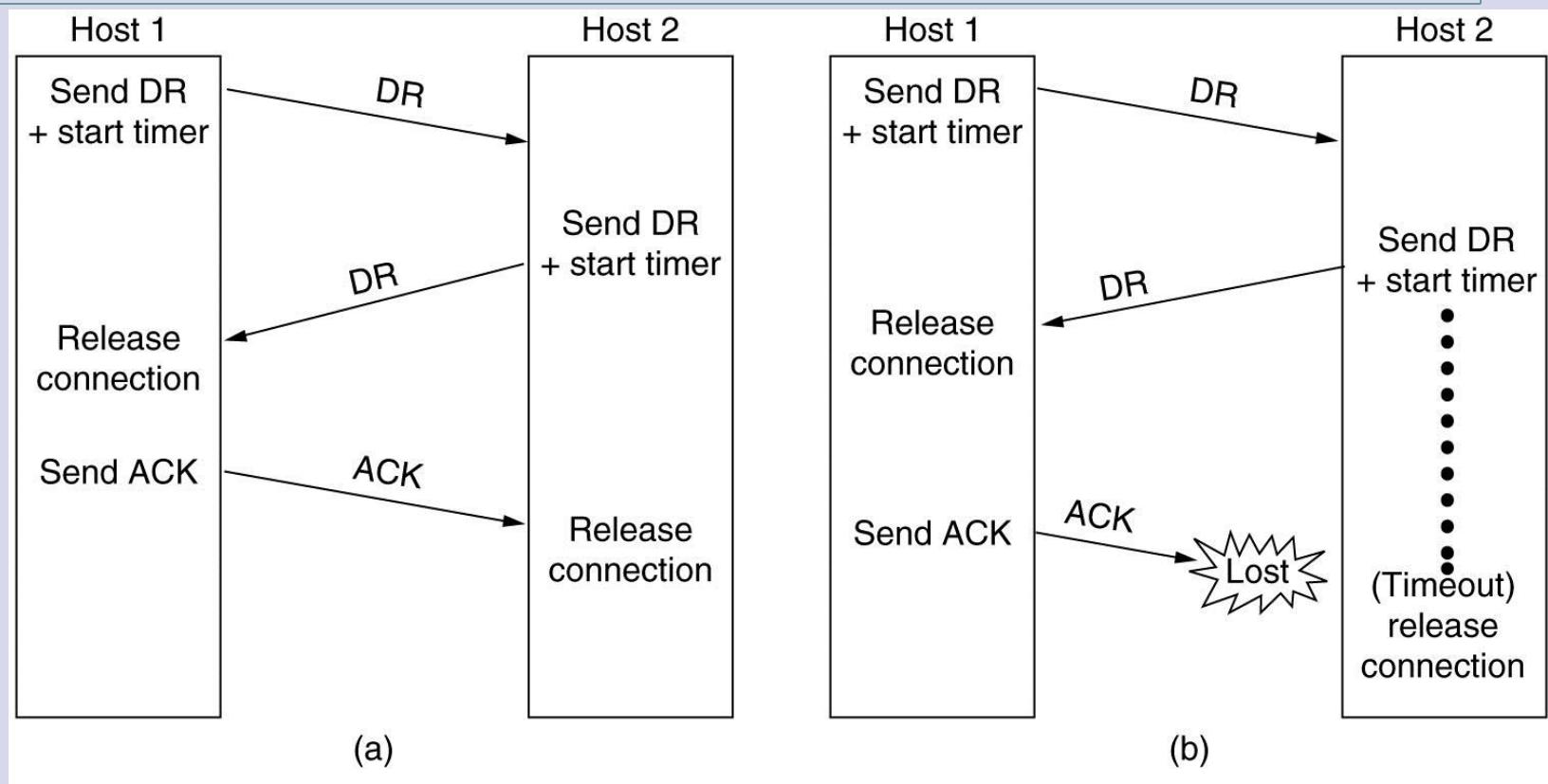
# Uvolnění spojení (2)



Problém dvou armád.

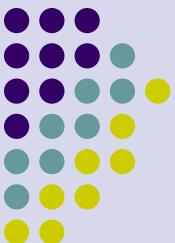


# Uvolnění spojení (3)

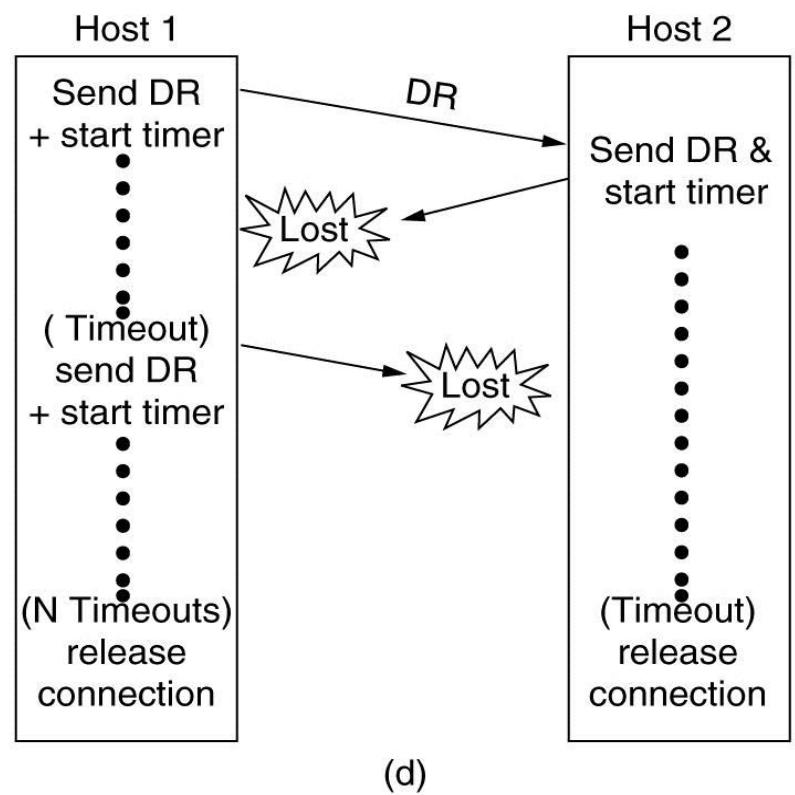
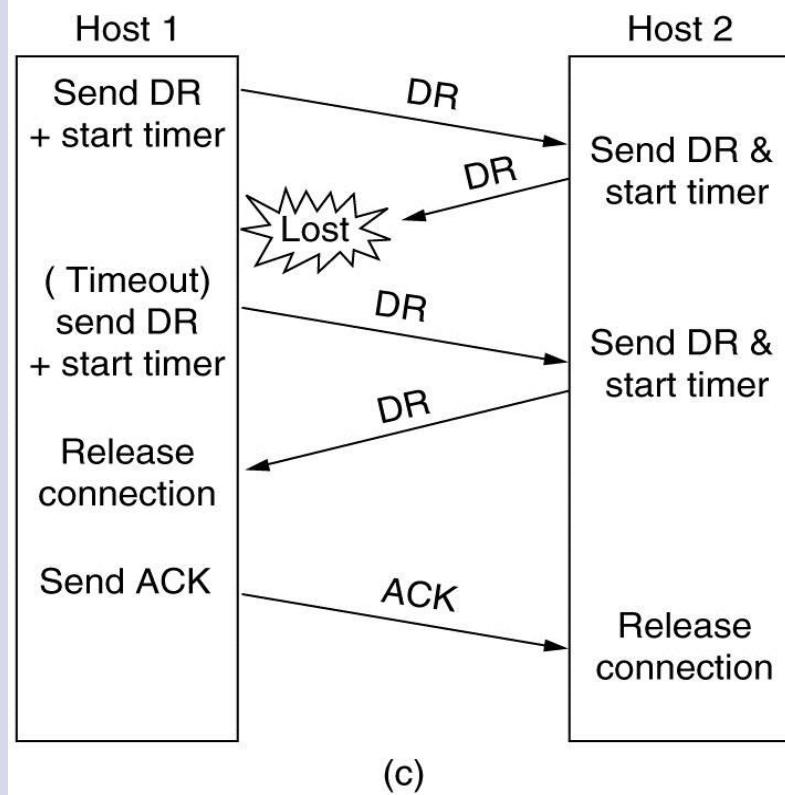


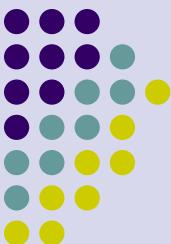
Různé případy ukončení spojení. DR – Disconnect Request

(a) normální postup, třífázové řízení. (b) ztráta posledního ACK.

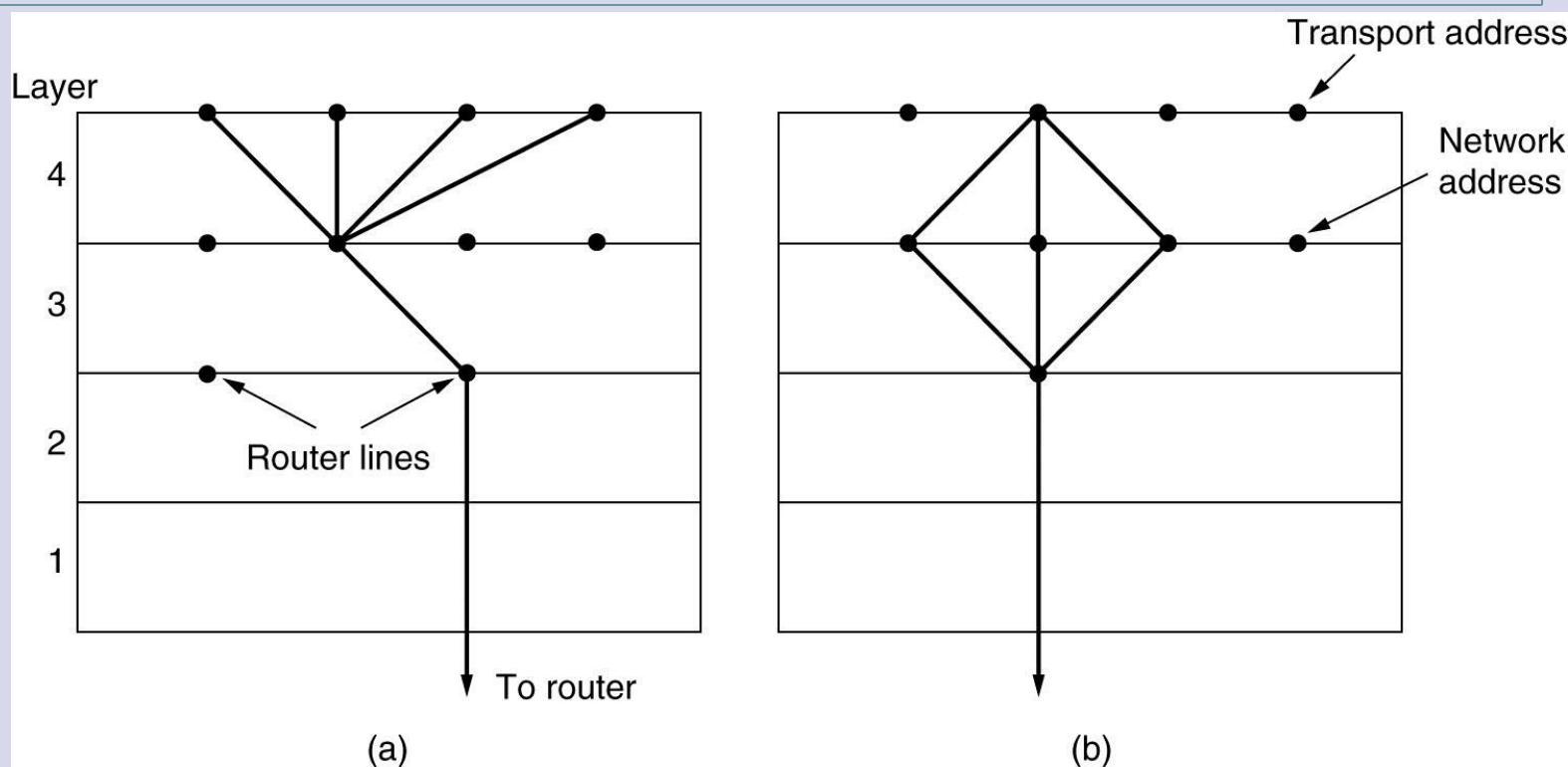


# Uvolnění spojení (4)





# Multiplexování



(a) Vzrůstající multiplexování. (b) klesající multiplexování.



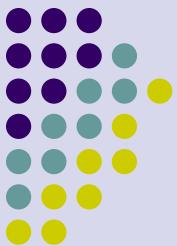
# Obnova po chybě

		Strategy used by receiving host					
		First ACK, then write			First write, then ACK		
Strategy used by sending host		AC(W)	AWC	C(AW)	C(WA)	W AC	WC(A)
	Always retransmit	OK	DUP	OK	OK	DUP	DUP
Never retransmit	LOST	OK	LOST	LOST	OK	OK	OK
Retransmit in S0	OK	DUP	LOST	LOST	DUP	OK	OK
Retransmit in S1	LOST	OK	OK	OK	OK	OK	DUP

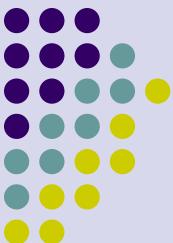
OK = Protocol functions correctly  
DUP = Protocol generates a duplicate message  
LOST = Protocol loses a message

Různé kombinace strategií serveru a klienta.

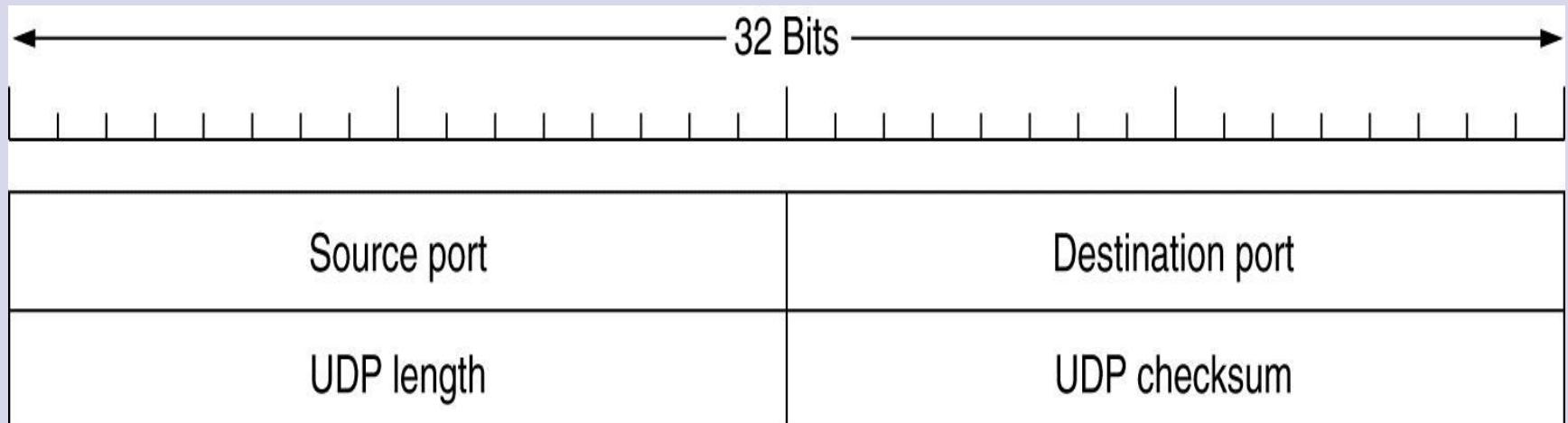
# Transportní protokol Internetu: UDP



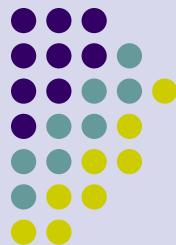
- Úvod do UDP
- Vzdálené volání procedur
- Real-Time Transport Protocol (RTP)



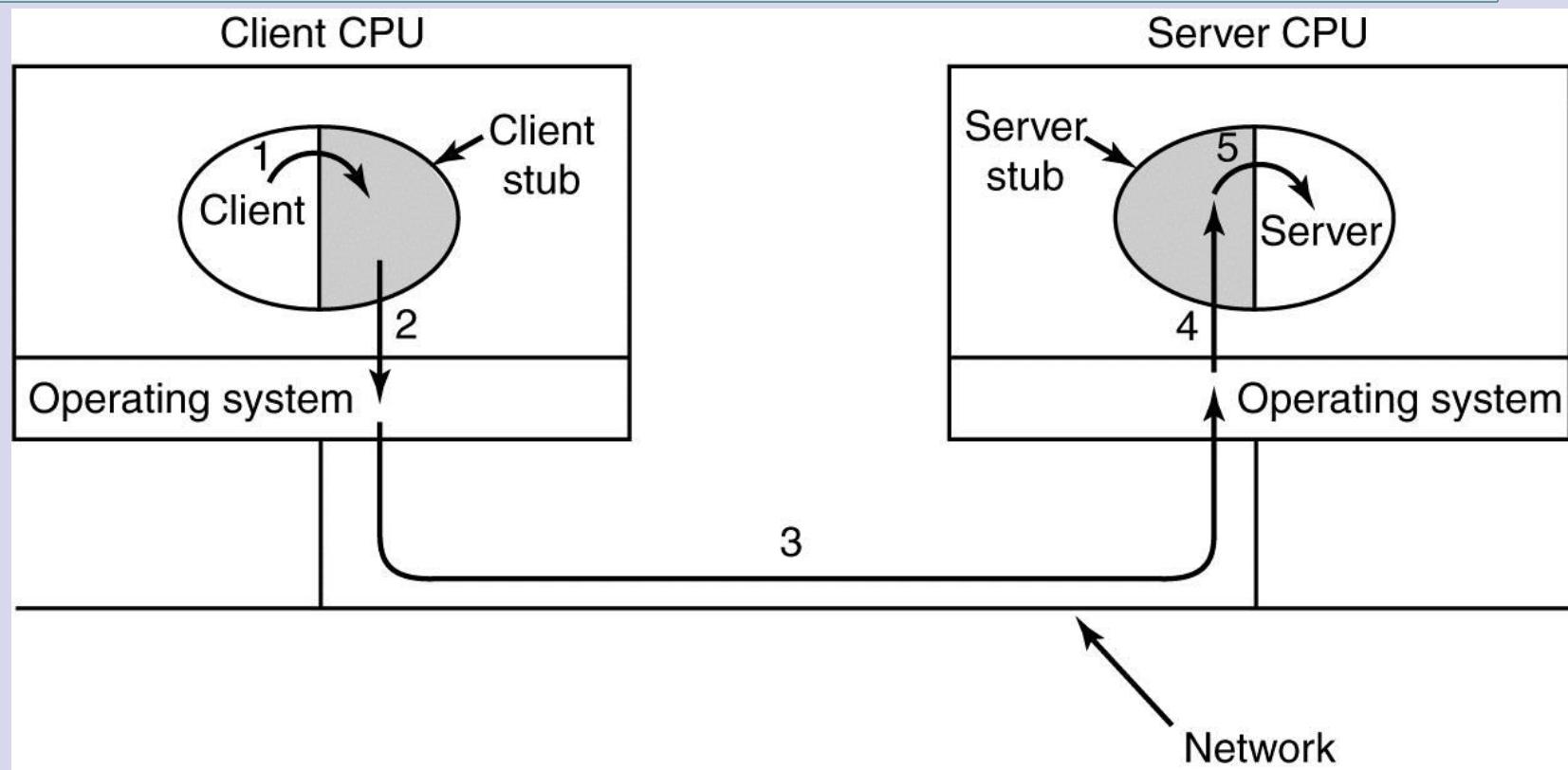
# Úvod do UDP



UDP záhlaví.



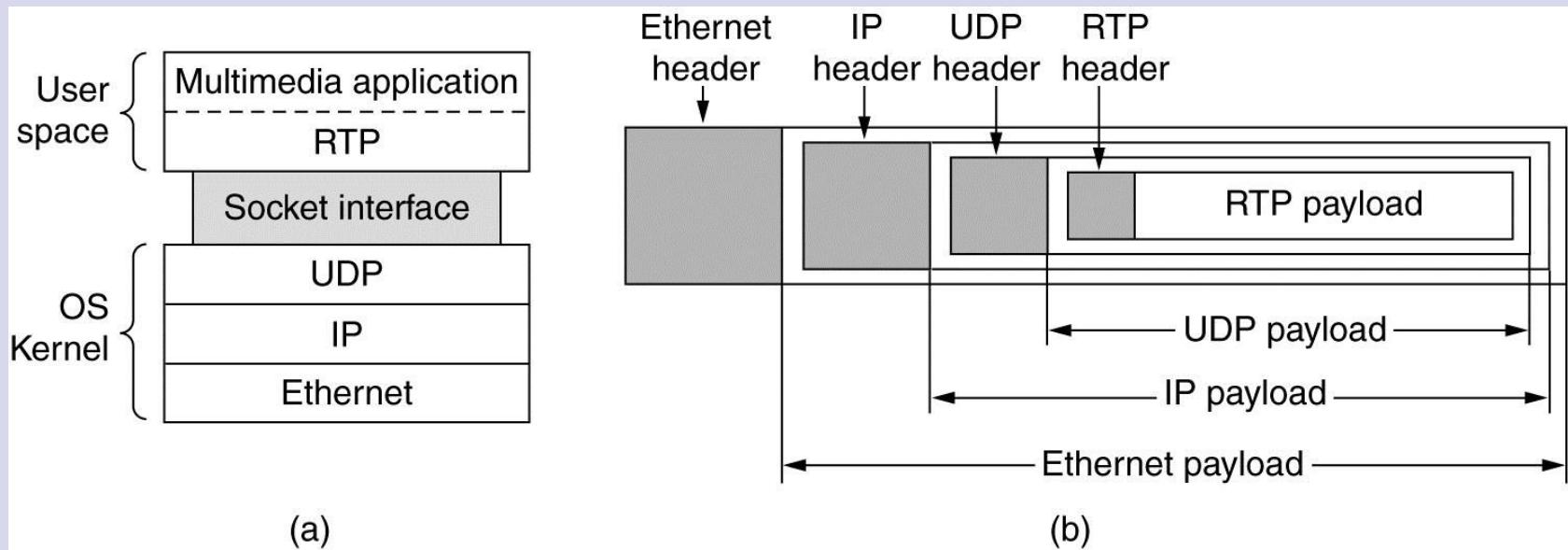
# Volání vzdálených podprogramů



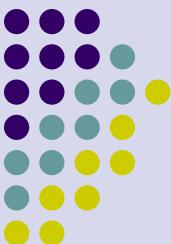
Kroky při vytváření volání vzdálené procedury. Spojky jsou vyznačeny šedě.



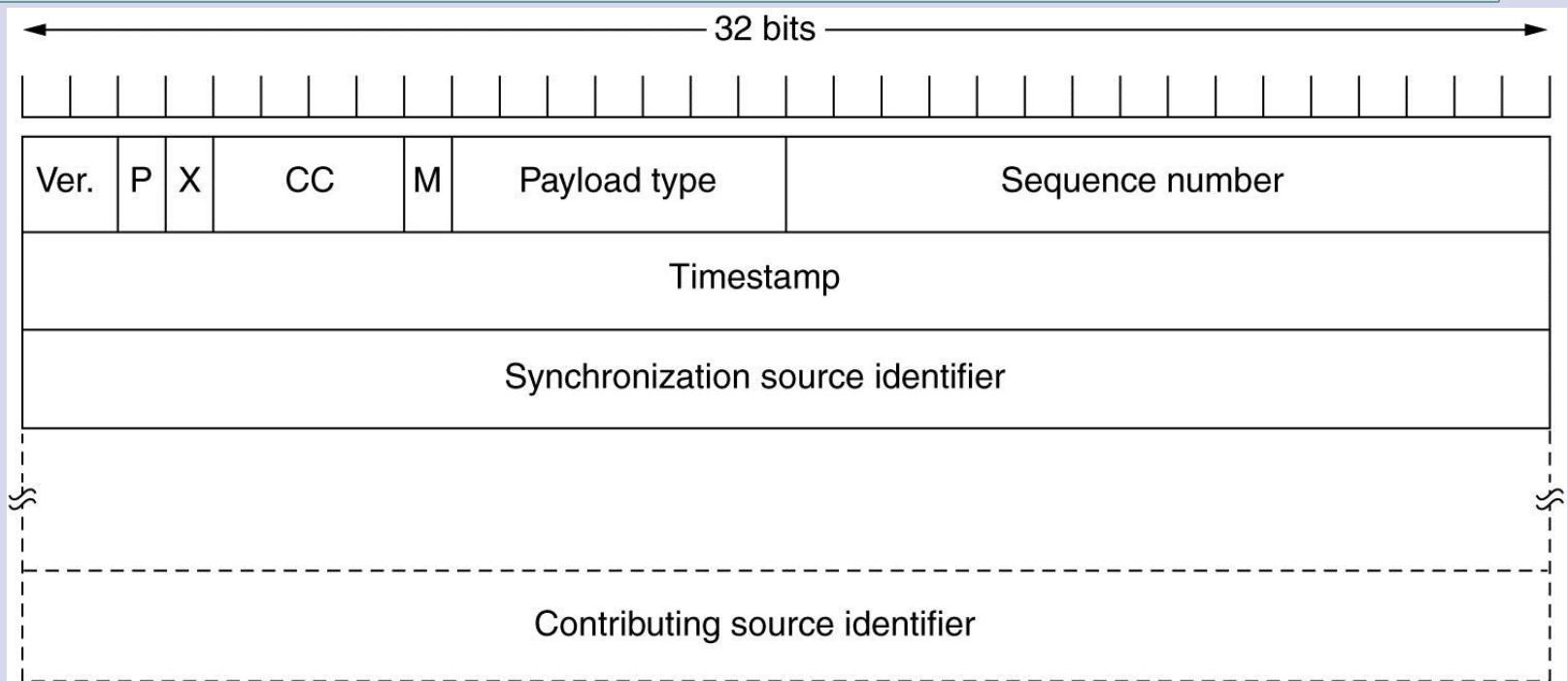
# Real-Time Transport Protocol



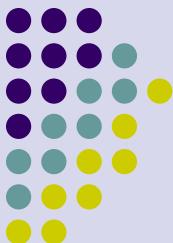
- (a) Umístění RTP v zásobníku protokolů.
- (b) Zapouzdření paketu.



# Real-Time Transport Protocol (2)



Záhlaví RTP.



# Transportní protokol Internetu: TCP

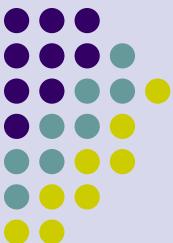
- Úvod do TCP
- Model služeb TCP
- Fragmentace
- Protokol TCP
- Záhlaví segmentu TCP
- Vytváření spojení
- Koncepce TCP vysílání
- TCP – obrana proti zahlcení
- Transakční TCP



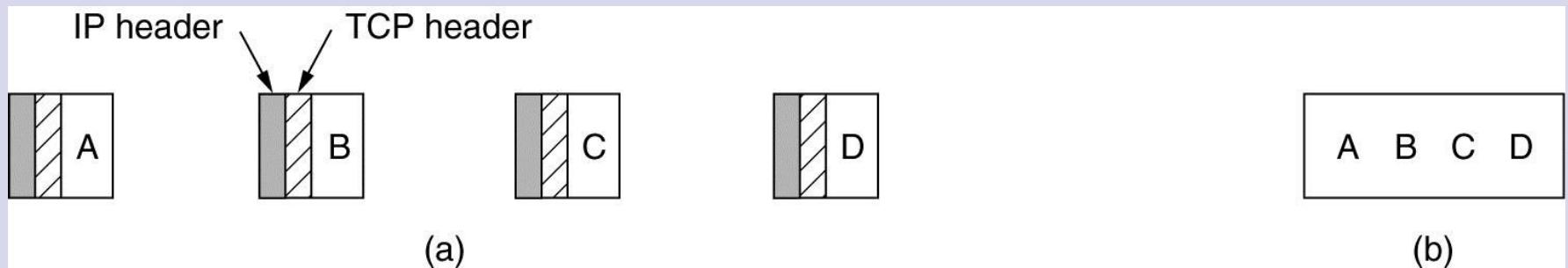
# Model služeb TCP

## Některé používané porty.

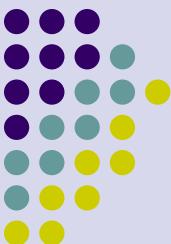
Port	Protocol	Use
21	FTP	File transfer
23	Telnet	Remote login
25	SMTP	E-mail
69	TFTP	Trivial File Transfer Protocol
79	Finger	Lookup info about a user
80	HTTP	World Wide Web
110	POP-3	Remote e-mail access
119	NNTP	USENET news



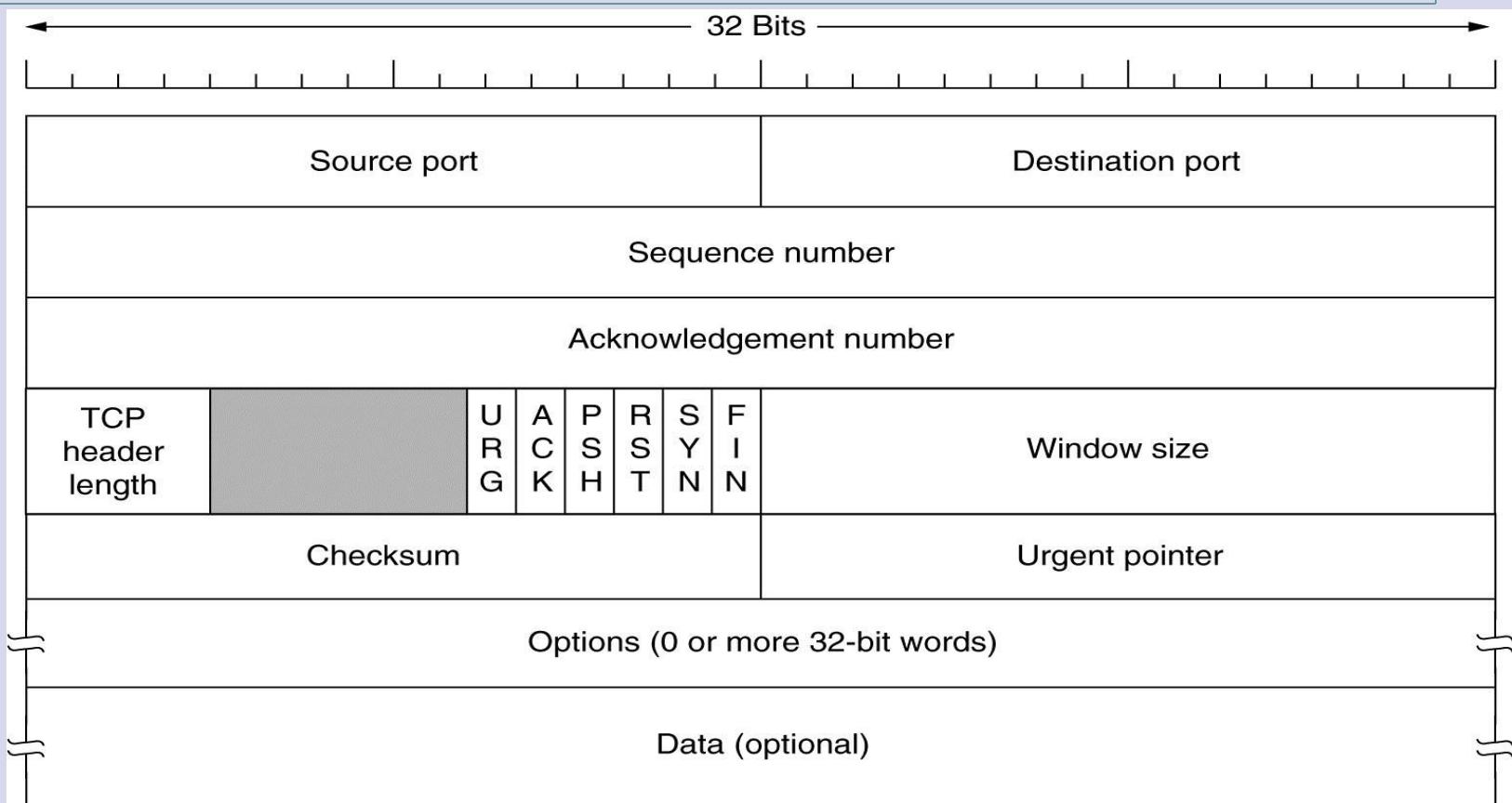
# Fragmentace



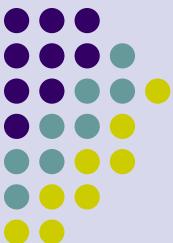
- (a) Fragmentace segmentů do několika datagramů.
- (b) Do aplikace může být několik datagramů přeneseno najednou.



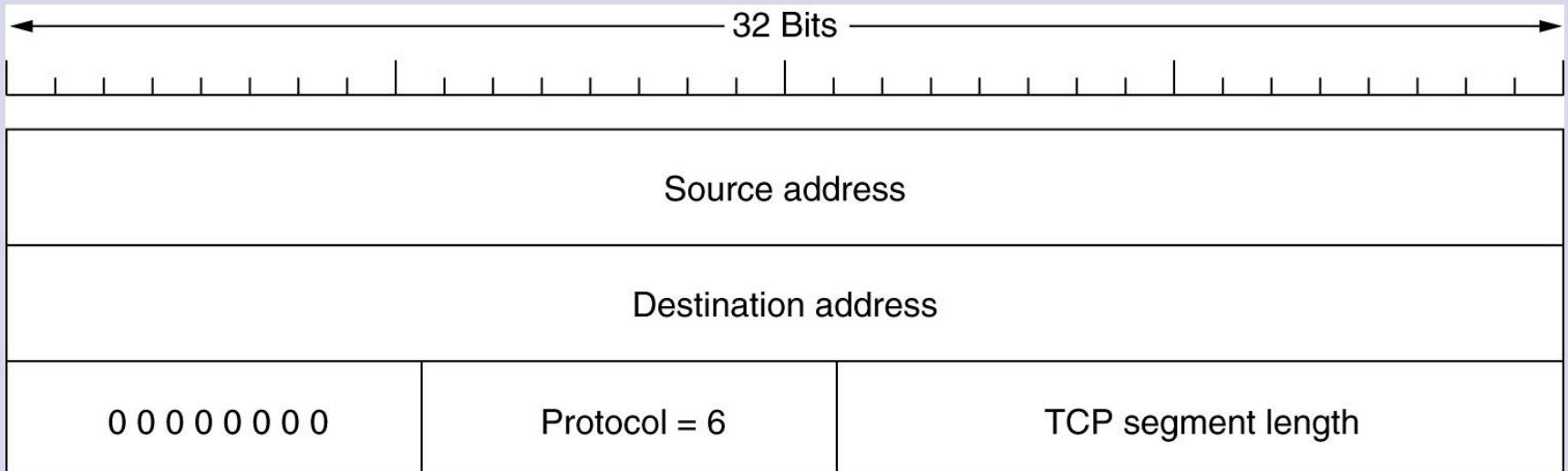
# Záhlaví segmentu TCP



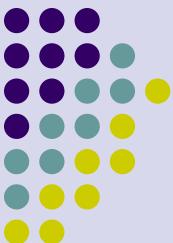
TCP záhlaví.



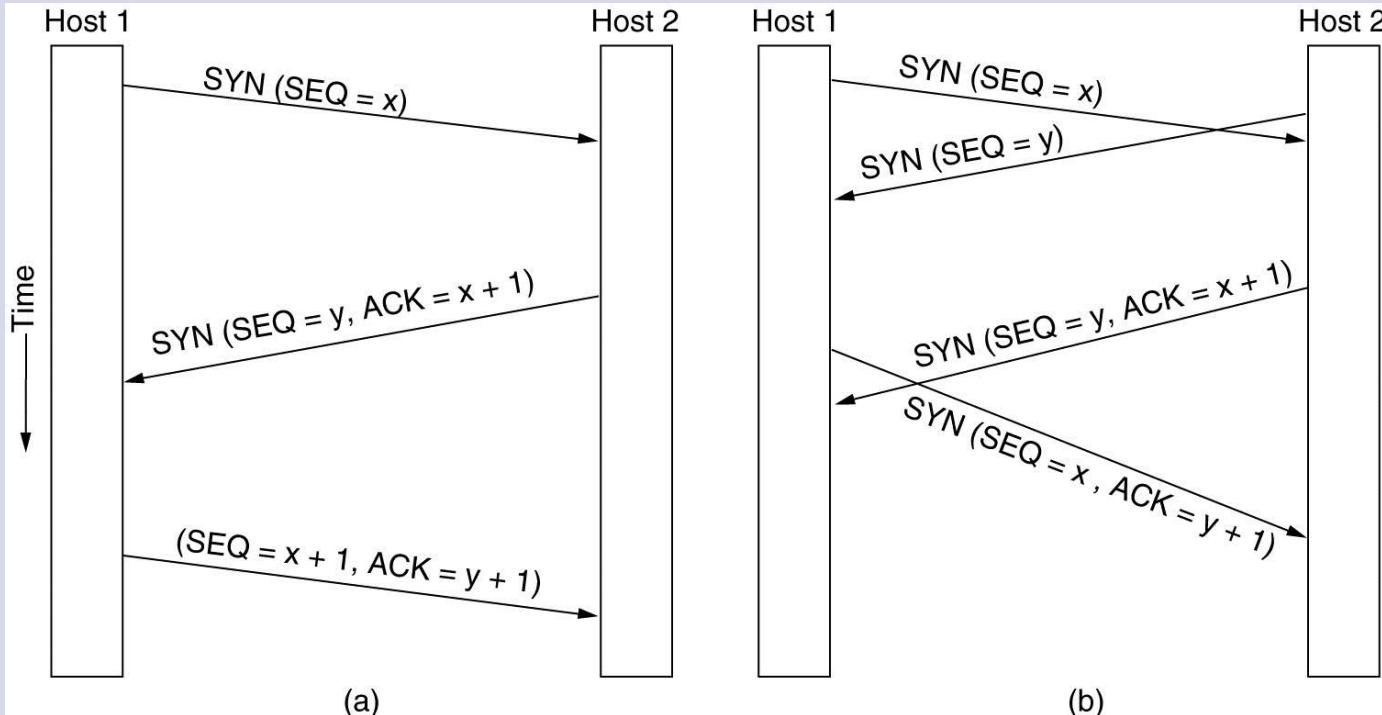
# Záhlaví segmentu TCP (2)



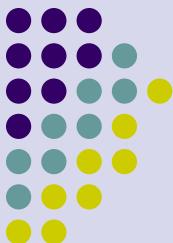
Pseudozáhlaví používané pro výpočet TCP kontrolního součtu.



# Vytváření spojení TCP



- (a) Vytváření TCP spojení – normální postup.  
(b) Kolize při vytváření spojení.



# Stavy konečného automatu protokolu TCP

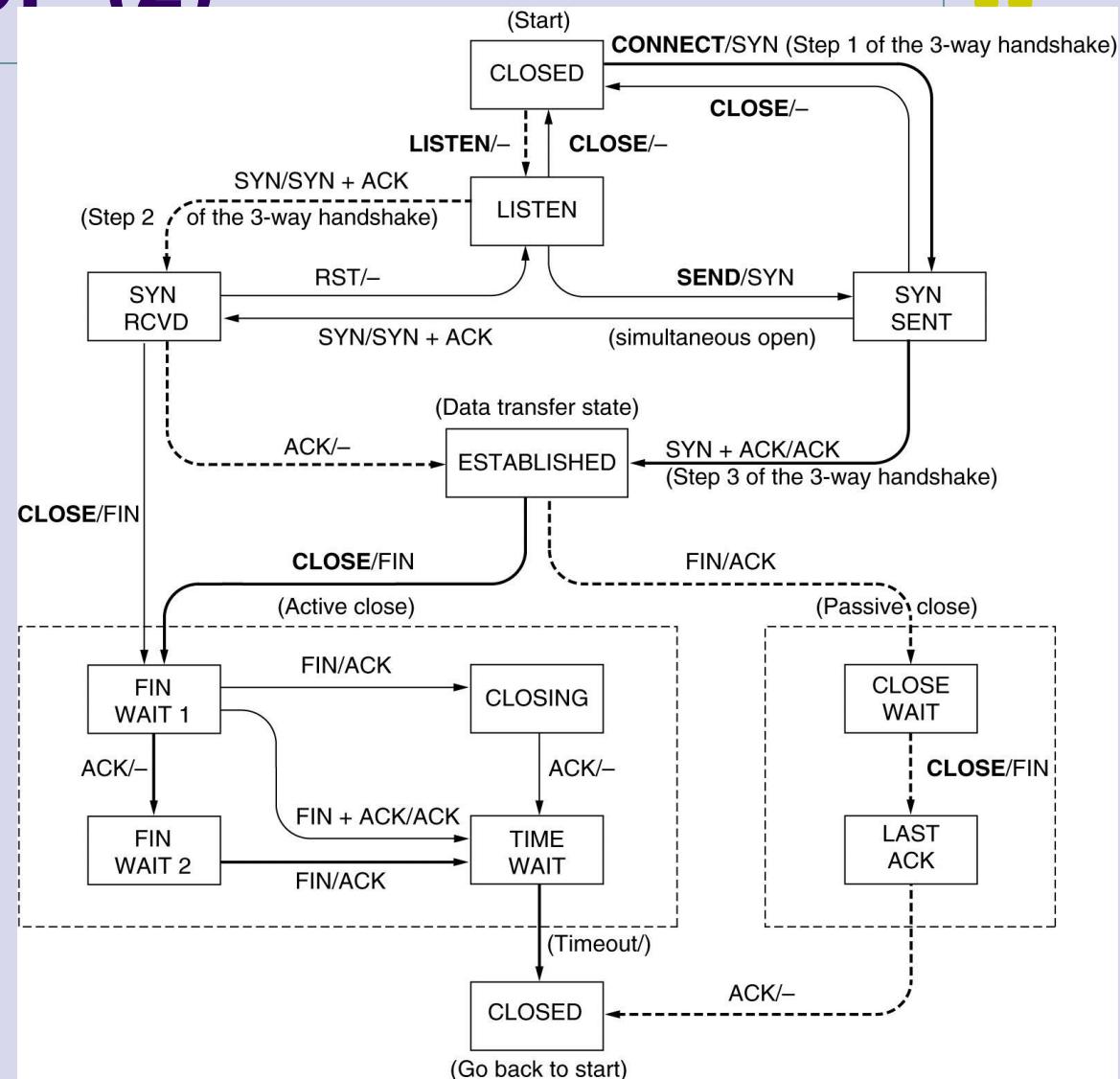
State	Description
CLOSED	No connection is active or pending
LISTEN	The server is waiting for an incoming call
SYN RCVD	A connection request has arrived; wait for ACK
SYN SENT	The application has started to open a connection
ESTABLISHED	The normal data transfer state
FIN WAIT 1	The application has said it is finished
FIN WAIT 2	The other side has agreed to release
TIMED WAIT	Wait for all packets to die off
CLOSING	Both sides have tried to close simultaneously
CLOSE WAIT	The other side has initiated a release
LAST ACK	Wait for all packets to die off

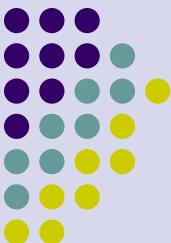
Stavy konečného automatu popisujícího činnost TCP ve všech režimech.



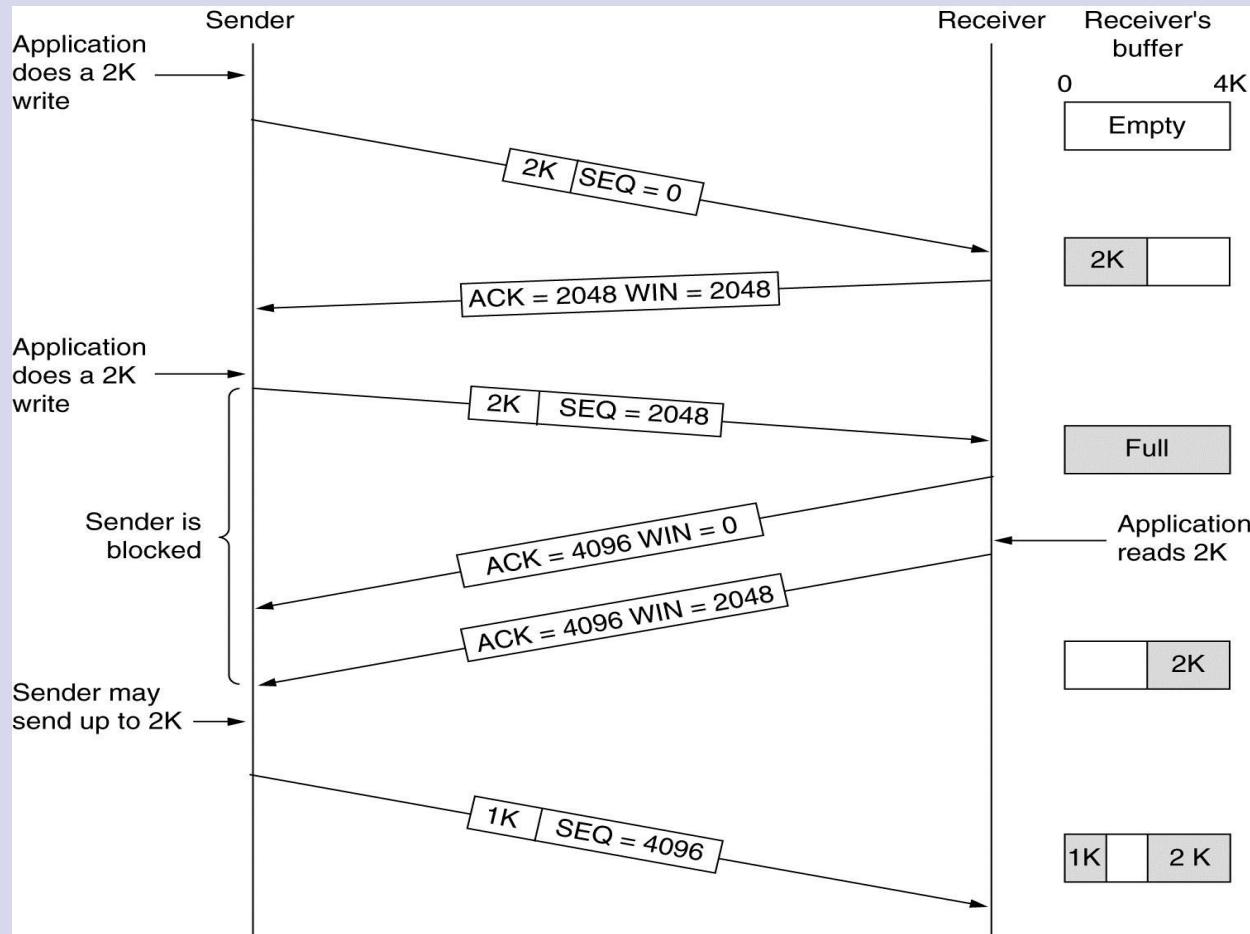
# Stavy konečného automatu protokolu TCP (2)

TCP diagram stavů.  
Silné čáry jsou pro klienta, silné čárkované pro server, slabé plné pro neběžné přechody klienta, slabé čárkované pro neběžné přechody serveru. Každý přechod je označen událostí a odpovídající akcí.





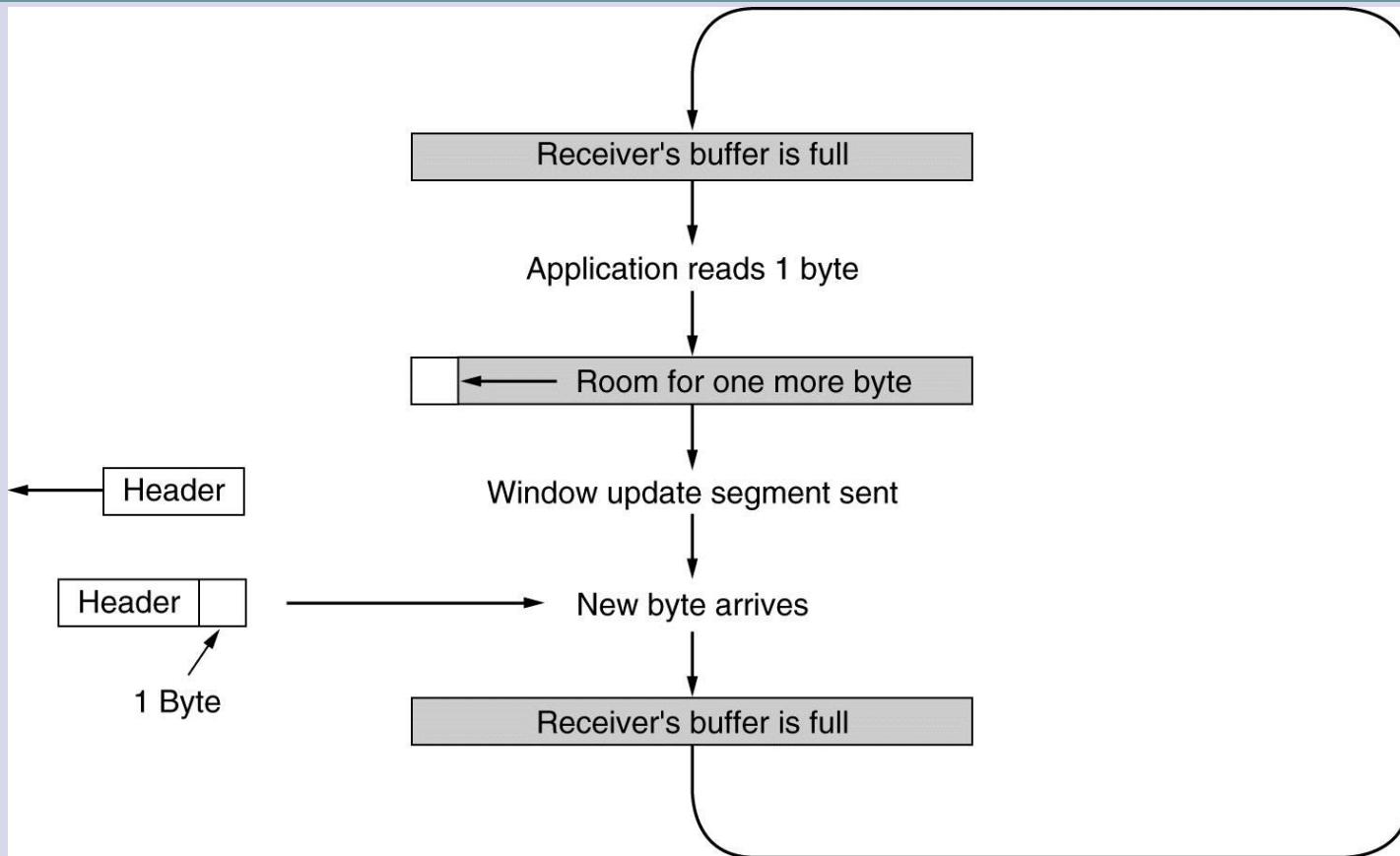
# Přenos dat TCP



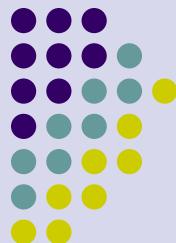
Manipulace s velikostí okna v TCP.



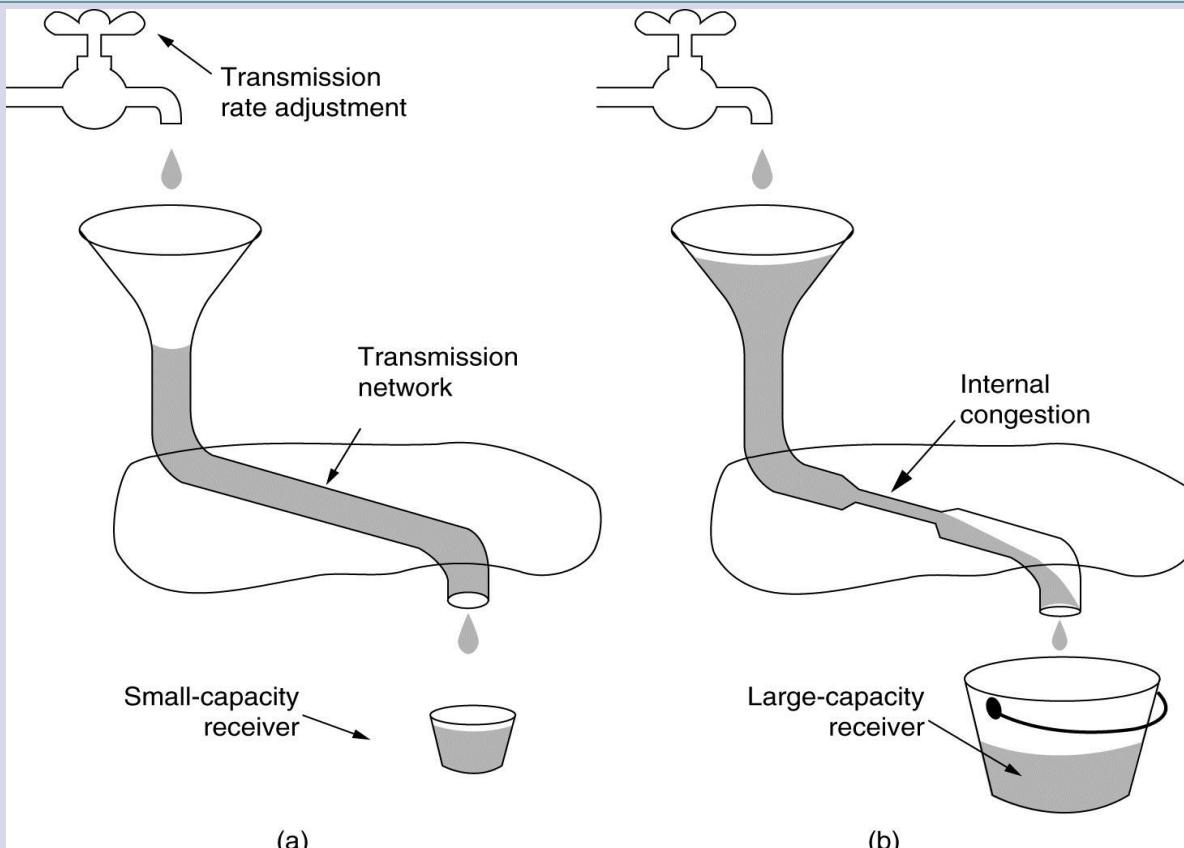
# Přenos dat TCP (2)



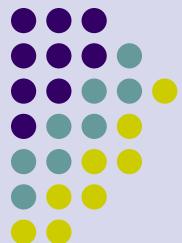
Syndrom „hloupého“ okna (silly window syndrome).



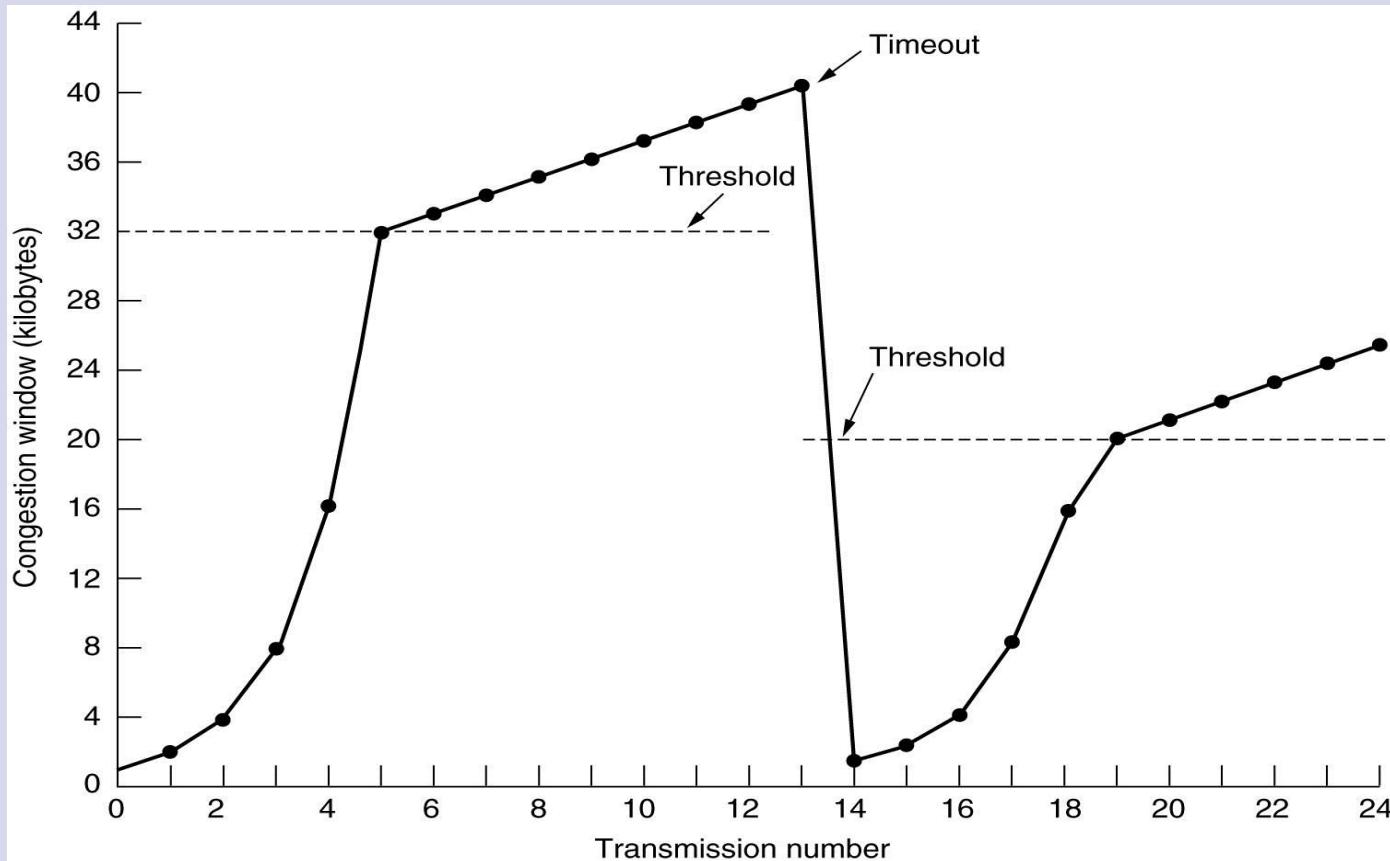
# TCP - obrana proti zahlcení



- (a) <sup>(a)</sup> Rychlé plnění sítí a přijímač s malou kapacitou.
- (b) <sup>(b)</sup> Pomalé plnění sítí a přijímač s velkou kapacitou.



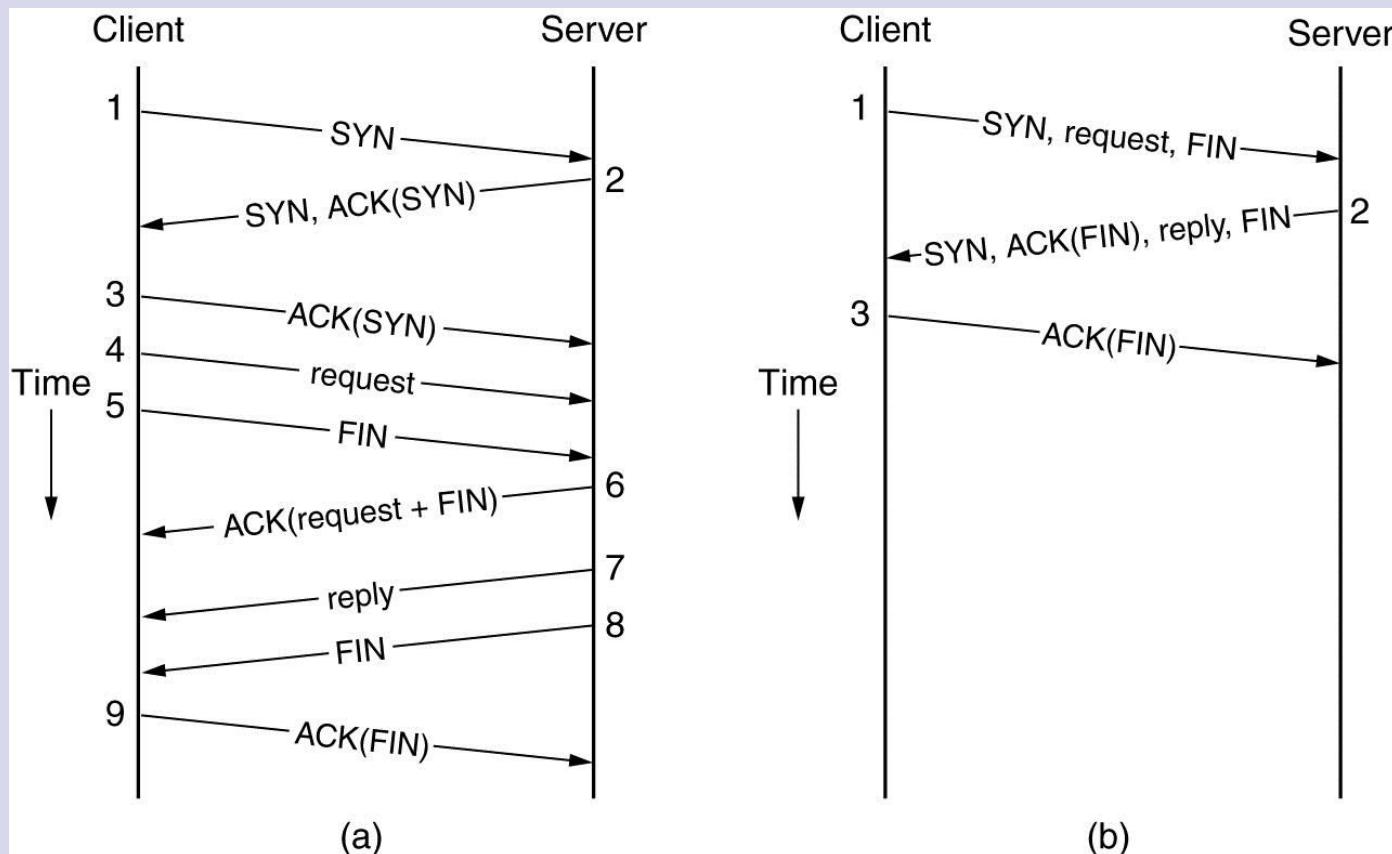
# TCP - obrana proti zahlcení (2)



Příklad - algoritmus ochrany proti zahlcení (pomalý start – slow start).



# Transakční TCP (T/TCP)



- (a) RPC používající klasické TCP.  
(b) RPC používající T/TCP.

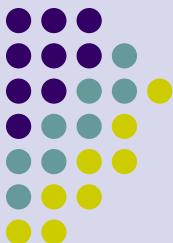
# **Relační, prezentační a aplikační služby**



Úvod do počítačových sítí

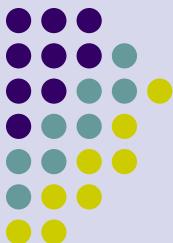
Lekce 11

Ing. Jiří Ledvina, CSc.



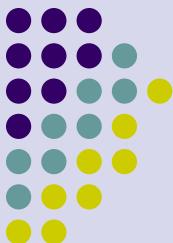
# Relační vrstva

- Zajišťuje spolehlivý přenos dat mezi dvěma aplikačními entitami
- Aktivity, dialogové jednotky
- Poloduplexní, duplexní přenos
- Synchronizace přenosu dat
  - Hlavních synchronizačních body
  - Vedlejších synchronizačních body
- Předávání pověření
- Různé typy přenášených dat
  - Data
  - Upřednostněná data
  - Capability data – přenos řídicí informace (mimo aktivity)
  - Normalní data



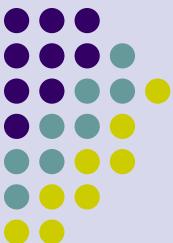
# Prezentační vrstva

- Zajišťuje konverzi aplikačních dat do podoby vhodné pro přenos sítí
- Dohadování syntaxe přenosu
- Typy dat
  - Jednoduchý
  - strukturovaný
- Prezentační kontext
  - Abstraktní syntaxe
  - Přenosová syntaxe
- Typy služeb
  - Úprava dat do univerzálního formátu
    - ASN.1, BER, DER, ...
    - XDR
  - Šifrování
  - Komprese



# Aplikační vrstva

- Aplikační služby
  - Společné (Common) aplikační služby (Common Application Service Elements)
    - Vzájemná komunikace (Association Control Service Element)
    - Volání vzdálených podprogramů (Remote Operation Service Element)
    - Transakční zpracování (Commitment, Concurrency and Recovery)
    - Spolehlivý přenos dat (Reliable Transfer Service Element)
  - Specifické (Specific) aplikační služby (Specific Application Service Element)
    - Přenos souborů
    - Adresářové služby
    - Vzdálený terminálový přístup
    - Přenos zpráv (el. Pošta a další)



# Aplikační služby TCP/IP

- Uživatelské
  - Přenos souborů (FTP, TFTP, SCP, HTTP)
  - Vzdálený přístup (Telnet, ssh, X-window)
  - Přenos správ (e-mail, chat, instant messaging)
- Systémové
  - Adresářové služby (DNS, LDAP)
  - Konfigurace systému (BOOTP, DHCP)
  - Síťový management (SNMP, RMON)
  - Bezpečnost (šifrování, ověřování, ... )



# File Transfer Protocol (FTP)

- Standard pro přenos souborů v Internetu
- Navržen pro spolupráci s různými systémy, podporuje omezený počet typů souborů a struktur
- Používá dva TCP kanály
  - Řídicí kanál
    - Klient otevří řídicí kanál TCP/21 na serveru
    - Spojení se vytváří na celou dobu komunikace
    - Pokud se nastavuje IP/TOS, pak na minimální zpoždění
  - Datový kanál
    - Vytváří se pokaždé když mají být přenesena data
    - Pokud se nastavuje IP/TOS, pak na maximální propustnost

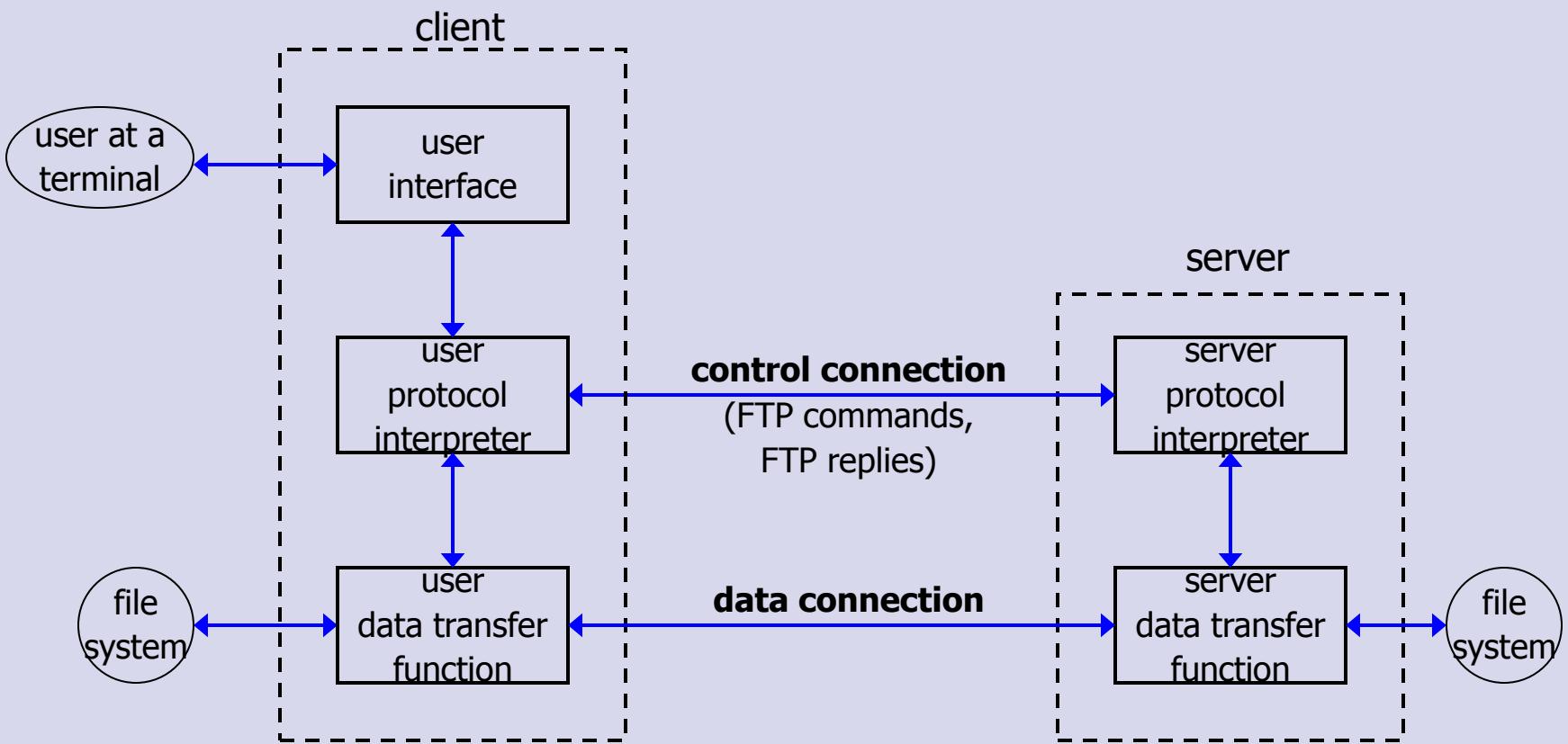


# File Transfer Protocol (FTP)

- Samostatný řídicí kanál – „out of band control“ – řízení mimo pásmo
- FTP server si pamatuje stav: aktuální adresář, předchozí ověření
- Dovoluje FTP klientovi vytvořit přenos dat mezi dvěma servery



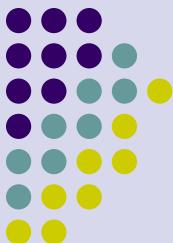
# FTP Client and Server





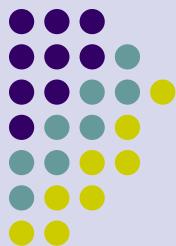
# FTP reprezentace dat

- Způsob přenosu souboru určují následujícími parametry
  - **Typ souboru (File type)**: ASCII file, EBCDIC file, binary file, local file
  - **Kódování řídicích znaků (Format control)**: nonprint, telnet format control, Fortran carriage control
  - **Struktura souboru (Structure)**: file structure (nestrukturovaný soubor dat - UNIX), record structure (soubor rozdělen na záznamy), page structure (soubor rozdělen do stránek)
  - **Režim přenosu (Transmission mode)**: stream mode (tok slabik – jako v UNIXu), block mode, compressed mode
- Typická implementace se omezuje na ASCII nebo binary, nonprint, file structure, stream mode.



# FTP Příkazy

- Příkazy jsou posílány v NVT ASCII řádky ukončené with CR, LF
- Příkazy jsou dlouhé 3 nebo 4 ASCII znaky
- Některé příkazy mají parametry
- Seznam příkazů viz help
- Lokální příkazy – viz telnet – zadávají se za znak !



# FTP vybrané příkazy protokolu

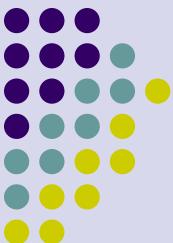
- USER username
- PASS password
- LIST – seznam souborů v aktuálním adresáři
- RETR filename – čtení souboru
- STOR filename – zápis souboru



# FTP odpovědi

- 3 ciferné číslo s uvedením významu odpovědi

<b>Reply</b>	<b>Description</b>
1yz	pozitivní předběžná odpověď
2yz	pozitivní finální odpověď
3yz	pozitivní okamžitá odpověď
4yz	dočasná negativní konečná odpověď
5yz	permanentní (stálá) negativní konečná odpověď
x0z	syntaktická chyba
x1z	informační zpráva
x2z	týká se spojení
x3z	ověřování a účtování
x4z	nespecifikováno
x5z	stav souborového systému



# FTP management spojení

- Spojení lze využít pro
  - Posílání souboru ze serveru do klienta
  - Posílání souboru z klienta do serveru
  - Posílání výpisu adresáře nebo seznamu souborů ze serveru do klienta
  - Existuje normální režim a pasivní režim



# FTP, NAP a PORT

- Normální FTP režim
  - Server má rezervovaný port 20 a 21
  - Klient inicializuje spojení po řídicím kanálu na port 21
  - Klient si přidělí port X pro přenos dat
  - Klient posílá příkazem PORT serveru číslo portu na kterém čeká navázání spojení a svoji IP adresu
  - Server vytváří spojení mezi portem 20 a vzdáleným portem a hostem podle obsahu příkazu PORT
  - Co se stane pokud je klient schován za NAT zařízením
    - NAT musí zachytit odcházející spojení určené pro port 21
    - NAT musí zachytit příkaz PORT a zapamatovat si port a adresu
    - Pokud bude FTP server pracovat na jiném portu než 21, bude mít NAT problémy



# FTP, NAP a PORT

- Pasivní režim (PASV)

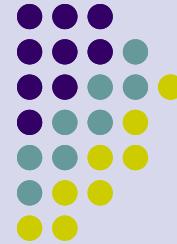
- Klient vytvoří řídicí spojení s portem 21 na serveru
- Klient povolí „pasivní“ režim (zpráva PASV)
- Server odpoví po řídicím kanále příkazem PORT se zadanou IP adresou a portem, které má klient použít k navázání spojení pro následující přenos dat (port 20)
- Klient iniciuje navázání spojení na daný port a danou adresu
- Tuto metodu používá většina web prohlížečů pro přenos pomocí FTP
- Co se stane pokud je server schován za NAT zařízením
  - NAT musí zachytit přicházející spojení na port 21
  - NAT musí zachytit příkaz PORT a zapamatovat si dvojici [port;adresa]
  - NAT povolí a přetransformsuje přicházející spojení na [port;adresa]



# Anonymní FTP

- Server může povolit komukoliv navázat spojení a pomocí FTP protokolu přenášet data
- K tomu slouží zvláštní konto, „anonymous“ nebo „ftp“. Jako heslo se zadá adresa el. pošty.
- FTP server může zabránit přístup z počítače, který nemá platné jméno.

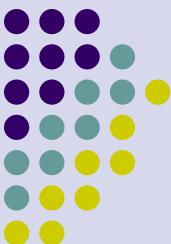
# Vzdálený terminál



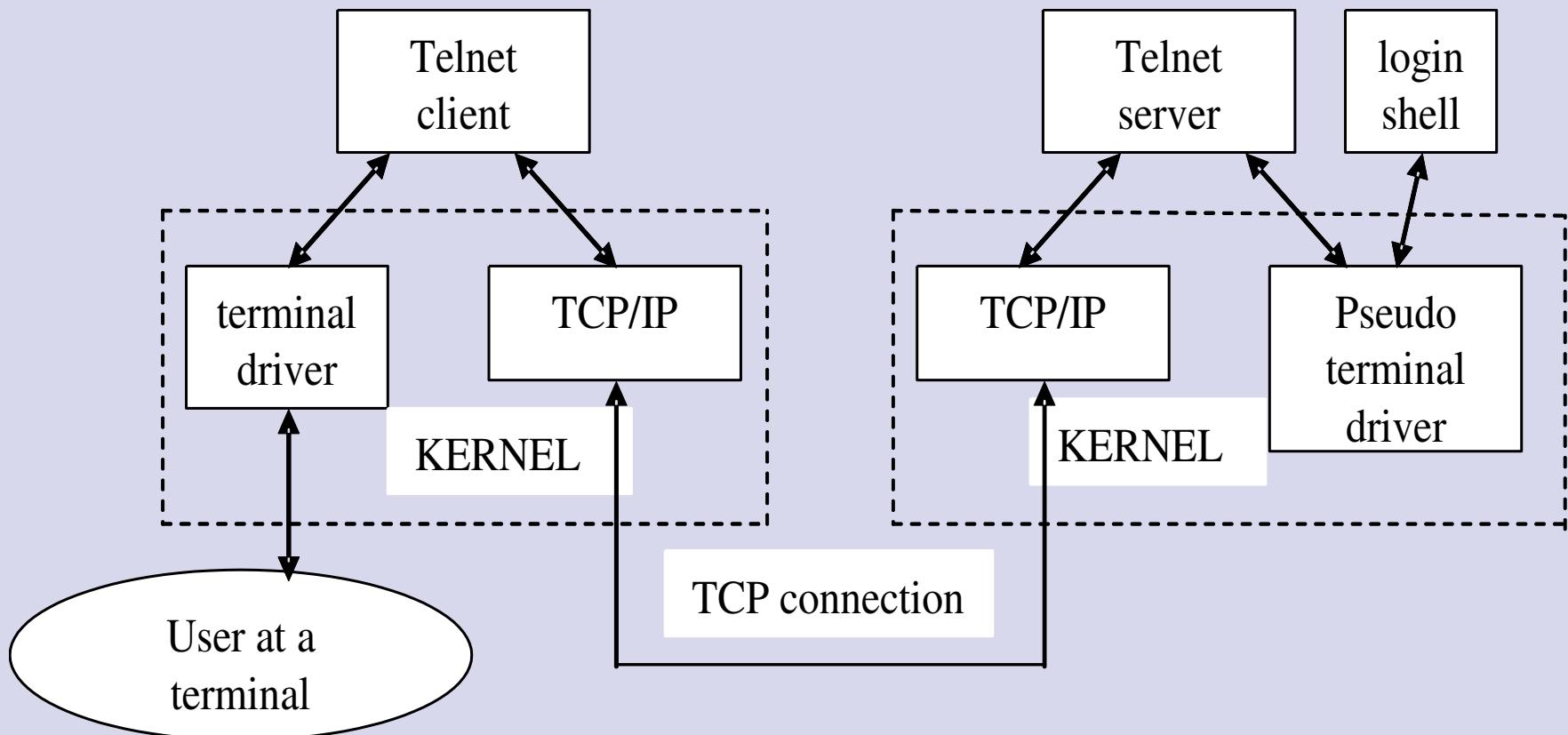


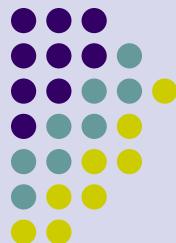
# Telnet (RFC 854)

- Protokol pro vzdálený přístup (emulace terminálu)
- Používá TCP spojení
- Přenos řídicí informace „v pásmu“ – rozlišení prefixem IAC (0xFF)
- Neobsahuje žádné záhlaví
- Podporuje vyjednávání parametrů
- Symetrický
- Definuje NVT (Network Virtual Terminal) pro komunikaci mezi serverem a klientem
- Dovoluje spolupráci různých systémů
- Definuje protokol pro přenos dat a řízení počítačovou sítí
- Pro komunikaci používá 8 bitové slabiky
- Dolních 7 bitů pro data (ASCII), od 128 výše kódování řídicích kódů



# Architektura systému





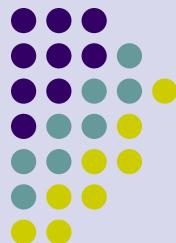
# Kódy příkazů

- Řídicí kódy povinně podporované

název	kód	hodnota	význam
NULL	NUL	0	Prázdná operace
Line Feed	LF	10	Nová řádka
Carriage Return	CR	13	Návrat vozíku

- Nepovinné řídicí kódy

název	kód	hodnota	význam
BELL	BEL	7	Zvukový signál
Back Space	BS	8	O znak zpět
Horizontal Tab	HT	9	Přechod na další pozici tabulátoru - vodorovně
Vertical Tab	VT	11	Přechod na další pozici tabulátoru - svisle
Form Feed	FF	12	Přechod na novou stránku/obrazovku



# Kódy příkazů

- IAC (Interpret as Command) – vysílá se IAC + kód příkazu

SE	240	Konec závorky – přenos parametrů při vyjednávání.
NOP	241	Prázdná operace
DM	242	Datová značka pro určení pozice synchronizační události v datovém toku.
BRK	243	Break. Stisknutí klávesy Break – přivolání pozornosti
IP	244	Pozastavení, přerušení nebo ukončení procesu ke kterému je NVT připojen.
AO	245	Abort output. Dovoluje ukončit běžící proces, ale bez výstupu dat na obrazovku.
AYT	246	Are you there. Test aktivního připojení terminálu.
EC	247	Erase character. Vypuštění posledního znaku z datového toku (přijímač).
EL	248	Erase line. Vypuštění poslední řádky z datového toku (přijímač).



# Kódy příkazů

- IAC (Interpret as Command) - pokračování

GA	249	Go Ahead. Používá se za určitých podmínek k oznámení protistraně, že chci přenášet.
SB	250	Začátek závorky (SB ... SE) pro přenos parametrů při vyjednávání.
WILL	251	Přání nebo potvrzení požadavku na nastavení parametru při vyjednávání.
WONT	252	Odmítnutí parametru při vyjednávání.
DO	253	Požadavek nebo potvrzení přání nebo požadavku na nastavení parametru při vyjednávání.
DONT	254	Odmítnutí požadavku.
IAC	255	Interpret as command, data 0xFF se přenáší zdvojením 0xFF



# Kódy příkazů

- Parametry pro vyjednávání (výběr)

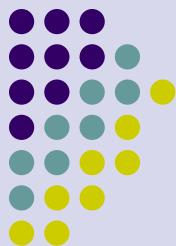
kód	název	RFC
0	Binary transmission	<a href="#">857</a>
1	echo	<a href="#">857</a>
3	suppress go ahead	<a href="#">858</a>
5	status	<a href="#">859</a>
6	timing mark	<a href="#">860</a>
24	terminal type	<a href="#">1091</a>
31	window size	<a href="#">1073</a>
32	terminal speed	<a href="#">1079</a>
33	remote flow control	<a href="#">1372</a>
34	linemode	<a href="#">1184</a>
36	environment variables	<a href="#">1408</a>



# Kódy příkazů

- Kódy pro dohadování

příkaz	odpověď	význam
WILL	DO	Vysílač by rád používal tento parametr, příjemce potvrzuje, že to dovede. Nastavení je platné.
WILL	DONT	Vysílač by rád používal tento parametr, příjemce jej nepodporuje. Nastavení není platné.
DO	WILL	Vysílač požaduje použití parametru, příjemce jej podporuje. Nastavení je platné.
DO	WONT	Vysílač požaduje použití parametru, příjemce jej nepodporuje. Nastavení není platné.
WONT	DONT	Vysílač nemůže použít daný parametr, parametr je nepovolen. Přijímač pouze toto potvrzuje.
DONT	WONT	Vysílač požaduje, aby příjemce nepoužíval daný parametr, parametr je nepovolen. Přijímač pouze toto potvrzuje.



# Dohadování parametrů

- příklad

255 (IAC), 251 (WILL), 3 (suppress go ahead) (povolení duplexního režimu přenosu)

- nebo

IAC, SB, kód parametru, 1, IAC, SE (požaduje parametr)  
a

IAC, SB, kód parametru, 0, hodnota, IAC, SE (nastavuje parametr)



# Dohadování parametrů

- Nabídka nastavení parametru

Klient: IAC, WILL, parametr

Server: IAC, DONT, parametr

Klient: IAC, WONT, parametr

- Požadavek nastavení parametru

Klient: IAC, DO, parametr

Server: IAC WONT, parametr

Klient: IAC DONT, parametr



# Dohadování parametrů

- Dodatečné dohadování – po dohodě o nastavování dohoda na parametrech

Klient: IAC, WILL, parametr

Server: IAC, DO, parametr

(( Server: IAC, DO, parametr, požadavek(1), IAC, SE ))

Klient: IAC, SB, parametr, nastavení(0), hodnota parametru, IAC, SE

- Příklad - poslání identifikace terminálu z klienta do serveru

Klient: 255 (IAC), 251 (WILL), 24 (terminal type)

Server: 255 (IAC), 253 (DO), 24 (terminal type)

Server: 255 (IAC), 250 (SB), 24 (terminal type), 1, 255 (IAC), 240 (SE)

Klient: 255 (IAC), 250 (SB), 24 (terminal type), 0, "VT220" 255 (IAC), 240 (SE)

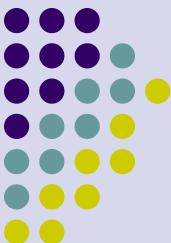


# Escape znak – změna režimu

- Možnost zadávat příkazy přímo klientovi
- Používá escape character Ctrl-]
- Nápověda ?
- Nastavení parametrů klienta
- Zobrazení nastavení
- Práce s lokálním počítačem (! příkaz)
- Připojení se / odpojení od vzdáleného stroje
- Nastavení režimu line/character
- Vysílání řídicích znaků serveru (AO, AYT, BRK, IP, ABORT, SUSP)
- Spuštění záznamu ladicích informací

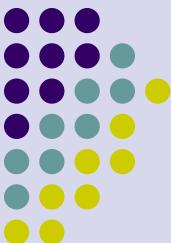
# Elektronická pošta





# Elektronická pošta

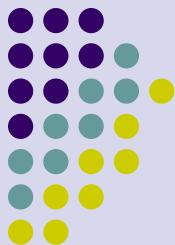
- Protokol pro přenos dat
  - RFC 822
- Formát přenášených dat
  - RFC 821
- Rozšíření formátu přenášených dat – MIME
  - Multipurpose Internet mail Exchange
  - RFC 2045
- Protokol pro doručení el. Pošty
  - POP3
    - Post Office Protocol RFC 1939
  - IMAP4
    - Internet Message Access Protocol RFC 2060



# Aplikační úroveň - Elektronická pošta

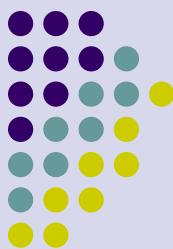
- Vlastnosti elektronické pošty
  - Přenos adresovatelných zpráv elektronicky
  - Veliký dosah (po celém světě)
  - Omezený objem dat (stovky kB)
  - Různý typ dat (text, soubory, abecedy)
  - Vysoká rychlosť doručení
  - Přenos v libovolnou dobu
  - Čtení zpráv v libovolnou dobu
  - Nadstandardní služby (potvrzení příjmu)
  - Správa
  - Bezpečnost (PGP, ... )

# Aplikační úroveň - Elektronická pošta



- Adresa elektronické pošty, poštovní server
  - Každý uživatel služby má na nějakém *poštovním serveru poštovní schránku*
  - Každé schránce přísluší jedinečná *e-mailová adresa* ve tvaru *jmeno@poštovní doména*
  - *Poštovní doména* obsahuje mimo jiné označení jmenné domény, kde je poštovní schránka umístěna
  - Poštovní server je většinou vyhrazený počítač, který běží nepřetržitě

# Aplikační úroveň - Elektronická pošta

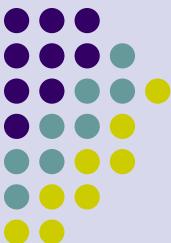


- Odesílání a přijímání el. pošty
  - Uživatel vytvoří elektronický dopis (soubor s dohodnutou strukturou) pomocí editoru, který je součástí *poštovního klienta*
  - Dopis obsahuje vlastní zprávu a záhlaví s parametry (adresa odesílatele, adresa příjemce, typ přenášených dat, ...)
  - Poštovní klient naváže spojení s poštovním serverem a pošle mu zprávu
  - Poštovní server podle cílové domény obsažené v poštovní zprávě zjistí adresu poštovního serveru adresáta (prostřednictvím jmenného serveru)



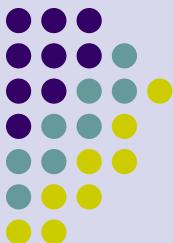
# Aplikační úroveň - Elektronická pošta

- Odesílání a přijímání el. pošty
  - Poštovní server naváže spojení s poštovním serverem adresáta a předá mu e-mail
  - Poštovní server adresáta zkонтroluje doručitelnost zprávy a uloží ji do poštovní schránky adresáta
  - Adresát vyzvedne zprávu ze schránky prostřednictvím svého poštovního klienta
  - Poštovní klient může pracovat vzdáleně (protokoly POP, IMAP, WWW e-mail klient – MS-Outlook) nebo lokálně (pine, elm, ... )



# Aplikační úroveň - Elektronická pošta

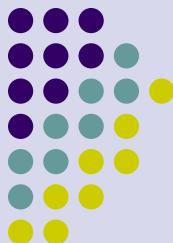
- Vlastnosti elektronické pošty
  - Přenos adresovatelných zpráv elektronicky
  - Veliký dosah (po celém světě)
  - Omezený objem dat (stovky kB)
  - Různý typ dat (text, soubory, abecedy)
  - Vysoká rychlosť doručení
  - Přenos v libovolnou dobu
  - Čtení zpráv v libovolnou dobu
  - Nadstandardní služby (potvrzení příjmu)
  - Správa
  - Bezpečnost (PGP, ... )



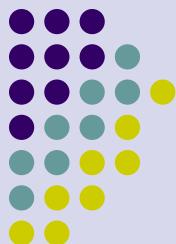
# Aplikační úroveň - Elektronická pošta

- Adresa elektronické pošty, poštovní server
  - Každý uživatel služby má na nějakém *poštovním serveru poštovní schránku*
  - Každé schránce přísluší jedinečná *e-mailová adresa* ve tvaru *jmeno@poštovní doména*
  - *Poštovní doména* obsahuje mimo jiné označení jmenné domény, kde je poštovní schránka umístěna
  - Poštovní server je většinou vyhrazený počítač, který běží nepřetržitě

# Aplikační úroveň - Elektronická pošta



- Odesílání a přijímání el. pošty
  - Uživatel vytvoří elektronický dopis (soubor s dohodnutou strukturou) pomocí editoru, který je součástí *poštovního klienta*
  - Dopis obsahuje vlastní zprávu a záhlaví s parametry (adresa odesílatele, adresa příjemce, typ přenášených dat, ...)
  - Poštovní klient naváže spojení s poštovním serverem a pošle mu zprávu
  - Poštovní server podle cílové domény obsažené v poštovní zprávě zjistí adresu poštovního serveru adresáta (prostřednictvím jmenného serveru)

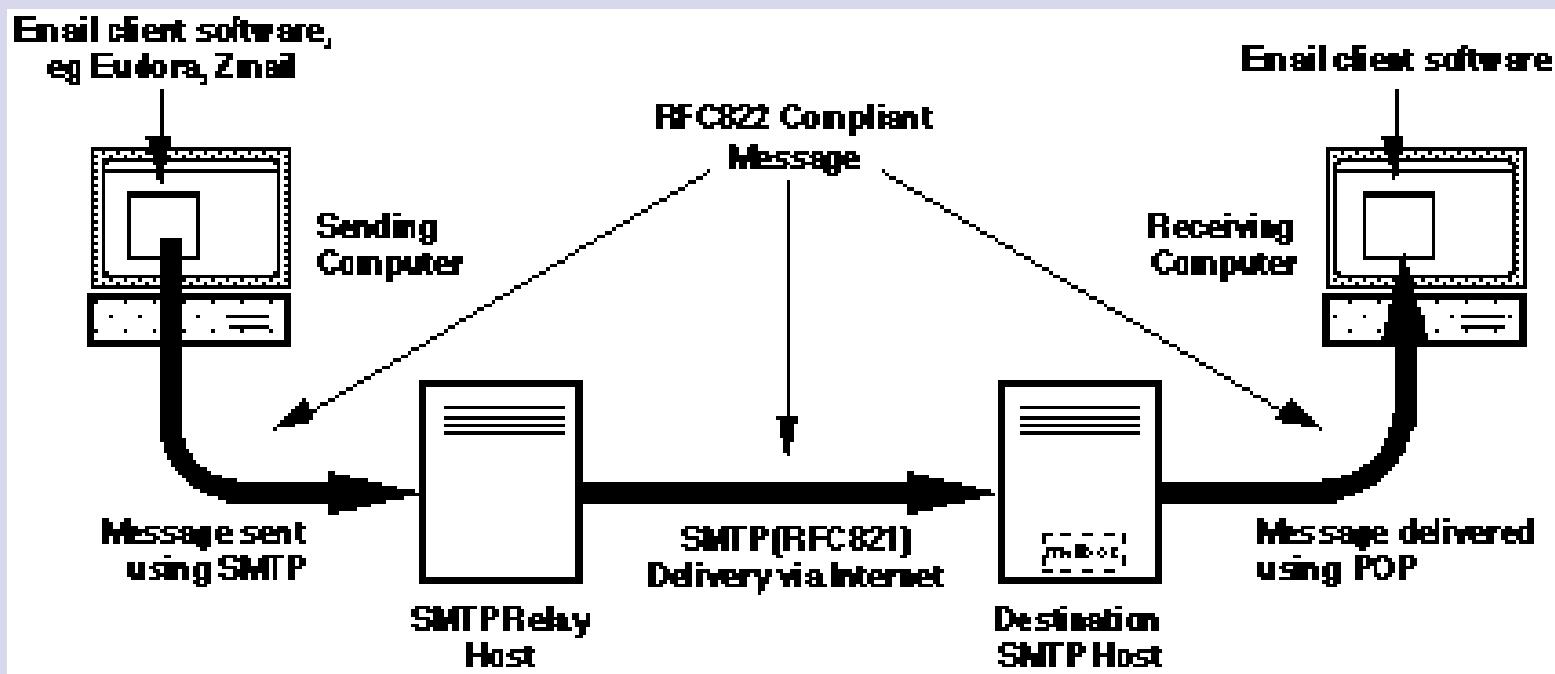


# Aplikační úroveň - Elektronická pošta

- Odesílání a přijímání el. pošty
  - Poštovní server naváže spojení s poštovním serverem adresáta a předá mu e-mail
  - Poštovní server adresáta zkонтroluje doručitelnost zprávy a uloží ji do poštovní schránky adresáta
  - Adresát vyzvedne zprávu ze schránky prostřednictvím svého poštovního klienta
  - Poštovní klient může pracovat vzdáleně (protokoly POP, IMAP, WWW e-mail klient – MS-Outlook) nebo lokálně (pine, elm, ... )



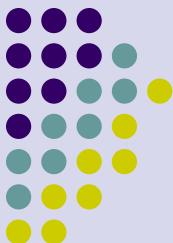
# Elektronická pošta





# SMTP příkazy

- Základní soubor příkazů zahrnuje:
  - HELO – iniciuje konverzaci s poštovním serverem. Příkazem se specifikuje jméno vlastní domény (HELO smtp.zcu.cz).
  - MAIL – oznamuje, kdo posílá e-mail. Obsahuje adresu odesílatele. jakýkoliv e-mail posílaný zpět bude posílan na tuto adresu (MAIL FROM: <someone@kiv.zcu.cz>).
  - RCPT – oznamuje, kdo je příjemcem zprávy. Posláním více příkazů RCPT je možné zadat více příjemců (RCPT TO: <user@email.cz>)
  - DATA – označuje že se bude posílat text zprávy. Zpráva musí končit sekvencí „\r\n.\r\n“ (tečka na samostatné řádce).
  - QUIT – konec konverzace.



# SMTP odpovědi

- na každý příkaz server posílá odpověď ve tvaru
  - tříciferné číslo
  - následované krátkým textem, popisujícím odpověď (250 OK)
  - (500 Syntax error, command unrecognized)



# Návratové kódy

- 211 A system status or help reply
- 214 Help message
- 220 The server is ready
- 221 The server is ending the conversation
- 250 The requested action was completed
- 251 The specified user is not local, but the server will forward the mail message
- 354 This is a reply to the DATA command. After getting this, start sending the body of the mail message, ending with „\r\n.\r\n“
- 421 The mail server will be shut down. Save the mail message and try it again later.
- 450 The mailbox that you are trying to reach is busy. Wait a little while and try again.
- 451 The requested action was not done. Some error occurred in the mail server.
- 452 The requested action was not done. The mail server ran out of system storage.



# Návratové kódy

- 500 The last command contained a syntax error or the command line was too long.
- 501 The parameters or arguments in the last command contained a syntax error.
- 502 The mail server has not implemented the last command.
- 503 The last command was sent out of sequence. For example, you might have sent DATA before sending RECV.
- 504 One of the parameters of the last command has not been implemented by the server.
- 550 The mailbox that you are trying to reach can't be found or you don't have access rights.
- 551 The specified user is not local; part of the text of the message will contain a forwarding address.
- 552 The mailbox that you are trying to reach has run out of space. Store the message and try again tomorrow or in a few days-after the user gets a chance to delete some messages.
- 553 The mail address that you specified was not syntactically correct.
- 554 The mail transaction has failed for unknown causes.



# Standard MIME

- dovoluje posílat jiná než alfanumerická data – binární data (formátovaný text, obrázky, zvuk, video)
- MIME znamená Multipurpose Internet Mail Extension
- dovoluje upravit binární data a připojit je jako přílohu k e-mailové zprávě
- k přenosu zpráv je třeba, aby odesílatel i příjemce používali klienty s podporou standardu MIME

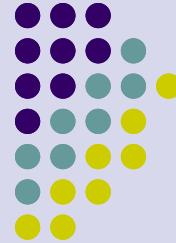


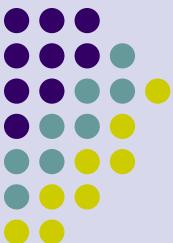
# Standard MIME - kódování

- k redukci množství dat posílaných sítí se používají kompresní a dekompresní algoritmy
- základní formáty pro kompresi dat jsou
  - zip
  - stuffit
  - binhex
  - UUencode
  - Unix compress
- další výhodou některých komprimačních programů, jako je zip, je to, že dovolují komprimovat skupinu souborů do jednoho, a tím vznikne pouze jedna příloha

# HTTP, HTML, URL

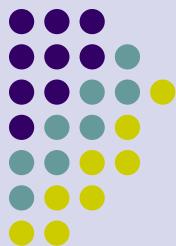
---





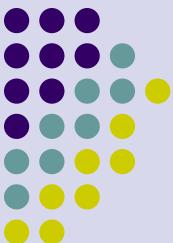
# Úvod

- Historie
- Webové komponenty
- HyperText Markup Language (HTML)
- Uniform Resource Locator (URL)
- Postup vytváření HTML dokumentu
- Statické, dynamické a aktivní stránky
- Hypertext Transport Protocol (HTTP)
- Cookies, vyrovnávací paměti, proxy,
- Vyhledávání a indexování
- RSS
- Bezpečný přenos dat, HTTPS



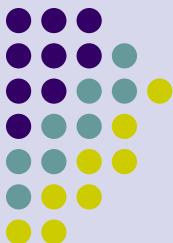
# Historie WWW

- Vytvořen Tim Berners-Lee v letech 1989 až 1990 v CERN (Evropská laboratoř pro fyziku částic)
- 1994 – Mark Andreesen vymyslel v NCSA (National Center for Super Computing Applications) MOSAIC
  - první grafický prohlížeč
  - první Internetová "killer application" – první opravdová aplikace, pro kterou začal opravdu Internet používat
  - volně přístupná
  - později Netscape Inc.



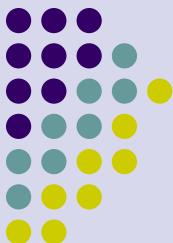
# Historie WWW

- 1995 – webové přenosy se stávají dominantními
  - exponenciální nárůst provozu na síti
  - elektronická komerce (E-commerce)
  - WWW konsorcium
- Tim Berners-Lee
  - Fyzik, ne počítačový specialista
  - Sdílení dat z fyzikálních experimentů
  - Protože FTP bylo příliš obtížné
  - Prostředek pro přenos textu i grafiky najednou
  - Nyní strategie "ukaž a klikni"



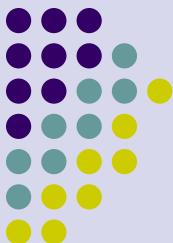
# Webové komponenty

- Prohlížeč
  - Webový klient. Nyní se upouští od označení prohlížeč, protože webový dokument se může „zobrazit“ i zvukově, ...
  - Internet Explorer, Firefox, Mozilla, Netscape, Opera, Mosaic, lynx
- Webový server
  - projekt Apache, Jakarta, Microsoft
- Reprezentace dokumentů (HTML)
  - Text, obraz, zvuk, video
- Identifikace dokumentů (URL)
- Přenosový protokol (HTTP)
  - K přenosu se využívá spolehlivý protokol TCP



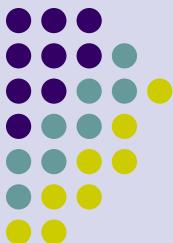
# Webový klient (browser)

- aplikační program
- představuje uživatelské rozhraní pro přístup k Webu
- stahuje informace z webového serveru
- zobrazuje stažené informace



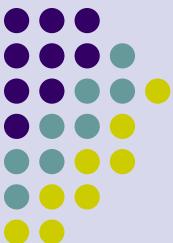
# Webový server

- úložiště webových dokumentů
- odpovídá na požadavky prohlížeče a posílá mu kopie dokumentů
- Spolupracuje s jinými servery při dynamickém generování dokumentů (jízdní řád, elektronické obchodování, STAG, ...)



# Webový dokument

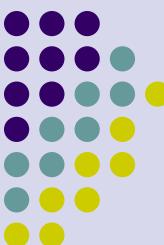
- webový dokument
  - Text, obrázky, zvuk, video
  - odkazy na ostatní webové stránky
- webový dokument a hypertextové odkazy
  - Hypertextový odkaz je spojen s objektem nebo oblastí na obrazovce
  - Vnitřně se jeví jako symbolický link
  - Výhoda - může odkazovat na dokument na jiném počítači
  - Nevýhoda - nemusí platit (neplatné URL)



# Webový dokument

- je označován jako webová stránka
- jednu webovou stránku tvoří jeden soubor
  - Používá se přípona \*.htm, \*.html
- může obsahovat
  - textový soubor
  - binární obrázek
- text je standardizován
  - známý jako HTML (HyperText Markup Language)
  - obsahuje ASCII znaky nebo znaky národních abeced
- HTML specifikuje obsah a rozvržení textu
  - Způsob zobrazení závisí na webovém klientovi

# HTML (HyperText Markup Language)



- Vychází z obecného jazyka pro popis dokumentů SGML (Standard Generalized Markup language)
- Jazyk pro popis obsahu a rozvržení dokumentu
- Na způsobu napsání dokumentu nezáleží (mezery a nové řádky neovlivní zobrazení – mohou se použít pro zvýšení přehlednosti zápisu dokumentu)
- Způsob zobrazení je dán zabudovanými značkami (tag)
- Značky jsou párové nebo nepárové
  - Formát značky
    - počáteční              <TAGNAME>
    - koncová              </TAGNAME>
  - Příklad – ***tučný text kurzívou***
    - <B><i> tučný text kurzívou</i></B>



# Obecný formát HTML dokumentu

```
<HTML>
  <HEAD>
    <TITLE>
      text který se zobrazí jako titulek dokumentu
    </TITLE>
      Další informace v záhlaví
  </HEAD>
  <BODY>
    tělo dokumentu, jeho obsah se zobrazí
    jako webová stránka
  </BODY>
</HTML>
```



# Typický příklad záhlaví

- Generováno editorem HTML stránek FrontPage 5.0

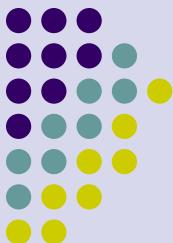
```
<!DOCTYPE html PUBLIC "-//w3c//dtd html 4.0 transitional//en">
<html> <head>
<meta http-equiv="Content-Language" content="cs">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1250">
<meta name="GENERATOR" content="Microsoft FrontPage 5.0">
<meta name="ProgId" content="FrontPage.Editor.Document">
<meta name="Author" content="Carl Ellison">
<meta name="Keywords" content="X.509, PGP, SPKI, SDSI">
<meta name="Microsoft Theme" content="waves 011">
<title>Porovnání certifikátů</title>
</head>
..... Tělo dokumentu .....
</html>
```

- Výrazně části záhlaví udávají použitý jazyk a znakovou sadu



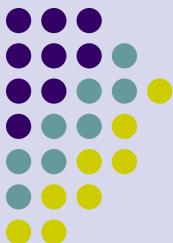
# Příklady HTML značek

- Začátek odstavce (nepárová)  
`<P>`
- Přechod na novou řádku  
(nepárová)  
`<BR>`
- Nadpis 1 (největší písma)  
`<H1> ...text... </H1>`
- Nadpis 2 (menší)  
`<H2> ...text... </H2>`
- komentář  
`<!-- ... -->`
- Tučné písma  
`<B> ...text... </B>`
- Kurzíva  
`<I> ...text... </I>`
- Podtržené písma  
`<U> ...text... </U>`
- Seznam (jeden prvek)  
`<ul> <li> </li> </ul>`
- Číslované seznamy  
`<ol> <li> </li> </ol>`



# Linky (odkazy)

- používají se značky <a> a </a>
- **relativní linky**
  - odkazují na stránku vztaženou k tomuto dokumentu
  - používají se pro zachování přenositelnosti dokumentů
  - např. (zvýrazněné se zobrazí v dokumentu, podtržené je odkaz)  
**Výsledky zkoušky ze dne <a href="/vysledky/18.11.2005.html">18.11.2005 </a>**
- **absolutní linky**
  - odkazují na cizí dokumenty
  - používají se pro přístup k dokumentům na „cizích“ serverech
  - např. (zvýrazněné se zobrazí v dokumentu, podtržené je odkaz)  
**Výsledky zkoušky ze dne  
<a href="http://home.zcu.cz/~novak/vysledky/18.11.2005.html">18.11.2005 </a>**



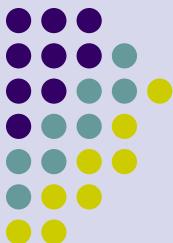
# Ukotvení (anchor)

- Zakotvení (anchor) – přechod na určené místo v dokumentu
  - může být umístěno kdekoliv v dokumentu  
`<a name="nazev_znacky"> Pozice značky</a>`
  - přechod na značku v tomtéž dokumentu  
`<a href="nazev_znacky"> Přechod na značku</a>`
  - přechod na značku z jiného dokumentu  
`<a href="cesta k dokumentu#nazev_znacky"> Přechod na značku</a>`
  - cesta k dokumentu může být relativní nebo absolutní



# Vkládání obrázků

- explicitně označeno jako obrázek
  - specifikace pomocí `<IMG SRC="jmeno_souboru">`
  - lze specifikovat i další parametry, např. zarovnání  
`<IMG SRC="jmeno_souboru" align=middle>`
  - Nebo rozměr obrázku a náhradní text pokud klient neumí obrázek zobrazit
- ``



# Kaskádové styly - CSS

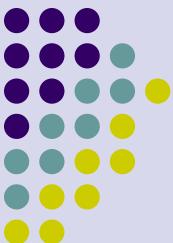
- Od popisu stránek přímo pomocí HTML značek se upouští pro malou pružnost při provádění dodatečných úprav
- Zavádí se kaskádové styly (Cascading Style Sheets - css)
- Nyní již ve verzi 3
- Používá značku <style>

<style>

Selektor {vlastnost:hodnota; vlastnost:hodnota}

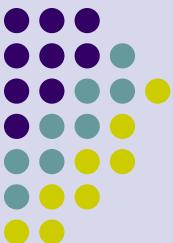
Selektor {vlastnost:hodnota}

</style>



# Kaskádové styly - CSS

- Příklady zápisu
  - přímé v dokumentu (style = )  
`<p style="text-align: center">Text odstavce ... ... ... </p>`
  - v hlavičce dokumentu `<style> ... </style>`  
`<head>  
 <title> ... </title>  
 <style type="text/css">  
 h2 {color: blue; font-style: italic}  
 </style>  
 </head>  
 <body>  
  
<h2>Nadpis </h2>  
<body>`

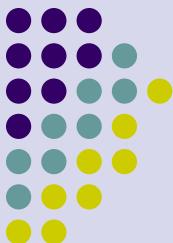


# Kaskádové styly - CSS

- Příklad zápisu
  - v externím souboru \*.css

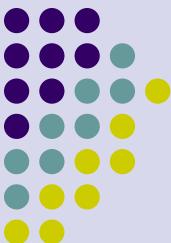
```
<link rel="stylesheet" href="soubor.css">
```
  - nebo

```
<style>
@import url("soubor.css")
</style>
```



# Kaskádové styly - CSS

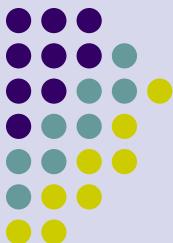
- Možnosti CSS (některé)
  - Jednotná změna fontu
  - Jednotný formát odstavce
  - Jednotná manipulace s barvami
  - Nastavení velikosti a obtékání
  - Nastavení okrajů
  - Jednotné seznamy
  - Jednotné tabulky
- Výhoda spočívá v tom, že určíme atribut, kterému přiřadíme definici vlastností. Pokud chceme vlastnosti změnit, stačí tak učinit na jednom místě
- Více na <http://www.jakpsatweb.cz/>



# XHTML

- Nová norma HTML
- Vývoj HTML skončil verzí 4.01
- X – extensible (rozšiřitelný)
- Zúžení možností HTML z důvodu lepší ověřitelnosti souladu s normou
- Nyní se používá XHTML 1.0 a 1.1
- Určení použitého XHTML (přípustnost tagů a jejich atributů) se definuje na začátku dokumentu např.  
`<?xml version="1.0" encoding="iso-8859-2"?>  
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"  
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">`

- Do dokumentu dosadí většinou HTML editor



# Rozdíly HTML a XHTML

- XHTML striktně vyžaduje
  - Všechny atributy mají hodnoty v uvozovkách
  - Zákaz křížení tagů
- Rozdíly mezi HTML a XHTML
  - Tagy a atributy jsou malými písmeny
  - Nepárové tagy končí lomítkem
  - Párové tagy jsou párové povinně
  - Všechny atributy musejí mít hodnotu
  - Interní javascript a styly se zapisují jiným způsobem
  - Dokument má mít XML prolog.
  - Dokument požaduje správný doctype.
- Více na <http://www.jakpsatweb.cz/html/xhtml.html>



# URL (Uniform Resource Locator)

- Slouží k identifikaci objektu
- Má textovou podobu
- Byl vytvořen pro identifikaci různých objektů, mimo jiné i webových stránek
- Má obecný tvar

protokol://uživatel:heslo@doménové\_jméno:port/cesta\_k\_souboru?parametry

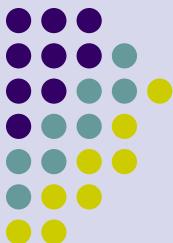
protokol://uživatel:heslo@doménové\_jméno:port/cesta\_k\_souboru#návěští

- Znaky ':', '/', '@', '?', '#' slouží k oddělení a určení jednotlivých částí URL



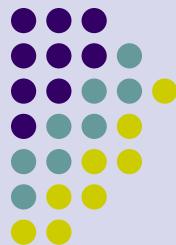
# URL (Uniform Resource Locator)

- Speciální znaky a jejich význam
  - ‘://’ - oddělení protokolu od jména nebo IP adresy počítače
  - ‘@’ - oddělení uživatelského jména od jména nebo IP adresy počítače
  - ‘#’ - označení odkazu na návěští ve stránce
  - ‘~’ - označení domovského adresáře pro webové stránky uživatele (public\_html)
  - ‘?’ - označení že následují parametry
  - ‘/’ nebo ‘\’ - oddělení jednotlivých podadresářů
  - ‘./’ - aktuální adresář
  - ‘../’ - adresář vyšší úrovně (používá se při relativním odkazování)



# URL (Uniform Resource Locator)

- Např. URL  
`http:// home.zcu.cz:8080/~novak/soubor.html`
- Se chápe následovně:
  - http - protokol
  - 8080 - číslo portu
  - home.zcu.cz - doménové jméno
  - ~novak - cesta k souboru
  - soubor.html - soubor
- Pokud některá část URL chybí, nahradí se předdefinovanou hodnotou
  - protokol – HTTP
  - port – 80
  - soubor – index.htm, index.html, ...



# URL (Uniform Resource Locator)

- Protokol určuje způsob přístupu k dokumentu
- Může být (na písmu (velké/malé) nezáleží)
  - HTTP - protokol HTTP
  - HTTPS - zabezpečený HTTP (šifrování)
  - FTP - přístup pomocí FTP
  - FILE - soubor na lokálním disku
  - GOPHER - předchůdce HTTP
  - MAILTO - adresa el. pošty
  - TELNET - vzdálený přístup



# Vytváření HTML dokumentu

- jakýmkoliv textovým editorem (Notepad, Wordpad a další)
- Speciálním HTML editory – WYSIWIG (Microsoft FrontPage, Microsoft Office Publisher, DreamWeaver a další – mnohé volně šířitelné – Nvu „new view“, Mozilla Composer, Netscape Composer, Trellian WebPAGE, )
- Existuje i export stránek z různých WYSIWIG editorů (MS word)
- v počátcích je výhodné používat textový editor nebo jednoduchý HTML editor – pochopení principu, jednodušší konstrukce stránek



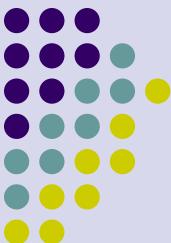
# Vytváření vlastních webových stránek

- Vytvoření samostatné stránky a její lokální odzkoušení www prohlížečem (file:// cesta k souboru), vytvoření vnitřních odkazů a jejich odzkoušení
- soubor opatřit příponou htm nebo html (dohoda)
- vytvoření dalších stránek, vzájemné propojení stránek relativními odkazy, vytvoření absolutních odkazů na cizí stránky
- lokální odzkoušení vytvořených vazeb



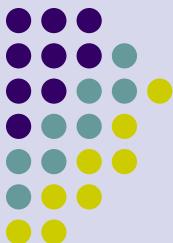
# Vytváření vlastních webových stránek

- stránky se ukládají do vhodně vytvořené adresářové struktury, např. html stránky do jednoho adresáře, obrázky do jiného, související dokumenty do dalšího, atd. (obecný předpis neexistuje)
- přesunutí stránek na webový server a odzkoušení webovým prohlížečem (např. [http://počítač.firma.doména/~login\\_name/cesta/.../soubor.html](http://počítač.firma.doména/~login_name/cesta/.../soubor.html) (~ znamená značku pro domácí adresáře uživatelů)



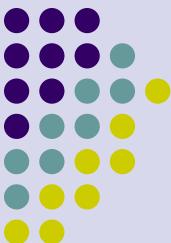
# Vytváření vlastních webových stránek

- Domácí adresář pro html stránky je obvykle `~/public_html`
- Pokud není uvedeno jinak (v URL není uveden odkaz na konkrétní dokument), hledá prohlížeč v tomto adresáři soubor `index.htm` nebo `index.html`
- např. uživatelské stránky na ZČU:  
`home.zcu.cz/~login_name`
- Prohlížení vytvořených webových stránek
  - zobrazení vybrané stránky prohlížečem
  - volba zobrazit/zdrojový kód



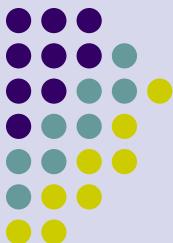
# Typy webových stránek

- statické
  - HTML stránky jsou uloženy v souboru
  - jsou neměnné, mohou obsahovat text, obrázky, odkazy, ...
- dynamické
  - jsou vytvářeny serverem za běhu, na přání
  - jsou výstupem nějakého programu
  - Např. CGI (Common Gateway Interface)
  - nyní častěji přímé volání programu ze serveru (PHP, Java, ... )
- aktivní
  - spuštěny v prohlížeči na straně klienta
  - obsahují program, mohou komunikovat s prostředím (uživatelem)
  - Mohou bezprostředně reagovat na pohyb myši, stisk klávesy
  - používají technologie Java, JavaScript nebo jiné



# CGI technologie

- URL specifikuje
  - adresu webového serveru
  - CGI program na serveru (název.cgi)
  - argumenty programu (?jméno=hodnota; ... )
- web server
  - používá TCP komunikaci
  - přijímá HTTP požadavek od klienta
  - spouští určený CGI program
  - vrací výsledek (textový výstup programu) klientovi



# CGI program

- provádí zadaný výpočet
- je často psán ve skriptovacím jazyce
- za běhu produkuje výstupní soubor
- na počátku svého běhu generuje hlavičku
- hlavička obsahuje informace ve tvaru klíčové slovo:informace, např.
  - Content Type: text/html; charset=UTF-8 - HTML dokument
  - Server: GWS/2.1 - informace o serveru
  - Content-Length: 1000 - délka datové části
  - Date: Thu, 23 Nov 2006 10:53:51 GMT



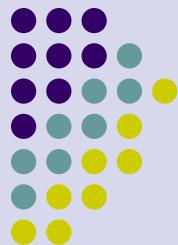
# Dynamické vytváření stránek

- CGI má velkou režii spojenou s vytvořením obslužného procesu a zavedením programového modulu do paměti
- Proto se častěji používá jiná metoda, kdy interpret jazyka programu pro vytvoření stránky je součást (modul) webového serveru
- Populárním jazykem je PHP
  - Programový modul se umístí jako zakomentovaný text do HTML stránky
  - Webový server stránku před odesláním analyzuje a zadaný program interpretuje – výstupem je statický text (statická část stránky) a dynamicky programem vygenerovaný text
  - Klient získá HTML dokument, o programu nic neví



# Dynamické vytváření stránek

- Dalším prostředkem je Java
  - Součástí webového serveru je interpret jazyka Java
  - Programy upravené pro volání webovým serverem se označují jako servlety
  - Nejsou součástí webové stránky, jsou umístěny v dohodnutém adresáři
  - Jsou jim předávány dohodnutou metodou i parametry
  - Aby nebylo třeba vše generovat programem, existují JSP (Java Server Page) – část statická (statický text) a část dynamická (servleты) – obdoba PHP

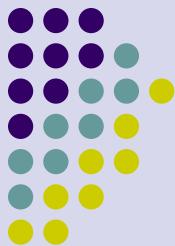


# Aktivní stránky

- Program se spouští na straně klienta (v prohlížeči)
- Prohlížeč musí obsahovat interpret jazyka (nejčastěji javascript nebo java)
- Výhoda je možnost reagovat okamžitě na události spojené s pohybem myši nebo zadáním z klávesnice
- Použití – hry, výpočty, bankovnictví
- Javascript je zakomentovanou součástí webové stránky – prohlížeč Javascript interpretuje
- Java se přenese jako samostatný modul – applet
  - V prohlížeči se interpretuje (spustí se) a výsledky zobrazuje do přiděleného prostoru (grafické okénko na webové stránce)

# HTTP

# HyperText Transfer Protocol

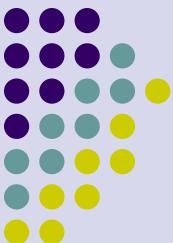


- HTTP je aplikační protokol, pracuje nad standardní síťovou infrastrukturou (TCP/IP)
- Existují 3 verze
  - 0.9 – původní návrh Berners-Lee
  - 1.0 – (RFC 1945) – používá se nejčastěji
  - 1.1 – (RFC 2068) – počet implementací neustále narůstá
- Komunikační protokol typu server/klient (komunikace typu požadavek – odpověď)
- Bezestavový protokol
  - Server otevře spojení, obslouží požadavek, uzavře spojení



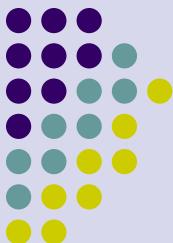
# HTTP požadavky (request)

- Klient může poslat serveru požadavek typu
  - GET – požadavek na zaslání dokumentu dle URL
  - PUT – uložení dokumentu určeného URL
  - HEAD – obnova informace o dokumentu dle URL
  - OPTIONS – obnova informace o dostupných volitelných parametrech
  - POST – dodání informace na server
  - DELETE – zrušení dokumentu dle URL
  - TRACE – vrácení zprávy s požadavkem z důvodu ladění
  - CONNECT – používají vyrovnávací paměti (cache)



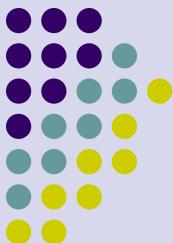
# HTTP požadavky (request)

- HTTP požadavek má tvar  
`<požadavek> URL HTTP <verze>`
- Např.  
`GET http://home.zcu.cz/~novak/index.html HTTP/1.1`
- Následuje záhlaví požadavku (parametry)
- Požadavek PUT má i tělo (text posílaný serveru)



# HTTP odpověď (response)

- HTTP server posílá odpověď ve tvaru  
*HTTP/<verze> xyz kód odpovědi slovně*
- následuje záhlaví s parametry
- Vlastní tělo zprávy s požadovaným dokumentem (odpověď na GET nebo POST)
- V záhlaví je např.
  - Date: Friday, 27-Apr-01 13:30:01 GMT
  - Content-length: 3001



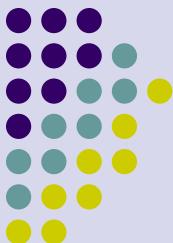
# HTTP kódy odpovědí

- Kód odpovědi je ve tvaru
  - XYZ slovní význam
  - Jsou rozděleny do pěti skupin podle významu
    - 1xx – informační – požadavek byl přijat a zpracovává se
    - 2xx – úspěšné volání – akce byla přijata, akceptována a zpracována
    - 3xx – redirekce – je třeba provézt další akci (přesměrování)
    - 4xx – chyba klienta – chybná syntaxe, nemůže být provedeno
    - 5xx – chyba serveru – server nemůže požadavek provézt (např. přetížení serveru)
  - Další dvě pozice kódu upřesňují jeho význam



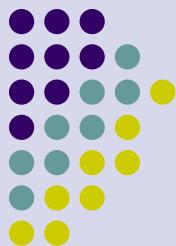
# Cookies – záznam stavu

- Vztah mezi klientem a serverem nevyžaduje zapamatování stavu komunikace na straně serveru
  - Výhoda je zjednodušení serveru
  - Zvýšení odolnosti proti zahlcení
  - Nevýhoda že si server nepamatuje, které stránky již uživatel navštívil
- Cookies (koláčky) slouží k zapamatování stavu z pohledu uživatele
  - Generuje je server a posílá klientovi
  - Ukládají se do speciální vyrovnávací paměti na disku
  - V případě potřeby je klient pošle serveru



# Cookies – záznam stavu

- Cookies obsahují informace, definované serverem, které by klient neměl měnit
  - Set-cookie: textový řetězec (posílá server)
  - Cookie: textový řetězec (posílá klient)
- Cookies obsahují (přibližně, liší se dle RFC specifikace)
  - Jméno domény – kde se mohou uplatnit
  - Cestu ke stránce – určení dokumentu na serveru
  - Obsah – vlastní rozlišovací informaci ve tvaru název=obsah
  - Dobu expirace
  - Bezpečné spojení ano/ne



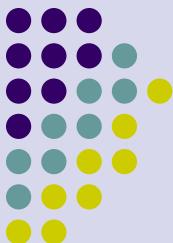
# Perzistentní spojení

- Původně komunikoval HTTP server s klientem pomocí TCP tak, že se vytvořilo spojení pro přenos pouze jednoho dokumentu
- Obsahoval-li dokument obrázky, vytvořilo se pro přenos každého obrázku další spojení
- Z důvodu snížení režie se přenáší během jednoho spojení celá stránka, tj. jak textová část, tak i obrázky



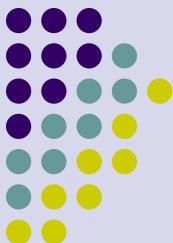
# Vyrovnávací paměti

- Slouží k omezení zbytečných přenosů v síti
- Vyrovnávací paměti (cache)
  - Na straně klienta (disk, paměť počítače)
    - Načtené stránky se ukládají do vyrovnávací paměti
    - Při požadavku opakovaného čtení stránky se zkontroluje není-li již načtena
    - Pokud se její obsah mezi tím nezměnil, načte se z vyrovnávací paměti
    - Ke kontrole slouží příkaz HEAD a porovnání s dobou života dokumentu
    - Ukládání do vyrovnávací paměti lze v dokumentu zakázat (např. při přístupu k bankovnímu účtu), příkazem mazat



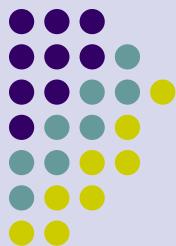
# Vyrovnávací paměti

- Vyrovnávací paměti (cache)
  - Na komponentách počítačové sítě
    - Konfigurovatelné servery (cache servery)
      - Webový klient může mít nakonfigurovánu adresu proxy serveru, přes který je umožněn přístup z firemní sítě do Internetu
      - Většinou se počítač označuje jako proxy.firma.cz nebo cache.firma.cz a používá implicitní port 3128
      - Součástí proxy serveru mohou být i vyrovnávací paměti
      - Webový klient posílá požadavek na proxy server, ten provede kontrolu dostupnosti dokumentu ve své paměti. Bud' na požadavek odpoví sám, nebo jej pošle originálnímu serveru
      - Odpovědi originálního serveru na požadavky automaticky ukládá do vyrovnávací paměti pro další použití



# Vyrovnávací paměti

- Vyrovnávací paměti (cache)
  - Na komponentách počítačové sítě
    - Transparentní servery (transparentní cache servery)
      - Jsou umístěny v páteřních částech Internetu
      - Nekonfigurují se (uživatel o nich neví – proto transparentní)
      - Směrovače v Internetu přesměrují automaticky HTTP požadavky na počítače s vyrovnávacími pamětími
      - provede se kontrola dostupnosti dokumentu a buď se poskytne kopie, nebo se požadavek předá originálnímu serveru
      - Existuje i protokol pro výměnu informací mezi cache servery – výměna zachycených souborů z důvodu dalšího zvýšení průchodnosti



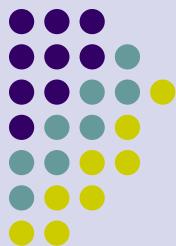
# Proxy

- Proxy znamená zástupce a v počítačových sítích se tento pojem vyskytuje v tomto významu poměrně často
- V tomto případě zprostředkovává proxy server spojení firemní sítě (intranetu) a vnější sítí (Internetem)
- Slouží jako součást ochrany vnitřní sítě před napadením zvenku



# Vyhledávání a indexování

- K poskytování informací nestačí HTTP servery, protože informací je moc
- Dochází k budování indexových serverů, které obsahují seznam dokumentů přístupných podle klíčových slov
- Indexy se vytváří
  - Na přání (manuálním zadáním dokument, klíčová slova)
  - Na základě informací uvedených v hlavičce dokumentu (Keywords=)
  - Automaticky pomocí prohledávacích strojů – robotů, kteří neustále prohledávají Internet, hledají HTTP servery a čtou všechny dostupné HTML stránky a třídí je podle slov (klíčových slov), získaných z textu



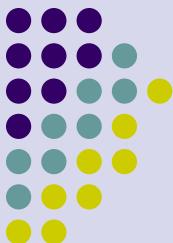
# Vyhledávání a indexování

- Pro získání informací (odkazů na webové stránky) slouží „vyhledávače“, které vyhodnotí zadaný výraz a vrátí relevantní odkazy
- Nejznámější vyhledávač Google
- Indexování a vyhledávání může být realizováno i na jednom webovém serveru (firemní weby – vyhledání informací vztahujících se k výrobku)



# Oznamování o změnách stránky

- Při sledování většího počtu webových stránek je problém se zjišťováním jejich změn
- RSS (Really Simple Syndication (0.9x) nebo RDF Site Summary (1.0))
- RDF (Resource Description Framework)
- Cílem je přebírat obsah zdrojů na Internetu a v přehledné formě je nabízet uživateli
- Informaci vytváří autor stránky ve formátu XML (eXtensible Markup Language) a v tomto formátu se přenáší Internetem do RSS čtečky
- RSS čtečka periodicky zjišťuje změny na zadané stránce, stahuje RSS dokument a interpretuje jeho obsah jako seznam změněných dokumentů
- Např. Headline Viewer, FeedReader, AmphetaDesk
- Viz <http://interval.cz/clanky/rss-rss/>



# Zabezpečení HTTP

- Přenos pomocí HTTP je otevřený – nelze takto přenášet citlivé informace
- Systém byl doplněn o SSL vrstvu (Secure Socket Layer), která leží mezi TCP a HTTP
- SSL zajišťuje šifrování přenášených dat
  - Je založeno na certifikátech
  - Dovoluje ověřit server (anonymní přístup klienta)
  - Vzájemné ověření serveru i klienta
  - Při ověřování (asymetrická šifra) se přenesou relační klíče (symetrická šifra) pro další komunikaci
- Takto zabezpečený protokol je označován jako HTTPS

# Šifrování a bezpečnost



Úvod do počítačových sítí

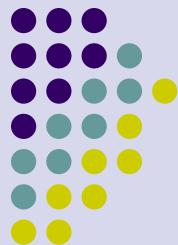
Lekce 12

Ing. Jiří lédvina, CSc.



# Bezpečnost

- požadavky na bezpečnost se v poslední době výrazně mění
- tradičně byla zajišťována zamezením přístupu (uzamykáním a administrativně)
- se zavedením výpočetní techniky vznikla potřeba vytvářet automatizované prostředky pro ochranu souborů a dalších informací
- použití počítačových sítí a komunikačních linek vyžaduje zajistit ochranu dat během přenosu
- Simon Singh: Kniha kódů a šifer (populární)



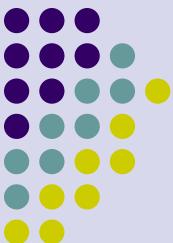
# Definice

- **počítačová bezpečnost** – všeobecný název pro soubor prostředků, navržených k ochraně dat a maření úsilí hackerů
- **sítová bezpečnost** – opatření k ochraně dat během přenosu
- **bezpečnost Internetu** – opatření k ochraně dat během přenosu přes soubor propojených sítí
  - spočívá v opatření k odrazení, prevenci, detekci a korekci bezpečnostních hrozeb poškozujících přenos informace



# Ochrana výpočetních systémů

- **ochrana zdrojů** – ochrana proti neoprávněnému použití prostředků v OS
- **bezpečná komunikace** – vlastní ochrana přenášené informace
- **ověřování uživatelů** – zabezpečení, aby zprávy přicházely od ověřeného zdroje a bez modifikace



# Napadení systému

- **Pasivní**

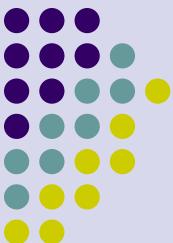
- odposlech
- analýza přenosu – odkud, kam, kolik, ...

- **Aktivní**

- modifikace, zadržování nebo podstrkávání zpráv
- modifikace toku dat – změna obsahu, opakování, změna pořadí, rušení, syntéza zpráv, změna adresy, změna dat, atd.
- Odepření služby

- **Cíl**

- Prevence pasivního útoku
- Detekce aktivního útoku



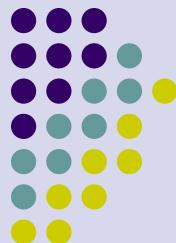
# Prostředky pro zajištění bezpečnosti

- Bezpečnostní služby
  - Zajištění soukromí
  - Ověřování pravosti
  - Zajištění integrity
- Kryptografické algoritmy
  - Symetrické šifrování (tajný klíč)
  - Asymetrické šifrování (tajný a veřejný klíč)
  - Otisk zprávy (kryptografický součet)



# Bezpečnostní mechanizmy

- Šifrování
- Digitální podpisy
- Řízení přístupu
- Integrita dat
- Ověřování výměny dat
- Vyplňování přenosu
- Řízené směrování
- Ověřování třetí stranou



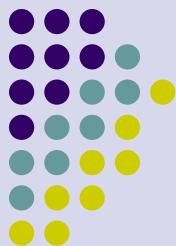
# Bezpečnostní architektura ISO

- **authentication** – ověření pravosti – ujištění, že entita je to, za co se vydává
- **access control** – řízení přístupu – zamezení neautorizovaného využívání zdrojů
- **data confidentiality** – důvěrnost dat – ochrana dat před neautorizovaným přístupem
- **data integrity** – integrita dat – ujištění, že přijatá data byla odeslána ověřenou entitou
- **non-repudiation** – nepopiratelnost – ochrana proti popření jednou z komunikujících entit



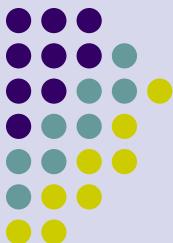
# Terminologie šifrování

- **otevřený text** (plaintext)
- **šifrovaný text** (ciphertext)
- **šifra** – algoritmus pro transformaci otevřeného textu na šifrovaný
- **klíč** – parametr šifrování
- **šifrování** – převod otevřeného textu na šifrovaný
- **dešifrování** – převod šifrovaného textu na otevřený
- **kryptografie** – studium šifrovacích principů a metod
- **kryptoanalýza** – studium principů a metod pro dešifrování bez znalosti klíče
- **kryptologie** – kryptografie a kryptoanalýza



# Základní operace šifrování

- Šifrovací operace
  - Substituce – náhrada znaků za jiné
  - Transpozice – přesun znaků (bitů) na jiné místo v kódu
- Šifra
  - Bloková – šifruje se po blocích pevné délky
  - Proudová – šifruje se po bitech nebo slabikách



# Základní šifrovací operace (historie)

- Substituce (s-box)
  - Každé písmeno nebo skupina písmen je nahrazena jiným písmenem nebo skupinou písmen
  - Např. Caesarova šifra – použita Caesarovými vojsky
  - Jednoduše prolomitelné
- Transpozice (p-box)
  - Přeuspořádání písmen, ale ne překódování (permutace)
  - Sloupcové šifrování – otevřený text je šifrován po sloupcích různými klíčovými slovy
  - Ne tak jednoduché prolomení jako u substitučních šifer.
- Složené šifry
  - Kombinace substituce a transpozice



# Základní šifrovací operace

- Jednorázová hesla

- Šifrovaný text je vytvářen konverzí otevřeného textu na bitový řetězec a XOR-ován s náhodným bitovým řetězcem. Délka přenášených dat je omezena délkou řetězce (klíče)
- Neprolomitelná šifra
- Klíč je obtížné si pamatovat – odesílatel i příjemce musí přenášet i kopii klíče
- Vyžaduje striktní synchronizaci mezi odesílatelem a příjemcem. Jeden chybějící bit může pomotat cokoliv



# Jednoduché šifry

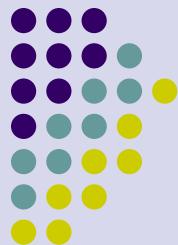
- Monoalfabetické šifry
  - Caesarova šifra (substituční) - posunutí abecedy o 3 pozice v abecedě
  - $E(x) = (x + k) \text{ mod } N; D(x) = (c - k) \text{ mod } N;$
  - pouze 26 možností - řešení → útok hrubou silou
  - Vylepšení - náhodné přiřazení (prohození) písmen (klíč 26 písmen dlouhý –  $26! = 4 \times 10^{26}$ )

Plain:	abcdefghijklmnopqrstuvwxyz
Cipher:	DKVQFIBJWPESCXHTMYAUOLRGZN
Plaintext:	i fwewi shto replace letters
Ciphertext:	WIRFRWAJUHYFTSDVFSUUUFYA



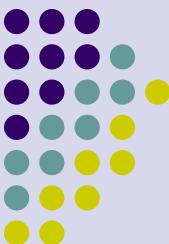
# Jednoduché šifry

- Affine cipher
  - $E(x) = (ax + b) \bmod N$
  - $D(x) = a^{-1} (E(x) - b) \bmod N$
- Musí existovať  $a^{-1}$ 
  - $a^{-1} a = 1 \bmod N$
  - $N$ ,  $a$  musí byť relativný prvočísla
  - $a^i \bmod N = \{1, 2, \dots, N-1\}; i = 1, \dots, N-1$
- Př.  $a = 3, N = 7$



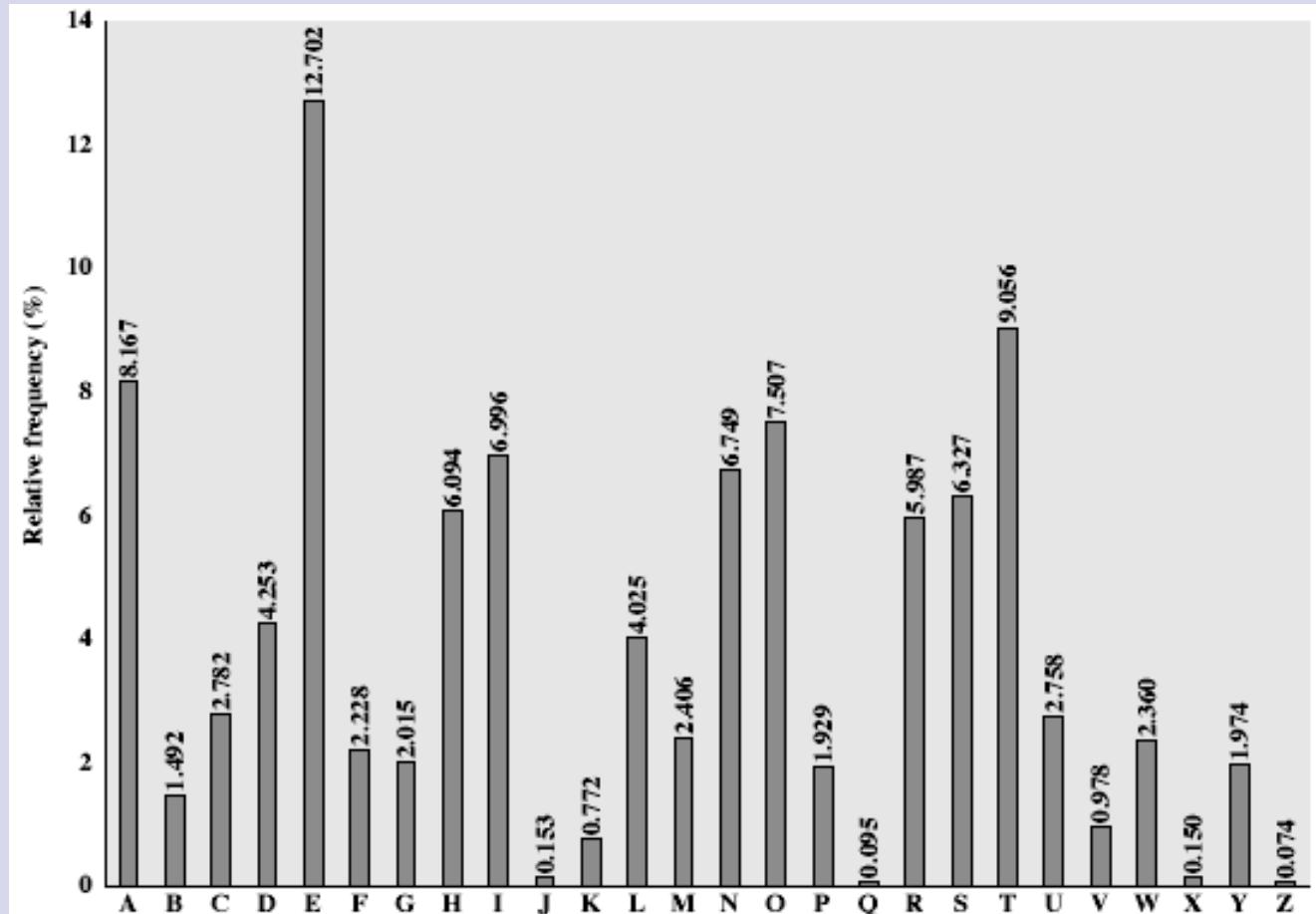
# Jednoduché šifry

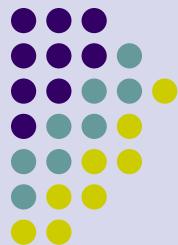
- Polyalfabetické šifry
  - kombinace transpozice a substituce
  - šifrování na dané pozici závisí na klíči, šifrování pozic se opakuje s periodou délka klíče
  - řešením je nalézt délku klíče, a pak jde a o několik monoalfabetických šifer
- Útok hrubou silou
  - Snaha odhalit klíč metodou pokus-omyl
  - Vyzkoušení „všech“ možností – výpočetně složité
  - Nalezení postupu, který by eliminoval počet pokusů



# Frekvenční analýza

- Frekvenční analýza výskytu znaků v anglické abecedě
- Frekvenční analýza skupin znaků (a, an, the, ...)
- Obrana – odstranění mezer mezi slovy





# Zabezpečení

- Předpoklad: Algoritmus je útočníkovi znám, není znám klíč
- Stupeň zabezpečení
  - **absolutní bezpečnost** – bez znalosti klíče nelze odhalit otevřený text
    - jednorázová hesla
    - Heslo (klíč použijeme pouze jednou)
  - **výpočetní bezpečnost** – šifra nemůže být prolomena pro nedostatečnou výpočetní výkonnost
    - Realizace specializovaných počítačů umožňujících prolomit šifru (útok hrubou silou)
    - Obrana (dočasná) prodloužením klíče



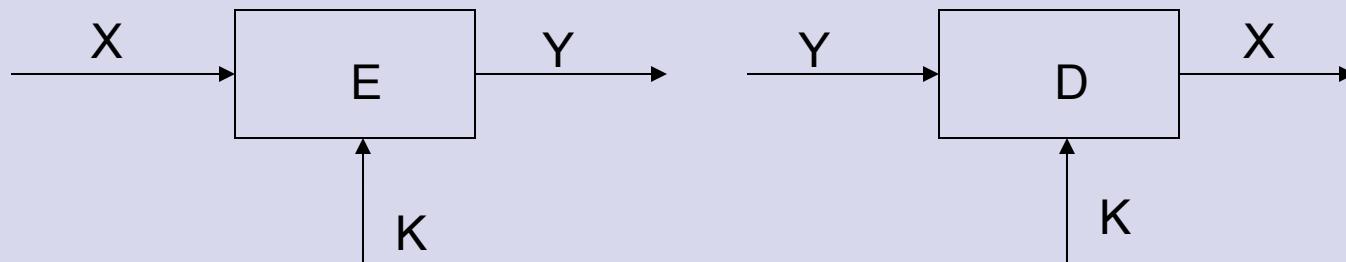
# Symetrické šifrování

## Požadavky

- Blokové a proudové šifry
- silný šifrovací mechanizmus
- šifrovací klíč zná pouze odesílatel a příjemce
- známý šifrovací (a dešifrovací) algoritmus
- Nutnost použití bezpečného kanálu pro distribuci klíče

$Y = E_K(X)$  - šifrování

$X = D_K(Y)$  - dešifrování

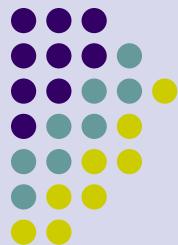




# Šifrování tajným klíčem

## DES – Data Encryption Systém

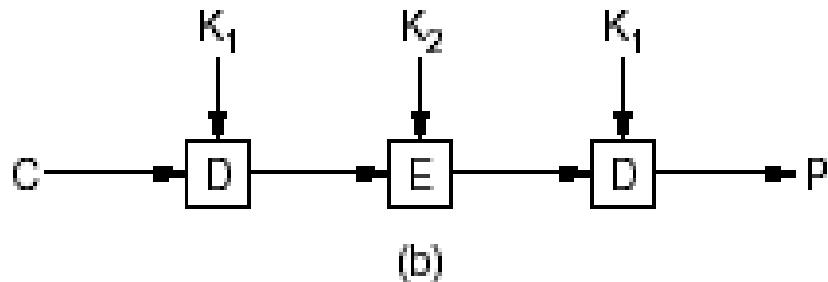
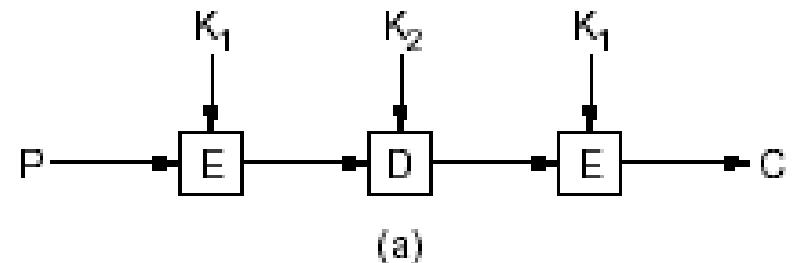
- Šifrovací algoritmus vyvinut v r. 1970 National Bureau of Standards and Technology a IBM.
- Vychází z šifry Lucifer (IBM, 128 bitů)
- Používá délku klíče 56 bitů a 19 různých stavů
- Každá iterace  $i$  používá jiný klíč  $K_i$ . Složitost závisí na komolící funkci  $f$ .
- Klíč  $K_i$  je odvozován od počátečního 56 bitového klíče.
- Velmi silný, ale prolomitelný
- Existují slabé klíče
- Režimy činnosti
  - ECB, CBC, ...

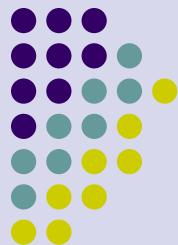


# Šifrování tajným klíčem

Triple DES – řeší problém příliš krátkého klíče DES jeho rozšířením na 112 bitů

- Pro šifrování postupně používá algoritmus šifrování klíčem K1, dešifrování klíčem K2 a šifrování klíčem K1.
- Pro dešifrování postupně používá algoritmus dešifrování klíčem K1, šifrování klíčem K2 a dešifrování klíčem K1





# Šifrování tajným klíčem

AES/Rijndael (AES – Advanced Encryption Standard) – Rijndael.

- vítěz konkurzu o šifrovací standard (2002)
- délka klíče 128, 196 nebo 256 bitů

IDEA – International Data Encryption Standard

- Publikován v r. 1990
- Používá klíč délky 128 bitů
- Velmi silné šifrování, nebyly publikovány žádné praktické útoky, útok hrubou silou není prakticky
- Pokrytý různými mezinárodními patenty

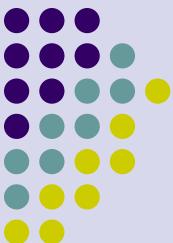
Skipjack

- Tajný algoritmus vyvinutý NSA
- Je použit v šifrovacím čipu Clipper
- Využívá klíč délky 80 bitů



# Asymetrické šifrování

- Symetrická šifra je dostatečně bezpečná
- Neřeší však problém distribuce klíče
- Začátek 70. let – problém s distribucí klíče v bankovnictví (nutná periodická výměna tajných klíčů klientů)
- Snaha o vyřešení problému
  - 1976 – výměna klíčů Diffie-Hellman
    - Vyžaduje kooperaci obou stran (on-line komunikace)
  - 1978 – asymetrické šifrování Rivest, Shamir, Adleman (RSA)
    - Klíče se dají vygenerovat předem – vhodné i pro off-line komunikaci

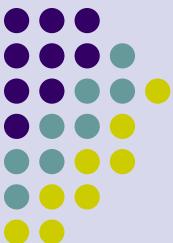


# Asymetrické šifrování

- Řeší problém distribuce klíče
- Používá dvojici (závislých) klíčů
  - Jeden je označován jako veřejný
  - Druhý jako tajný
- Šifrování

  - Šifrování veřejným klíčem
  - Dešifrování tajným klíčem

- Ověření pravosti (i nepopiratelnost)
  - Zabezpečení tajným klíčem
  - Ověřování veřejným klíčem



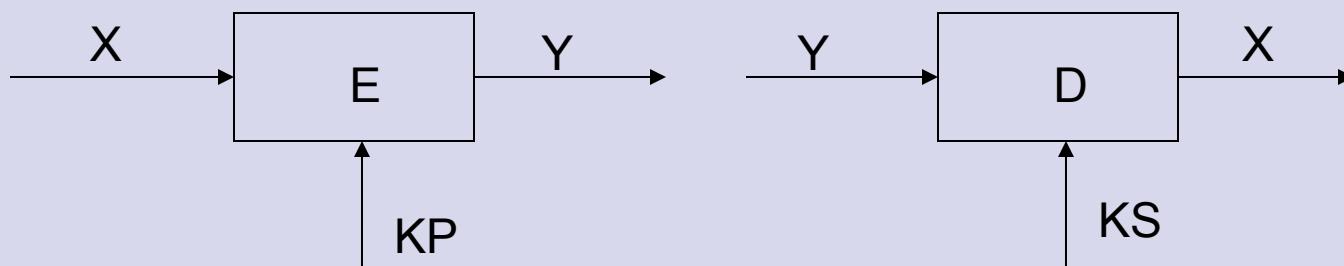
# Asymetrické šifrování

- Princip

- Existují dva klíče
  - P – public (veřejný)
  - S – secret (tajný)

$Y = E_{KP}(X)$  - šifrování

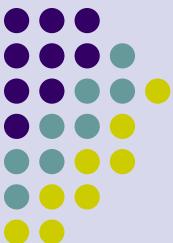
$X = D_{KS}(Y)$  - dešifrování





# Algoritmus RSA

- vytvořeno pány Rivest, Shamir a Adlemin v r. 1978
  - Velmi silná šifra
  - Podporuje proměnnou délku klíčů
  - Délka klíče 1024 bitů, 2048 bitů
  - Delší klíče zajišťují větší bezpečnost
- Algoritmus založen na počítání s velkými prvočísly
  - $p, q \dots$  velká prvočísla               $N = p \cdot q$
  - $\phi(N) = (p-1) \cdot (q-1)$
  - $\text{NSD}[P, \phi(N)] = 1; P \cdot S = 1 \pmod{\phi(N)}$
- šifrování                                       $C = M^P \pmod{N}$
- dešifrování                                       $M = C^S \pmod{N}$ 
  - $P \dots$  public key,  $S \dots$  secret key
  - předává se  $P, N$  a utají  $S$
  - výpočet  $P, S, N$  musí být jednoduchý



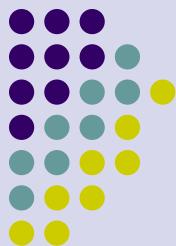
# Asymetrické šifrování

- Další algoritmy
  - Elgamal (Taher Gamal)
  - DSA (Digital Signature Algorithm)
  - Eliptické křivky
- Základní použití
  - Šifrování
  - Výměna klíčů
  - Digitální podpis



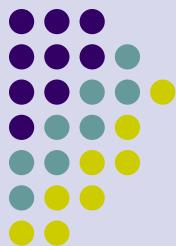
# Použití asymetrického šifrování

- **šifrování zpráv**
  - časově náročné, není vhodné
- **šifrování relačního klíče**
  - asymetrické šifrování se použije pro šifrování relačního (tajného) klíče
  - relační klíč se použije k šifrování (symetrické) vlastní zprávy,
- **ověření integrity dat**
  - ke zprávě se pomocí hashovací funkce vygeneruje otisk, který se zašifruje tajným klíčem odesílatele
  - je schopen provézt pouze majitel tajného klíče
  - ověření pravosti veřejným klíčem
- **Nepopratelnost**
  - informace zašifrovaná tajným klíčem
  - Ověření veřejným klíčem



# Hashovací funkce

- Jednosměrná funkce
  - Jednoduchý výpočet  $h = f(m)$
  - Výpočetně složité nebo nemožné  $m = f^{-1}(h)$
  - Platí pokud  $h_1 \neq h_2 \Rightarrow m_1 \neq m_2$   
pokud  $m_1 = m_2 \Rightarrow h_1 = h_2$   
ale existuje  $m_1 \neq m_2$  a  $h_1 = h_2$
- Algoritmy
  - SHA (Secure Hash Algorithm)
  - MD5 (Message Digest)



# Ověřování

- Autentikace je technika, pomocí které se ověřuje, že komunikující partner je ten, za kterého se vydává a ne podvodník.
- Existují tři způsoby autentikace
  - Řekni něco co víš (heslo)
  - Ukaž něco co máš (identifikační karta)
  - Nech systému něco tvého změřit (otisk prstu)



# Ověřování

- **Ověřovací schémata**

- musí obsahovat aspoň jedno tajemství
- musí být schopna rozpoznat jeho správné použití

- **Ověřovací metody**

- jednoduché (založeny na heslech)
- přísné (založeny na šifrovacích metodách)

- **Jednoduché ověřování**

- identifikace jménem a heslem,
- přenos otevřeného textu, použití ověřovacího serveru



# Ověřování

- **Přísné metody**

- elementární metody – použití symetrických a nesymetrických kódů
- metody založené na ověřovacích serverech
- metody založené na protokolech s minimální znalostí
  - uživatel dokazuje svoji identitu odpovídáním na šifrované otázky serveru

M1: {R, ID}

M2: {C}<sub>K</sub>

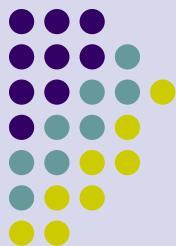
M3: {f(C)}<sub>K</sub>

R ... požadavek,

K ... tajný klíč,

C ... náhodné číslo,

f(C) ... domluvená funkce



# Ověřovací servery

- slouží k ověření „pravosti“ uživatele
- Používá symetrické šifrování
- lepší utajení klíčů
- používá se KDC (Key Distribution Center) – databáze klíčů (je tajná a indexována podle jmen uživatelů)
- Příklad – ověřování pomocí Kerberos serveru



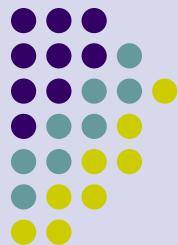
# Distribuce veřejného klíče

- Veřejný klíč je možné šířit v otevřené podobě
- Existuje nebezpečí podvržení veřejného klíče
  - Útok typu Man in the Middle
- Problém bezpečné distribuce veřejného klíče řeší certifikáty
- Problém vydávání, ověřování a zneplatnění certifikátu řeší certifikační autority



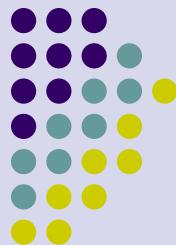
# Certifikát

- Certifikát je blok dat (soubor), obsahující
  - Verze (V3)
  - Sériové číslo (02 1c 6a)
  - Algoritmus podpisu (md5RSA)
  - Vystavitel (CN = CA GE Capital Bank, OU = Direct Banking, O = GE Capital Bank, a.s., C = CZ)
  - Platnost od (28. dubna 2003 12:31:30)
  - Platnost do (27. dubna 2005 12:31:30)
  - Předmět (E = [ledvina@kiv.zcu.cz](mailto:ledvina@kiv.zcu.cz), CN = uid: 120295, CN = Ing. Jiri Ledvina, ... adresa)
  - Veřejný klíč (30 81 87 02 81 81 00 bf 4a ... )



# Certifikát

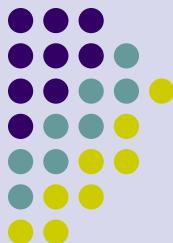
- Pokračování
  - Distribuční místo (URL=[http://www.gecb.cz/ca\\_ge.crl](http://www.gecb.cz/ca_ge.crl))
  - Použití klíče (Digitální podpis, Zakódování klíče)
  - Algoritmus miniatury (sha1)
  - Miniatura (72 19 13 5c 6a 9b 4e ab 30 cf 6b 6f 49 df 15 c0 62 94 79 09)
  - Popisný název (Ing. Jiri Ledvina)
- Certifikát musí být nezpochybnitelný – zneplatnění certifikátu
- Existují různé formáty certifikátů
  - Personal Information Exchange (PEX), PKCS #12 (P12) (Public Key Cryptography Standard)
  - Cryptographic Message Syntax Standard PKCS#7 (P7B)
- PGP certifikáty



# Ověřování certifikátů

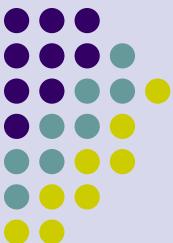
- přímé ověřování (nejjednodušší model)
  - Ověřování certifikátů mezi důvěryhodnými subjekty
  - V prohlížečích jsou certifikáty uznávaných autorit instalovány – můžeme (musíme) jim věřit. Existují ale i další certifikační autority, které nejsou uznávané – prohlížeč se na důvěryhodnost ptá.
- hierarchické ověřování – zřetězení certifikátů
  - Certifikačních autorit je hodně – získání certifikátu může být otázkou osobní návštěvy (důvěryhodné získání certifikátu).
  - Certifikační autority mohou vytvářet hierarchický strom – důvěryhodnost CA nižší úrovně je potvrzována CA vyšší úrovně. CA nejvyšší úrovně potvrzuje důvěryhodnost sebe sama.
  - Zřetězení CA je součástí certifikátu.
- kumulativní model – zahrnuje předchozí (přímé, zřetězené)

# Protokoly pro bezpečnou komunikaci



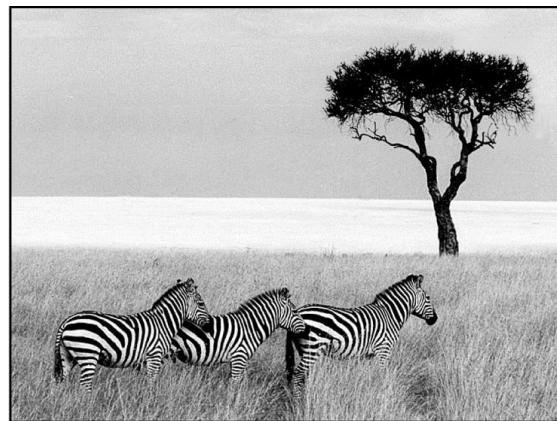
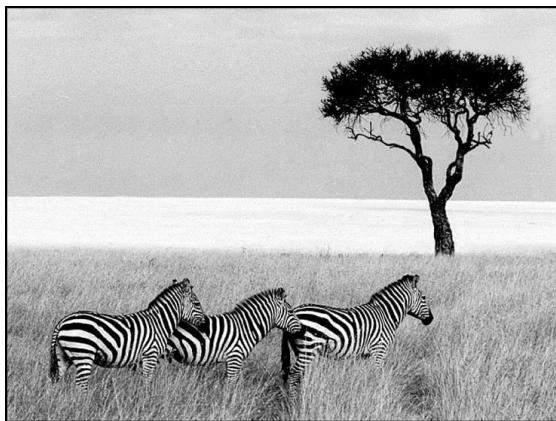
## Kerberos – ověřování v systému Orion na ZČU

- Používá symetrické šifrování
- Vychází z centralizované databáze uživatelů (každý uživatel musí být registrován)
- Základní část je ověřovací server (Kerberos)
- Po přihlášení (ověření) dostane uživatel lístek, obsahující práva přístupu k požadovanému serveru.
- K dalšímu ověřování uživatele se používá pověřovací listiny (credentials), obsahující jméno uživatele a adresu jeho počítače.



# Steganography

## Steganography



- (a) Three zebras and a tree. (b) Three zebras, a tree, and the complete text of five plays by William Shakespeare.

# Protokoly pro bezpečnou komunikaci



## SSL – Secure Socket Layer

- Vyvinuto fy. Netscape, používá se zejména pro bezpečné přenosy mezi prohlížečem a webovým serverem.
- K ověřování serveru se používají certifikáty serveru. Uživatel není ověřován.
- Po ověření se veřejný klíč použije pro vygenerování relačního klíče, sloužícího k šifrování komunikace.
- Schéma bezpečného HTTP se označuje HTTPS
- SSL se používá i u dalších protokolů (POP, IMAP)
- Je možné je využít univerzálně – vytváří mezivrstvu mezi protokolem TCP a aplikací – před použitím je třeba aplikaci (program) modifikovat.
- Obdobou SSL je TLS (Transport Level Security)

# Protokoly pro bezpečnou komunikaci



## SSH – Secure Shell

- Používá se pro vytvoření šifrovaného kanálu mezi aplikacemi (aplikační úroveň).
- Pro šifrování používá opět relační klíč, vytvořený na základě výměny informací (Diffie - Hellman algoritmus pro výměnu klíčů) nebo na základě asymetrické kryptografie – RSA.
- Využívá se pro
- bezpečný vzdálený přístup – náhrada Telnetu (ssh – secure shell),
- bezpečný přenos souborů – náhrada ftp (scp – secure copy),
- vytvoření bezpečného kanálu mezi libovolnými aplikacemi.

# Protokoly pro bezpečnou komunikaci



## IPsec

- Soubor protokolů pro zajištění bezpečnosti na síťové úrovni
  - Ověřování původu
  - Integrita dat
  - Utajení dat
- Vzhledem k transportním protokolům a aplikacím je transparentní – nevidí ho
- Vzhledem k linkovému protokolu neprůhledný – nerozumí přenášeným datům
- Přizpůsobivý

## Režimy činnosti

- Transparentní – mezi koncovými uživateli
- Tunelovaní – mezi dvěma síťovými prvky (směrovači, obrannými valy, ... )
- Kombinace předcích – mezi koncovým uživatelem a síťovým prvkem



# Zabezpečení elektronické pošty

## PEM (Privacy Enhancement for Internet Electronic Mail)

- Dnes historický protokol pro vytváření a zpracování bezpečných zpráv.
- Vznikl v druhé polovině 80. let.
- Původní specifikace RFC989, poslední specifikace RFC1421 až RFC1424 (1993).
- V praxi nedošlo k jeho masovému využití nejširší veřejnosti - nebyl totiž běžně dostupný software, který by jej podporoval.
- Na přelomu 80. a 90. let nebyla ještě masová poptávka po software tohoto druhu.
- Stal základem pro novější protokoly (S/MIME)



# Zabezpečení elektronické pošty

## S/MIME

- Podobné PEM
- Kontrolní součet (otisk) SHA-1 a MD5
- Asymetrické šifrování (šifrování symetrických šifrovacích klíčů a elektronický podpis): RSA s délkou klíče minimálně 512 bitů.
- Symetrické šifrování - šifrování textu zprávy (DES-CBC, triple DES).
- Norma PKCS-7 pro tvorbu bezpečných zpráv - elektronický podpis, šifrování, obojí.
- Definuje MIME hlavičku Content Type: Application/pkcs7-mime



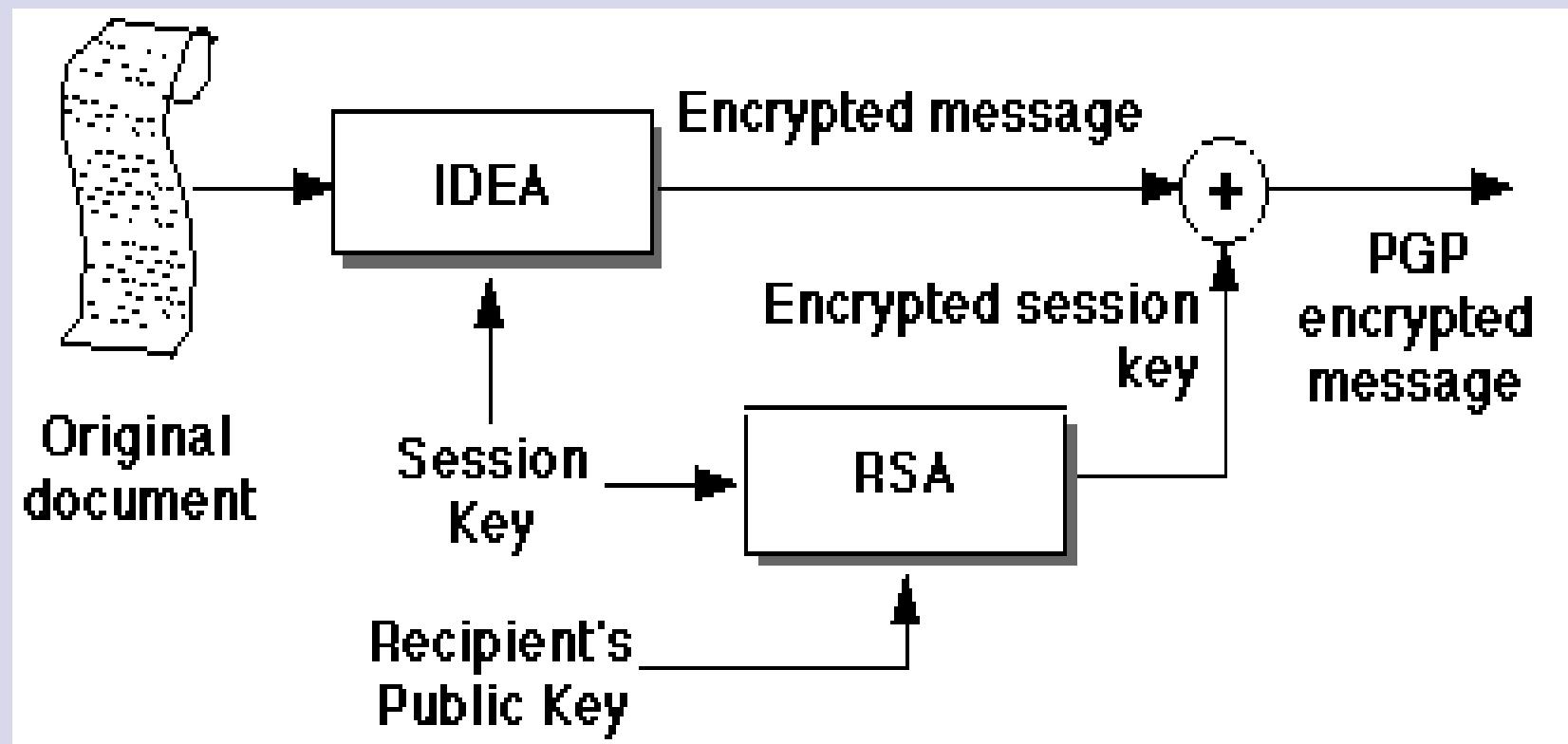
# Zabezpečení elektronické pošty

## PGP (Pretty Good Privacy)

- Uživatelsky jednoduchý program dostupný nejširší veřejnosti.
- PGP je nejrozšířenější prostředek pro zpracování bezpečných zpráv (RFC1991).
- Vytvořil Američan P.R.Zimmerman (1991).
- Bezpečný přenos zpráv pomocí SMTP, POP, IMAP (nepotřebuje nový protokol, nadstavba nad stávajícími).
- Asymetrické šifrování - RSA (šifrování symetrického relačního klíče pro šifrování vlastní zprávy).
- Symetrické šifrování algoritmus - IDEA.
- Komprese dat před šifrováním - PKZIP.
- Výpočet kontrolního součtu (otisku) - MD5.
- Převod binárních dat na ASCII - Radix-64.

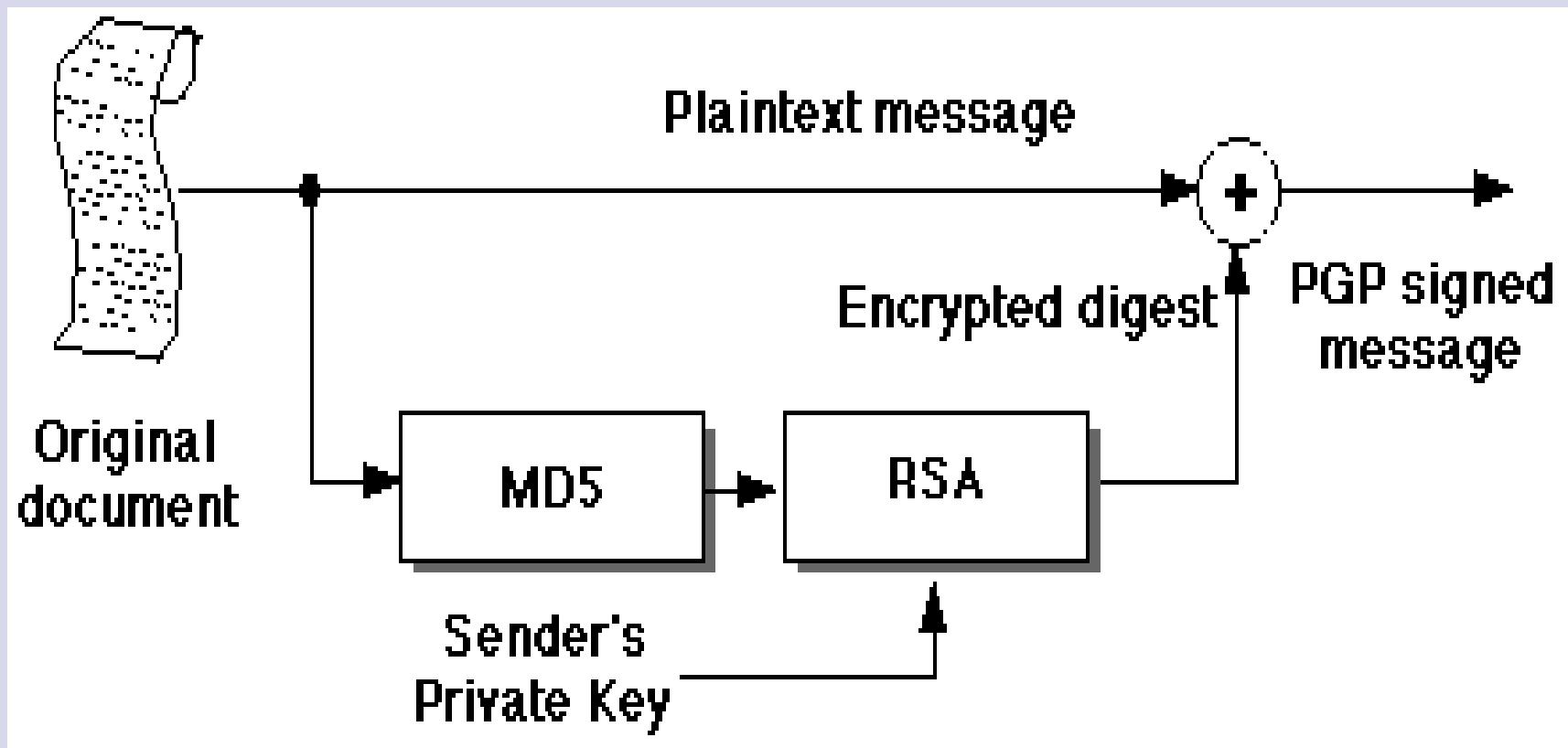


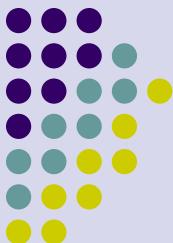
# Zabezpečení elektronické pošty





# Zabezpečení elektronické pošty





# Obranné valy

- Provádí ochranu sítě před napadením (ochrana počítačů nestačí)
- Odděluje uživatele (prvek nespolehlivosti) od prvků ochrany

## Vlastnosti

- Filtrování paketů a vlastnost odstínění
- Různé úrovně ověřování
- Přihlašování (registrace) a účtování
- Transparentnost a přizpůsobení uživatelům
- Ovladatelnost (management)
- Rozlišení požadavků dle klientů nebo sítí



# Typy obranných valů

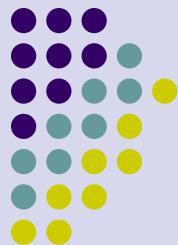
- **Filtrující směrovač (Screening Router)**
  - Provádí filtraci paketů podle směru přenosu, IP adresy a čísla portu
- **Opevněný počítač (Bastion Host )**
  - Používá se při realizaci důležitých serverů, které mají být navíc velmi bezpečné. Např. SMTP, FTP, DNS, HTTP, atd.
- **Brána se dvěma vstupy (Dual Homed Gateway)**
  - Úplně odděluje vnitřní a vnější síť. Služby musí být umístěny na této bráně, přístupné jak z vnitřní sítě, tak i z vnější sítě.
- **Screened Host Gateway**
  - Vnitřní síť je chráněna filtrujícím směrovačem, který propouští pouze pakety určené pro vybraný počítač (Bastion Host).
- **Screened Subnet**
  - Pomocí dvou filtrujících směrovačů se vytvoří demilitarizovaná zóna.
- **Brána aplikacní úrovni**



# Útoky

## Útoky Denial of Service

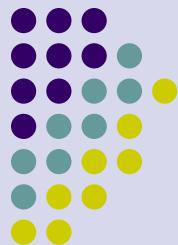
- Jeden z mnoha základních forem útoků na vnitřní síť
  - Založen na přetížení systému
  - Výsledkem je omezení výkonnosti serveru nebo úplný výpadek cílového systému
- Útok může být zaměřen na síťové komponenty nebo na hostitelské systémy
- Dochází k vytěsňování reálných přenosů
  - Klienti na základě detekce zahlcení zpomalují vysílání
  - Směrovače musí přebytečné pakety odstraňovat



# Útoky

## Usnadnění DoS útoků

- V počítačové síti běží mnoho systémů
- Počítačová síť je velmi rozlehlá
- Mnozí uživatelé jsou naivní – dávají šanci uchvatit vzdálený systém
- Protokoly internetu jsou známé, to vytváří podmínky pro využití jejich slabin
- Mnoho volného software, ve kterém mohou být zahrnuty utajené funkce
- Nedostatečná ochranná politika používání a managementu
- Velmi rozsáhlý software s mnoha známými děrami
- Nedostatek prostředků pro zastavení útoků

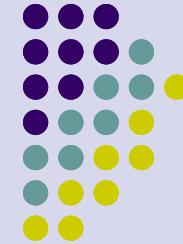


# Útoky

## Snort (Open Source Intrusion Detection System)

- Systém pro detekci útoků (Intrusion Detection Systém)
- Je schopen provádět analýzu toku dat v reálném čase a logování paketů v IP sítích
- Může provádět analýzu protokolů, vyhledávání údajů
- Je schopen detektovat různé útoky a sondování
- Používá jazyk pro popis toku dat
- Obsahuje automat pro detekci podle tohoto popisu
- Umožňuje informovat o útoku v reálném čase (syslog, soubor, sockety, ... )

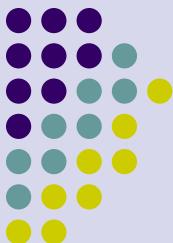
# Prostředky pro řízení počítačových sítí



Úvod do počítačových sítí

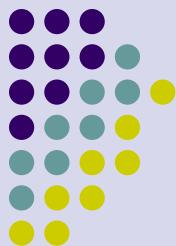
Lekce 13

Ing. Jiří Ledvina, CSc.



# Network Management System

- ISO Network Management Forum
  - Fault Management
  - Configuration Management
  - Security Management
  - Performance Management
  - Accounting Management
- Fault Management
  - proces lokalizace problémů nebo chyb počítačové sítě
    - odhalení problému
    - isolování problému
    - odstranění problému
  - rychlé odhalení problému a náprava



# Network Management System

## • Configuration Management

- prostředí sítě je řízeno konfiguracemi všech zařízení v ní
- konfigurace je chápána jako proces
  - natavení konfigurací těchto zařízení
  - čtení konfigurací těchto zařízení
  - modifikace konfigurace těchto zařízení

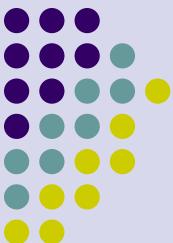
## • Security Management

- proces pro řízení přístupu k informacím v síti
- pomoc při údržbě zabezpečení této informace
- sledování neúspěšných pokusů přihlašování
- automatické sledování a varování



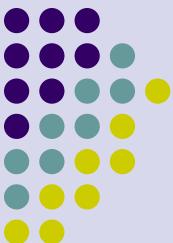
# Network Management System

- Performance Management
  - měření využití hardware, software a médií v síti
  - měřené aktivity
    - celková propustnost
    - procento využití
    - četnost chyb
    - časy odezvy
  - snaha odhalit problémy dříve, než na ně přijde uživatel
- Accounting Management
  - sledování jednotlivců a skupin jak využívají síťové zdroje
  - zabránění monopolizace přístupu ke zdrojům



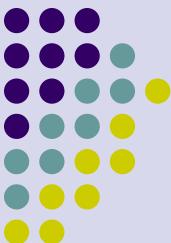
# Ad - hoc techniky řízení sítí

- ICMP (Internet Control Message Protocol)
  - Echo, Echo reply, Timestamps
- Ping (Packet Internet Groper)
  - využívá ICMP Echo request + reply
- Traceroute
  - využívá datových paketů (UDP)+ICMP odpovědi, Doba života paketu, nedosažitelný port
- Pasivní řízení
  - zachycování paketů
  - analýza paketů

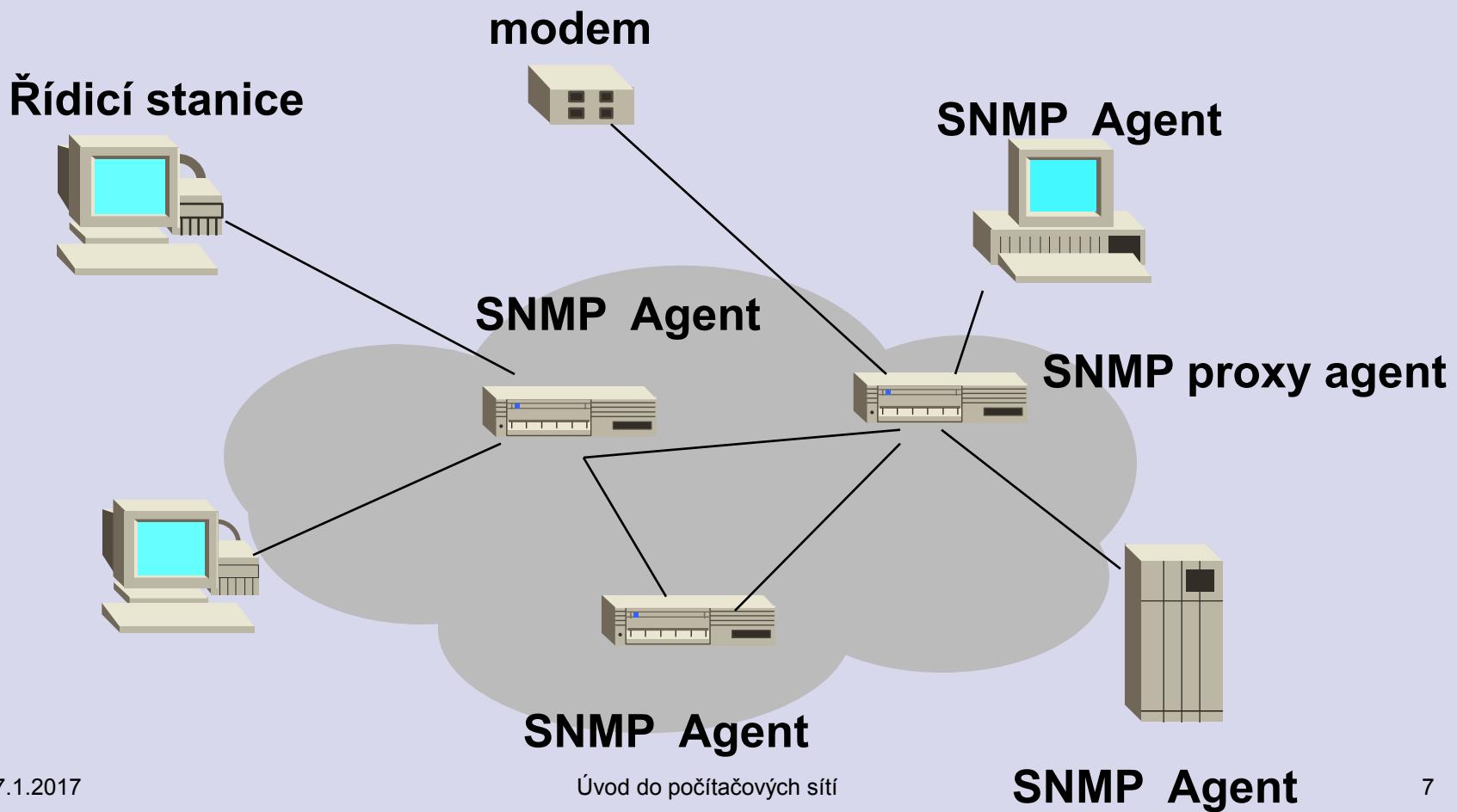


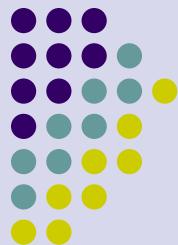
# Model SNMP

- Řízené uzly - agenti
  - hostitelské systémy
  - směrovače, mosty, multiplexory, hub
- Řídicí stanice
  - protokol pro řízení sítě
  - aplikace pro řízení sítě
- Komunikační protokol
  - čtení, zápis
  - procházení seznamem proměnných
  - asynchronní události (trap)
- Proxy agenti



# Uspořádání sítě





# Network Management System

- Přehled protokolů pro monitorování
  - SGMP - Simple Gateway Management Protocol
  - HEMS - High Entity Management System
  - CMIP - Common Management Information Protocol
  - CMOT - CMIP over TCP/IP
  - SNMP - Simple Network Management Protocol
  - SNMPv2
- Data
  - MIB - Management Information Base
  - MIB - 2
  - RMON - Remote Monitoring
  - RMON - 2

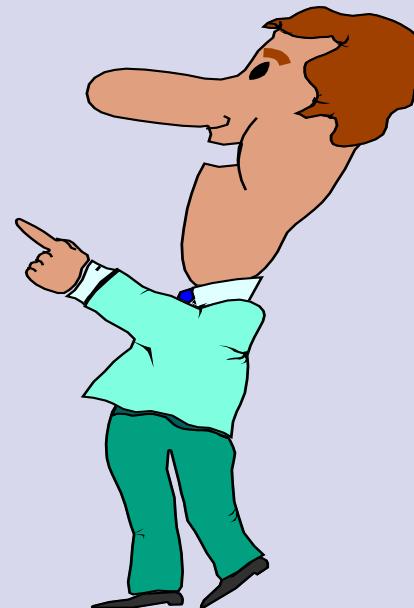


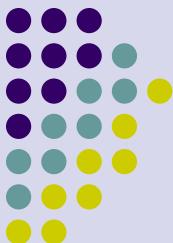
# Reprezentace dat

*Interní reprezentace dat*

*Externí reprezentace dat - nezávislá na prostředí*

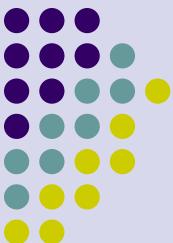
- ASN.1
  - definuje formát datových jednotek
  - definuje objekty které jsou ovládány
- Moduly
- Typy a hodnoty
  - jednoduché typy
  - konstruované typy
  - odvozené typy
  - subtypy
- Identifikatory objektů





# SMI a MIB

- MIB - Management Information Base
  - databáze řízených objektů
  - popsáno podmnožinou ASN.1
- SMI - Structure of Management Information
  - popis schemat databáze
  - popsáno podmnožinou ASN.1
  - standardní popis typů objektů

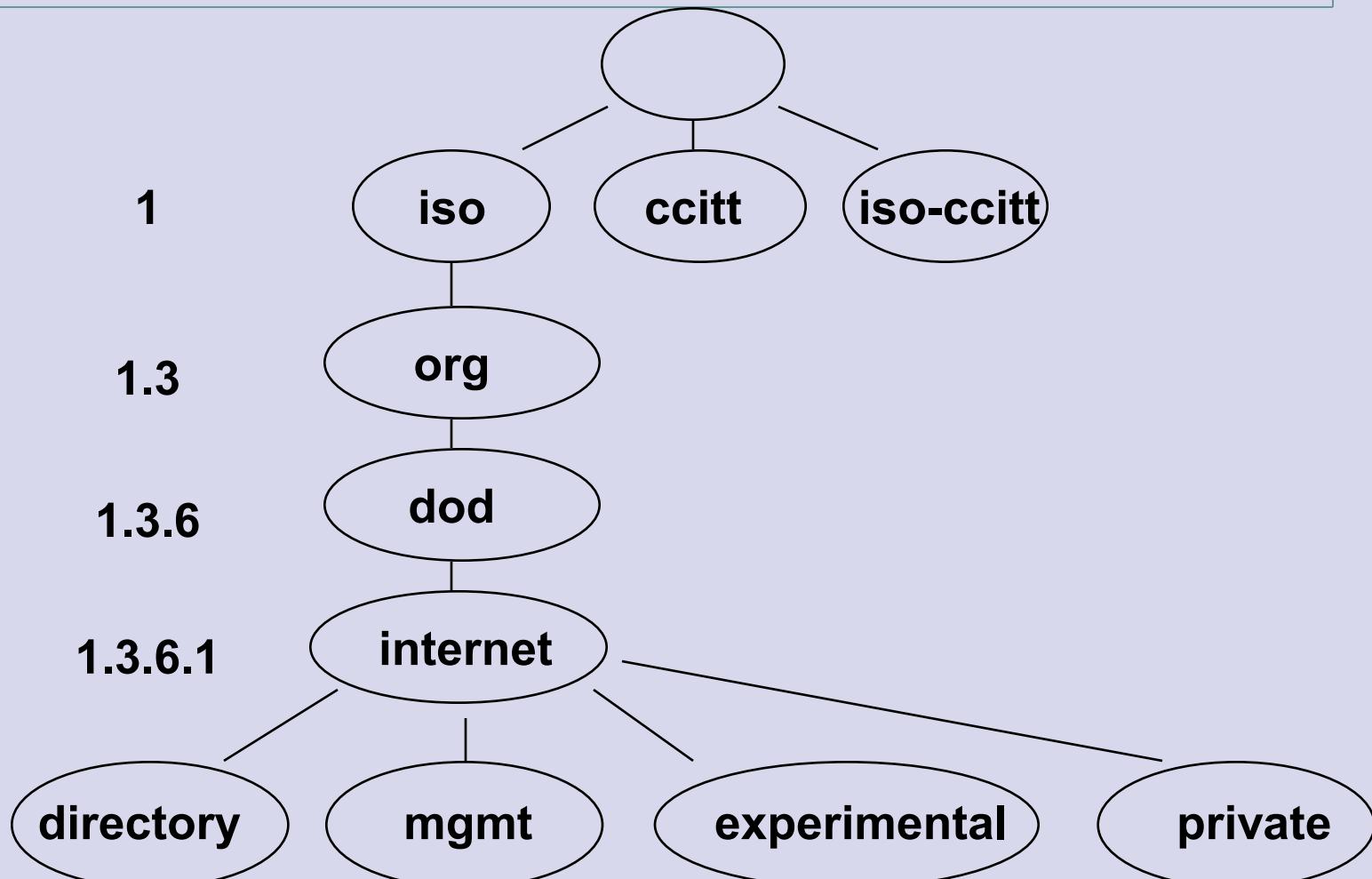


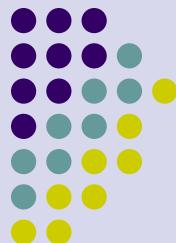
# Objekty

- Syntax - syntaxe objektu
- Access - úroveň přístupu k objektu
  - read-only
  - read-write
  - write-only
  - not-accessible
- Status - požadavky implementační
  - mandatory
  - optional
  - obsolete
- Name - identifikátor objektu



# Identifikátory objektů





# Identifikátory objektů - pokračování

## 1.3.6.1.2.1

1.3.6.1.2.1.1

system

1.3.6.1.2.1.2

interfaces

1.3.6.1.2.1.3

at

1.3.6.1.2.1.4

ip

1.3.6.1.2.1.5

icmp

1.3.6.1.2.1.6

tcp

1.3.6.1.2.1.7

udp

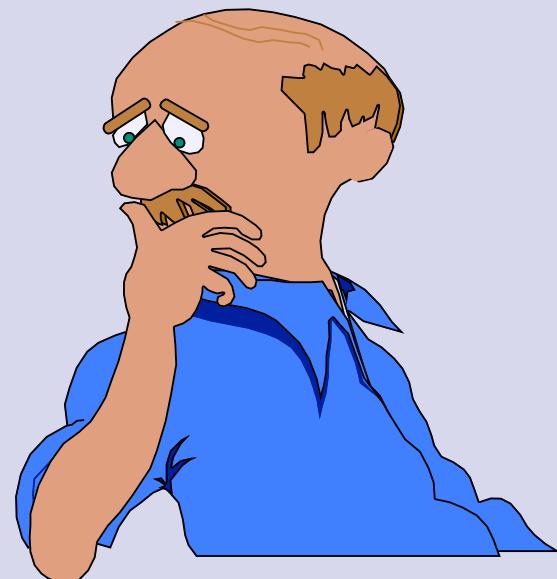
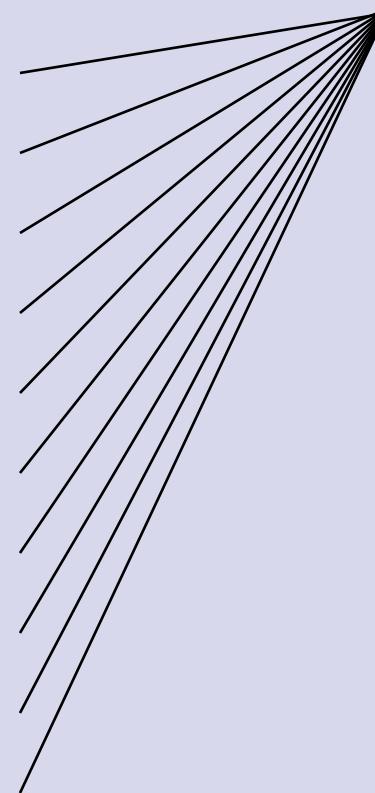
1.3.6.1.2.1.8

egp

1.3.6.1.2.1.9 transmission

snmp

mgmt





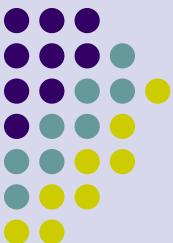
# MIB

## Základní skupiny MIB I

- system ( 1 )
- interfaces ( 2 )
- at ( 3 )
- ip ( 4 )
- icmp ( 5 )
- tcp ( 6 )
- udp ( 7 )
- egp ( 8 )

## Základní skupiny MIB II

- system ( 1 )
- interfaces ( 2 )
- at ( 3 )
- ip ( 4 )
- icmp ( 5 )
- tcp ( 6 )
- udp ( 7 )
- egp ( 8 )
- transmission ( 9 )
- snmp ( 10 )



# MIB - System ( sys )

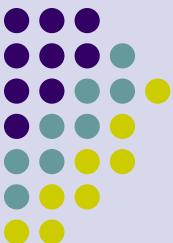
## skálarní objekty

- sysDescr
- sysObjectID
- sysUpTime
- sysContact
- sysName
- sysLocation
- sysServices



# Mechanizmus SNMP

- Filosofie
  - operace
    - get
    - get-next
    - set
    - trap
  - typy rámce
    - get-request
    - get-next-request
    - get-response
    - set-request
    - trap
- Protokol (UDP, port 161, 162)
  - formát rámce
    - version
    - community
    - data
  - “normální data”
    - PDU type
    - request-id
    - error-status
      - tooBig, noSuchName, badValue, readOnly, genErr
    - error-index
    - variable-bindings



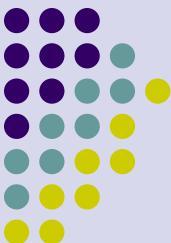
# Mechanizmus SNMP

- Asynchronní události (TRAP)
  - PDU type
  - enterprise -- system.sysObjectID
  - agent-addr -- síťová adresa agenta
  - generic-trap
    - coldStart
    - egpNeighborLoss
    - enterpriseSpecific
    - warmStart
    - linkDown
    - linkUp
    - authenticationFailure
    - egpNeighborLoss
    - enterpriseSpecific
  - specific-trap
- timeStamp
- variable-bindings



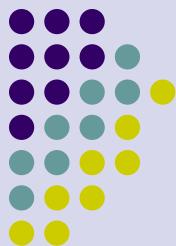
# Řídicí stanice - SNMP monitory

- periodické dotazování na stav agentů
- příjem a zpracování asynchronních událostí
  - automatická reakce na došlé alarmy
- kompletní vyhodnocení a prezentace
  - grafické uživatelské rozhraní
  - mapy sítě, jejich automatické vytvoření
  - seskupování zařízení do logických celků
  - grafická prezentace získaných dat
- doplňkové služby
  - telnet
  - ping
  - Trascend



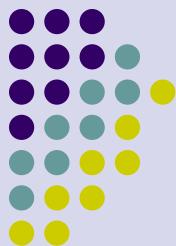
# Příklady monitorů

- Platformy
  - UNIX
  - DOS (Windows)
- Příklady
  - SunNet Manager (SUN, Solaris)
  - OpenView NNM (HP-UX, SUN)
  - NetView (IBM, AIX)
  - D-View (D-Link, MS-Windows)



# Zhodnocení

- jednoduchá autentikace
- zatěžování sítě při čtení rozsáhlých tabulek
- zatěžování sítě při periodickém monitorování
- postrádá přímou podporu pro distribuované řízení
- není kompatibilní s novější verzí SNMPv2
- zavedení RMON (Remote Monitoring)

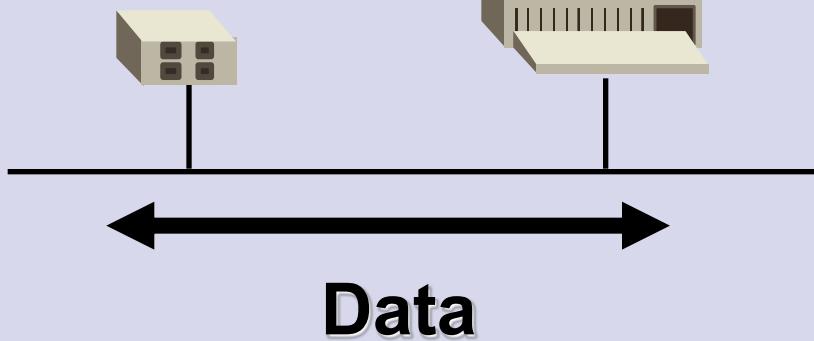


# Co je RMON?

Sonda RMON

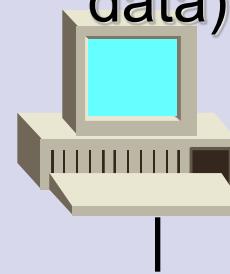
(Agent)

Promiskuitně sleduje data na síti LAN, ke které je připojena

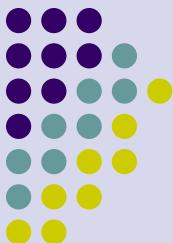


Uživatelské  
PC

Konsole pro řízení sítě  
(kontroluje a zobrazuje data)

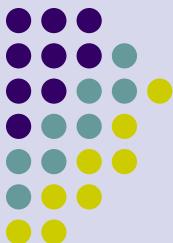


(Musí být připojena do sítě - i mimo pásmo, nebo na jiný segment sítě LAN, než na který je připojena sonda)



# RMON

- Autonomní ovládání sítě
- Sonda
  - Oznamuje výjimky (Alarms)
  - Naslouchá promiskuitně LAN
    - Statistiky hostitelských systémů (MAC adresy)
    - Historie pro analýzu trendů
    - Statistiky kdo s kým hovoří (pouze v MAC Adresách)
    - Zachycování paketů pro statistiku
- Konzole
- Dekódování informací



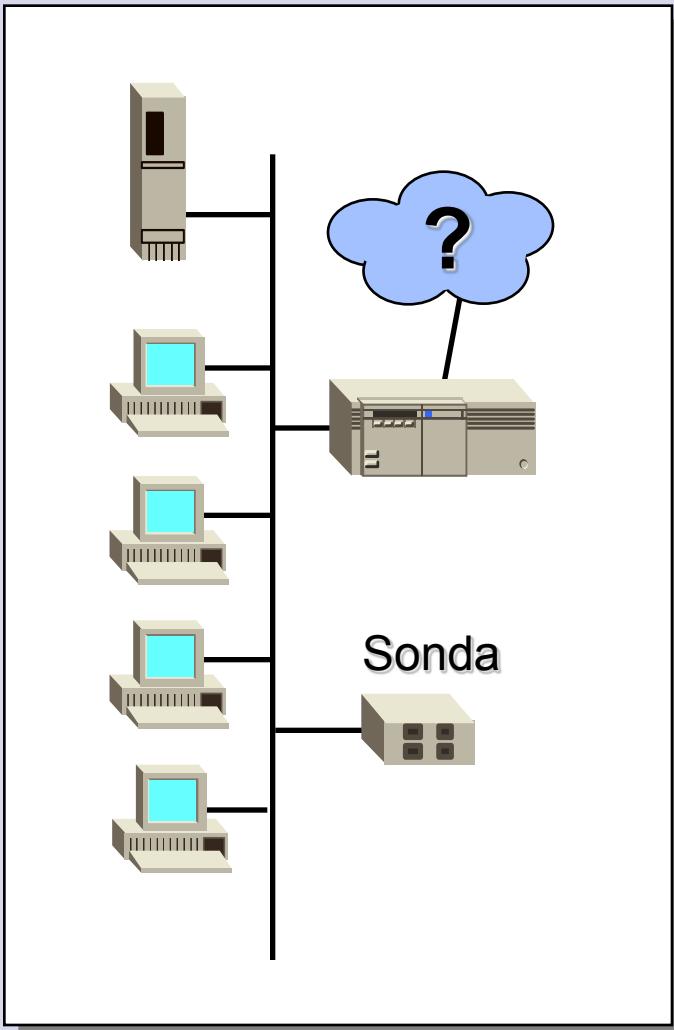
# Skupiny RMON

- Definováno IETF v RFC1271 jako standard pro vzdálené monitorování
- Původně definováno pouze 9 skupin, skupina statistiky definována pouze pro Ethernet
- Další skupiny pro ostatní média (např. Token Ring) jsou definovány v dalších RFC

- |  |  |
|--|--|
| <ul style="list-style-type: none"><li>• Historie</li><li>• Host. systémy</li><li>• Statistiky</li><li>• Alarmy</li><li>• Prvních N hostů</li></ul> | <ul style="list-style-type: none"><li>• Matice</li><li>• Události</li><li>• Filtr</li><li>• Zachycování</li><li>• Token Ring</li></ul> |
|--|--|



# Statistiky RMON

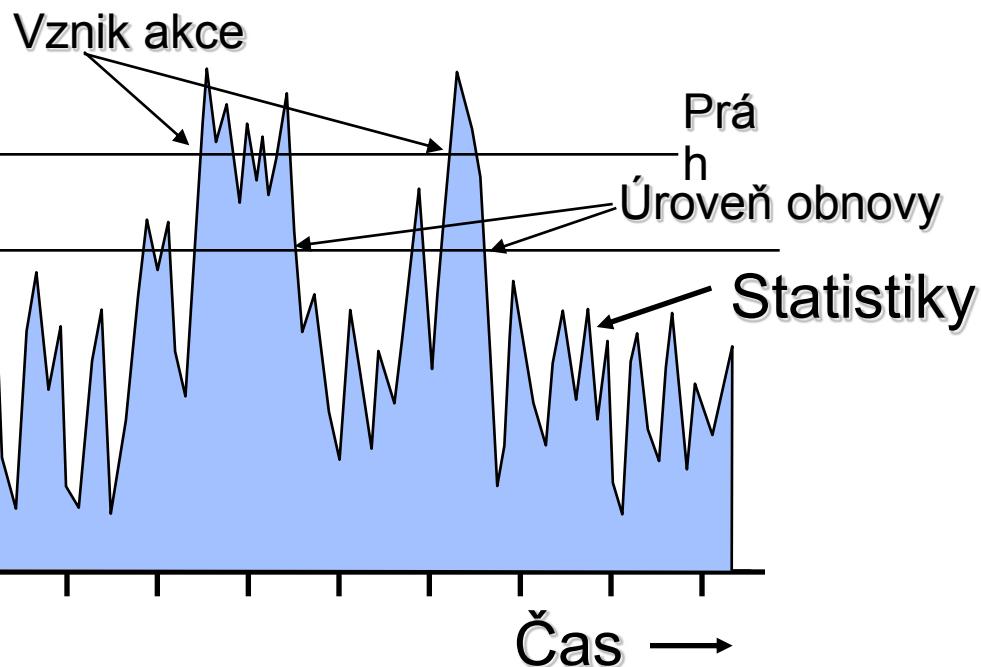


## Statistiky

- Ukazuje statistiky LAN segmentu
- Není vztázen k individuálním host. systémům
- Nepracuje přes mosty, přepínače (switch) a směrovače



# Alarmy RMON

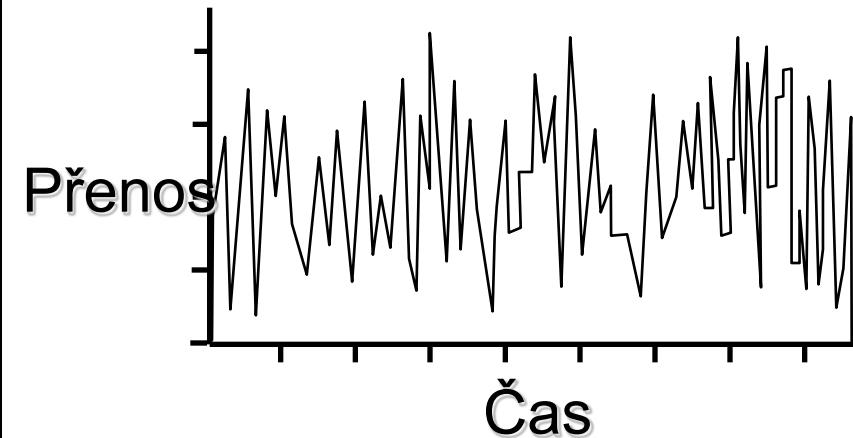
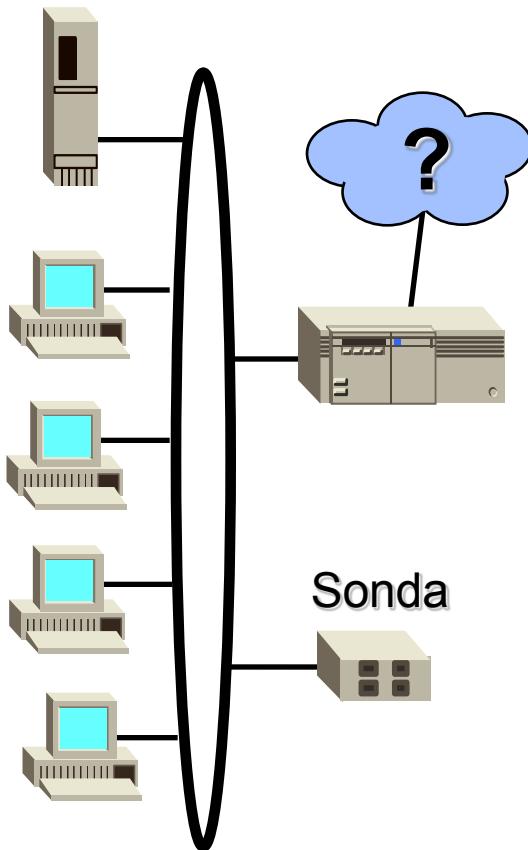


## Alarmy

- Sonda RMON monitoruje jakékoliv statistiky podle MIB. Je-li překročena prahová hodnota, vytvoří vnitřní RMON událost.
- Dokud hodnota neklesne pod úroveň obnovy, není spuštěna žádná další akce (action).

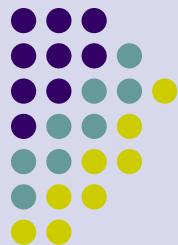


# RMON Historie

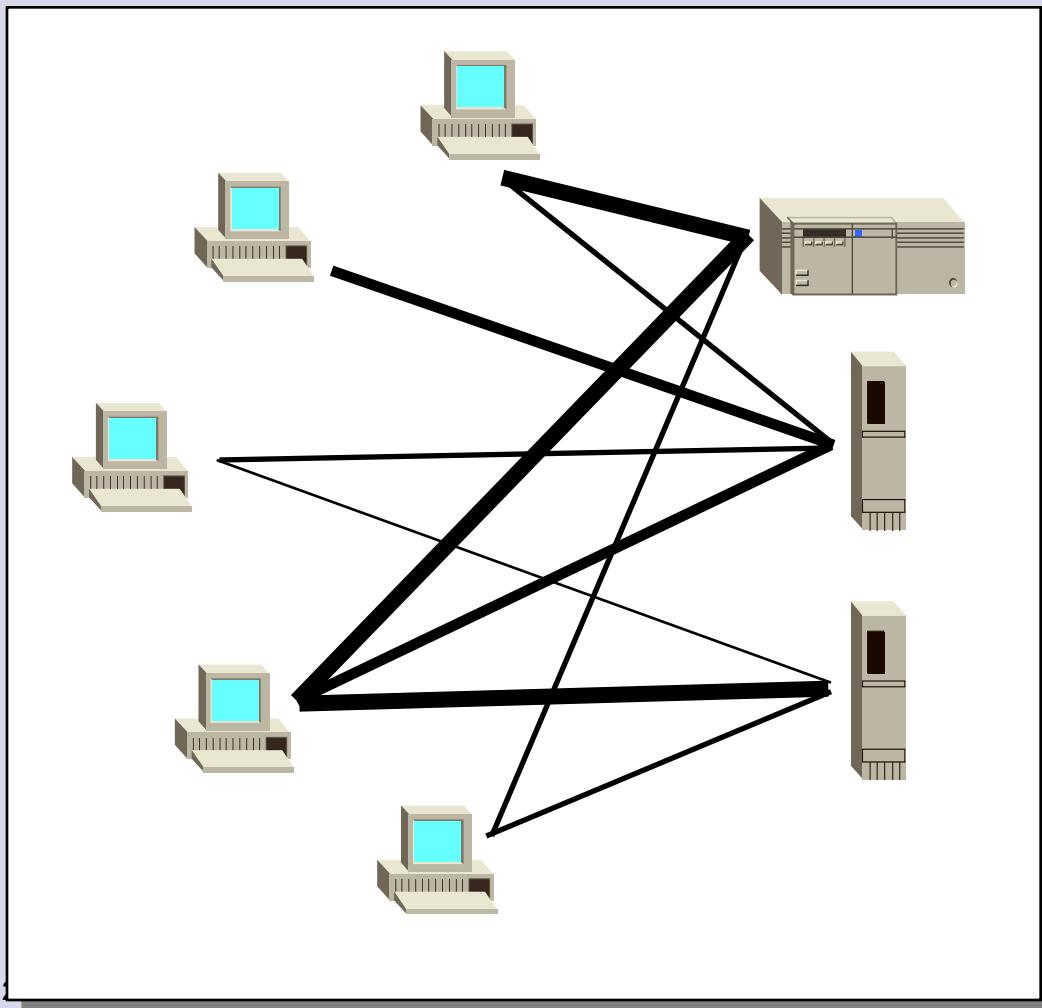


## Historie

- Zachycuje časové statistiky segmentu LAN
  - Není vztázena k individuálním host. systémům
- Nepracuje přes mosty, přepínače (switch) ani směrovače

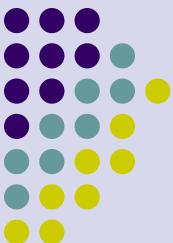


# Matice RMON

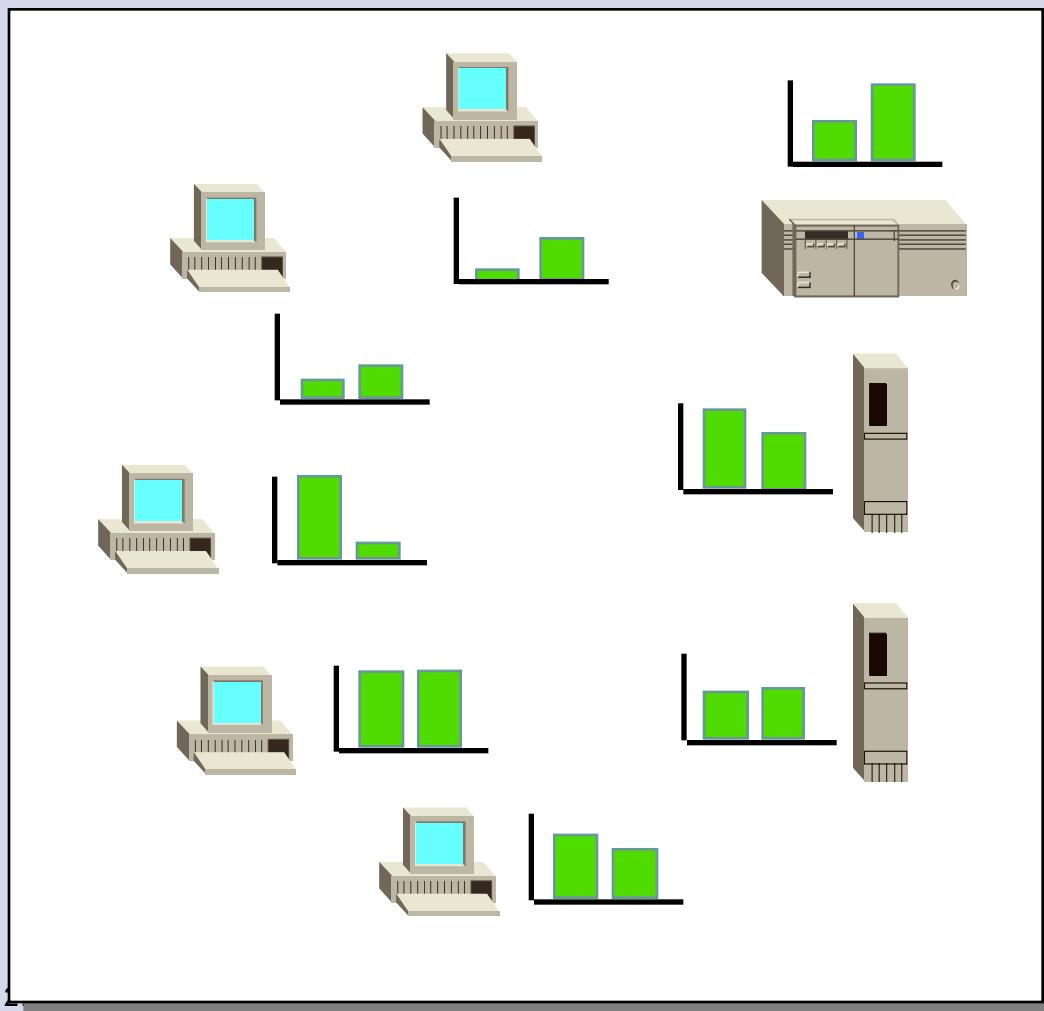


## Skupina matice

- 'Kdo s kým komunikuje'
  - Poskytuje statistiky vztažené k páru komunikujících **MAC adres** (nikoliv síťových adres)
  - MAC i síťové adresy jsou pro host. systém unikátní
  - MAC adresy nejsou mimo segment LAN zachovány (síťové adresy ano)



# RMON Host. systémy

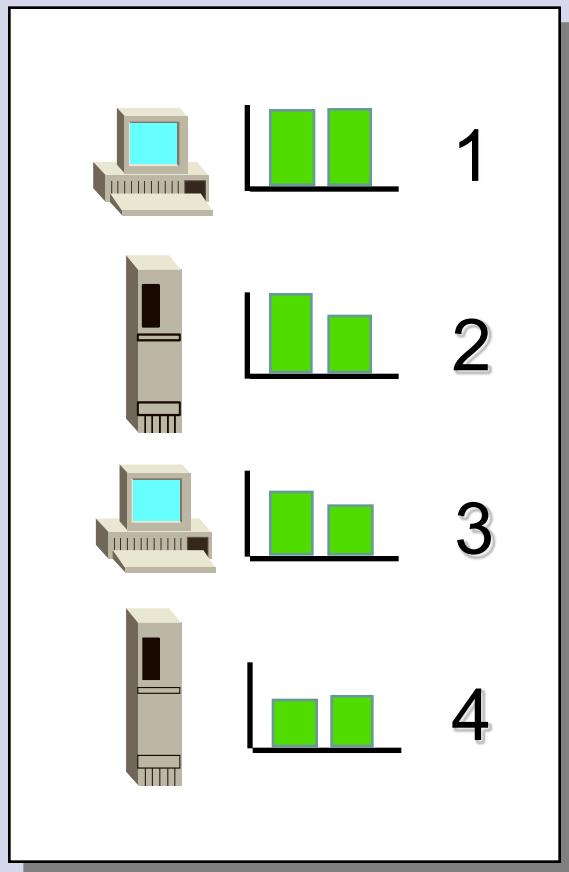


## Skupina host. systémů

- 'Kdo přenáší'
  - Poskytuje statistiky založené na MAC adresách (ne na síťových adresách)
  - MAC i síťové adresy jsou pro host. systém jedinečné
  - MAC adresy nejsou mimo segment LAN zachovány (síťové adresy ano)

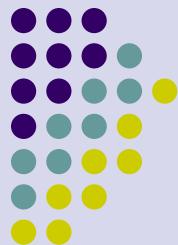


# RMON - Horních N (TopN Hosts)



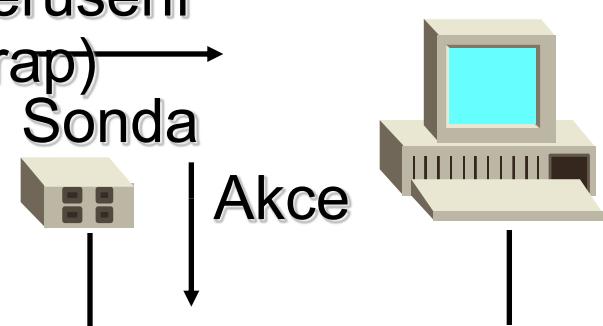
## Skupina horních N (TopN Host)

- ‘Kdo přenáší nejvíce’
  - Uspořádané statistiky založené na MAC adresách (ne na síťových adresách)
  - MAC a síťová adresa jsou pro host. systém jedinečné
  - MAC adresy nejsou mimo segment LAN zachovány (síťové adresy ano)



# RMON Události (Events)

Příchod události:  
Asynchronní  
přerušení  
(Trap) →  
Sonda

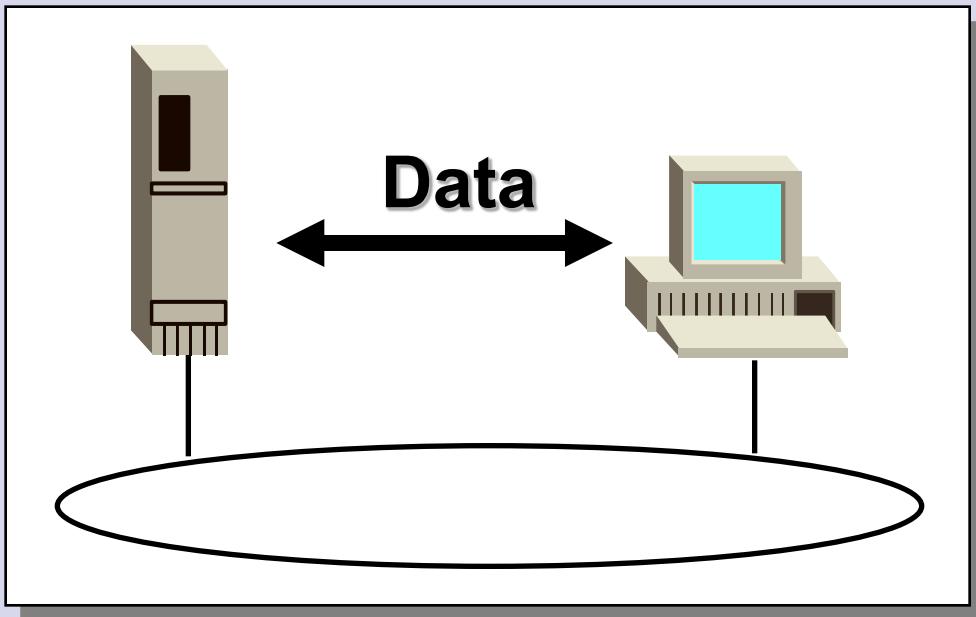


## Události

- Událost vznikne je-li překročen práh RMON alarmu. S každou událostí jsou spojeny akce jako je záznam do logu, poslání SNMP trapu a pod. Je možné vyvolat i další akce, které nejsou definovány ve standardu RFC1271.
- Definované akce jsou záznam do interního logu a poslání SNMP trapu do konsole síťového manageru.



# RMON Filtr

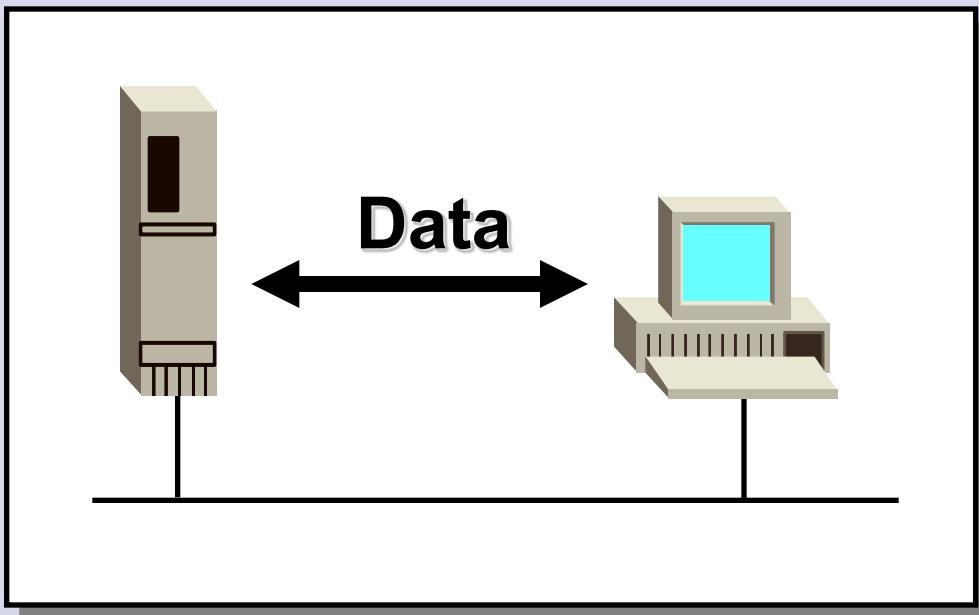


## Filtr

- Podle parametrů v paketu (např. aplikace, protokol, adresa), dovoluje nastavit podmínky, které zajistí bud' monitorování, nebo záznam paketů.

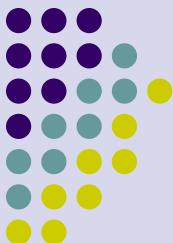


# RMON Zachycování paketů



## Zachycování paketů

- Podle parametrů, definovaných ve skupině filtrů (Filter Group), zachycuje v sondě pakety.
- Zachycování paketů je použitelné zvláště při odhalování chyb



# Skupiny RMON 2

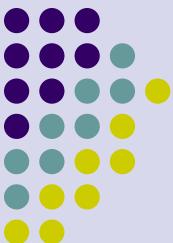
- RFC 2021 - RMON2 MIB
- RFC1997 - RMON2 MIB Protocol Identifiers

- Skupiny:**
- Adresář protokolů
  - Distribuce protokolů
  - Mapa adres
  - Host systémy síťové úrovně
  - Matice hostů síťové úrovně
  - Host systémy aplikační úrovně
  - Matice hostů aplikační úrovně
  - Historie
  - Konfigurace sondy

# Protokol IP verze 6

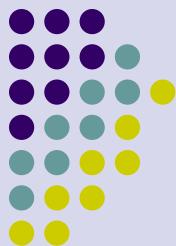


Úvod do počítačových sítí  
Ing. Jiří Ledvina, CSc.



# Co je to IPv6

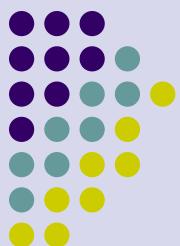
- Architektura adres
- Plug and Play
- Systém jmenných domén
- Přechod IPv4 na IPv6



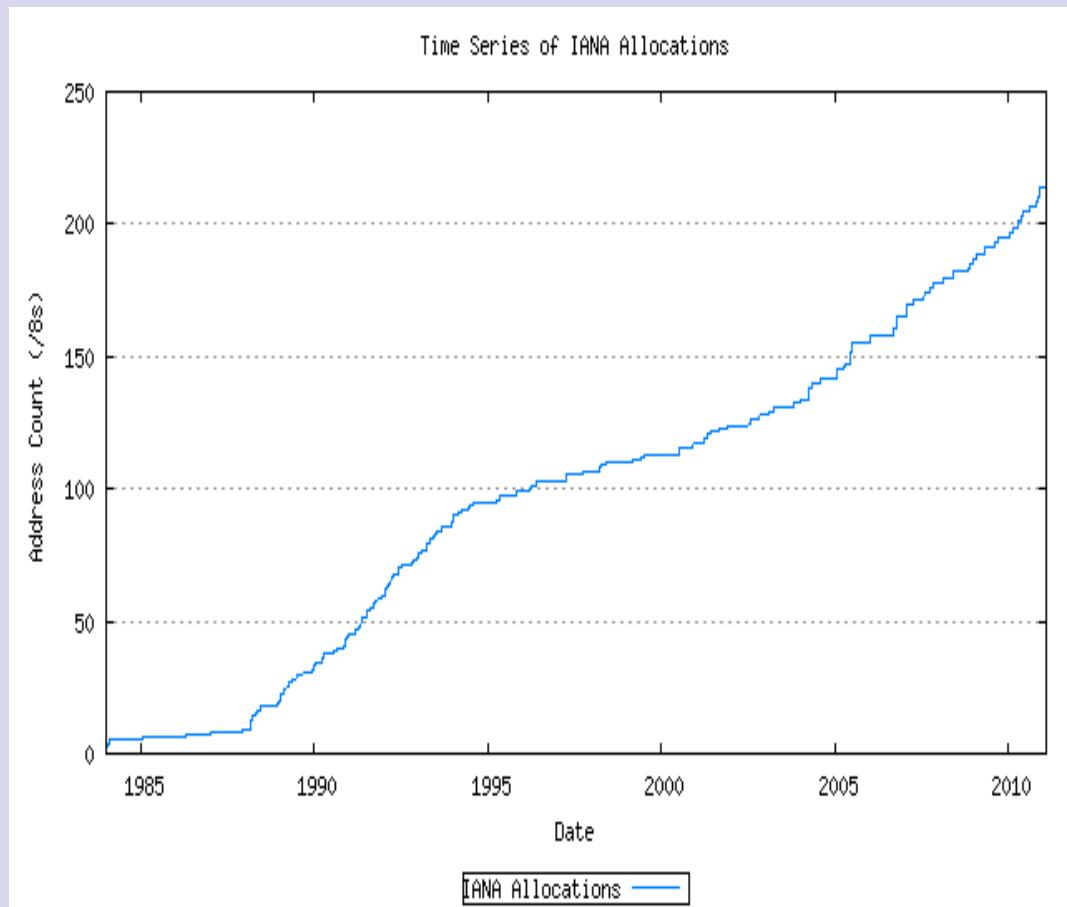
# Problémy IPv4

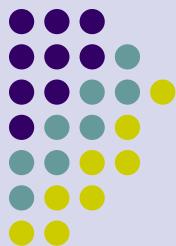
- Vyčerpání IPv4 adres
- 4 slabiky = 4,3 miliard adres (4,294,967,296)
- 16 slabik =  
340,282,366,920,938,463,463,374,607,431,768,211,456
- Méně než je populace lidí (6,1 miliard)
- Vyčerpá se již okolo roku 2008
- K registraci IPv4 adres se používá několik politik
- Lepší situace je v USA, špatná v jihovýchodní Asii (Čína)
- Nikdo neobdrží dost IPv4 adres

# Vyčerpání adresového prostoru IPv4



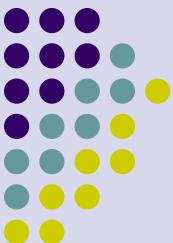
- Spravuje IANA (Internet Assigned Numbers Authority)
- Regionální registrátoři
  - \* ARIN (American registry for Internet Numbers)
  - \* APNIC (Asia Pacific)
  - \* AfriNIC (African Internet Community)
  - \* LACNIC (Latin American and Caribbean Internet Address Registry)
  - \* RIPE (Réseaux IP Européen)





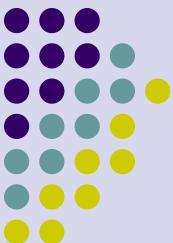
# Nárůst směrovací informace

- Směrovací informace nemůže být efektivně agregována
- Adresy jsou přidělovány neagregovatelným způsobem
- V současné době 80,000 položek
- Nákladné pro páteřní směrovače
- Nestabilita, poruchy



# Nedostatek adres

- Rozšíření NAT
- Narušení architektury Internetu
- Izolování uživatelů



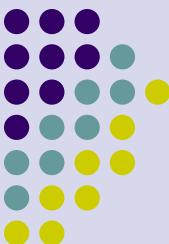
# Historie IPv6

- Co se stalo s IPv5
  - Verze 5 v IP záhlaví byla přiřazena protokolu ST (Internet Streaming protocol)
  - Experimentální protokol (RFC1819)
  - Nenalezl širší využití

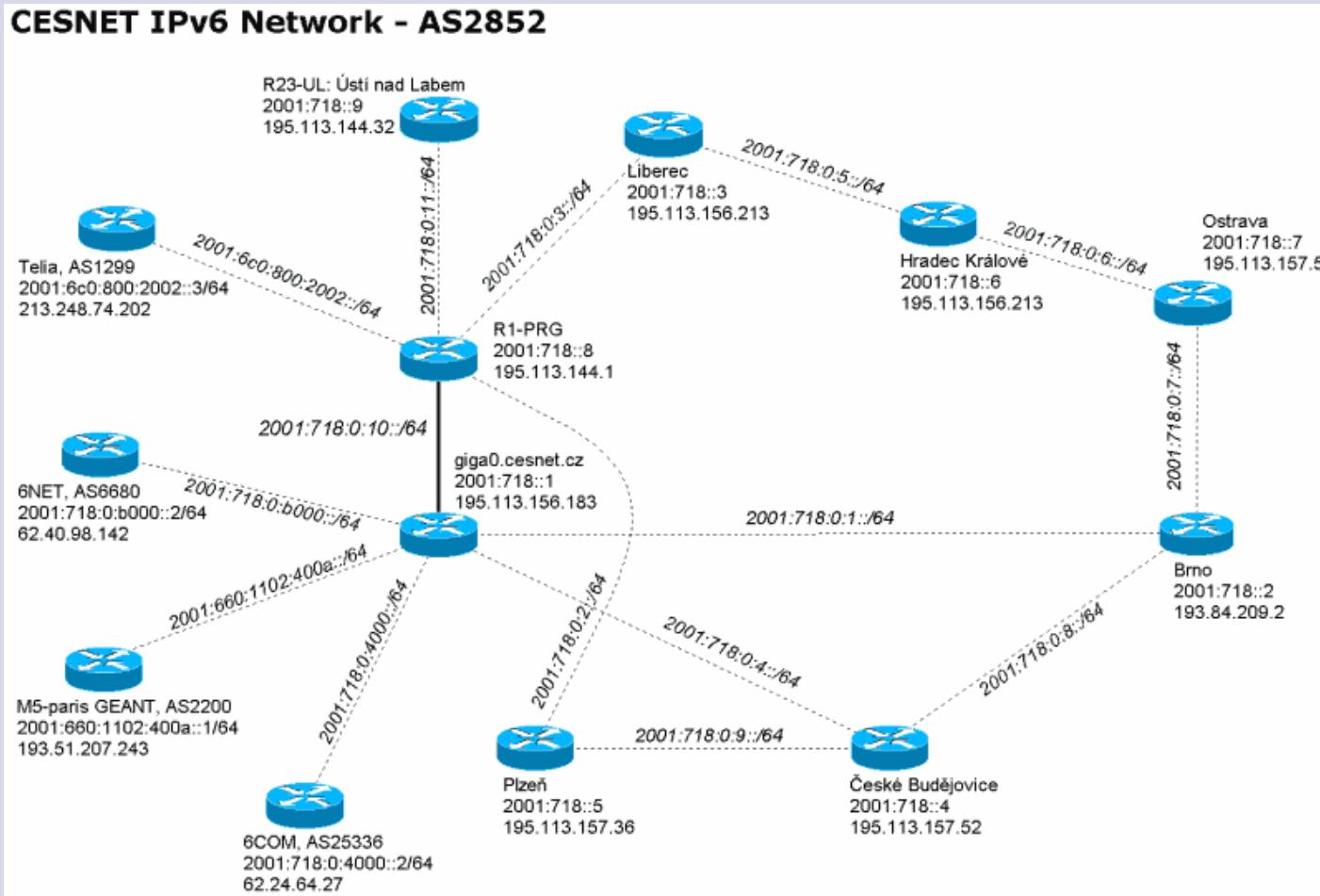


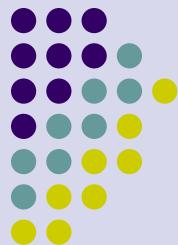
# Přínos IPv6

- Rozšíření adresního prostoru
- 16 slabik =  $3,4 \times 10^{38}$   
(340,282,366,920,938,463,463,374,607,431,768,211,456)
- Minimálně 65536 subsítí pro každého (/48)
- Třída A z IPv4 pro každou stranu
- Některé technologie jsou povinné
- Plug and play
- Bezpečnost mezi koncovými uzly (jako IPsec)
- Od počátku agregovatelné globální adresy
- Redukce externí směrovací informace na 8,192 položek



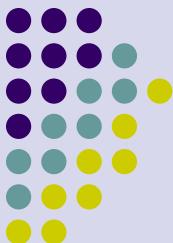
# CESNET IPv6 Network - AS2852





# Architektura adres

- Adresy jsou přiřazeny rozhraním, ne uzlům
- Jako identifikátor uzlu může být použito jakékoliv rozhraní – jakákoliv adresa
- Unicast adresy (individuální) – identifikace jednoho rozhraní
- Multicast (skupinové) – identifikátor více rozhraní (typicky různých uzelů)
- Anycast (výběrové) – identifikátor množiny rozhraní (typicky různých uzelů), paket je doručen na jedno (nejbližší) rozhraní (podle směrovače)
- Broadcast – tento typ adres IPv6 nezná, adresa samé 0 i samé 1 je legální



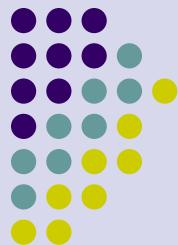
# Zápis adres

- Oddělení 4 znaků znakem „::“
  - ff02: 0000: 0000: 0000: 0000: 0000:0001
  - 3ffe:0501:0008:1234:0260:97ff:fe40:efab
- Počáteční nuly pro každou skupinu mohou být potlačeny
  - ff02: 0: 0:0: 0: 0: 0:1
  - 3ffe:501:8:1234:260:97ff:fe40:efab
- Posloupnost nul může být vypuštěna a nahrazena „::“ (maximálně jednou)
  - ff02::1
- Délka prefixu je umístěna za lomítko
  - 3ffe:500/24



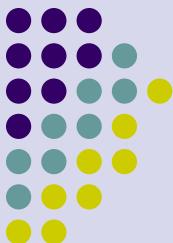
# Typy unicast adres

- Nespecifikovaná adresa – samé 0 (::)
  - Používá se jako zdrojová během inicializace, také jako implicitní
- Loopback adresa – (::1)
  - Obdoba 127.0.0.1 v IPv4
- Link-local adresa
  - Unikátní na subsíti, automaticky konfigurovatelná
  - Vyšší část – fe80::/10
  - Nižší část – identifikátor subsítě a rozhraní
  - Směrovače nesmí forwardovat pakety s cílovou nebo zdrojovou link-local adresou



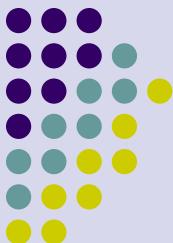
# Typy unicast adres

- Site-local adresa – unikátní pro „site“
  - Vyšší část – fec0::/10
  - Nižší část – identifikátor subsítě a rozhraní
  - Použití je-li síť izolována a nejsou dostupné globální adresy
  - Obdoba privátních adres IPv4
  - Bylo zrušeno, protože se nedohodli co je to „site“
- Unique Local Unicast Address (ULA) – RFC 4193
  - Náhrada site-local adresy
  - Použití jako lokální adresa, přiděluje správce
  - Prefix FC::/7 plus L bit (1 – přiděleno lokálně, 0 - přiděleno jinak)
  - Zatím FD::/8 + 40 bitů náhodné číslo (generátor prefixů pro ULA) + 16 bitů identifikátor podsítě + 64 bitů identifikátor rozhraní



# Typy unicast adres

- Mapované IPv4 adresy - ::ffff:a.b.c.d
  - ::FFFF:147.228.54.10 (prefix ::FFFF/96)
  - Použití u počítačů s duálním zásobníkem IPv4 i IPv6 pro komunikace přes IPv4 s použitím IPv6 adresování
- Kompatibilní IPv4 adresy - ::a.b.c.d
  - Použití v IPv6 hostech pro komunikaci přes automatické tunely
  - ::147:228.54.10 (prefix ::/96)
  - Odmítnuto RFC 4291



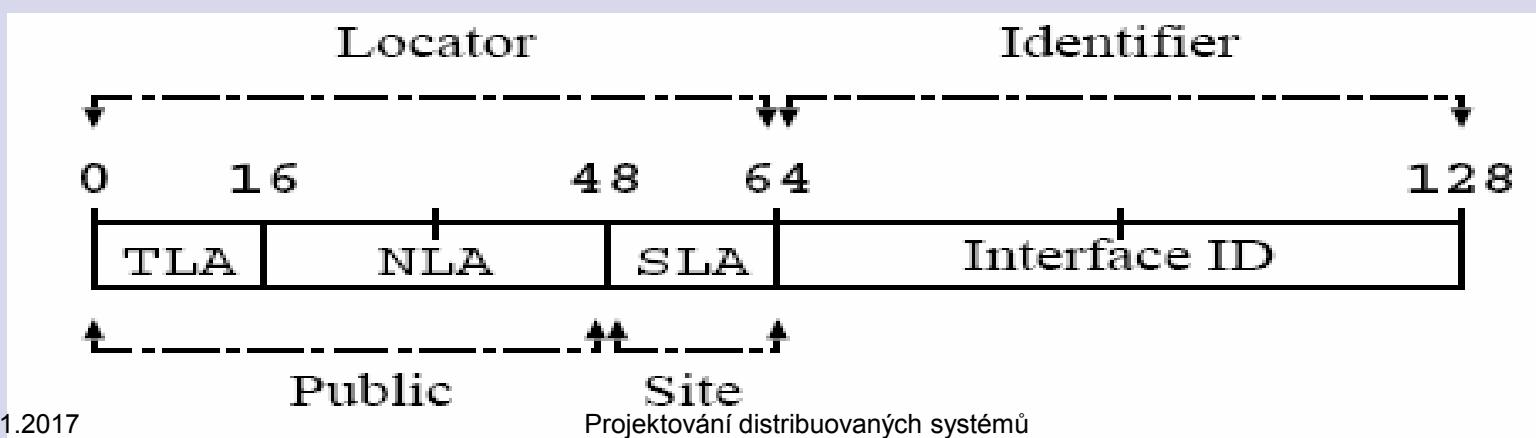
# Adresní bloky

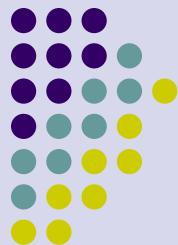
- Adresní prostor je rozdělen do 8 bloků po 3 bitech
- Lépe by bylo 16 bloků po 4 bitech
- Počáteční cifra
  - 0,1 speciální (loopback)
  - 2,3 globální adresy (agregovatelné globální adresy)
  - 4,5 není obsazeno
  - 6,7
  - 8,9
  - a,b
  - c,d
  - e,f link-local, (site-local), multicast



# Globální adresy

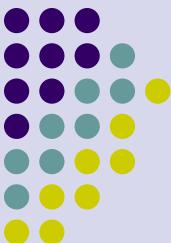
- Cíl zavádění: minimalizace rozměrů globálních směrovacích tabulek
  - Lokátor obsahuje 4 pole
  - TLA (16 bitů) - Top Level Aggregator
  - Rezervováno (8 bitů)
  - NLA (24 bitů) - Next Level Aggregator
  - SLA (16 bitů) - Site Level Aggregator





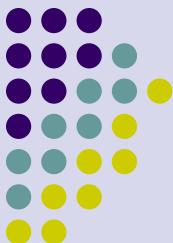
# Globální adresy

- TLA, NLA a SLA se dále v RFC nepoužívají – prefix(3), Global routing prefix(45), Subnet identifier(16), Interface ID(64)
  - Přidělování od 2000::/3
  - Fixní rozdělení 8 slabik síťová část, 8 slabik hostitelská část
- Síťová část (8 slabik)
  - Délka prefixu pevná /64
  - Není třeba určovat délku prefixu pro subsítě
  - /48 je přiřazeno umístění (site)
  - 16 bitů = 65536 subsítí pro jedno umístění (pro jednu stranu)



# Kritéria pro přidělování

- Praha - 2001:718:0::/42
- Brno - 2001:718:800::/42
- Ostrava - 2001:718:1000::/42
- Hradec Králové - 2001:718:1200::/42
- Olomouc - 2001:718:1400::/42
- Ústí nad Labem - 2001:718:1600::/42
- Plzeň - 2001:718:1800::/42
- Liberec - 2001:718:1C00::/42
- České Budějovice - 2001:718:1A00::/42



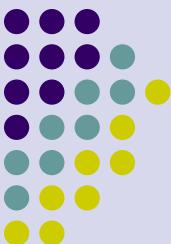
# Přiřazování adres

- **Anycast adresy (výběrové)**
  - Více rozhraní má tutéž adresu, nižší bity (typicky 64 a více jsou nulové)
- **Multicast adresy (skupinové)**
  - Od ff00::/8
  - Struktura 1111 1111 | flags(4) | scop(4) | group ID (112)
  - Flags: 000T – T=0 – všeobecně známá adresa, T = 1 – dočasná adresa
  - Group ID – identifikátor skupiny (nikoliv identifikátor rozhraní)
  - Scope: (dosah)
    - 1 – interface local
    - 2 – link – local
    - 3 – subnet - local
    - 4 – admin – local
    - 8 – organisation – local
    - E – global

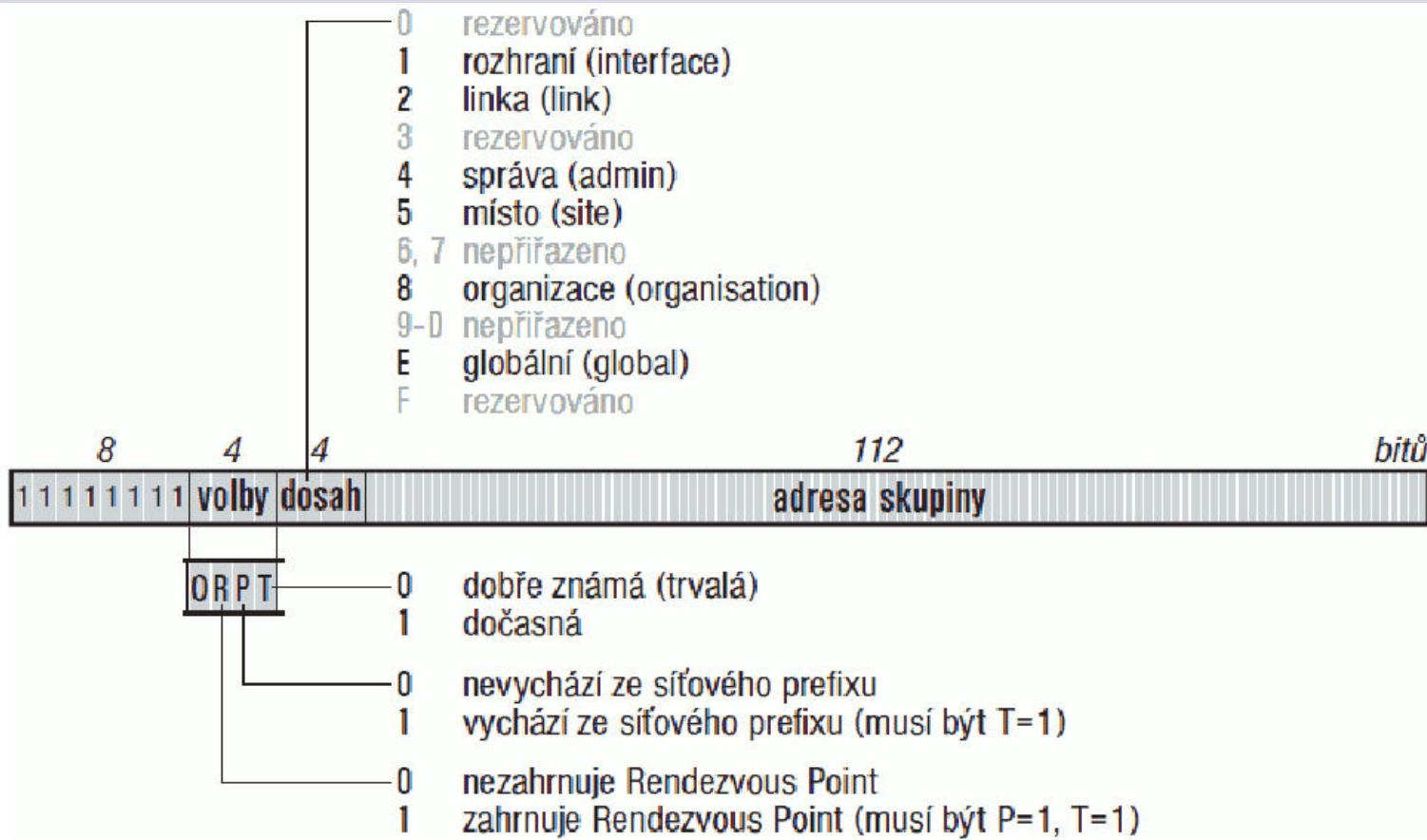


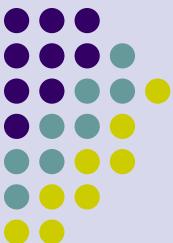
# Přiřazené skupinové adresy

- Všechna rozhraní uzlu ff01::/96
- Všechna rozhraní linky ff01::/96
- Všechny směrovače na uzlu ff02::/96
- Všechny směrovače na lince ff02::/96
- Všechny servery a agenti podporující DHCP ff0c::/96
- Mapování skupinových adres IPv6 na MAC
  - Prefix MAC adresy 3333: + skupinová adresa na 4 slabiky



# Multicast





# Multicast

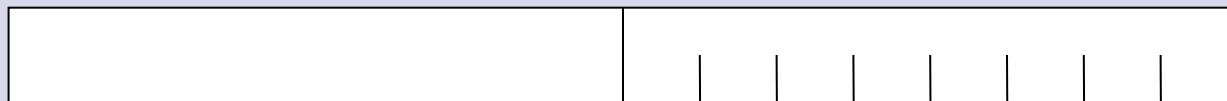
- Mapování MAC adresy
  - Prefix 33:33, zbývajících 32 bitů shodných (MAC, IPv6)
  - IPv6 ff02::1:2233:4455 na MAC 33:33:22:33:44:55
- Multicastové vysílání
  - Dynamické členství ve skupinách
  - Zjišťování členství v podsíti pomocí MLD (Multicast Listener Discovery)
- Směrování multicastu
  - PIM hustý,
  - PIM řídký – rendezvous point



# Plug and Play, Autokonfigurace adres

- Očekává se, že počítač bude v síti fungovat okamžitě po instalaci, bez konfigurace
- Noční můra administrátorů – okamžité zprovoznění velkého počtu počítačů
  - Dolních 8 slabik z MAC adresy

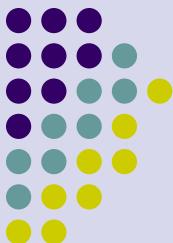
MAC adresa





# Autokonfigurace - bezestavová

- Link-local address
  - Horních 8 slabik ze směrovače
  - Globální adresa
  - Není třeba DHCP server (bezestavové přidělení adresy)
  - (Stavové přidělení – DHCPv6)
- Konverze MAC adresy na interface ID
  - EUI64 adresa (8 slabik)
  - Neguje také 2. bit 1. slabiky (příznak globání adresy)
  - 00:08:05:01:23:45 --> 0208:05ff:fe01:2345
- Generování link-local adresy
  - fe80:: interface ID
  - fe80::208:05ff:fe01:2345



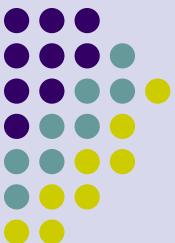
# Objevování sousedů

- Neighbor Discovery – nahrazuje ARP v IPv4
  - Zjišťování linkových adres sousedních uzlů
  - Hledání směrovačů
  - Přesměrování
  - Zjišťování síťových parametrů pro automatickou konfiguraci
  - Ověřování dosažitelnosti sousedů
  - Detekce duplicitních adres
- Využívá zprávy protokolu ICMPv6
  - Router advertisement – síťové parametry
  - Router solicitation – vyžádání Router advertisement
  - Neighbor advertisement – informace o sousedovi
  - Neighbor solicitation – výzva ohlášení souseda
  - Redirect - přesměrování na jiného souseda



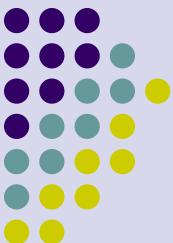
# Autokonfigurace - stavová

- Host obdrží adresu rozhraní nebo konfigurační informaci a parametry od serveru
- Host je identifikován jednoznačným identifikátorem (MAC adresa, ale uvažuje se i o ID nezávislém na MAC karty)
- Servery udržují databázi, obsahující mapování adres přiřazených hostům
- Jedno z možných schémat odpovídá DHCPv6
- Stavová a bezestavová autokonfigurace může být použita souběžně – výhodné z hlediska udržení stavu přidělených adres (není třeba)
- DHCP ale přidělí ostatní parametry (adresa DNS)
- Administrátor určuje typ nastavením odpovídající položky v Router Advertisement zprávách



# DHCPv6

- Stavová autokonfigurace
  - Solicit - výzva na adresu ff02::1:2 (DHCP relay agenti a servery, ff05::1:3 DHCP servery)
  - Advertise – odeslání nabídek
  - Request – požadavek na přidělení prexifu
  - Reply – potvrzení přidělených parametrů
  - Decline – uvolnění
  - Confirm – potvrzení
  - Reconfigure – obnova
  - Relay-Forw, Relay-Reply – forwardování zpráv serveru nebo jinému Relay agentovi
- DHCP Unique Identifier (DUID)
  - identifikátor klienta (10 byte)
  - Daný výrobcem, vygenerování
  - Nezávislý na technickém vybavení klienta



# Povinné adresy

- **Povinné adresy uzlu**

- Lokální linková adresa pro každé rozhraní  
(fe80::208:05ff:fe01:2345)
- Přidělená individuální adresa  
(2001:718:1800:11:208:05ff:fe01:2345)
- Loopback (::1)
- Všechna rozhraní uzlu (ff01::1)
- Všechna rozhraní na lince (ff02::1)

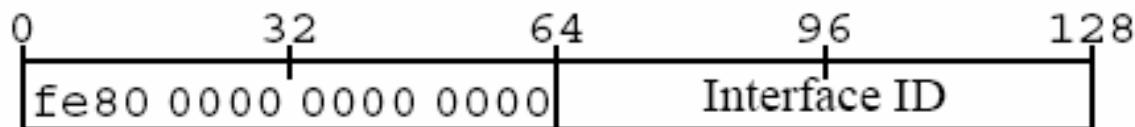
- **Povinné adresy směrovače**

- Povinné adresy uzlu
- Všechny skupinové adresy směrovače, linky, LAN

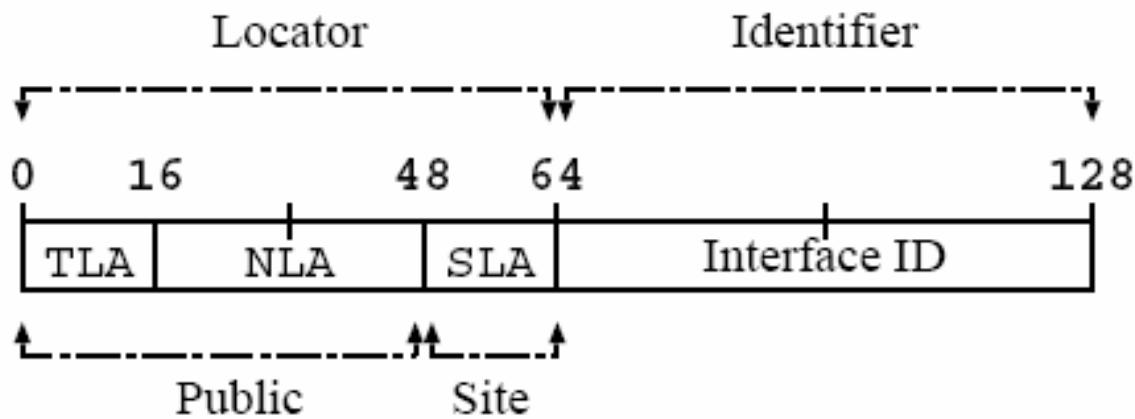


# Povinné adresy

## Linklocal address



## Aggregatable global address





# Systém jmenných domén

- Počítač může používat stejné jméno pro síť IPv4 i IPv6
- Uživatel to nerozlišuje
- Zadávání IPv6 adresy může být složité
- 2001:718:1800::208:05ff:fe01:2345
- V URL: [http://\[2001:718:1800::208:05ff:fe01:2345\]/](http://[2001:718:1800::208:05ff:fe01:2345]/)



# Systém jmenných domén

- Přidány položky (typy)
  - AAAA pro převod jméno --> adresa

```
$ORIGIN mew.org.  
ftp    AAAA    3ffe:501:8:1234:260:97ff:fe40:efab  
www    A        133.5.2.1
```

- PTR pro převod adresa --> jméno
  - in-addr.arpa
  - Ipv6.arpa

```
$ORIGIN 4.3.2.1.8.0.0.0.1.0.5.0.e.f.f.3.IP6.INT.  
b.a.f.e.0.4.e.f.f.7.9.0.6.2.0 PTR ftp.mew.org.  
$ORIGIN 2.5.133.IN-ADDR.ARPA.  
1                                              PTR www.mew.org.
```

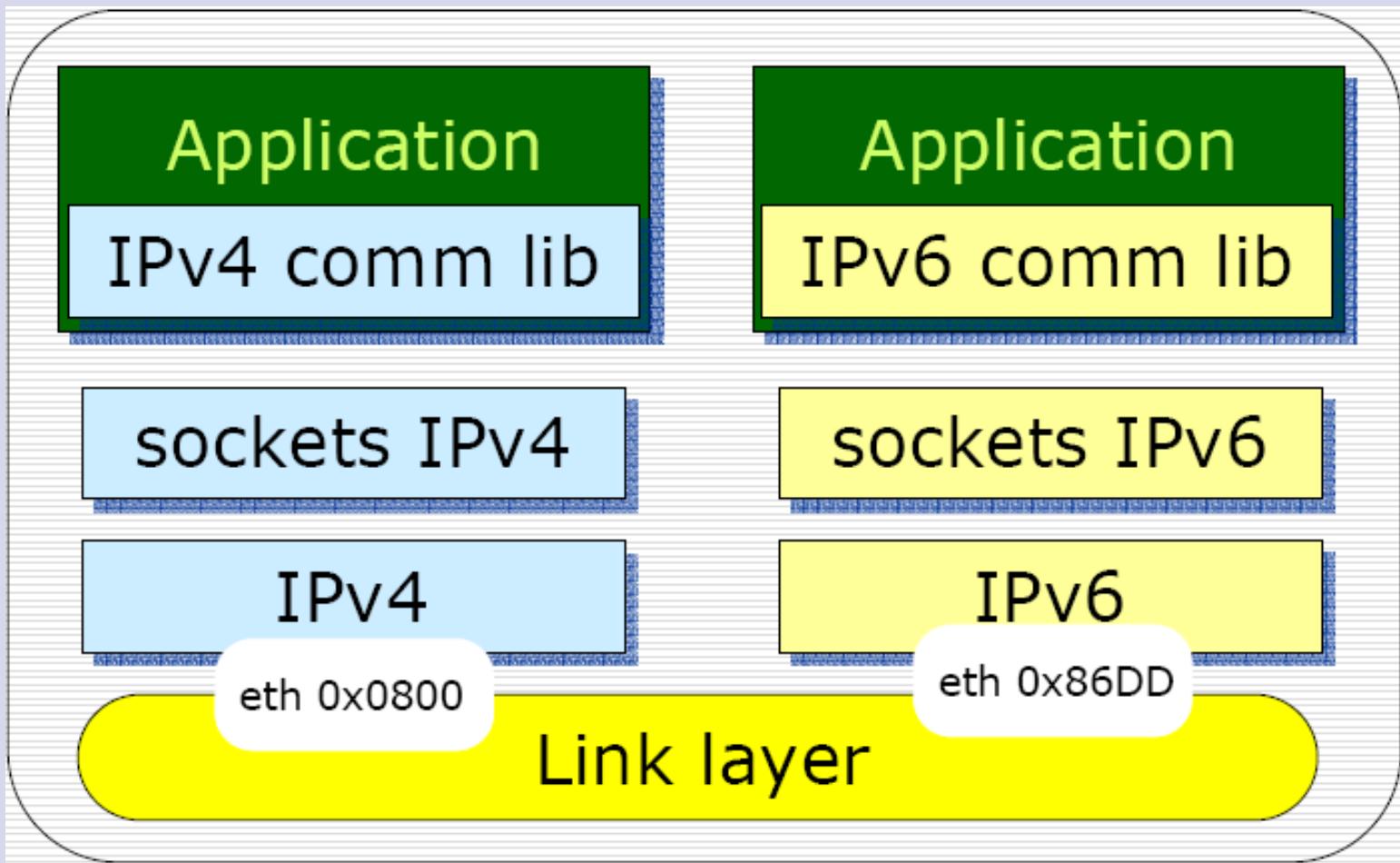


# Přechod IPv4 na IPv6

- **Technologie pro přechodné stádium**
  - Dvojitý zásobník
  - Tunelování
  - Převodník
- **Dvojitý zásobník**
  - Podporuje IPv4 i IPv6
  - IPv4 aplikace jsou dostupné bez modifikací
  - Dvojitý zásobník funkční bez instalace OS
  - Náhrada IPv4 ovladače



# Dvojitý zásobník





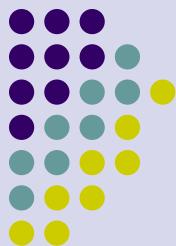
# Přechod IPv4 na IPv6

## ● IPv6 v IPv4 tunelu

- Předpoklad: IPv6 jsou ostrovy v IPv4
- Tunel propojuje IPv6 ostrovy
- Zapouzdření paketů IPv6 do IPv4
- Příkladem je 6BONE (50 států)

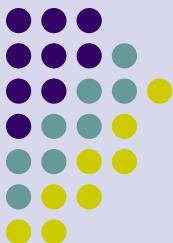
## ● Převodníky

- V prvopočátku – málo IPv6 uzelů nebo duálních uzelů
- Později – adresy IPv4 se stávají nedostupné
- Protože musí existovat IPv4 a IPv6 souběžně, převodníkům se nevyhneme



# Tunelování IPv6

- Propojení několika počítačů (sítí) IPv6 přes síť IPv4
  - Problém protokolu
  - Problém dat (balení IPv6 do paketu IPv4)
  - Adresování
- Konfigurované tunely
  - Registrace
  - Permanentní tunel mezi klientem a serverem
  - Např. SiXXS
- Automatické tunely
  - Bez registrace
  - Tunel se vytváří dynamicky
  - Např. 6to4, Teredo



# Mobilní IPv6 (MIPv6)

- Obdoba MIPv4
  - RFC3775
  - Mobilní klient není problém (DHCP)
  - Mobilní server (je třeba s ním navázat spojení)
  - Komponenty
    - Home agent
    - Care of Address
    - Není Foreign agent
  - Trojúhelníkové směrování, možnost předat CoA
- Implementace
  - MIPL (Linux), Cisco, Microsoft(2000,XP,CE), KAME (FreeBSD), HP-UX



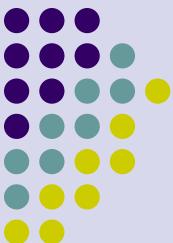
# IP směrování

- Směrování navazuje na směrování IPv4
- Problém s novým typem adres
- Algoritmy směrování zůstávají
  - DVA (RIPng)
  - LSA (OSPF pro IPv6, OSPFv3)
  - Multiprotocol BGP pro IPv6



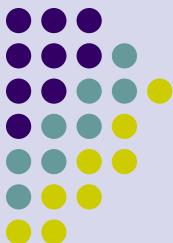
# Formát rámce IPv6

Version	Priority	Flow Label				
Payload Length		Next Header		Hop Limit		
Source Address – 128b.						
Destination Address – 128b.						



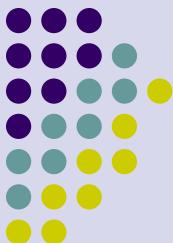
# Formát rámce IPv6

- Priority
  - 0 – nespecifikováno
  - 1 – na pozadí
  - 2 – best effort
  - 4 – objemný přenos dat
  - 6 – interaktivní přenos
  - 7 – správa a řízení (směrování, správa sítě)
  - 8 – 15 – přenosy v reálném čase



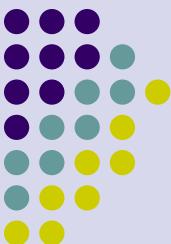
# Formát rámce IPv6

- Flow label – identifikace toku dat – možnost přiřazení priority (QoS)
- Payload length – délka ve slabikách za standardním záhlavím (data + dodatečná záhlaví)
- Hop limit – místo TTL (v počtu přeskoků)
- Next header – následující záhlaví (IPv6, TCP, typy zapouzdření)

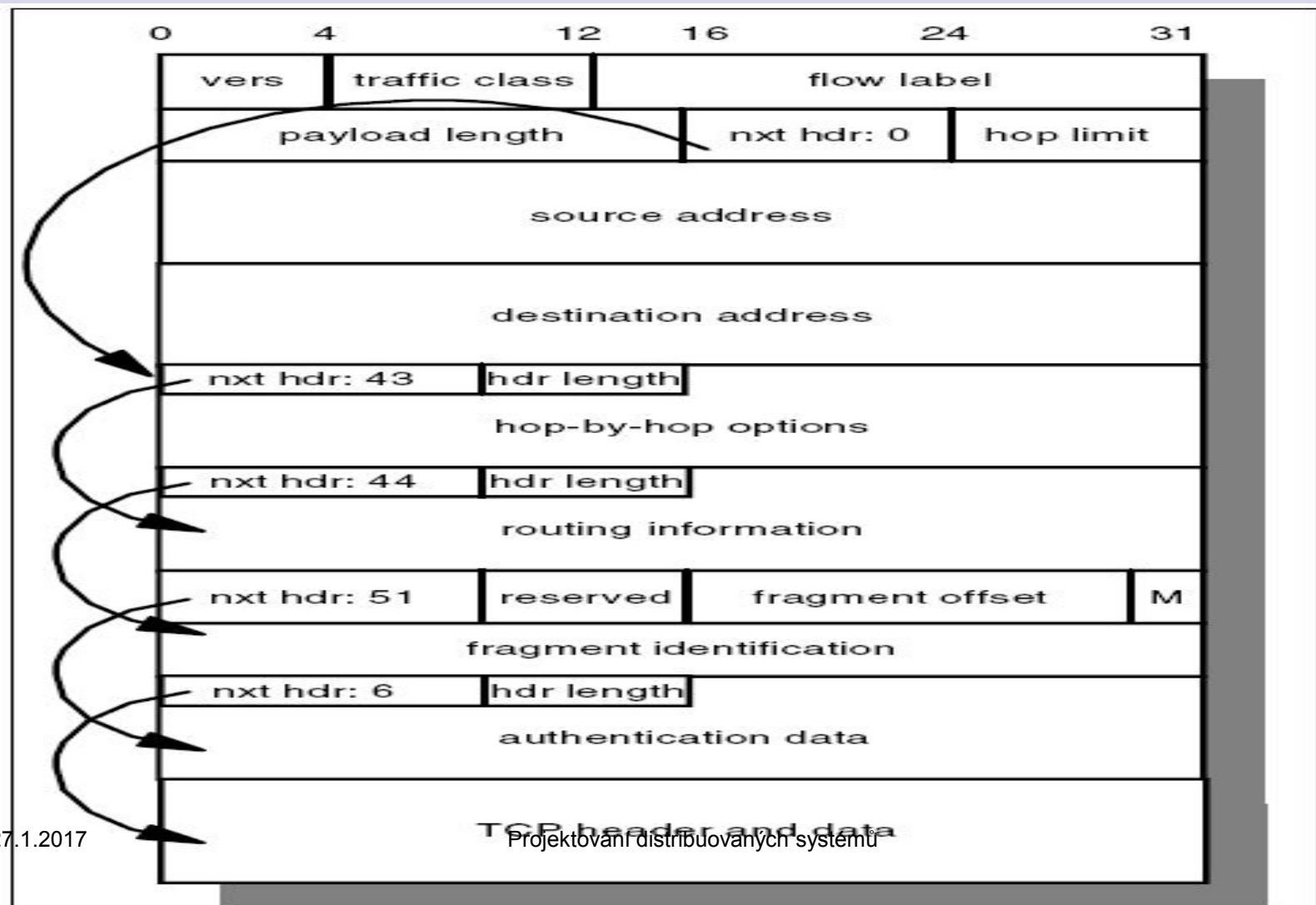


# Next header – následující záhlaví

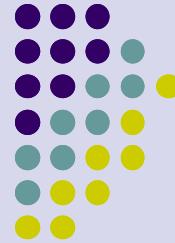
- 0 – Hop-by-Hop option header
- 4 – IPv4 datagram
- 6 – TCP segment
- 17 – UDP segment
- 43 – Routing Header
- 44 – Fragment Header
- 45 – protokol IDRP (Interdomain Routing Protocol)
- 46 – protokol RSVP
- 50 – Encapsulating Security Payload
- 51 – IPv6 Authentication Header
- 58 – ICMPv6
- 59 – No Next Header
- 60 – Destination Option Header
- 89 – OSPF



# Zřetězení záhlaví IPv6

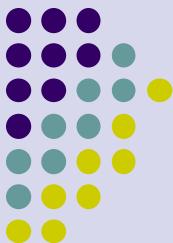


# **Quality of Services v IP sítích**



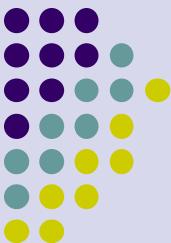
---

Úvod do počítačových sítí  
Ing. Jiří Ledvina, CSc.



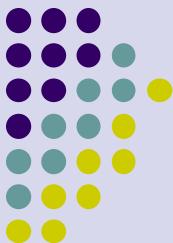
# Úvod

- Původní koncepce IP – strategie „best effort“
- Telefonní sítě – přirozená vlastnost – přidělení konstantní šířky pásma každému hovoru
- IP sítě – sdílená šířka pásma pro všechny přenosy
- Parametry spojené s kvalitou přenosu (některé)
  - Šířka pásma (propustnost)
  - Maximální (průměrné) zpoždění (krátkodobé/dlouhodobé)
  - Chybovost (ztrátovost) přenosu
  - Rozptyl zpoždění (jitter)
- QoS – pro LAN, MAN, WAN
  - IP, Ethernet, ATM, Frame Relay, ...
  - Nejen úroveň 3, ale i 2



# Úvod

- Např. ATM sítě
  - QoS integrované v protokolu
  - Constant bit rate, variable bit rate, available bit rate, unspecified bit rate
  - Zajišťuje AAL1 až AAL5 (ATM Application Level)
- Typy požadavků
  - Interaktivní přístup – min. doba odezvy, bez tolerance k chybám
  - Přenos objemných dat – max. šířka pásma, bez tolerance ke ztrátám
  - Přenos zvuku – malá šířka pásma, konstantní zpoždění, min. tolerance ke ztrátám
  - Přenos obrazu – velká šířka pásma, shluky dat, variabilní zpoždění, tolerance ke ztrátám



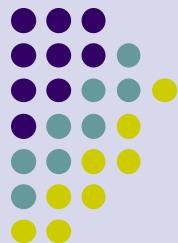
# Quality of Service

- QoS musí zajistit
  - Předvídatelnou dobu odezvy
  - Řízení aplikací citlivých na zpoždění
  - Řízení aplikací citlivých na jitter
  - Ovládání ztrát paketů během zahlcení způsobeného shluky
  - Nastavení priorit přenosu
  - Vyhrazení pásma pro vybrané aplikace
  - Předcházení zahlcení (úplnému)
  - Ovládání stavu zahlcení pokud mu nelze zabránit
- QoS mohou pracovat v prostředí
  - Best effort
  - Rozlišované služby – mohou se zabývat mezi různými úrovněmi QoS na úrovni jednotlivých paketů
  - Integrované služby – úroveň služeb je vyžadována aplikací a garantovaná (potvrzovaná) „sítí“



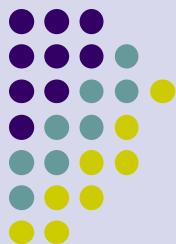
# QoS v IP sítích

- IETF aktivity – QoS v IP sítích (zlepšení strategie best effort – s maximálním úsilím)
- Zahrnuje
  - RSVP (Reservation Protocol,
  - Differentiated (rozlišované)
  - a Integrated (sjednocené) služby
- Jednoduchý model pro sdílení média



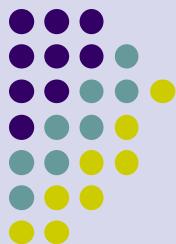
# Principy QoS

- **Princip 1 – značkování paketů**
  - je třeba označit (značkovat) pakety tak, aby směrovač mohl rozlišovat mezi různými třídami přenosu
  - to je nová politika směrovače, kdy je s pakety zacházeno podle třídy
- Příklad – IP telefon 1Mbps, FTP, sdílení linky 1,5Mbps
  - Nárazové požadavky FTP mohou zahltit směrovač a způsobit ztrátu audio dat
  - Audio musí mít vyšší prioritu než FTP



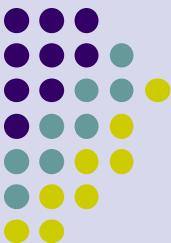
# Principy QoS

- **Princip 2 – vzájemná izolace tříd**
  - vyžaduje mechanizmus, který by zajistil zařazení zdrojů podle požadavků na šířku pásma
  - Musí kontrolovat dodržování dohodnutých rychlostí
  - označování paketů musí být realizováno na hranách (okrajích) sítě
  - Alternativní řešení – přidělení části pásma každému aplikačnímu toku
    - vede k neefektivnímu využití pásma (pásmo zůstane nevyužito, pokud jej aplikace nepotřebuje)



# Principy QoS

- **Princip 3** – při izolaci tříd je třeba využít zdroje co nejefektivněji
  - nepodporovat přenosy, které překračují kapacitu linky
- **Princip 4** – je třeba realizovat proces „kontroly na vstupu“ (Call Admission Process)
  - aplikační tok musí deklarovat své potřeby předem
  - síť může volání blokovat pokud nemůže potřeby zajistit



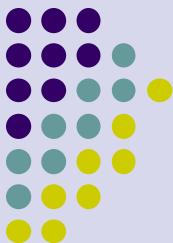
# Principy QoS

- QoS pro síťové aplikace vyžaduje
  - klasifikaci paketů
  - izolaci: rozvrhování a politiku rozhodování
  - vysokou míru využití zdrojů
  - kontrolu na vstupu (Call Admission)



# Klasifikace paketů

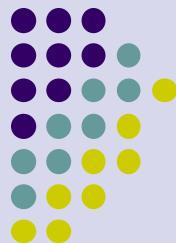
- Na 2. úrovni ISO/OSI se zavádí Class of Services (CoS)
- Definováno v 802.1p
  - Dovoluje definovat až 8 tříd přenosu
  - Nejnižší priorita je 0 = normální obsluha
  - Různým portům nebo mostům mohou být přiřazeny různé počty tříd přenosu
  - Jsou doporučovány čtyři priority
    - Časově a bezpečnostně kritické aplikace
    - Časově kritické aplikace
    - Časově nekritické, citlivé na ztráty při přenosu
    - Časově nekritické, necitlivé na ztráty



# Klasifikace paketů

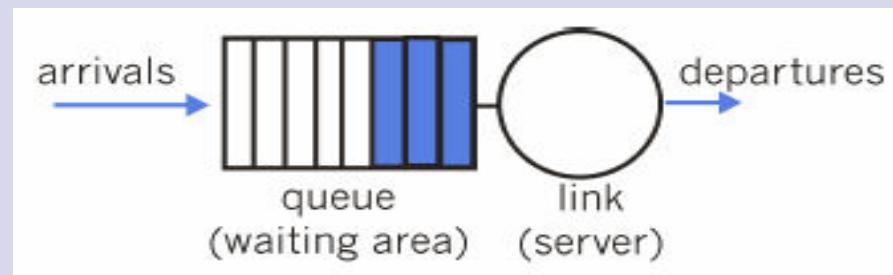
- Priority

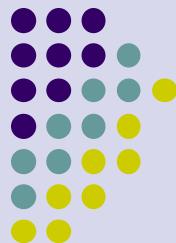
- 000 best effort, běžná priorita
- 001 na pozadí, hromadné přenosy, hry
- 002 interaktivní přenosy,
- 003 best effort pro významné uživatele
- 004 řízený přenos, důležité aplikace
- 005 přenos obrazu, zpoždění 100ms
- 006 přenos hlasu, zpoždění 10ms
- 007 řízení sítě



# Rozvrhování a kontrola

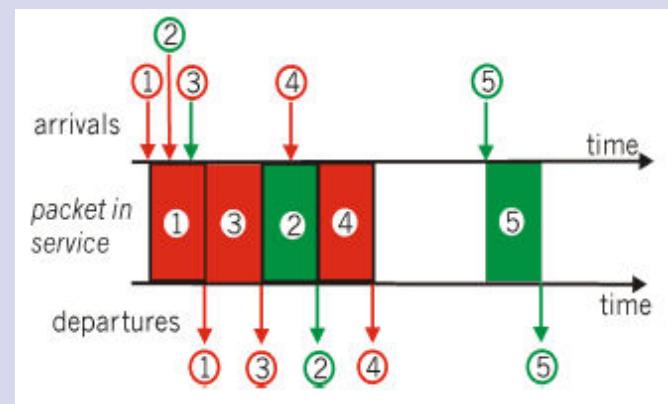
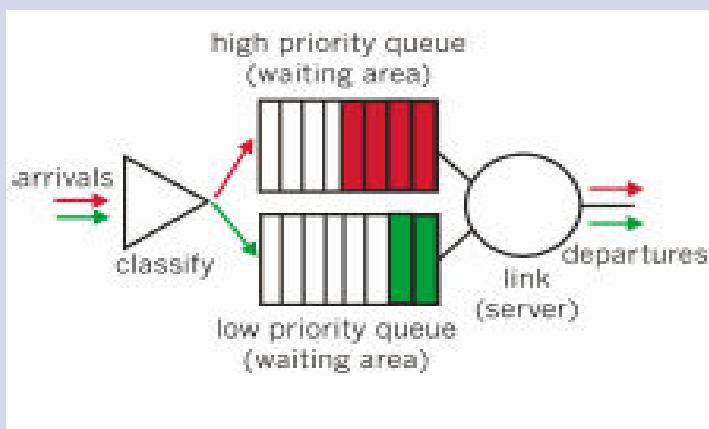
- Rozvrhování a kontrolní mechanizmus (Scheduling and Policing Mechanisms)
- Rozvrhování – výběr dalšího paketu pro přenos linkou
  - existuje několik použitelných mechanizmů
  - FIFO
    - výběr v pořadí příchodu
    - pakety přicházející do plné vyrovnávací paměti jsou zahozeny
    - může být použit kontrolní mechanizmus pro určení který paket bude zahozen a který zařazen do fronty

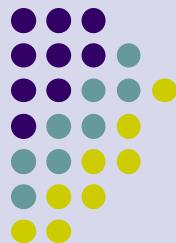




# Rozvrhování a kontrola

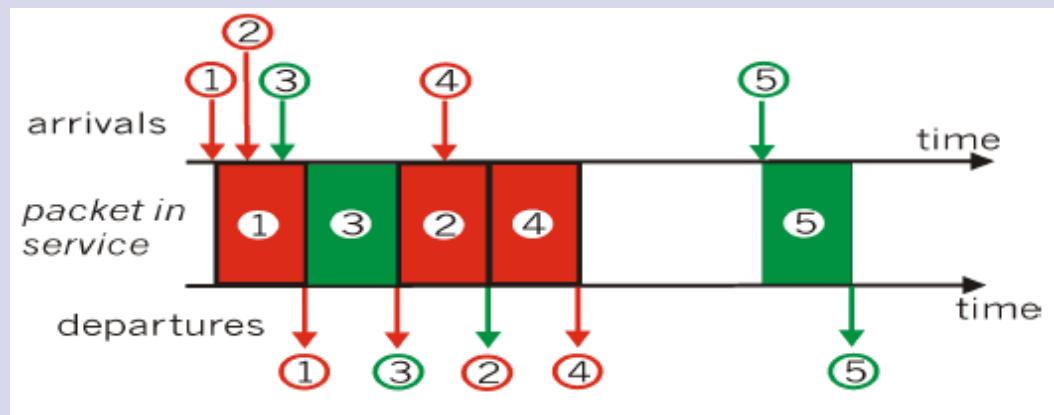
- Prioritní rozvrhování - třídám je přiřazena různá priorita
  - přiřazená třída může záviset na explicitním značkování nebo informaci v záhlaví (IP adresy, TCP porty, ... )
  - nejdříve se vysílají pakety z fronty s nejvyšší prioritou
  - mohou existovat preemptivní i nepreemptivní (bez přerušení) verze

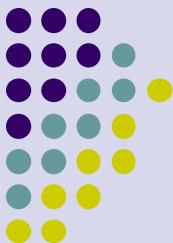




# Rozvrhování a kontrola

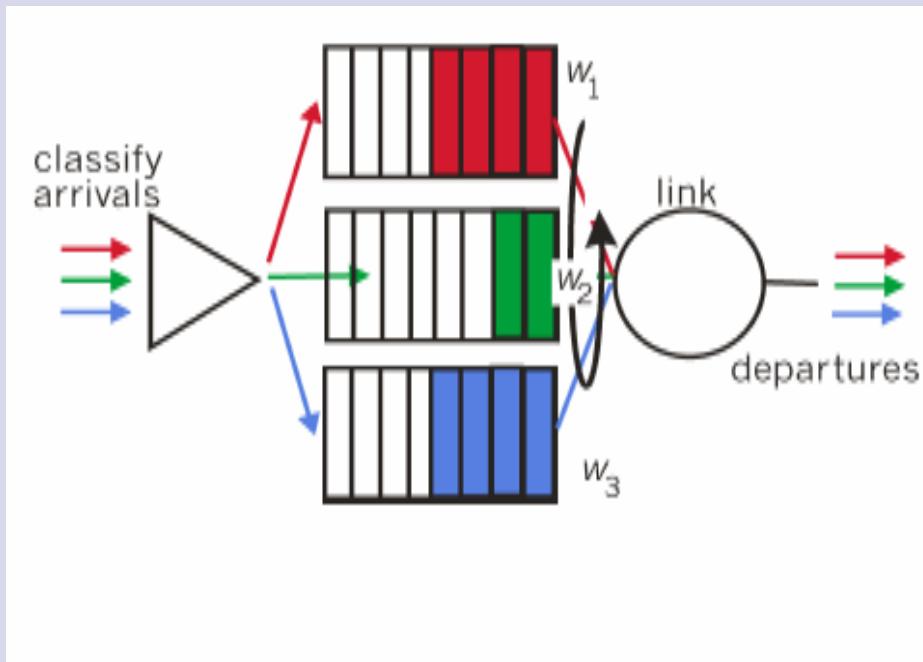
- Plánování podle cyklické obsluhy (Round Robin)
  - Více tříd obsluhy
  - Cyklicky testuje fronty jednotlivých tříd, obsluhuje z každé jeden požadavek

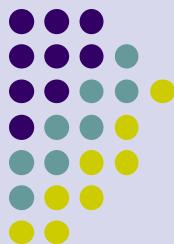




# Rozvrhování a kontrola

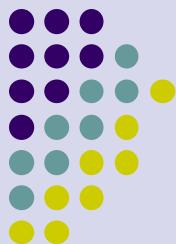
- Weighted Fair Queuing (WFQ)
  - Zobecněná metoda Round Robin
  - Obsluha front (tříd) rozdílně podle priority
  - Obsluha v dané časové periodě





# Mechanizmy politiky

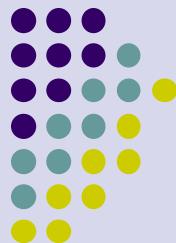
- Cíle – omezit přenosy tak, aby nepřekračovaly deklarované parametry
- Mechanizmy politiky – pro kontrolní mechanizmus (policing) existují následující kritéria
  - průměrná rychlosť (počet paketů za sek.)
    - rozhodující aspekt je délka intervalu měření
    - dlouhodobé měření
  - špičková rychlosť (počet paketů za ?)
    - krátký časový interval
    - krátkodobé měření
  - velikost shluku (burst size)
    - maximální počet paketů poslaných najednou
    - krátký časový interval



# Mechanizmy politiky

## Leaky Bucket

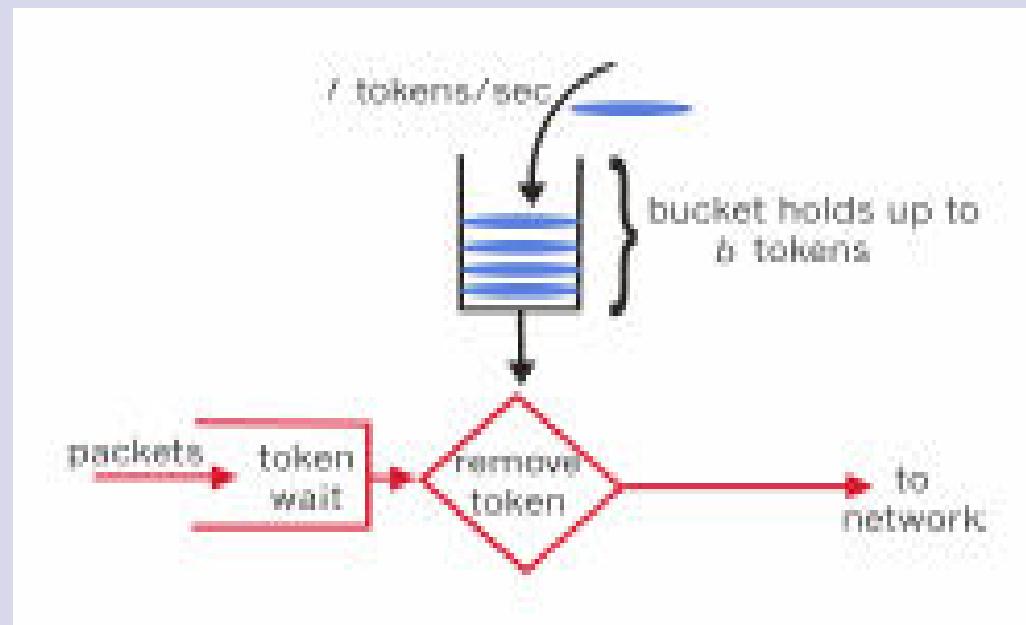
- „Ořezání“ přenosu na konstantní, předem danou hodnotu.
- „Odkapávání vody z vědra“ konstantní rychlostí
- Nevýhoda – nezpracuje „záplavovou vlnu“

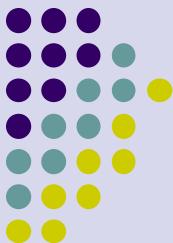


# Mechanizmy politiky

## Token Bucket

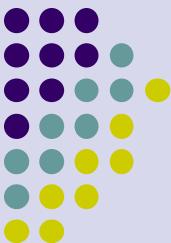
- Token bucket mechanizmus
  - bucket = vědro, nalévat, vylévat, oblast paměti
  - mechanizmus zajišťující omezení vstupu na předem specifikovanou velikost shluku (burst size) a průměrnou rychlosť (average rate)





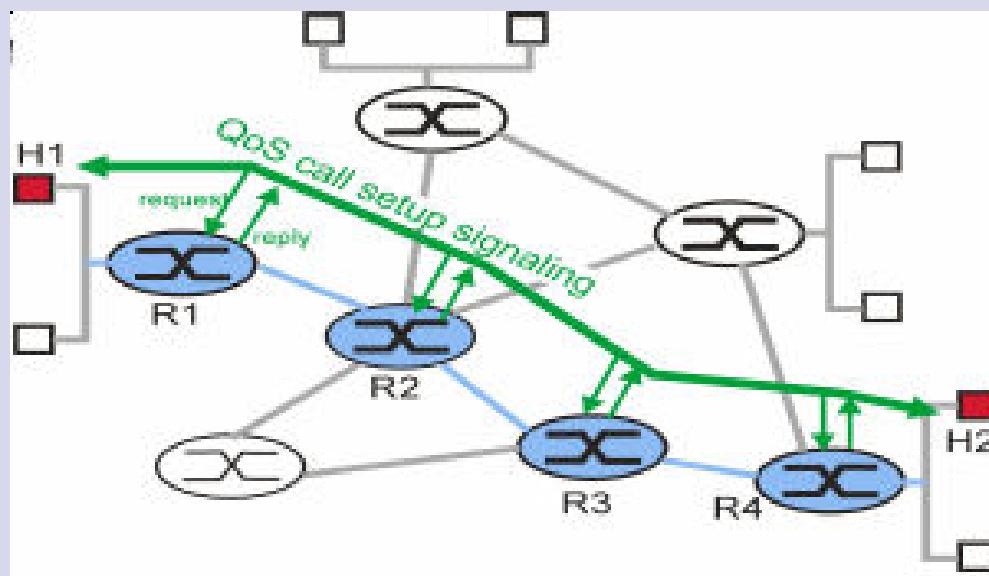
# Integrated Services

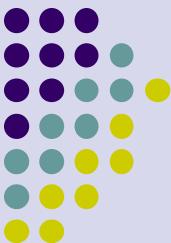
- **Integrated services (jednotné, sjednocené služby)**
- architektura pro garantování QoS v IP sítích pro individuální aplikační relace
- spoléhá se na rezervaci zdrojů
- směrovače si musí udržovat stavovou informaci (obdoba virtuálních okruhů)
- záznamy o přidělených zdrojích
- reakce na přicházející požadavky vytváření spojení



# Integrated Services

- Rezervace zdrojů
  - Vytvoření spojení (call Setup) podle RSVP
  - Vlastní přenos, definice QoS
  - Vstupní kontrola na každém prvku

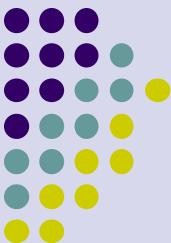




# RSVP

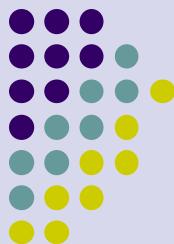
## • Vlastnosti RSVP

- podporuje rezervaci pásma pro zprávy typu unicast i multicast
- dovoluje účastníkům relace v multicastu požadovat různé QoS
- pracuje nad existujícím směrováním, využívá existující směrovací tabulky
- nespecifikuje jak bude požadované pásmo rezervováno
- není směrovací protokol, ale je signalizační protokol – dovoluje hostům vytvořit a rušit rezervaci pro datový tok



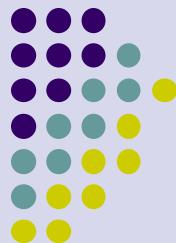
# RSVP

- Způsoby rezervace – filtry
  - existují 3 způsoby rezervace (RFC 2205)
  - **Fixed filter (FF)** – dovoluje danému zdroji, aby byl explicitně spojen s daným flowspec a relací (unicast aplikace)
  - **Shared Explicit filter(SE)** - dovoluje více zdrojům, aby byly explicitně spojeny s daným **flowspec** a relací. Vyžaduje, aby klasifikátor paketů měl vstup pro každé číslo relace.
  - **Wildcard filter(WF)** – sdílí **flowspec** zdrojů mezi toky od různých zdrojů. Není vyžadován **filterspec**. Dovoluje směrovači rezervovat zdroje pouze s jedním klasifikátorem.
  - Styly filtrování nemohou být mixovány v jedné relaci



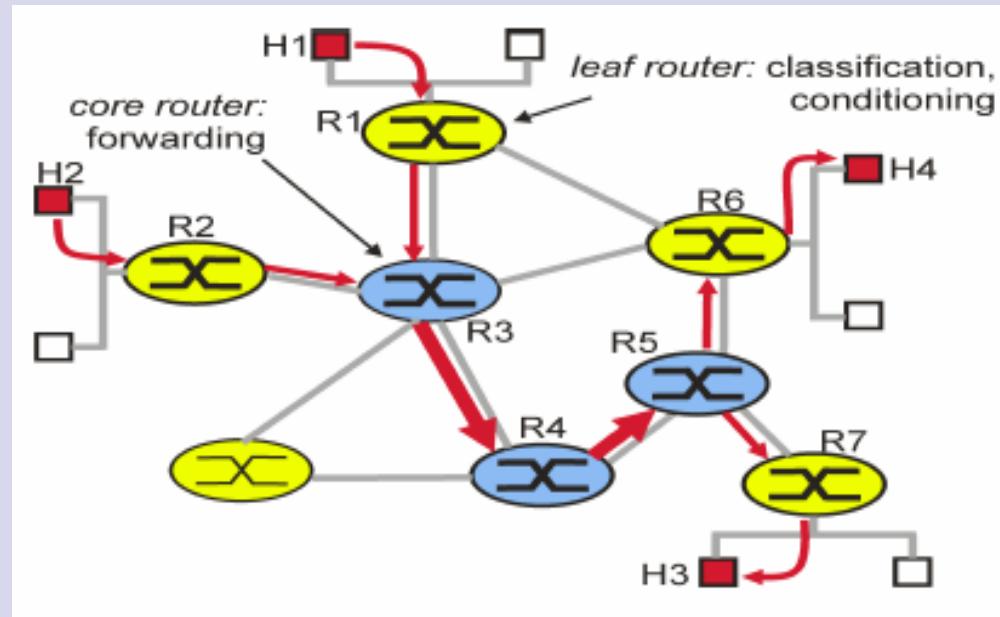
# Differentiated Services

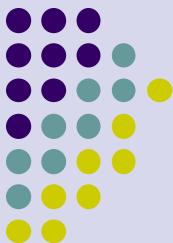
- **Differentiated Services (rozlišované služby)**
  - jsou určeny pro odstranění následujících problémů IntServ a RSVP
    - skalabilita – směrovače s RSVP údržují velký počet toků současně
    - flexibilita modelu služeb
    - složitá signalizace – týká se RSVP
- Základní přístup
  - jednoduché funkce uvnitř sítě, složité funkce na vstupech a výstupech
  - nedefinuje třídy obsluhy, pouze nabízí prostředky pro vytvoření služeb



# Differentiated Services

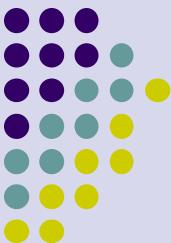
- Hranová zařízení, funkce hranových zařízení
  - na vstupu a výstupu subsítě jsou tzv. hranová zařízení, která klasifikují pakety (modifikace paketů)
  - klasifikace – označování paketů podle pravidel klasifikace (specifikováno protokolem nebo administrátorem)
  - formování přenosu – zadržování, odmítání paketů





# Differentiated Services

- Základní funkce
  - forwardování – podle „Per-Hop-Behavior“ – chování za (při) přeskoku
    - PHB – specifikováno pro danou třídu paketů
    - PHB – je založeno na značkování paketů podle tříd
  - Na směrovačích není udržována stavová informace



# Differentiated Services

- Klasifikace a formování přenosu
  - paket je značkován v poli TOS v IPv4 a Trafic Class v IPv6
  - je označován DSCP (Differentiated Service Code Point)
    - délka je 6 bitů
    - určuje PHB (RFC 2474, RFC 3140)
    - CU – currently unused

