KOMUNIKAČNÍ TECHNOLOGIE (BPC-KOM)

Ústav telekomunikací
Fakulta elektrotechniky a komunikačních technologií
VUT v Brně

doc. Ing. Jan Jeřábek, Ph.D.
jerabekj@feec.vutbr.cz

SÍŤOVÁ VRSTVA PŘENOSOVÝCH SYSTÉMŮ

Plán přednášky

- Přepojování paketů
- Služby síťové vrstvy
- Úloha síťové vrstvy s IP protokolem
- Struktura síťové vrstvy s IP protokolem
- Adresy síťové vrstvy u IPv4 protokolu
- Techniky směrování
- IPv4 datagramy
- Fragmentace paketů
- Tunelování
- Návaznost IP adres na adresy nižší úrovně
- Překlad síťových adres (NAT)
- Mechanizmy řízení provozu v síťové vrstvě
- Internet Control Message Protocol (ICMPv4)
- Internet Protocol verze 6 (IPv6)
- Zařízení síťové vrstvy

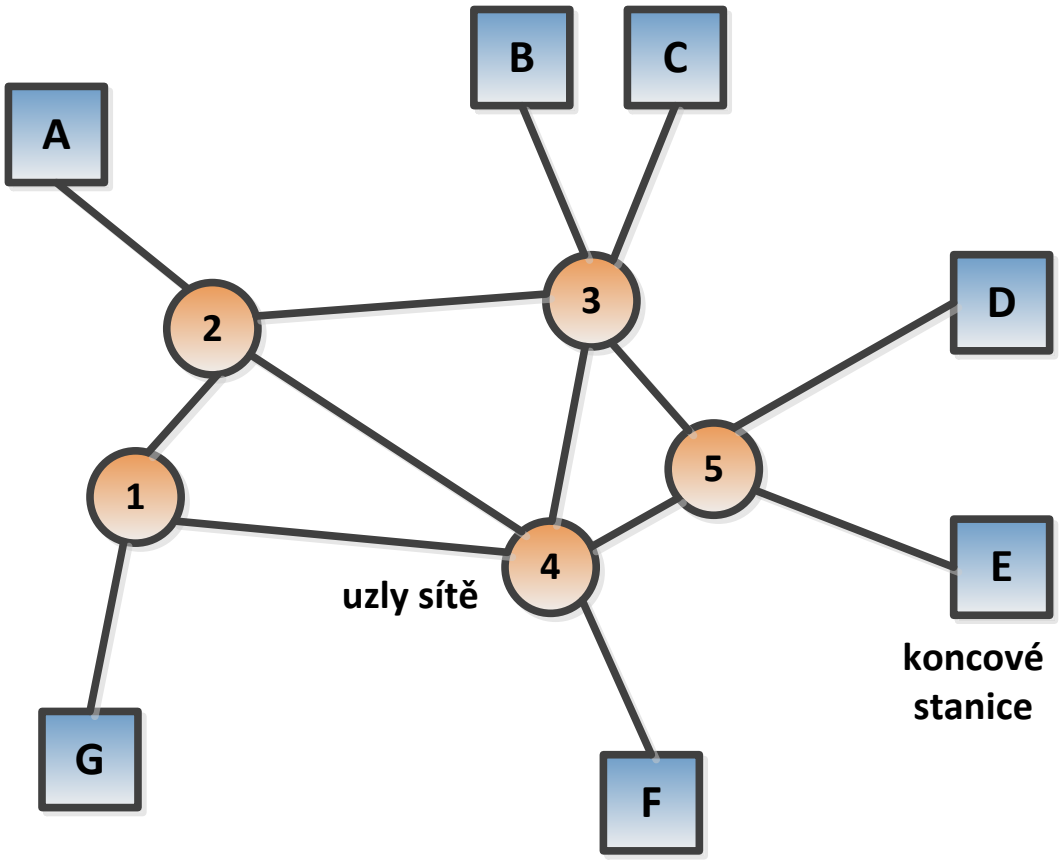
Principy přepojování paketů

- síťová vrstva
  - nezbytná pro komunikaci dvou nesousedících účastníků (bez přímého spojení)
  - hledání a výběr vhodné cesty přes mezilehlé uzly
  - více možných druhů komutace, typicky přepojování paketů
    - když není třeba trvalý přenos dat mezi stranami
- pakety běžně max. 1000 – 1500 B, data dělena na části
  - každý má záhlaví s informací odkud kam je směrován

Principy přepojování paketů

přenos z A do E

- A –> 2
- 2 určí cestu (např. 3)
- 2 –> 3
- 3 určí cestu (např. 5)
- 3 –> 5
- 5 –> E



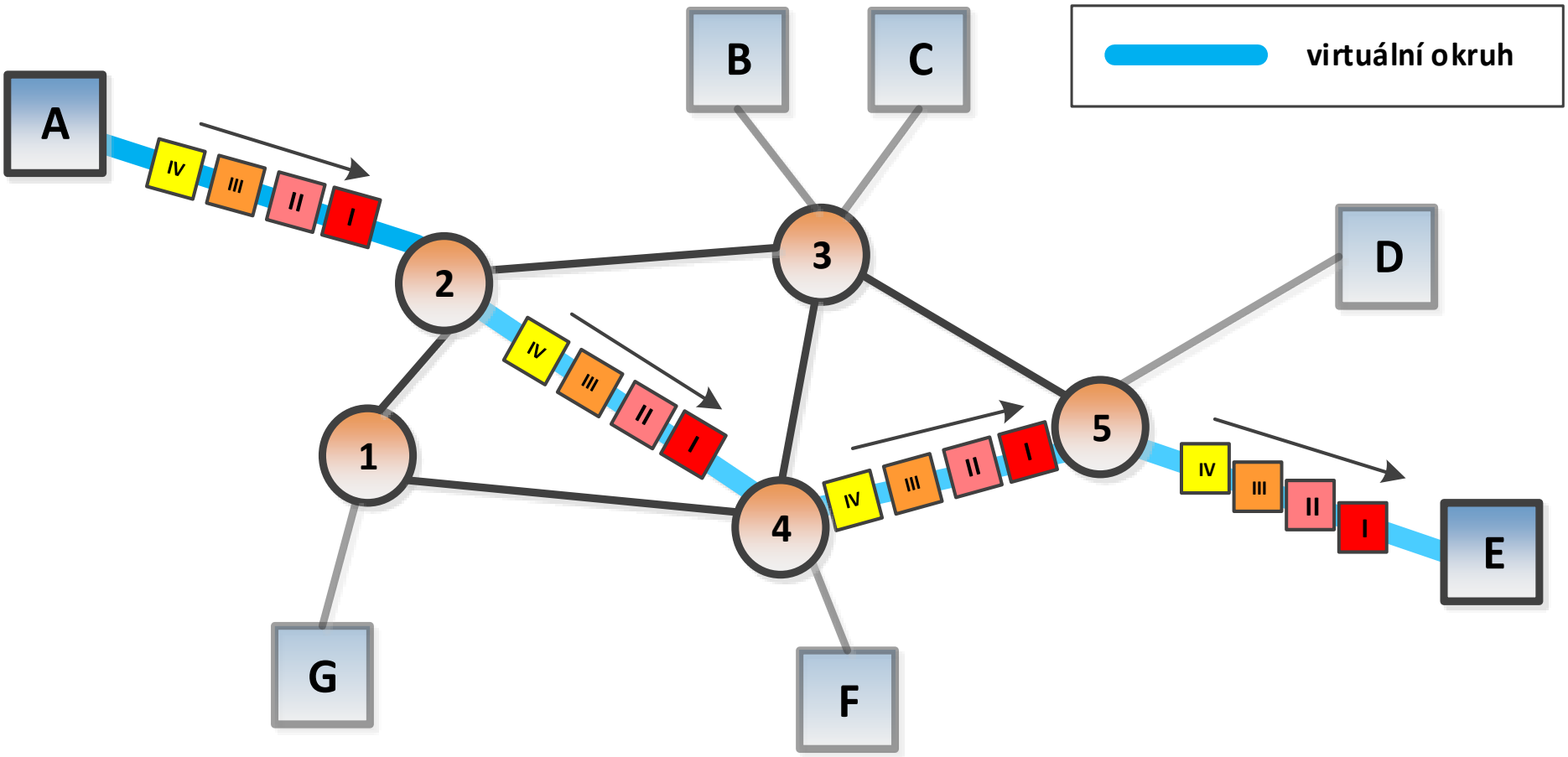
Techniky přepojování paketů

- síťové spojení – prostředky přenosu mezi transportními jednotkami
- dva způsoby přepojování paketů
  - **služby se spojením** (*Connection-Oriented Network Services*)
  - **služby bez spojení** (*ConnectionLess Network Services*)

Služba se spojením

- přenos paketů, ale určitá forma navazování spojení
- méně časté na síťové vrstvě
- zpravidla pakety obsahují identifikátor toku (*flow label*)
  - umožňuje identifikovat související pakety a zasílat je stejným směrem
- tzv. služba **virtuálních okruhů**
  - síťová vrstva se snaží poskytovat bezchybný kanál dodržující pořadí datových jednotek při přenosu
  - **dva druhy**
    - **dočasný virtuální okruh** (SVC = *Switched Virtual Connection*)
      - tři fáze spojení: příprava, udržení a ukončení
      - nadefinováno pouze na dobu konkrétního přenosu
    - **pevný virtuální okruh** (PVC = *Permanent Virtual Connection*)
      - spojení sestaveno dlouhodobě
      - stabilně nadefinováno i v komunikačních uzlech
      - tento kanál nemůže být dále využit pro jiného uživatele

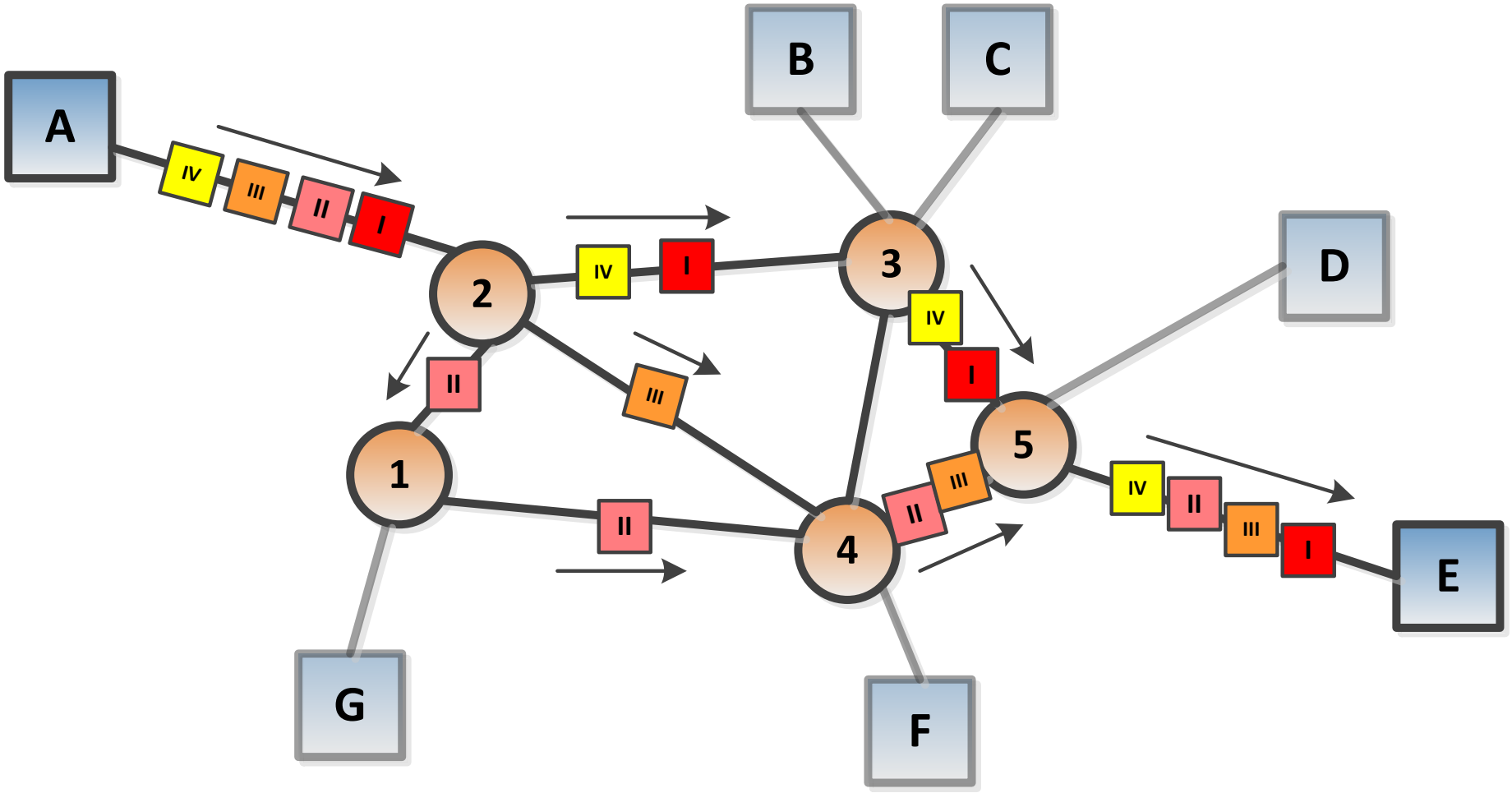
Služba se spojením



Služba bez spojení

- každý paket nezávislou jednotkou
- na síťové vrstvě nejčastější
- opatřen cílovou adresou
- datagramová služba
- riziko
  - změny pořadí u příjemce
  - nedoručení paketu

Služba bez spojení



Porovnání tří základních komunikačních technologií síťové vrstvy

- **Komutace okruhů**
  - Vyhrazená přenosová cesta
  - Průběžný přenos dat
  - Dostatečně rychlé pro interaktivní komunikaci
  - Zprávy nejsou uchovávány v síti
  - Cesta se sestavuje jednou pro celou délku spojení
  - Zpoždění při sestavování spojení, nepatrné přenosové zpoždění
  - Obsazovací signál, jestliže volaná stanice je obsazena
  - Přetížení sítě smí blokovat zřízení cesty, ale neomezuje již zřízená spojení
  - Uživatelská ochrana pro případy ztráty zprávy při přenosu
  - Pevná šířka přenosového pásma
  - Nevyžaduje záhlaví po sestavení spojení
  - Klasické telekomunikace (komutace okruhů)

Porovnání tří základních komunikačních technik síťové vrstvy

- **Služby s (virtuálním) spojením (komutace buněk)**
  - Není vyhrazena zvláštní přenosová cesta
  - Přenos dat v paketech
  - Dostatečně rychlé pro interaktivní komunikaci
  - Pakety jsou uchovány do jejich předání příjemci
  - Směrování se provádí jednou pro celé spojení
  - Zpoždění při sestavování spojení, zpoždění při přenosu každého paketu
  - Odesílatel je informován, jestliže spojení je odmítnuto
  - Přetížení smí blokovat sestavení spojení, zvyšuje zpoždění paketu v síti
  - Síť je zodpovědná za posloupnost přenášených paketů
  - Dynamické přidělování šířky pásma
  - Každý paket musí obsahovat záhlaví s adresou cíle

Porovnání tří základních komunikačních technik síťové vrstvy

- **Služby bez spojení (komutace paketů)**
  - Není vyhrazena zvláštní přenosová cesta
  - Přenos dat v paketech
  - Dostatečně rychlé pro interaktivní komunikaci
  - Pakety smí být uchovány do jejich předání příjemci
  - Směrovací procedury jsou prováděny pro každý paket zvlášť
  - Zpoždění přenosu paketu
  - Odesílatel smí být informován o tom, že paket nebyl předán
  - Přetížení zvyšuje zpoždění paketů v síti
  - Síť je odpovědná za jednotlivé pakety
  - Dynamické přidělování šířky pásma (možnost priorit)
  - Každý paket musí obsahovat záhlaví s adresou cíle
  - Komutace paketů (většina současných datových sítí)

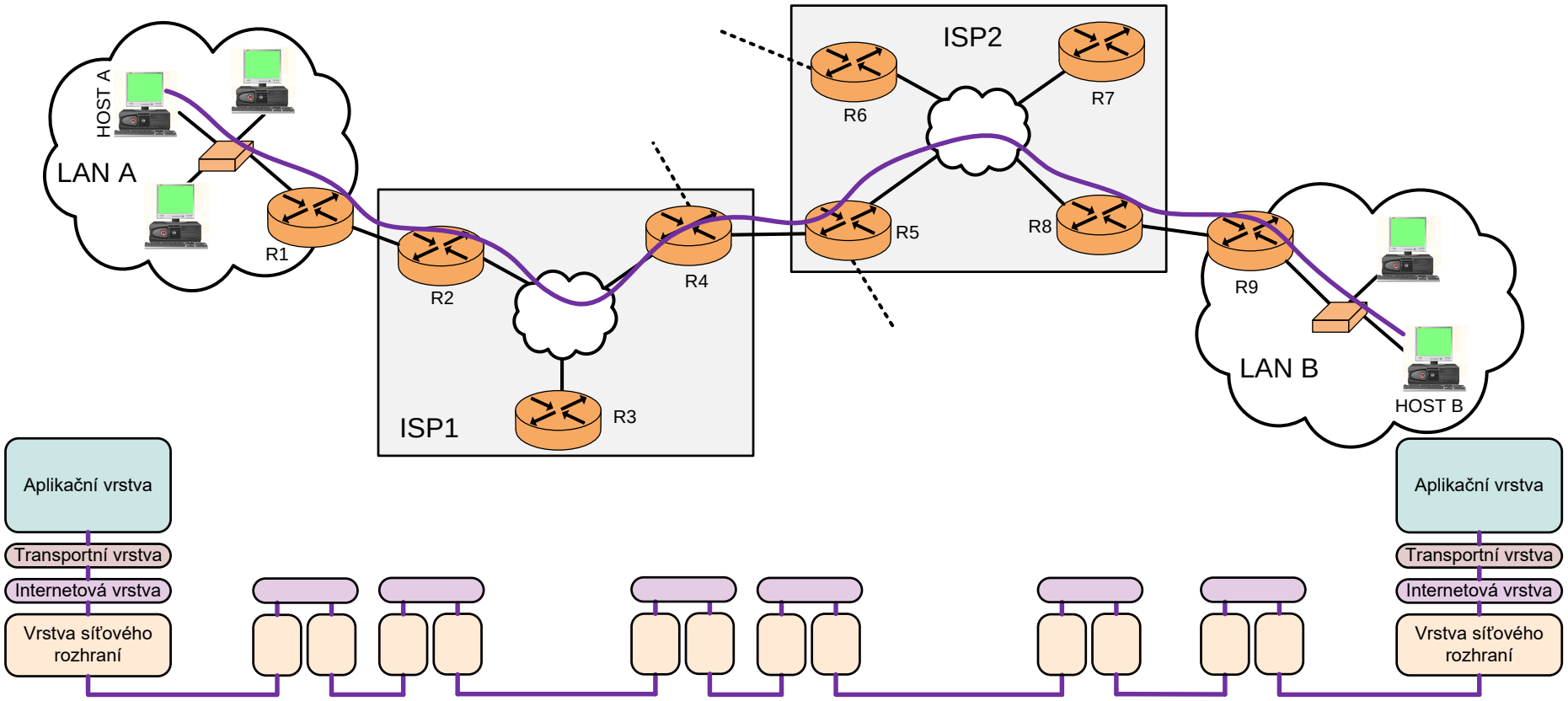
Vliv velikosti paketu na přepojování

- velikost paketu velmi důležitá, vliv na zpoždění
- malý paket
  - rychlé předávání komunikační sítí
  - problém délky záhlaví a efektivity (poměr k délce dat), propustnost
- **tři základní druhy zpoždění paketové sítě** – ovlivněny velikostí paketu
  - **zpoždění dané šířením signálu** dopad zejména při komunikaci na velké vzdálenosti
  - **doba vysílání**
    - doba nutná k odeslání paketu z uzlu
  - **zpoždění v uzlu**
    - doba nutná pro zpracování paketu v uzlu

SLUŽBY SÍŤOVÉ VRSTVY

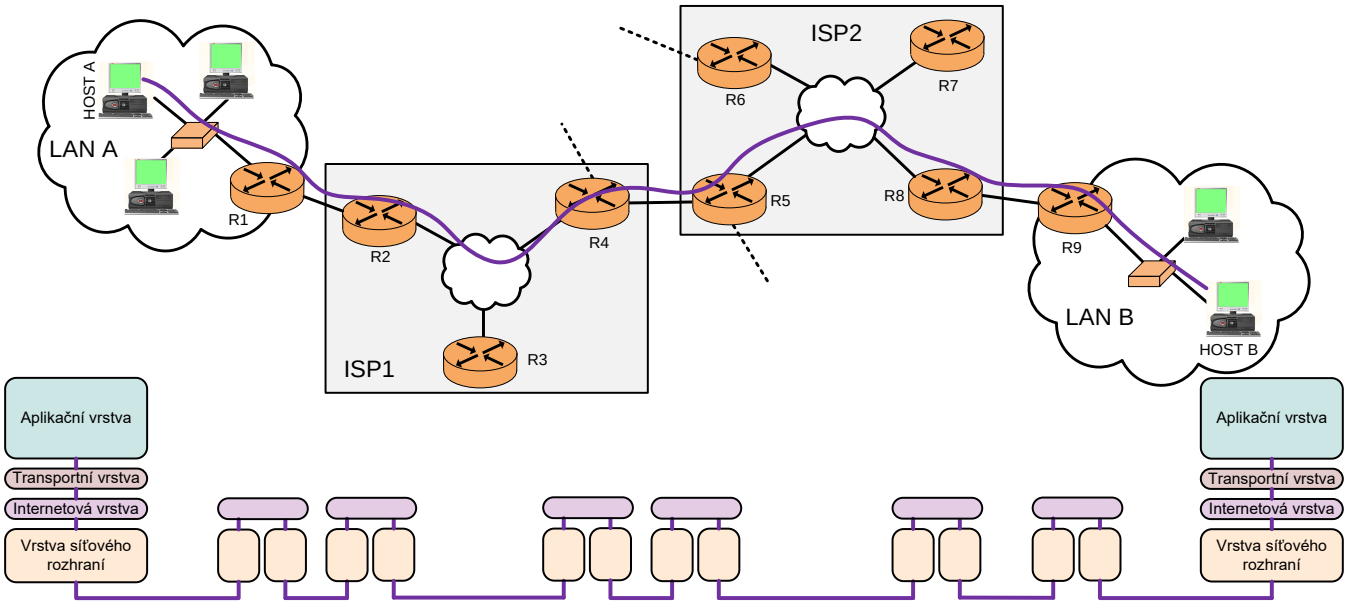
Úvod do služeb síťové vrstvy

- Komunikace mezi Host A (LAN A) a Host B (LAN B)



Úvod do služeb síťové vrstvy

- Komunikace mezi Host A (LAN A) a Host B (LAN B)
  - všechny vrstvy modelu aktivní pouze na koncích komunikace
  - v mezilehlých uzlech síťová a nižší vrstvy
  - problematika první míle z pohledu síťové vrstvy pominuta

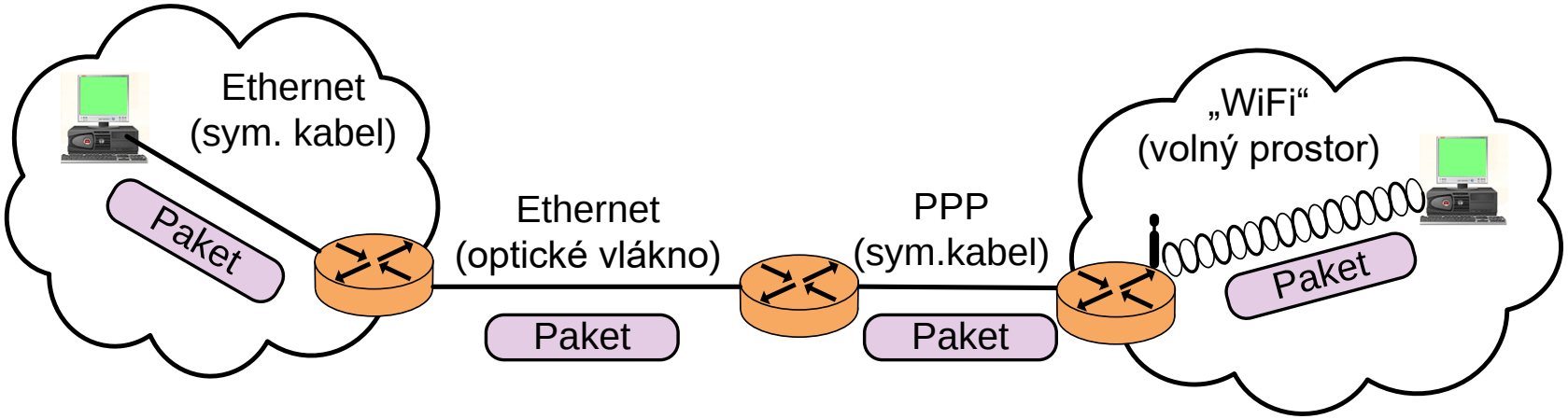


Účel výchozí brány

- komunikace v rámci sítě či podsítě
  - přímo, teoreticky bez síťové vrstvy
- komunikace vně
  - přes zprostředkovatele
  - výchozí brána (směrovač)
    - propojuje sítě
    - usnadňuje existenci koncovým stanicím
    - potřebuje znát adresy dalších skoků

Nezávislost síťové vrstvy na přenosové technologii

- síťová vrstva do určité míry nezávislá na konkrétní přenosové technologii
- fungování protokolů síťové vrstvy (nejčastěji IPv4 a IPv6) téměř vždy stejné
- konkrétní jednotka síťové vrstvy (paket) v nezměněné podobě přenášena
- datagram vždy zapouzdřen za pomocí rámce dané spojové vrstvy



Logické adresování

- přenos mezi koncovými stanicemi, vyžaduje univerzální identifikační prostředek jednotlivých uzlů
- logické adresy
  - označovány jako
    - síťové adresy
    - IP adresy
  - slouží ke globální identifikaci daného uzlu
  - přidělovány z určitého rozsahu
  - více později

Základní služby síťové vrstvy z pohledu zdrojové stanice

- **vytváření paketů**
  - zapouzdření jednotky vyšší vrstvy do datagramu
  - přidání záhlaví s odpovídajícími údaji
- **vyhledávání logické adresy dalšího uzlu směrem k cíli**
  - paket prochází přes mezilehlé sítě, nutné dohledat další skok trasy
  - proces směrování a směrovací tabulka
- **vyhledání linkové adresy tohoto uzlu**
  - doručení paketů do dalšího uzlu není úlohou síťové vrstvy, ale vrstvy spojové
  - spojová vrstva potřebuje znát linkovou adresu dalšího skoku, adresu zjišťuje vrstva síťová
- **rozdělení datagramu na menší jednotky**
  - pokud je nezbytné
  - pokud síťový protokol povoluje
  - rozdělení datagramu na fragmenty dle maximální povolené velikosti daného prostředí

Základní služby síťové vrstvy na směrovači

- dvě spojové vrstvy (příchozí a odchozí kanál)
- kontrola bezchybnosti přenosu paketu
- vyhledávání logické adresy dalšího uzlu směrem k cíli
  - dohledání dalšího skoku trasy
  - proces směrování a směrovací tabulka
- vyhledání linkové adresy tohoto uzlu
- rozdělení datagramu na menší jednotky

Základní služby síťové vrstvy z pohledu cílové stanice

- kontrola bezchybnosti přenosu paketu
- seskládání datagramu z jeho fragmentů
  - pokud došlo po trase k rozdělení původního paketu
- předání transportní vrstvě

Další důležité služby síťové vrstvy

- zabezpečeny např. přídavnými protokoly
- některé nemusí být implementovány
- či souvisí více se službami na vyšších vrstvách
- jsou to
  - **řízení chybových stavů** (*error control*)
  - **řízení toku dat** (*flow control*)
  - **řízení provozu sítě v případě zahlcení** (*congestion control*)
  - **kvalita služeb** (*quality of service* = QoS)
  - **směrování** (*routing*)
  - **bezpečnost** (*security*)

Další důležité služby síťové vrstvy

- **řízení chybových stavů**
  - pokročilejší oprava chyb a ztrát jednotek
  - může být zabezpečeno
    - spojovou vrstvou
    - či řešeno na síťové vrstvě
  - běžně pouze jednoduché řízení v IP sítích
    - ICMP (*Internet Control Message Protocol*) či ICMPv6
- **řízení toku dat**
  - snaha o nezahlcení přijímací strany
  - běžně síťová vrstva tuto problematiku přímo neřeší
  - u koncové komunikace problém spadá do vyšší vrstvy

Další důležité služby síťové vrstvy

- **řízení provozu sítě v případě zahlcení**
  - významné když v síti příliš vysoké množství paketů
  - směrovače mohou začít zahazovat vybrané pakety
    - možné zlepšení situace × vyšší mechanizmy
  - liší se podle toho, zda je přenos v síti provozován
    - bez spojení
      - nutné nějakým způsobem informovat odesilatele paketů, že má zpomalit vysílání
      - forma signalizace, není běžné
      - využití protokolu ICMP, tzv. škrtící paket (*choke packet*)
      - nebo rozlišování paketů z hlediska jejich důležitosti pomocí značky v záhlaví paketu
    - se spojením
      - situace o něco snazší
      - dohodnutí vhodných parametry, přenos bez zahlcení

Další důležité služby síťové vrstvy

- **kvalita služeb**
  - vyřešení problému, jak zabezpečit rychlou a dostatečně kvalitní výměnu dat u aplikací, které ji vyžadují
    - hovory
    - videokonference
    - obecně systémy přenosu v reálném čase
  - typicky řešena na vyšší vrstvě
- **směrování**
  - směrovač může dynamicky zjišťovat informace o vzdálených sítích
  - zpravidla využívány speciální protokoly (směrovací)
    - řazeny do síťové nebo vyšší vrstvy
- **bezpečnost**
  - holá síťová vrstva bez zabezpečení
  - vyšší vrstvy × řešení IPsec

Dělení služeb síťové vrstvy dle vrstvy využívání výsledků

- služby uvnitř síťové vrstvy
  - ke splnění funkcí, které jsou vyšší vrstvou očekávány
- služby poskytované transportní vrstvě

Služby síťové vrstvy poskytované transportní vrstvě

- **přenos datových jednotek**
  - z pohledu transportní vrstvy transparentní
- **výběr kvality služeb**
  - pokud je implementováno
  - kvalita služeb definována parametry
    - chybovost, dostupnost služby, spolehlivost, propustnost, zpoždění
- **výběr typu síťového spojení**
  - pokud existuje více variant
    - se spojením nebo bez spojení
- **oznamování chyb**
  - neopravených síťovou a nižšími vrstvami
- **dodržení pořadí datových jednotek**
  - sledování pořadí paketů a případně přeuspořádání před předáním
- **řízení toku dat**
  - dle pokynů transportní vrstvy úprava rychlosti přenosu

Služby uvnitř síťové vrstvy

- **směrování**
  - přepojování mezi různými sítěmi
- **realizace síťového spojení**
  - pomocí protokolů na spojové úrovni
  - možný multiplexing více síťových spojení
- **fragmentace a defragmentace**
  - rozdělování a znovu seskládání jednotek z důvodů přílišné velikosti
- **detekce chyb**
  - kontrola kvality síťového spojení
- **zotavení se z chyb**
  - mechanizmy opakovaných přenosů na této úrovni
  - pokud je implementováno

Služby uvnitř síťové vrstvy

- **řízení síťové vrstvy**
  - předávání chybových a řídících zpráv mezi entitami síťové vrstvy
  - typicky pomocí protokolu ICMP nebo i směrovacích protokolů
  - např.:
    - test dosažitelnosti uzlu
    - informace o nedoručitelnosti datagramu
    - žádost o zpomalení vysílání datagramů
    - zpráva o zničení datagramu z důvodů vypršení doby života
    - detekce nesprávného záhlaví datagramu
    - žádost o opravu směrovací tabulky – informace o změnách v propojení sítě

Úloha síťové vrstvy s IP protokolem

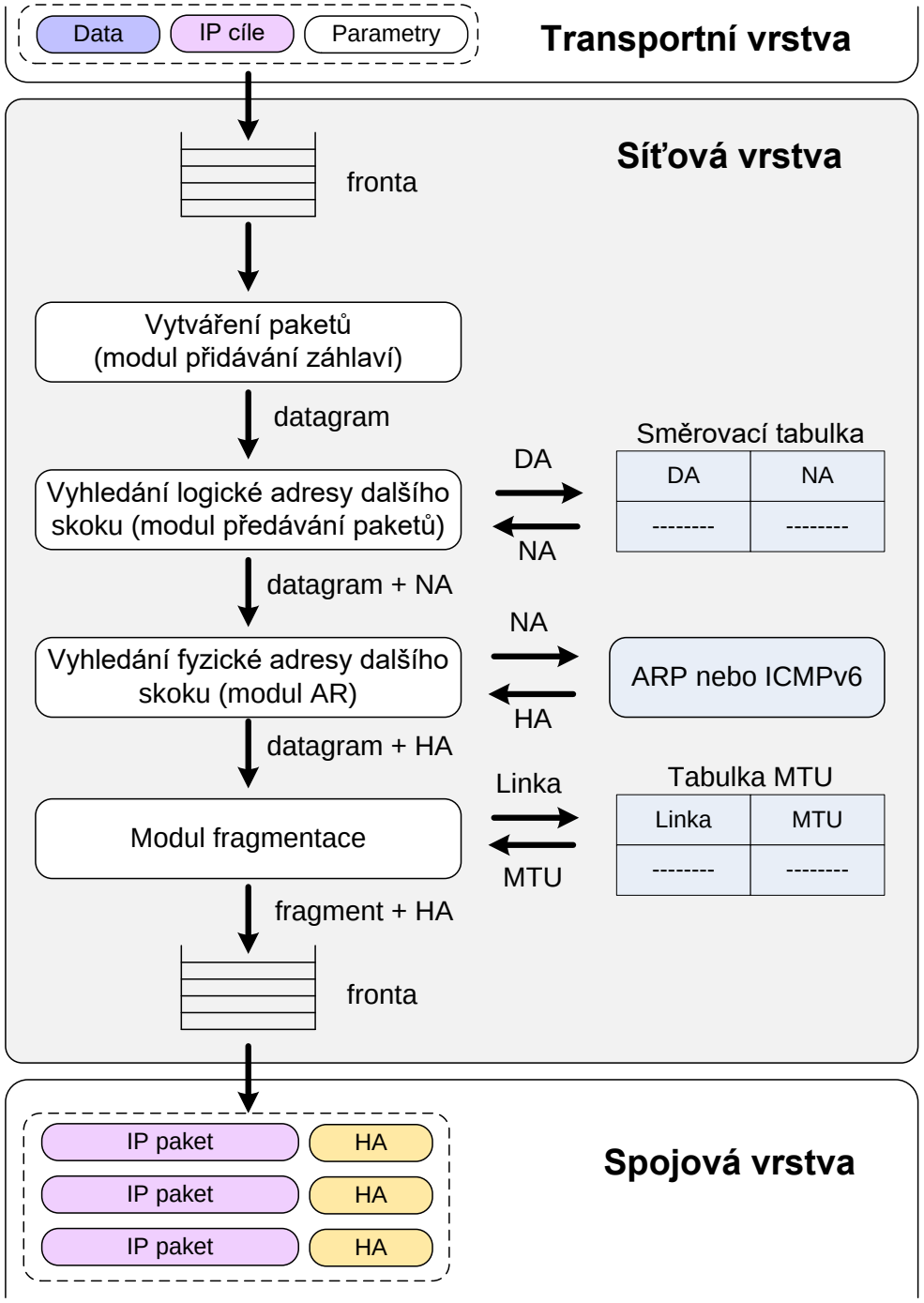
- IP protokol hlavním protokolem síťové vrstvy sady TCP/IP
- síťová vrstva
  - řešení problematiky směrování
  - iluze homogenní sítě × vzájemné propojení
  - řešení odlišností jednotlivých sítí
    - odstínitelné problémy
      - různý formát rámce
      - různý charakter poskytovaných služeb
    - problémy, které nelze odstínit
      - různá maximální délka rámce
      - různé linkové adresy

Úloha síťové vrstvy s IP protokolem

- Jednotná abstrakce utvářená síťovou vrstvou s IP protokolem
  - **způsob adresování** (IP adresy)
    - každý uzel má svoji unikátní adresu
    - z pohledu vyšších vrstev lineární
    - z pohledu síťové vrstvy dvousložková
      - adresa sítě
      - adresa stanice v rámci sítě
    - abstraktní adresy musí být vždy převedeny na linkové
  - **formát datových paketů** (IP datagramy)
    - jednotný tvar na síťové vrstvě
    - přenášeny v rámcích spojové vrstvy
  - **nespolehlivá a nespojovaná přenosová služba**
    - nezávisle na charakteru spojové vrstvy
    - dostupná všude
    - implementace spojované služby možná na vyšší vrstvě

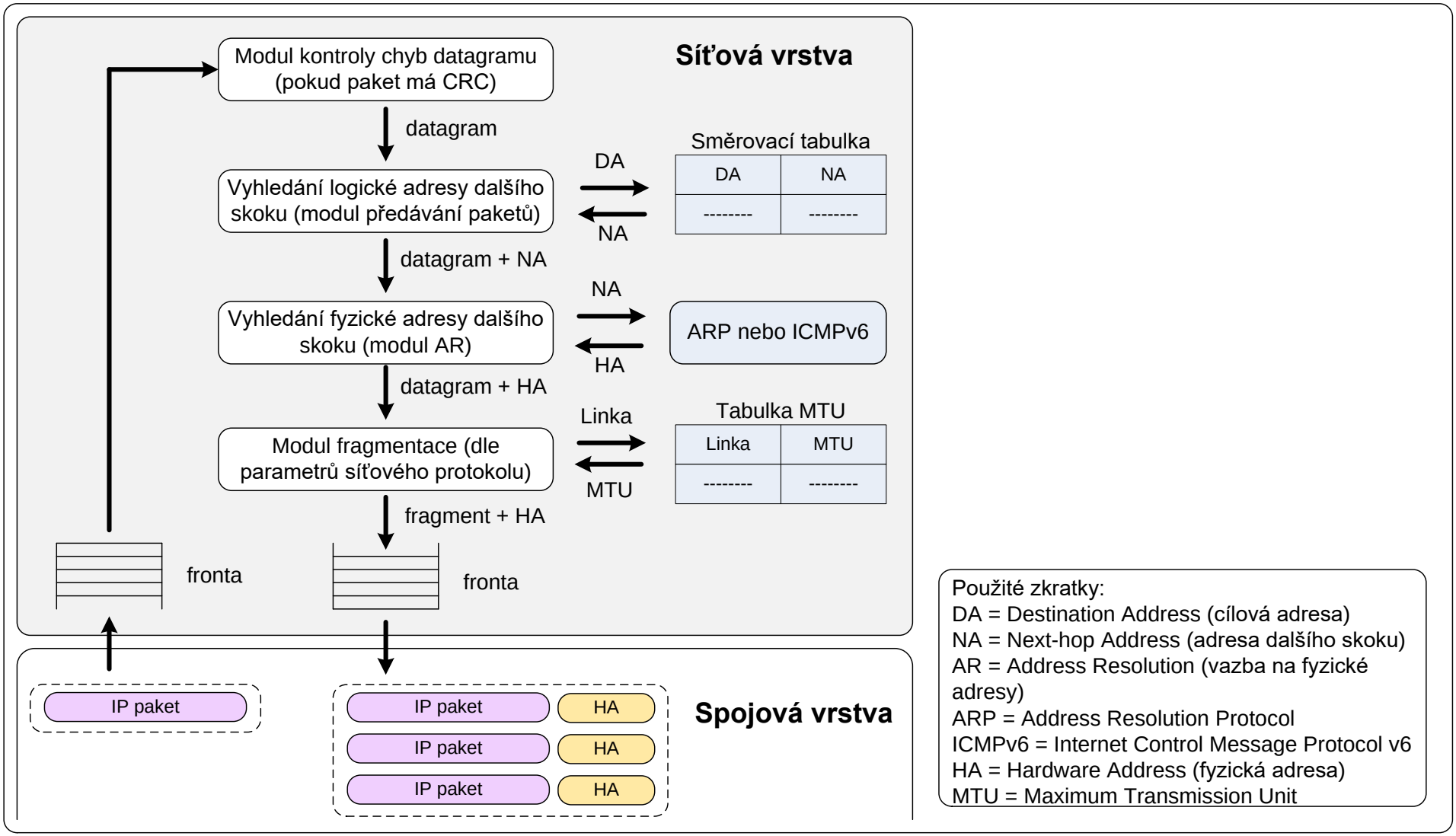
Struktura síťové vrstvy s IP protokolem – zdroj

- zobrazen pouze průchod při odesílání paketu
- návaznost na dvě sousední vrstvy
- hlavní zajišťované funkce



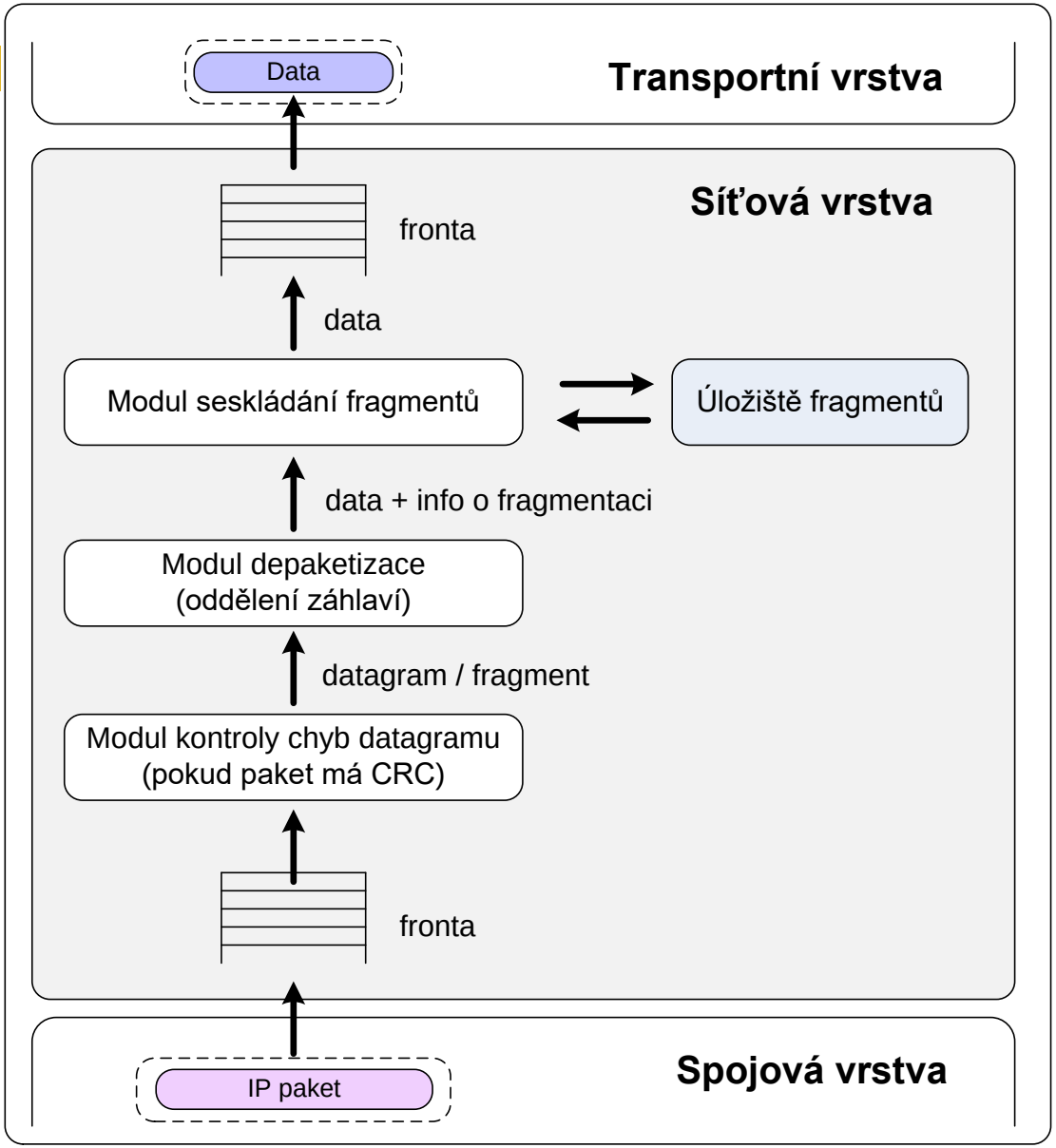
Použité zkratky:
DA = Destination Address (cílová adresa)
NA = Next-hop Address (adresa dalšího skoku)
AR = Address Resolution (vazba na fyzické adresy)
ARP = Address Resolution Protocol
ICMPv6 = Internet Control Message Protocol v6
HA = Hardware Address (fyzická adresa)
MTU = Maximum Transmission Unit

Struktura síťové vrstvy s IP protokolem – mezilehlý uzel (směrovač)



Použité zkratky:
DA = Destination Address (cílová adresa)
NA = Next-hop Address (adresa dalšího skoku)
AR = Address Resolution (vazba na fyzické adresy)
ARP = Address Resolution Protocol
ICMPv6 = Internet Control Message Protocol v6
HA = Hardware Address (fyzická adresa)
MTU = Maximum Transmission Unit

Struktura síťové vrstvy s IP protokolem – příjemce



ADRESY SÍŤOVÉ VRSTVY U IPV4 PROTOKOLU

Úvod do adresování v IPv4

- TCP/IP – každé zařízení *unikátní* IP adresu (IPv4)
- zařízení se síťovou vrstvou
- více rozhraní – více adres
- IPv4 adresa má 32 bitů = 4 bajty
- adresní prostor (*address space*)
  - 2^{32} = 4 294 967 296
  - reálně nižší počet

Přidělování IP adres

- Internet vyvíjen formou otevřené spolupráce, množství organizací
- IANA (*Internet Assigned Numbers Authority*)
  - podčást ICANN (*Internet Corporation for Assigned Names and Numbers*)
  - technický správce, přidělování a správa různých veličin
  - spravuje systém DNS
    - administrace tzv. DNS root zóny (.)
    - provozuje domény .int a .arpa
  - **správa a přidělování IP (v4 a v6) adres**
  - správa a přidělování čísel autonomních systémů (větších Internetových sítí)
  - správa registru protokolů ve spolupráci s IETF (*Internet Engineering Task Force*)

Přidělování IP adres

- Zastoupení v jednotlivých regionech – **RIR** (*Regional Internet Registry*)
  - AFRINIC (*African Network Information Center*) – Afrika
  - APNIC (*Asia Pacific Network Information Centre*) – Asie a Pacifik
  - ARIN (*American Registry for Internet Numbers*) – Serverní Amerika
  - LACNIC (*Latin American and Caribbean Internet Addresses Registry*) – Latinská Amerika
  - **RIPE NCC** (*Réseaux IP Européens Network Coordination Centre*) – Evropa a Blízký východ
- V regionech organizace označované jako **LIR** (*Local Internet Registry*)
  - komunikují přímo s koncovými zákazníky
  - získání adresního prostoru IP
  - Seznam LIR působících v ČR https://www.ripe.net/membership/indices/CZ.html

Zápis IP adres

- počítače – binární reprezentace (celá kladná dvojková čísla)
- lidé – tečkovaná desítková notace (*dotted decimal notation*)
  - rozdělení na bajty
  - převedení na desítkové číslo (0 – 255)
  - oddělení tečkami
- Př.:
  - 10010011 11100101 10010111 00000001 (2)

    ×
  - 147.229.151.1 (10)
  - hexadecimální zápis možný, ale využíván až u IPv6 adres

Maska sítě

- IP adresy dvojsložkové
  - adresa sítě — *x* bitů
  - adresa stanice v rámci sítě — (32 – *x*) bitů
- *x* není dle IP adresy známo, musí být stanoveno jinak
- *x* bitů souvisle zleva adresou sítě, zbytek adresa stanice
- Maska sítě
  - označení bitů pro adresu sítě jako „1“
  - bity pro adresu stanice jako „0“
  - délka 32 bitů
  - zápis obdobně jako IP adresa
- Př.:
  - 147.229.151.1 — IP (10) (např. 16 bitů adresa sítě)
  - 10010011 11100101 | 10010111 00000001 — IP (2)
  - 11111111 11111111 00000000 00000000 — maska (2)
  - 255.255.0.0 — maska (10)

Maska sítě

- délka prefixu
  - počet jedniček binární reprezentace masky sítě
  - stručnější zápis
  - psáno za IP adresu, formát: /x
  - př.:
    - 147.229.151.1 255.255.0.0
    - 147.229.151.1 / 16
- *wildcard* maska
  - převrácená hodnota síťové masky (NOT)
  - př.:
    - 255.255.0.0 — maska (10)
    - 11111111 11111111 00000000 00000000 — maska (2)
    - 00000000 00000000 11111111 11111111 — wildcard (2)
    - 0.0.255.255 — wildcard (10)

Rozsah adres, adresa sítě a všesměrová adresa

- praxe často pracuje s rozsahy adres, mocniny 2
- **adresa sítě** (*network address* × *subnet address*)
  - první adresa rozsahu
  - není přiřazena konkrétnímu uzlu
  - využívána pro směrování
- **všesměrová adresa** (*broadcast address*)
  - poslední adresa rozsahu
  - pakety odeslány všem stanicím dané sítě
- **adresy stanic**
  - vše mezi adresou sítě a všesměrovou adresou
  - rozsah dán počtem bitů pro adresy stanic
  - př.:
    - 16 bitů pro adresy stanic
    - $(2^{16} - 2) = 65\,534$ unikátních adres

Rozsah adres, adresa sítě a všesměrová adresa

- **výpočet adresy sítě**
  - na základě znalosti libovolné IP a masky sítě
  - binární operace AND (po bitech)
  - př.:
    - 147.229.230.55 IP (10)
    - 255.255.0.0 maska (10)
    - 10010011 11100101 11100110 00110111 IP (2)
    - 11111111 11111111 00000000 00000000 maska (2)
    - 10010011 11100101 00000000 00000000 adresa sítě (2)
    - 147.229.0.0 adresa sítě (10)

Rozsah adres, adresa sítě a všesměrová adresa

- **výpočet všesměrové adresy**
  - na základě znalosti libovolné IP a wildcard masky
  - binární operace OR (po bitech)
  - př.:
    - 147.229.230.55 IP (10)
    - 0.0.255.255 wildcard (10)
    - `10010011 11100101 11100110 00110111` IP (2)
    - `00000000 00000000 11111111 11111111` wildcard (2)
    - `10010011 11100101 11111111 11111111` broadcast (2)
    - 147.229.255.255 broadcast (10)

Třídy IPv4 adres

- **třídní adresování** (*classful addressing*)
  - původní koncepce IP adres
  - dělení adresního prostoru na pevně dané bloky
  - problematické, postupně odstraněno
  - důležité znát, zakořeněno v protokolech (směrování)
  - podle prvních bitů adresy definována třída
- **beztřídní adresování** (*classless addressing*)
  - to, co bylo dosud popisováno
  - nutná existence masky
  - *libovolně* veliké rozsahy

Třídy IPv4 adres – historické dělení

Třída	Rozsah prvního oktetu adresy (dekadicky)	Dělení adresy na adresu Sítě a Hosta	Standardní maska sítě (dekadicky)	Délka prefixu sítě	Počet možných sítí / hostů na jednu síť
A	0 – 127	S.H.H.H	255.0.0.0	/8	128 / 16 777 214
B	128 – 191	S.S.H.H	255.255.0.0	/16	16 383 / 65 534
C	192 – 223	S.S.S.H	255.255.255.0	/24	2 097 150 / 254
D	224 – 239	-	Multicastové adresy		
E	240 – 255	-	Experimentální adresy		

Třídy IPv4 adres

- **třídy**
  - **A**
    - velké sítě (příliš velké)
    - 50 % rozsahu
  - **B**
    - střední sítě
    - 25 % rozsahu
  - **C**
    - malé sítě (příliš malé)
    - 12,5 % rozsahu
  - problémem příliš hrubé a neefektivní dělení
  - výhoda – z každé IP adresy jasné kolik bitů na co využito
  - původně přidělovány rozsahy třídně
  - následně jemnější dělení –> podsíťování

Podsíťování (*subnetting*)

- IP adresa
  - původně dvojsložková adresa
    - adresa sítě
    - adresa stanice
  - s podsíťováním trojsložková
    - adresa sítě (nezměněna)
    - adresa stanice rozdělena na
      - adresa podsítě
      - adresa stanice

n bitů	m bitů	$(32 - n - m)$ bitů
adresa sítě	adresa podsítě	adresy stanic

Podsíťování

- výhody
  - možnost rozdělit vlastní blok na menší části
    - vytvoření menších jednotek – podsítí
    - usnadnění správy
  - možnost přidělovat variabilně dlouhé bloky
    - dle potřeb konkrétní sítě
- nevýhody
  - musíme pracovat i s maskou sítě (maskou podsítě)
    - vymezení hranic rozsahu
  - vyšší počet sítí = vyšší počet směrovacích záznamů
    - zpomalení směrování
  - problematické pojmosloví adresa sítě × adresa podsítě
- pravidla
  - využívány bity v souvislé řadě zleva za adresou sítě
  - maska sítě a podsítě stejný formát
  - počet bitů není úplně libovolný
  - musí v rozsahu zbýt bity pro adresy stanic (min. 2 bity)

Možnosti podsíťování

Třída dělené sítě	Délka prefixu dělené sítě	Pořadí bitů použitelných původně pro adresaci stanice	Pořadí bitů použitelných pro adresu podsítě	Možná délka prefixu podsítě	Celkem bitů použitelných pro podsítě	Maximální možný počet podsítí v rámci jedné původní sítě
A	/8	9. – 32.	9. – 30.	/9 – /30	22	2^{22}
B	/16	17. – 32.	17. – 30.	/17 – /30	14	2^{14}
C	/24	25. – 32.	25. – 30.	/25 – /30	6	2^{6}

Podsíťování – příklad

- Původní adresa sítě: 193.1.1.0
- Adresa sítě binárně: 11000001 00000001 00000001 | 00000000
- Maska sítě binárně: 11111111 11111111 11111111 00000000
- Maska sítě (10): 255.255.255.0
- Délka prefixu (počet jedniček v masce sítě): 24
- Adresu sítě lze zapsat 193.1.1.0 / 24 – běžný způsob zápisu
- Počet možných uzlů je 254

Podsíťování – příklad

- Původní adresa sítě: 193.1.1.0
- Adresa sítě binárně: 11000001 00000001 00000001 | 00000000
- Maska sítě binárně: 11111111 11111111 11111111 00000000
- Maska sítě (10): 255.255.255.0
- Délka prefixu (počet jedniček v masce sítě): 24
- Adresu sítě lze zapsat 193.1.1.0 / 24 – běžný způsob zápisu
- Počet možných uzlů je 254

Podsíťování – příklad

- Původní adresa sítě: 193.1.1.0
- Adresa sítě binárně: 11000001 00000001 00000001 | 00000000
- Maska sítě binárně: 11111111 11111111 11111111 00000000
- Maska sítě (10): 255.255.255.0
- Délka prefixu (počet jedniček v masce sítě): 24
- Adresu sítě lze zapsat 193.1.1.0 / 24 – běžný způsob zápisu
- Počet možných uzlů je 254

Podsíťování – příklad

- Původní adresa sítě: 193.1.1.0
- Adresa sítě binárně: 11000001 00000001 00000001 | 00000000
- Maska sítě binárně: 11111111 11111111 11111111 00000000
- Maska sítě (10): 255.255.255.0
- Délka prefixu (počet jedniček v masce sítě): 24
- Adresu sítě lze zapsat 193.1.1.0 / 24 – běžný způsob zápisu
- Počet možných uzlů je 254

Podsíťování – příklad

- Původní adresa sítě: 193.1.1.0
- Adresa sítě binárně: 11000001 00000001 00000001 | 00000000
- Maska sítě binárně: 11111111 11111111 11111111 00000000
- Maska sítě (10): 255.255.255.0
- Délka prefixu (počet jedniček v masce sítě): 24
- Adresu sítě lze zapsat 193.1.1.0 / 24 – běžný způsob zápisu
- Počet možných uzlů je 254

Podsíťování – příklad

- Původní adresa sítě: 193.1.1.0
- Adresa sítě binárně: 11000001 00000001 00000001 | 00000000
- Maska sítě binárně: 11111111 11111111 11111111 00000000
- Maska sítě (10): 255.255.255.0
- Délka prefixu (počet jedniček v masce sítě): 24
- Adresu sítě lze zapsat 193.1.1.0 / 24 – běžný způsob zápisu
- Počet možných uzlů je 254

Podsíťování – příklad

- Původní adresa sítě: 193.1.1.0
- Adresa sítě binárně: 11000001 00000001 00000001 | 00000000
- Maska sítě binárně: 11111111 11111111 11111111 00000000
- Maska sítě (10): 255.255.255.0
- Délka prefixu (počet jedniček v masce sítě): 24
- Adresu sítě lze zapsat 193.1.1.0 / 24 – běžný způsob zápisu
- Počet možných uzlů je 254

Podsíťování – příklad – vytvoření čtyř podsítí

- podSíťA: 193.1.1.0
- podSíťB: 193.1.1.64
- podSíťC: 193.1.1.128
- podSíťD: 193.1.1.192

- Adresa podSíťA (2): 11000001 00000001 00000001 00000000
- Adresa podSíťB (2): 11000001 00000001 00000001 01000000
- Adresa podSíťC (2): 11000001 00000001 00000001 10000000
- Adresa podSíťD (2): 11000001 00000001 00000001 11000000

Podsíťování – příklad – vytvoření čtyř podsítí

- podSíťA: 193.1.1.0
- podSíťB: 193.1.1.64
- podSíťC: 193.1.1.128
- podSíťD: 193.1.1.192

- Adresa podSíťA (2): 11000001 00000001 00000001 00000000
- Adresa podSíťB (2): 11000001 00000001 00000001 01000000
- Adresa podSíťC (2): 11000001 00000001 00000001 10000000
- Adresa podSíťD (2): 11000001 00000001 00000001 11000000

Podsíťování – příklad – vytvoření čtyř podsítí

- podSíťA: 193.1.1.0
- podSíťB: 193.1.1.64
- podSíťC: 193.1.1.128
- podSíťD: 193.1.1.192

- Adresa podSíťA (2): 11000001 00000001 00000001 00000000
- Adresa podSíťB (2): 11000001 00000001 00000001 01000000
- Adresa podSíťC (2): 11000001 00000001 00000001 10000000
- Adresa podSíťD (2): 11000001 00000001 00000001 11000000

Podsíťování – příklad – vytvoření čtyř podsítí

- podSíťA: 193.1.1.0
- podSíťB: 193.1.1.64
- podSíťC: 193.1.1.128
- podSíťD: 193.1.1.192

- Adresa podSíťA (2): 11000001 00000001 00000001 | 00 | 000000
- Adresa podSíťB (2): 11000001 00000001 00000001 | 01 | 000000
- Adresa podSíťC (2): 11000001 00000001 00000001 | 10 | 000000
- Adresa podSíťD (2): 11000001 00000001 00000001 | 11 | 000000

Podsíťování – příklad – vytvoření čtyř podsítí

- podSíťA: 193.1.1.0
- podSíťB: 193.1.1.64
- podSíťC: 193.1.1.128
- podSíťD: 193.1.1.192

- Adresa podSíťA (2): 11000001 00000001 00000001 | 00 | 000000
- Adresa podSíťB (2): 11000001 00000001 00000001 | 01 | 000000
- Adresa podSíťC (2): 11000001 00000001 00000001 | 10 | 000000
- Adresa podSíťD (2): 11000001 00000001 00000001 | 11 | 000000

- Maska podsítě: 11111111 11111111 11111111 **11**000000
  (u všech podsítí stejná)

Podsíťování – příklad – vytvoření čtyř podsítí

- podSíťA: 193.1.1.0
- podSíťB: 193.1.1.64
- podSíťC: 193.1.1.128
- podSíťD: 193.1.1.192

- Adresa podSíťA (2): 11000001 00000001 00000001 | 00 | 000000
- Adresa podSíťB (2): 11000001 00000001 00000001 | 01 | 000000
- Adresa podSíťC (2): 11000001 00000001 00000001 | 10 | 000000
- Adresa podSíťD (2): 11000001 00000001 00000001 | 11 | 000000

- Maska podsítě: 11111111 11111111 11111111 **11**000000
  (u všech podsítí stejná)
- Maska podsítě (10) 255.255.255.**192**

Podsíťování – příklad – vytvoření čtyř podsítí

- podSíťA: 193.1.1.0
- podSíťB: 193.1.1.64
- podSíťC: 193.1.1.128
- podSíťD: 193.1.1.192

- Adresa podSíťA (2): 11000001 00000001 00000001 | 00 | 000000
- Adresa podSíťB (2): 11000001 00000001 00000001 | 01 | 000000
- Adresa podSíťC (2): 11000001 00000001 00000001 | 10 | 000000
- Adresa podSíťD (2): 11000001 00000001 00000001 | 11 | 000000

- Maska podsítě: 11111111 11111111 11111111 **11**000000

(u všech podsítí stejná)

- Maska podsítě (10) 255.255.255.**192**

Délka prefixu: 26 (počet jedniček)

Podsíťování – příklad – vytvoření čtyř podsítí

- podSíťA: 193.1.1.0 / **26**
- podSíťB: 193.1.1.64 / **26**
- podSíťC: 193.1.1.128 / **26**
- podSíťD: 193.1.1.192 / **26**

- Adresa podSíťA (2): 11000001 00000001 00000001 00 000000
- Adresa podSíťB (2): 11000001 00000001 00000001 01 000000
- Adresa podSíťC (2): 11000001 00000001 00000001 10 000000
- Adresa podSíťD (2): 11000001 00000001 00000001 11 000000

- Maska podsítě: 11111111 11111111 11111111 **11**000000
  (u všech podsítí stejná)
- Maska podsítě (10) 255.255.255.**192**

Podsíťování – příklad – přehled vytvořených podsítí

Číslo podsítě	Adresa podsítě (první adresa rozsahu)	Maska dané podsítě	Rozsah adres použitelných pro stanice v podsíti	Počet možných stanic v podsíti	Všesměrová adresa podsítě
0	193.1.1.0	255.255.255.192	193.1.1.1 – 193.1.1.62	62	193.1.1.63
1	193.1.1.64	255.255.255.192	193.1.1.65 – 193.1.1.126	62	193.1.1.127
2	193.1.1.128	255.255.255.192	193.1.1.129 – 193.1.1.190	62	193.1.1.191
3	193.1.1.192	255.255.255.192	193.1.1.193 – 193.1.1.254	62	193.1.1.255

Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o níž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť

Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o níž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť

Logický součin (AND)

Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o níž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť

Logický součin (AND)

Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o niž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť

Logický součin (AND)

Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o níž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť

Logický součin (AND)

Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o niž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť

Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o niž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť

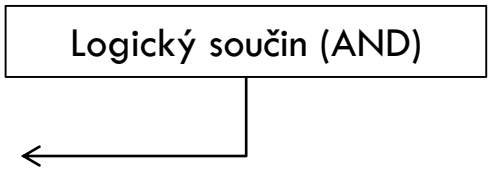
Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o níž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť

Logický součin (AND)

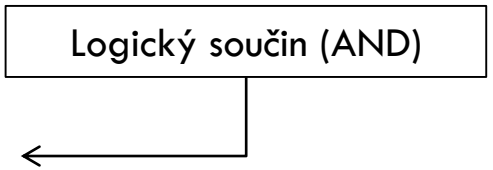
Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o níž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť



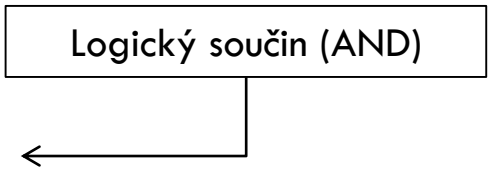
Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o níž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť



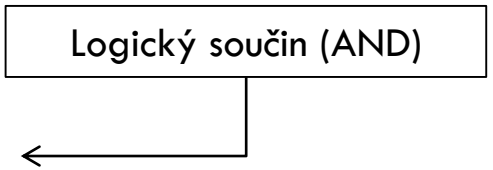
Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o níž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť



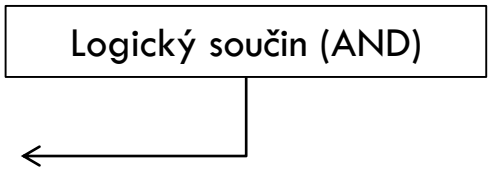
Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o niž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť



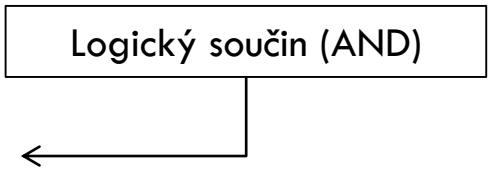
Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o niž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť



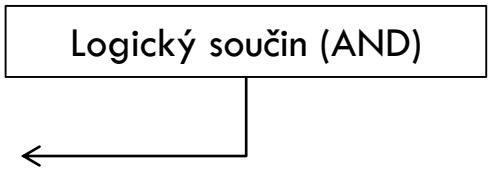
Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o niž ví, že má IP adresu 193.1.1.138
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť



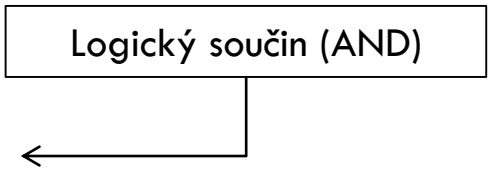
Maska sítě / podsítě – opodstatnění existence

- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o niž ví, že má IP adresu **193.1.1.138**
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť



Maska sítě / podsítě – opodstatnění existence

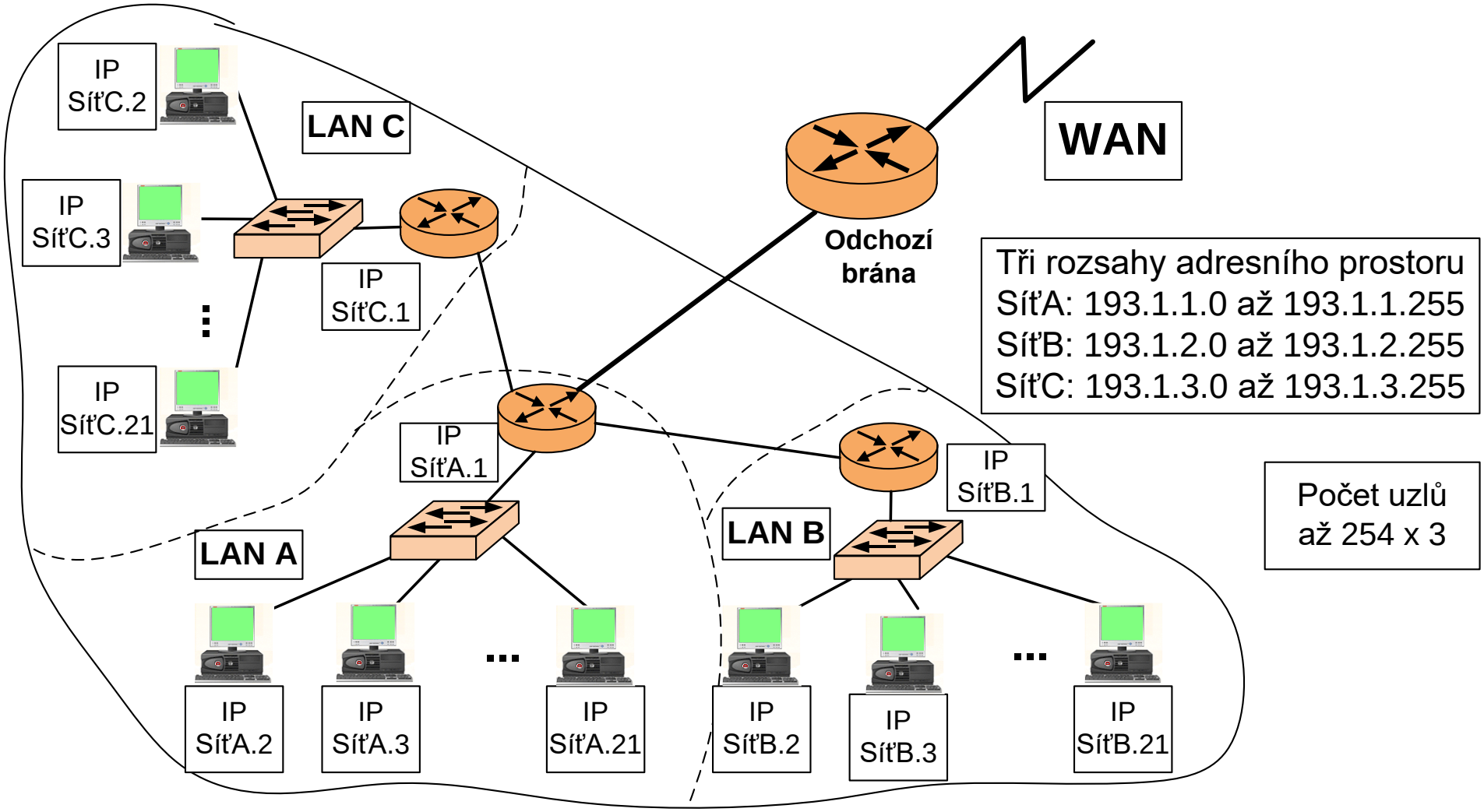
- Stanice má k dispozici parametry:
  - IP adresa 193.1.1.105
  - Maska podsítě 255.255.255.192
  - Výchozí brána 193.1.1.65
- Chce se spojit se stanicí o níž ví, že má IP adresu **193.1.1.138**
  - Je tato stanice ve stejné (pod)síti ???
  - Díky masce stanice ví v jaké (pod)síti se nachází:
  - IP (2) (poslední bajt): … 01101001
  - Maska (2) (poslední bajt): … 11000000
  - Adresa sítě (2) (poslední bajt): … 01000000
  - Adresa sítě (10) (poslední bajt) … .64
  - Broadcast adresa (2) (poslední bajt) … 01111111
  - Broadcast adresa (10) (poslední bajt) … .127
  - Rozsah podsítě: 193.1.1.64 až 193.1.1.127
  - Stanice 193.1.1.138 je tedy mimo tuto podsíť



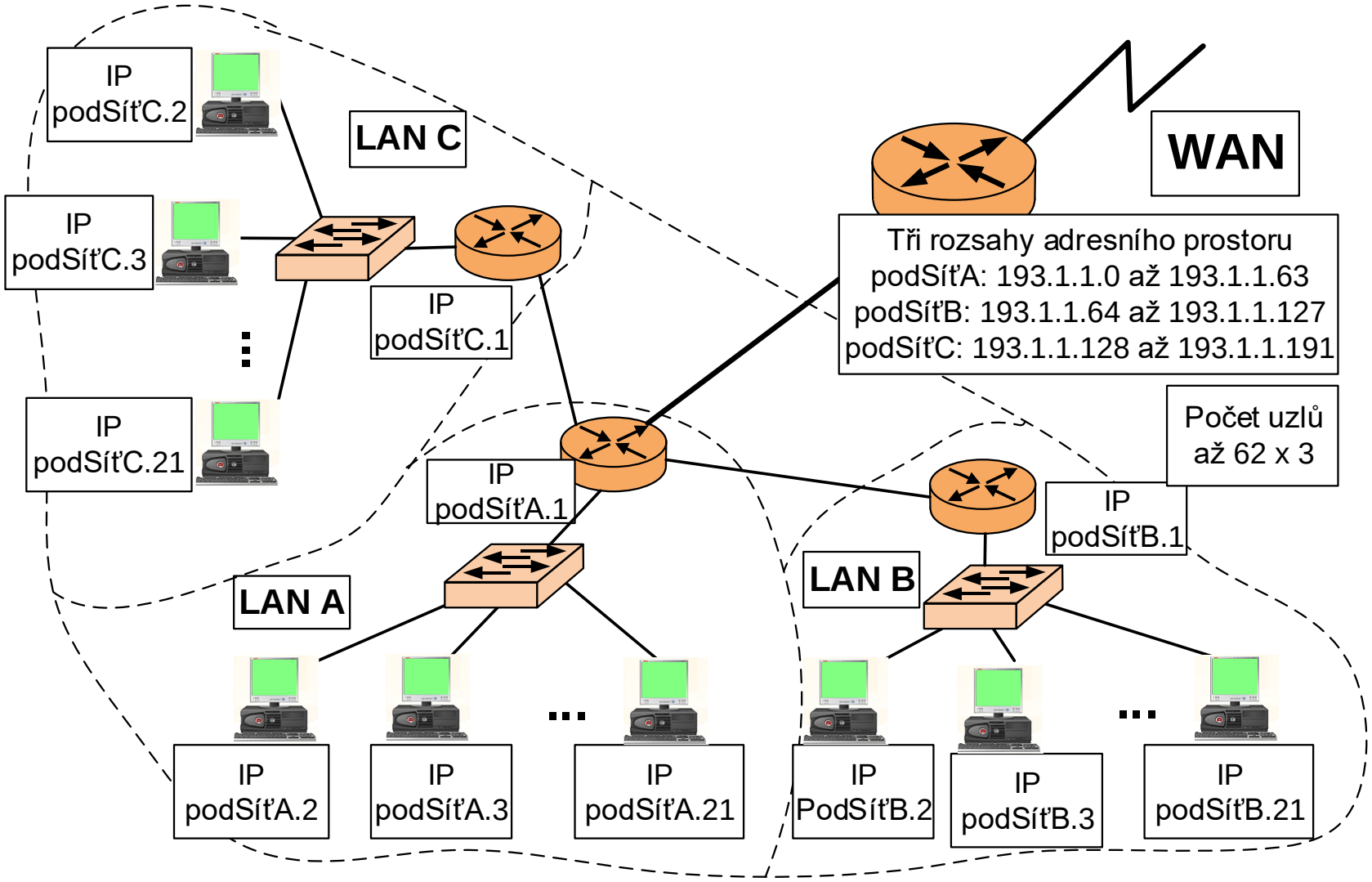
Podsíťování z jiného úhlu pohledu

- **Varianta 1 (bez podsíťování)**
  - 3 sítě á 20 stanic
  - nutné tři bloky C třídy, např.:
    - 193.1.1.0/24
    - 193.1.2.0/24
    - 193.1.3.0/24
  - nevyužito 3× 230 IP adres
- **Varianta 2 (s podsíťováním)**
  - potřebujeme cca 70 IP adres
  - postačuje jeden blok C třídy, např.:
    - 193.1.1.0/24
  - 4 podsítě, každá až 62 stanic
  - třetinové náklady

Podsíťování z jiného úhlu pohledu – bez podsíťování



Podsíťování z jiného úhlu pohledu – s podsíťováním



Beztřídní adresování, major network a supernet

- **Beztřídní adresování** (*classless addressing*)
  - původní třídy vůbec nevyužívány nebo fakticky podsíťovány
  - zpátky k dvousložkové adrese sítě (či podsítě)
    - variabilní
    - nezbytná maska

***n* bitů**	**(32 – *n*) bitů**
prefix (síť)	**suffix (stanice)**

- **Major network**
  - původní třídní adresa sítě, do které libovolná adresa spadá
  - př.:
    - síť 149.10.10.0 / 24
    - její major network 149.10.0.0 / 16
- **Supernet**
  - sloučení více major network; sumarizace či agregace
  - př.:
    - sítě 149.10.0.0 / 16 a 149.11.0.0 / 16
    - vytvořený supernet 149.10.0.0 / 15

Speciální typy IPv4 adres

- **Lokální smyčka** (*loopback*)
  - softwarová smyčka uvnitř počítače, pakety neopustí počítač
  - rozsah 127.0.0.0 / 8
  - vhodné pro meziprocesovou komunikaci, či lokální testování sady TCP/IP
- **Privátní adresy** (*private addresses*)
  - navrženy pro adresování sítí nepřipojených k Internetu
  - dnes využívány pro lokální sítě za NATem (překlad na veřejné adresy)
  - musí být unikátní pouze v rámci konkrétní sítě; jinak jsou to std IP adresy
  - nejsou směrovány Internetem; vyčleněné rozsahy
    - 10.0.0.0 / 8
      - 1 classful síť třídy A o 16 777 214 možných hostech
    - 172.16.0.0 / 16 až 172.31.0.0 / 16
      - 16 classful sítí třídy B, každá o 65 534 hostech
    - 192.168.0.0 / 24 až 192.168.255.0 / 24
      - 256 classful sítí třídy C, každá o 254 hostech

Speciální typy IPv4 adres

- **Lokální linkové adresy** (*link-local addresses*)
  - 169.254.0.0 až 169.254.255.255
  - pro případy selhání automatické konfigurace adresování (DHCP)
  - využitelné pro lokální komunikaci
  - stanice si adresy vybírají náhodně
- **Lokální identifikace stanic**
  - rozsah 0.0.0.0/8
  - 0.0.0.0/32 vyhrazena pro identifikaci stanice dosud bez IP adresy (komunikace s DHCP)
- **Lokální všesměrová adresa**
  - 255.255.255.255/32
  - pakety doručeny všem stanicím dané sítě
  - využívána opět např. pro komunikaci s DHCP
- **Další speciální bloky**
  - TEST-NET-1 192.0.2.0/24 pro příklady v textech
  - Tunely 6to4 192.88.99.0 / 24 mechanizmy přechodu na IPv6
  - mnohé další http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

Důvody a způsoby rozdělování stanic do samostatných sítí

- **způsoby členění stanic do samostatných sítí**
  - **geografie**
    - stanice geograficky v jedné lokalitě (městě, budově, patru, případně místnosti) sdruženy do jedné sítě
  - **účel**
    - rozdělení podle účelu či primárních potřeb
    - typicky rozdělení sítě dle jednotlivých oddělení společnosti
    - nezávisle na geografickém uspořádání
  - **vlastnictví**
    - základní stanice dané organizace tvoří jednu síť
    - zařízení určená pro vzdáleně připojené uživatele, druhá síť
    - hostující zařízení (typicky v bezdrátové síti), třetí síť
- vytváření nových sítí – proč nedát všechny do jedné sítě?
  - zpravidla nevýhodné

Důvody a způsoby rozdělování stanic do samostatných sítí

- **důvody členění stanic do samostatných sítí**
  - **výkonnostní**
    - příliš velká síť – může docházet k zahlcení nebo přetížení centrálních síťových prvků, případně přenosových tras
    - rozdělením do samostatných sítí, zvýšíme celkový počet síťových prvků a přenosových tras, čímž celkově zvýšíme přenosovou kapacitu systému
  - **bezpečnostní**
    - rozdělení do skupin, typicky dle vlastnictví nebo účelu, můžeme mezi těmito sítěmi snáze definovat bezpečnostní pravidla
  - **adresní**
    - se sousedy na síti komunikují stanice přímo
    - po rozdělení bude přímých sousedů méně – menší počet adres
    - menší sítě, role stanic snazší

TECHNIKY SMĚROVÁNÍ

Úvod do technik směrování

- síťová vrstva
  - transparentní přenos dat mezi transportními vrstvami
  - hledání cesty přes mezilehlé uzly = **směrování**
  - popis směrování
    - **doručování paketů** (*delivery*)
      - způsob zacházení s pakety v sítích řízených síťovou vrstvou
      - přímé doručování paketů když zdrojová a cílová stanice na stejné síti
    - **předávání paketů** (*forwarding*)
      - způsob jak je paket doručen následující stanici v řetězci od odesilatele k příjemci, dalšímu skoku přenosové trasy
      - tato funkce zpravidla považována za směrování jako takové
  - dostává od transportní vrstvy informaci o konečném příjemci
    - jednoznačná identifikace podle síťové adresy
    - následuje rozhodnutí o směru odeslání
    - předání spojové vrstvě zvoleného směru

Úvod do technik směrování

- síťová vrstva a směrování
  - vyžadovány informace o topologii sítě a adresách uzlů
  - existuje řada způsobů směrování
    - jednoduché
    - adaptabilní (přizpůsobení se aktuálním podmínkám sítě)
  - mechanizmus závislý na topologii (zásadní je redundance linek)
    - stromová topologie (jedna cesta)
    - úplný polygon (přímé spojení)
    - neúplný polygon (více alternativních cest)

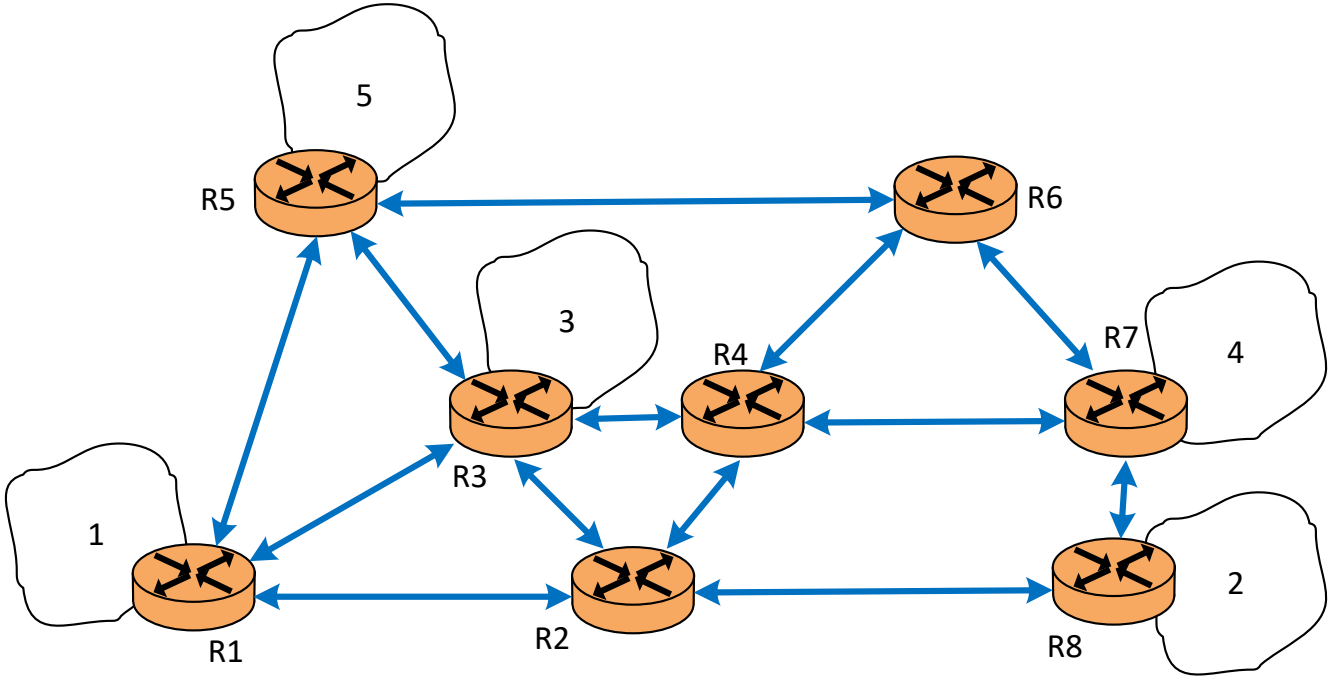
Úvod do technik směrování

- **atributy směrovacích technik a protokolů**
  - **výkonnostní kritéria**
    - množství uzlů, náklady, zpoždění a propustnost
  - **rozhodovací čas**
    - pro datagramy, virtuální obvody
  - **rozhodovací místo**
    - každý uzel, tj. distribuovaně; centrální uzel, tj. centralizovaně
  - **zdroje informací o síti**
    - žádné, místní, připojené uzly, všechny uzly
  - **směrovací techniky**
    - pevné, lavinovité, nahodilé, adaptivní
  - **časová aktualizace adaptivního směrování**
    - průběžné, periodické, hlavní změny zátěže, změny topologie

Možné strategie směrování nedynamického charakteru

- **Použití pevných cest** (statické směrování)
  - v každém uzlu definováno co má být kam směrováno
  - ve formě [kam, kudy]
  - fixní nastavení neumí pružně reagovat na změny, výpadky
  - stejné chování pro datagramovou službu i virtuální kanál
- **Náhodné směrování**
  - teoretická možnost (použitelné ve více deterministické variantě)
  - pakety odesílány náhodně, neduplikovány, jejich pohyb je chaotický
  - postupem času dorazí k cíli
  - velké zatížení sítě; jednoduchá metoda

Možné strategie směrování nedynamického charakteru



R4 staticky

např.

Cílová síť	Cesta kudy (další skok)
1	R2
2	R7
3	R3
4	R7
5	R6

Možné strategie směrování nedynamického charakteru

- **Lavinové směrování**
  - paket v každém uzlu nakopírován a odeslán všemi kanály (kromě příchozího)
  - test zda již paket v uzlu nebyl
  - odolné vůči poruchám
  - teoreticky rychlost doručení maximální
  - enormní zátěž sítě (*flooding*)
  - použitelné u sítí s malou hustotou provozu či v počáteční fázi komunikace k dohledání nejlepší cesty
  - využíván u mechanizmů hromadné komunikace (*multicast*)

Možné strategie směrování dynamického charakteru

- **obecný popis**
  - cílem reakce na poruchy linek/uzlů či přetížení
  - funguje pouze pokud existuje znalost alternativních cest
  - potřeba služebních hlášení o mimořádných událostech
  - aktivní úprava směrovacích tabulek
  - vyšší složitost, nároky na paměť a čas procesoru
- **Centralizované směrování**
  - všechny informace shromažďovány v centrálním uzlu
  - optimální rozhodování se znalostí celé sítě
  - snadná správa systému
  - problémy
    - časové měřítko zjišťování informací
    - výpadek směrovacího centra = kolaps
    - zátěž přenosových tras (přenos do centra a zpátky)

Možné strategie směrování dynamického charakteru

- **Izolované směrování**
  - každý uzel rozhoduje sám
  - bez spolupráce s ostatními uzly = problém
  - okrajové použití, ve formě zpětného učení
    - sledování odkud přichází pakety kterého zdroje
    - učení se kdo kde je a následné využití
  - nereaguje na výpadky
- **Distribuované směrování**
  - žádný centrální prvek + povolení výměny informací mezi uzly
  - průběžná výměna informací o stavu sítě, dynamická volba cest
  - dnes nejčastější (vyhovuje necentralizovanému charakteru Internetu)
  - každý uzel se rozhoduje sám
  - **= dynamické směrování** dnešního pojetí
  - mechanizmy výměny = **směrovací protokoly**

Fungování směrování v sítích TCP/IP

- v TCP/IP využíváno distribuované dynamické směrování
- provádí směrovač (*router*)
  - problémem volba *optimální* cesty (*route*) ze sítě A do B v měnícím se prostředí
  - lokální rozhodování kam dále předávat pakety
    - založeno na určité znalosti globální topologie (složitá a rozsáhlá), nesnadný zisk informací
  - potřebuje zpravidla k úspěšnému plnění **směrovací úlohy** tyto informace:
    - adresátovu adresu (IP)
    - možné cesty do *všech* vzdálených sítí
    - aktuálně zvolenou nejlepší cestu do cílové sítě
    - sousední směrovače, od kterých se může dozvědět o cestách, a poslat jim data
    - způsob jak se dozvědět o cestách, jak tyto informace aktualizovat a udržovat
  - může nastat i situace, že směrovač nebude vědět kudy paket směrovat
    - paket zahodí a měl by odesilatele paketu informovat zprávou ICMP

Fungování směrování v sítích TCP/IP

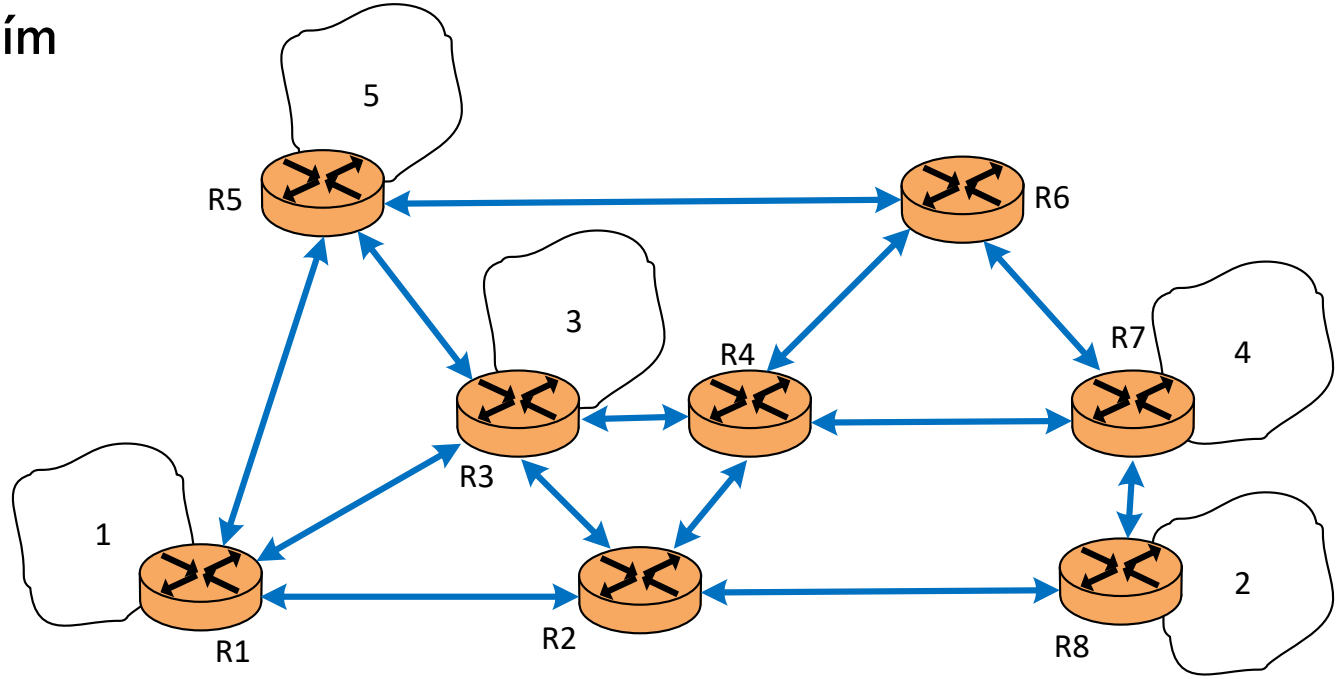
- v Internetu hierarchické směrování
  - rozdělení do tzv. autonomních systémů (AS)
    - jedna úroveň směrování uvnitř AS (směrovací protokoly jednoho typu)
    - druhá úroveň mezi AS (směrovací protokoly druhého typu)
- úlohou směrovacích protokolů efektivní shromažďování relevantních informací
- **základní požadavky na tyto protokoly**
  - **minimalizace velikosti směrovacích tabulek**
    - ovlivňuje rychlost vyhledávání a množství vyměňovaných informací mezi sousedy
  - **minimalizace počtu přenášených kontrolních zpráv**
    - zbytečné zatížení přenosových linek provozem servisního charakteru
  - **robustnost**
    - nesmí docházet ke vzniku chyb směrování, *černých děr*, kde by se ztrácely pakety, nebo směrovacích smyček
    - žádoucí je rychlá konvergence procesu
  - **využívání optimálních tras**
    - *optimální* nemusí vždy být nejkratší nebo nejrychlejší

Fungování směrování v sítích TCP/IP

závislé na konkrétním protokolu

R4 aktuálně

např.



Cílová síť	Cesta kudy (další skok)
1	R2
2	R7
3	R3
4	R7
5	R6

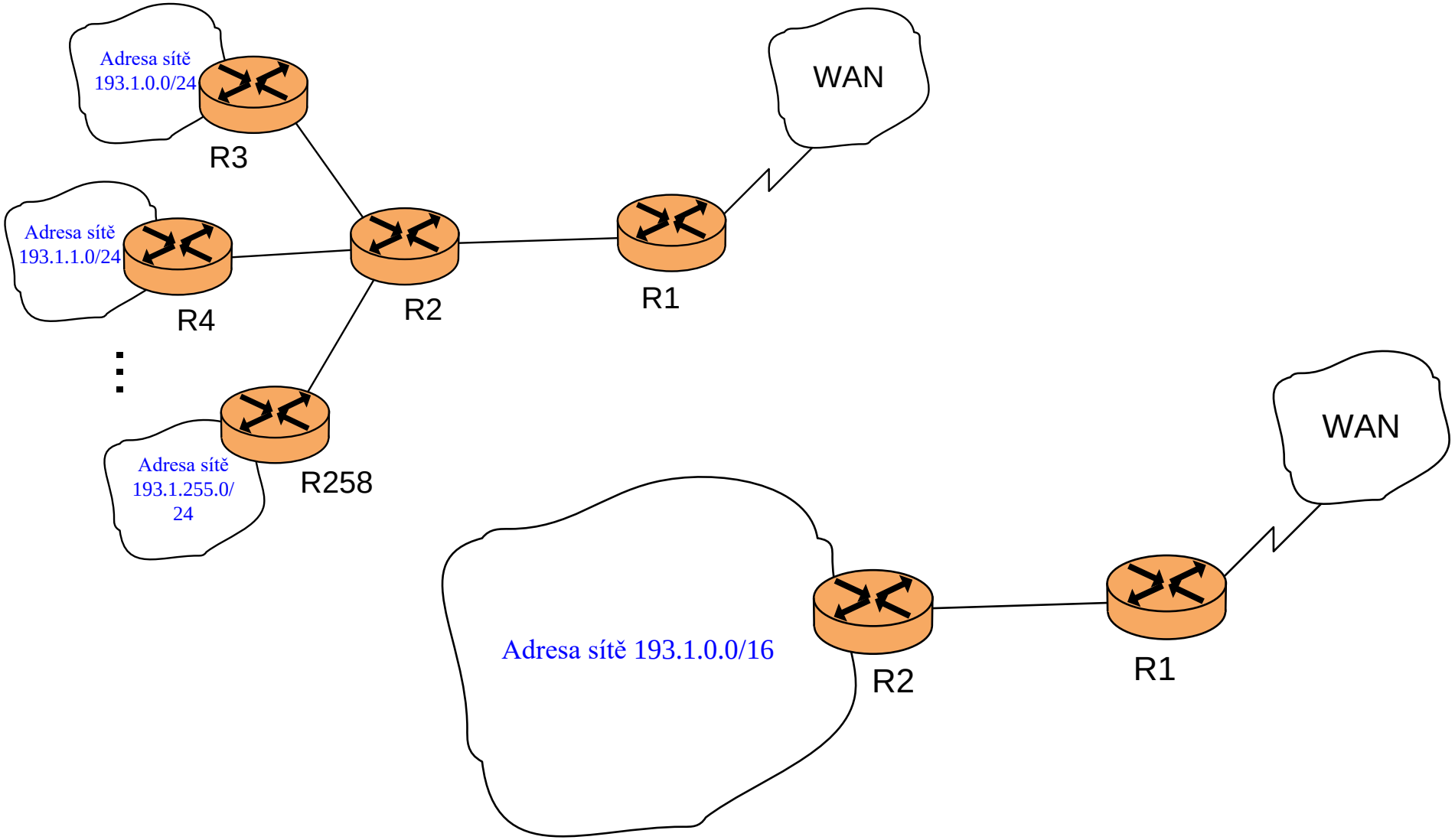
Shrnutí směrování z pohledu síťové vrstvy

- směrování založeno na adresách sítí (podsítí)
  - efektivita
- stanice umí rozpoznat zda adresát je na stejné nebo jiné síti
  - přímé doručení
  - využití výchozí brány
- směrovač (i stanice) pracují se směrovací tabulkou
  - záznamy <cílová síť; následující skok>
  - mezilehlé uzly sledují pouze adresu sítě (předávání)
  - poslední směrovač sleduje i adresu stanice (doručení)

Agregace směrovacích cest

- **Agregace** (*aggregation*) (nazývána i jako **sumarizace,** *summarization*)
  - základním cílem redukce počtu směrovacích záznamů
  - shrnutí několika směrovacích informací do jedné nadřazené
  - na základě binárního vyjádření pouze po mocninách dvou; zkracování masky sítě
  - hledání nejbližšího nadřazeného adresního prostoru
  - možný beztřídní i třídní přístup
  - síť /22 pojme
    - dvě sítě /23
    - čtyři sítě /24
    - …
  - popis k obrázkům (další slajd)
    - 256 sítí na R3 až R258
    - z pohledu R1 a WAN možné sloučit – úspora 255 záznamů
    - automatická nebo ručně nastavitelná sumarizace
    - izolace od nepodstatných změn, zvýšení stability směrování

Agregace směrovacích cest



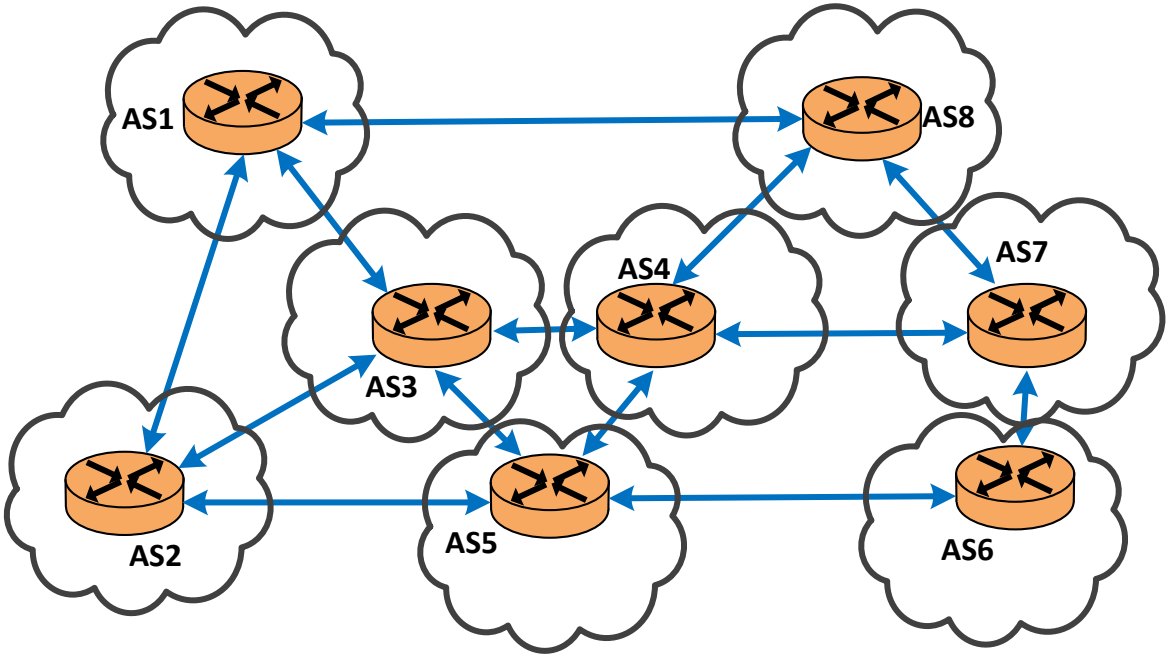
Autonomní systémy

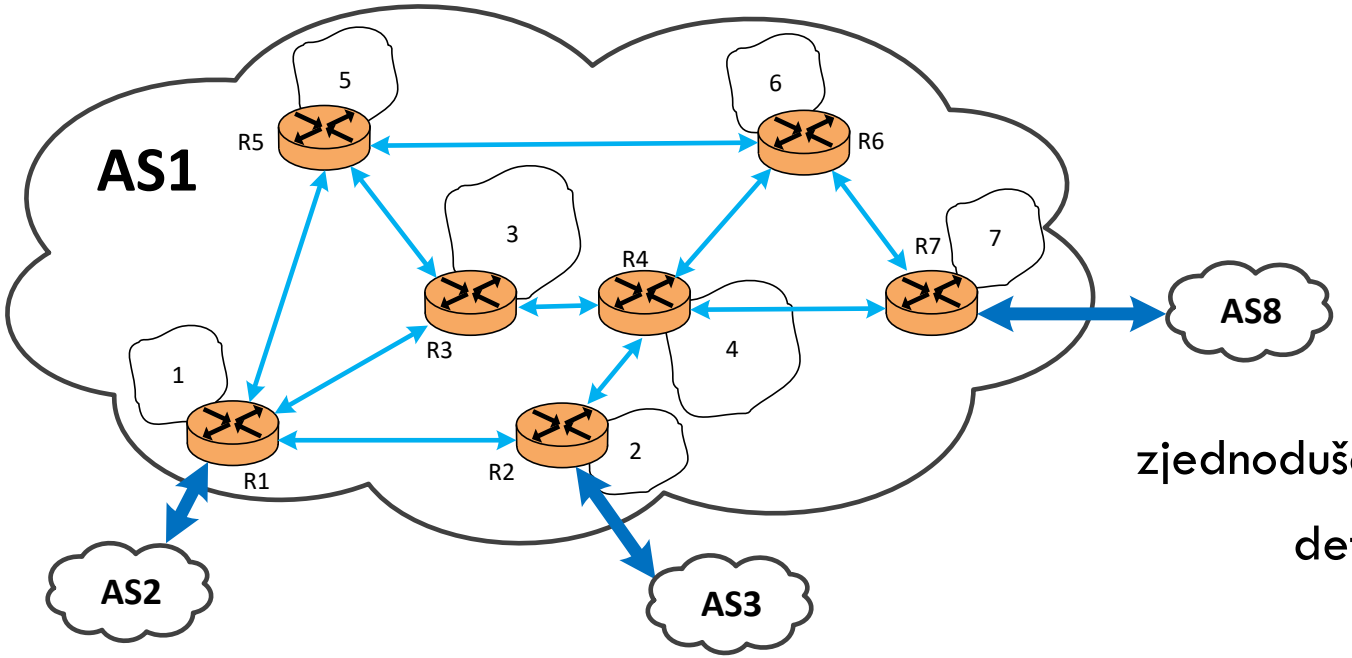
- jednotlivé sítě představují příliš malou jednotku
  - řadově jich existují milióny
- úloha směrování v globálním měřítku na úrovni sítí by byla velice složitá
- proto existují vyšší jednotky Internetové sítě z hlediska topologie, tzv. autonomní systémy
  - řádově desetisíce
- **Autonomní systém (AS)**
  - síť sítí
  - souhrn sítí pod společnou správou
  - s vlastní vnitřní směrovací strategií
  - identifikace pomocí 16-bit nebo 32-bit čísla ASN (AS Number)
  - výměna směrovacích informací mezi AS dle předem domluvených pravidel (jednotně)
  - lze si představit jako geograficky distribuovaný směrovač, jeho porty jsou hraničními porty všech hraničních směrovačů

Autonomní systémy

zjednodušený pohled na

část struktury Internetu





zjednodušený pohled na

detail jednoho AS

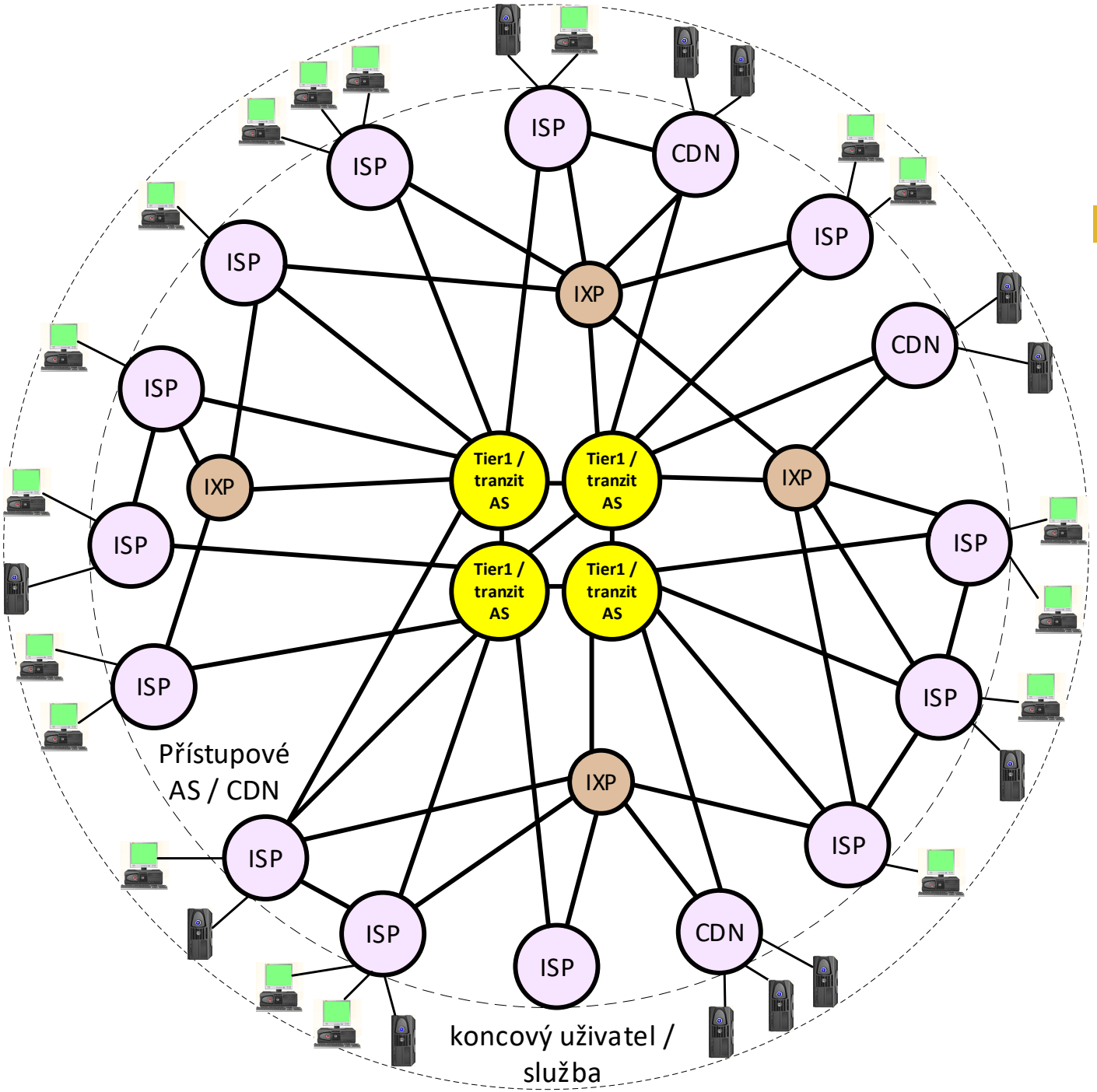
Směrovací protokoly

- dvě skupiny
  - **Protokoly pro použití uvnitř autonomního systému** (*interior protocols*), či *Internal Gateway Protocols* = IGP
    - používané pro přenos směrovacích informací mezi jednotlivými směrovači uvnitř autonomního systému
    - mezi používané IGP protokoly patří např.:
      - **RIPv2** (*Routing Information Protocol* verze 2)
      - **EIGRP** (*Enhanced Interior Gateway Routing Protocol*)
      - **OSPF** (*Open Shortest Path First*)
      - **IS-IS** (*Intermediate System to Intermediate System*)
    - hlavní odlišnosti mezi těmito protokoly
      - jakým způsobem mají nastaveny parametry komunikace mezi směrovači
      - různé výpočtové mechanizmy pro určení optimální trasy z jedné sítě do druhé
    - podrobnější seznámení s IGP protokoly nad rámec tohoto předmětu

Směrovací protokoly

- **Protokoly pro použití mezi autonomními systémy** (*exterior protocols*), či *External Gateway Protocols* = EGP
  - výměna směrovacích informací na úrovni AS (přímá i nepřímá)
  - zde v současnosti využíván výhradně protokol **BGP** (*Border Gateway Protocol*)
    - základem jeho fungování je o něco menší úroveň automatizace a o něco větší zásah administrátorů do procesu výběru nejlepších cest pro přenos paketů z jednoho AS do druhého AS
    - jako autonomní systém si můžeme představit např. síť poskytovatele připojení (ve které je více různých sítí)
    - detaily nad rámec kurzu

Použití směrovacího protokolu BGP



Detailní pohled na směrovací tabulku

- místo, kam si směrovač ukládá směrovací informace
  - jak má naložit s pakety z hlediska různých cílových sítí, kam je má dále předat
- naplnění je typicky důsledkem běhu některého ze směrovacích protokolů, případně více protokolů
- obvykle obsahuje větší množství záznamů, každý obsahuje zejména:
  - **původce informace**
    - typicky některý ze směrovacích protokolů,
  - **síťová adresa a maska**
    - které definují, pro jaký okruh cílových adres tento záznam platí
  - **metrika**
    - vyjadřující typicky vzdálenost cílové sítě nebo normovanou rychlost tras
  - **adresu dalšího skoku**
    - síťová adresa sousedního směrovače, směrem k adresátovi
  - **další údaje informativního charakteru**
    - např. doba jak dlouho je cesta aktivní

Detailní pohled na směrovací tabulku

- Ukázka směrovací tabulky ze směrovače Cisco (zjednodušeno)
- R = RIP, O = OSPF

R **192.168.51.0/24** [1] **via 172.16.12.1**, 00:00:04
R **192.168.50.0/24** [1] **via 172.16.12.1**, 00:00:24
R **192.168.49.0/24** [1] **via 172.16.12.1**, 00:00:16
O **192.168.30.0/24** [1563] **via 172.16.23.3**, 00:00:37
O **192.168.25.0/24** [1563] **via 172.16.23.3**, 00:00:37
O **192.168.40.0/24** [1563] **via 172.16.23.3**, 00:00:37

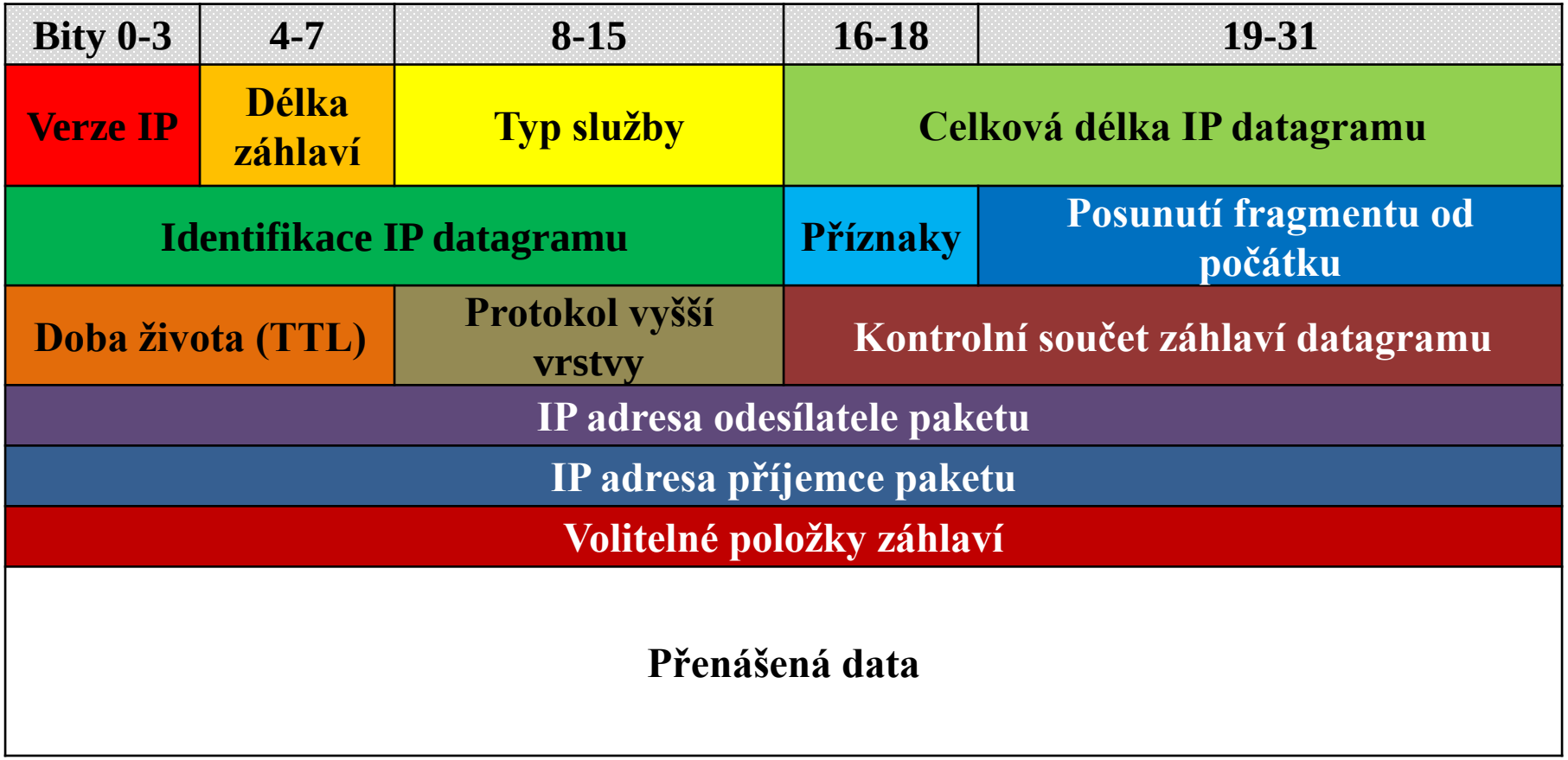
IPV4 DATAGRAMY

IPv4 datagramy

- jednotná abstrakce ve formátu datových jednotek
- na spojové vrstvě zabalen do rámce, který se mění podle technologie
- paket se nemění při přenosu (s výjimkou proměnných polí)

20 – 60 bajtů	až (65 535 – záhlaví) bajtů
Záhlaví	Datová část (segment)

Formát IPv4 datagramu



IPv4 datagramy

- **Verze** – obsahuje verzi protokolu IP a zajišťuje, aby mohla být různá pole datagramu správně použita (hodnota 4)
- **Délka záhlaví** – záhlaví může mít proměnnou délku v násobcích 32 bitů. Minimum je 5 . 32 bitů = 20 bajtů, maximum 15 . 32 bitů = 60 bajtů
- **Typ služby** – položka měla sloužit ke specifikaci požadované kvality přenosu IP datagramu. V současnosti se položka nese značku pro mechanismy zajišťující služby s definovanou kvalitou služby (QoS)
- **Celková délka IP datagramu** – definuje úplnou délku datagramu včetně záhlaví a uživatelských dat. Maximum je 65535 bajtů
- **Identifikace IP datagramu** – primárně určeno k identifikaci k sobě patřících fragmentů, přiděleno odesilatelem
- **Příznaky** – používají se:
  - DF-bit (*don't fragment*) označuje případný požadavek na nepoužití fragmentace
  - MF-bit (*more fragments*) říká, že datagram byl fragmentován a že bude následovat další část

IPv4 datagramy

- **Posunutí fragmentu od počátku** – indikuje pozici obsahu dat datagramu vzhledem k začátku původního (rozděleného) paketu
- **Doba života datagramu** (TTL = T*ime-To-Live*) – hodnota definuje maximální počet skoků na přenosové trase
- **Protokol vyšší vrstvy** – obsahuje identifikaci protokolu vyšší vrstvy
- **Kontrolní součet záhlaví datagramu** – je použit na záhlaví datagramu, pokud součet nesedí, paket se zahodí; přepočítává se v každém uzlu
- **IP adresa odesílatele/příjemce paketu** – každá 32 bitů
- **Volitelné položky záhlaví** – až do délky 40 bajtů, nevyužívá se příliš často
  - zaznamenej směrovače – zjištění kudy paket procházel
  - zaznamenávej čas
  - explicitní směrování – umožňuje zadat, přes které směrovače má být IP datagram dopravován
- **Přenášená data** – např. TCP segment

Fragmentace paketů

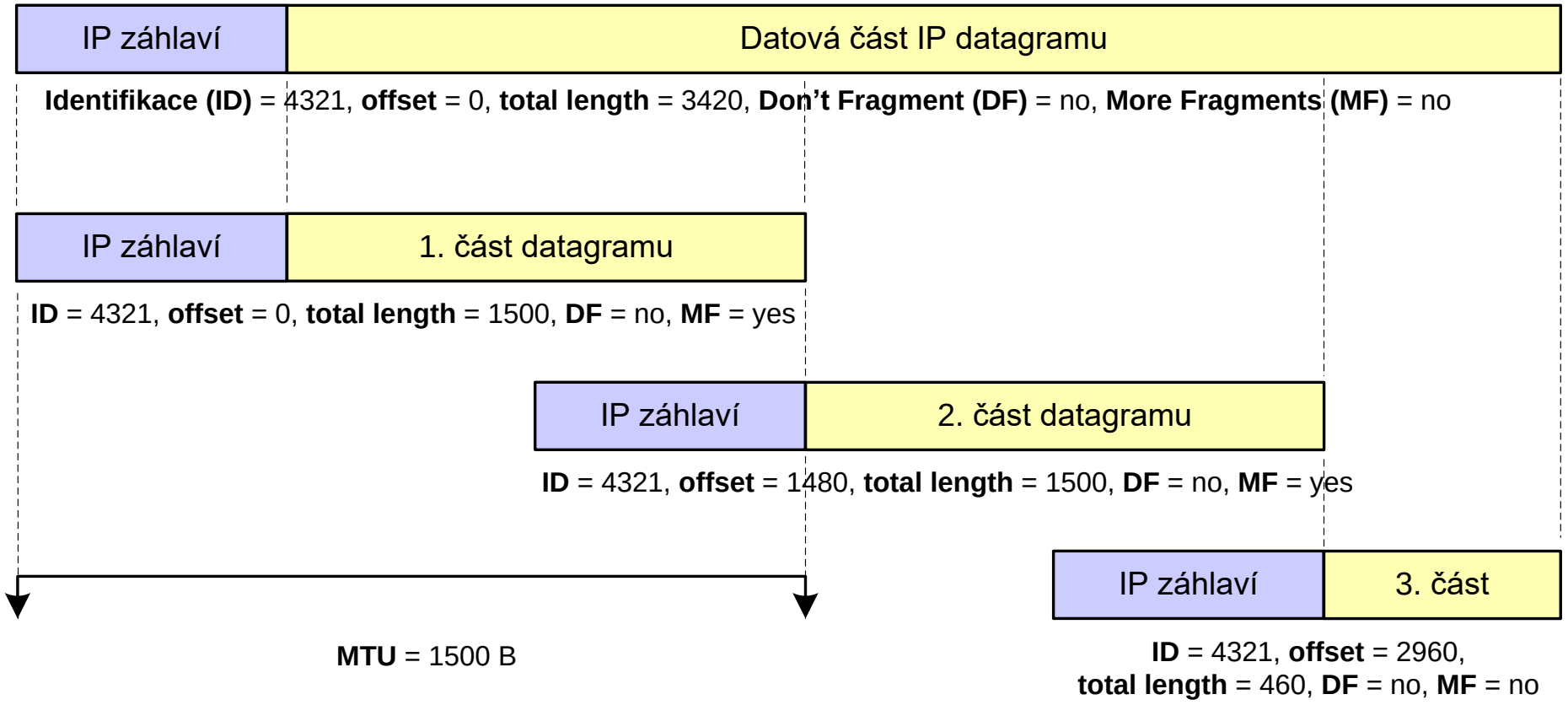
- maximální velikost IP datagramu teoreticky 65535 bajtů
- v reálných sítích je však maximální povolená velikost různá dle technologie
  (MTU – *Maximum Transmission Unit*)

Linkový protokol	MTU [bajty]
Ethernet II	1500
Ethernet 802.3 SNAP	1492
Frame Relay	1600
FDDI	4352
PPP	296
ATM	48

Fragmentace paketů

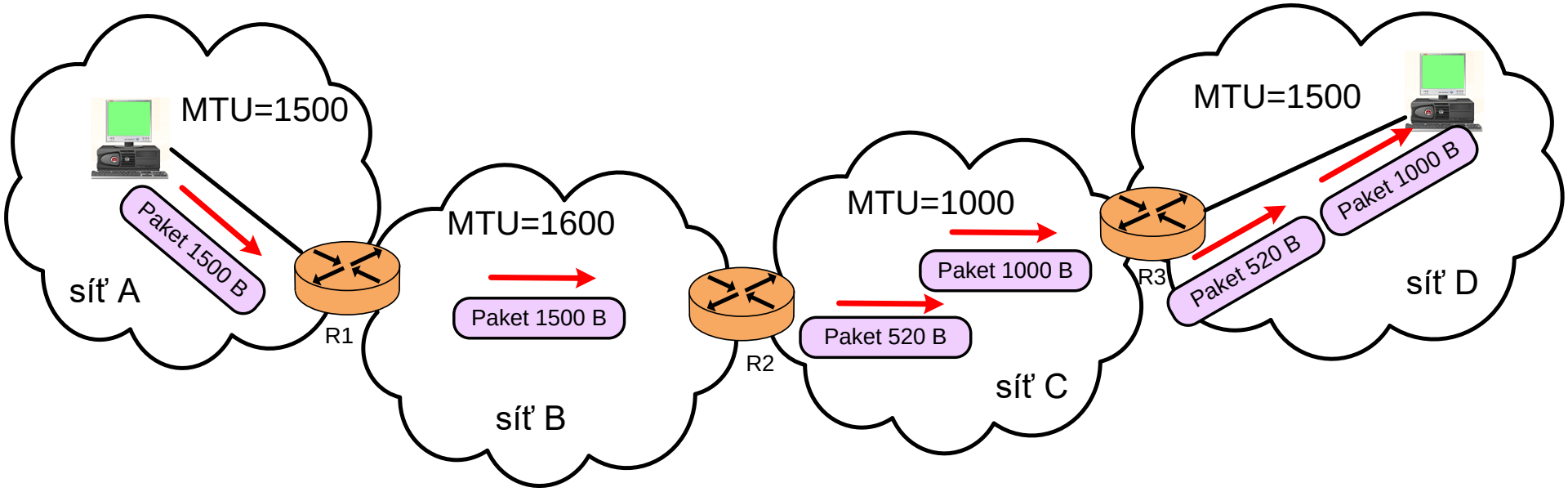
- stanice v IPv4 síti
  - dopředu neví jaké přenosové technologie směrem k adresátovi budou použity
  - není schopna stanovit délku paketu průchozí celou trasou
  - vyšle paket délky přenositelné na síti, kde se nachází
- paket může být větší než MTU další sítě, mohou nastat dvě varianty
  - zahození paketu (odesilatel by měl být informován)
  - rozdělení paketu na menší části (každá přenášena samostatně)
- pokud síť umožňuje fragmentaci
  - provede se, pokud není zakázána v záhlaví paketu (bit DF)
  - neprovede se, pokud je bit DF nastaven (odesilatel by měl být informován)

Ukázka fragmentace paketu



Fragmentace paketů

- fragmentované pakety jsou dále směrovány samostatně
- složení probíhá až u konečného adresáta, ne v síti
- vždy určitá režie

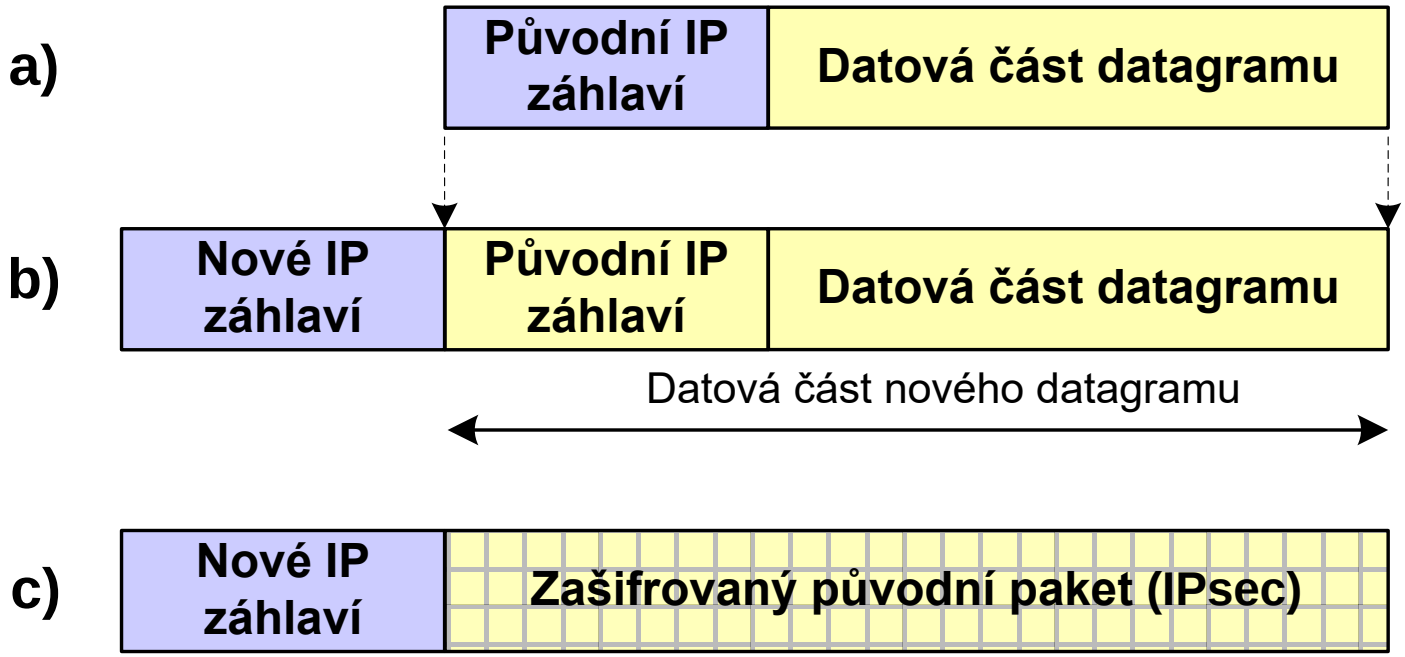


Tunelování paketů

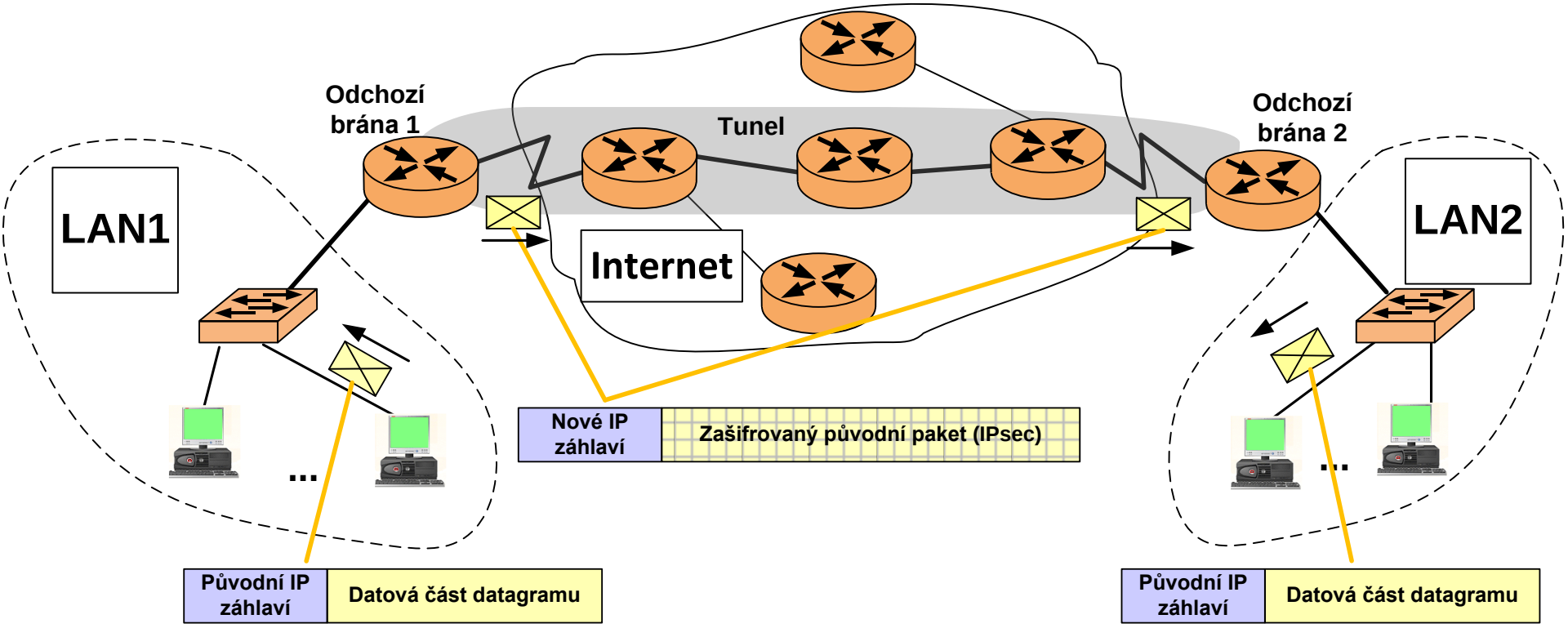
- situace, kdy je nutné propojit několik vzdálených sítí tak, aby se tvářily jako jedna síť
- sítě jsou propojeny přes veřejný Internet
- principem tunelování je zapouzdřování původního IP paketu do nového IP paketu (záhlaví)
- nový IP paket
  - liší se především cílovou IP adresou (a zdrojovou)
  - zapouzdření typicky provádí odchozí brána jedné lokální sítě
  - zapouzdřený paket směrován Internetovou sítí
  - po přijetí bránou cílové sítě zbaven přídavného záhlaví a zaslán standardními postupy k adresátovi
- **dva základní druhy tunelování**
  - **tunelování ve spolupráci s IPsec protokolem**
  - **tunelování mezi verzemi IP protokolu**

Tunelování paketů s IPsec

- celý obsah paketu, včetně vnitřní IP adresy zdroje a cíle hostitelského počítače vnitřní sítě, je skrytý vnějšímu světu

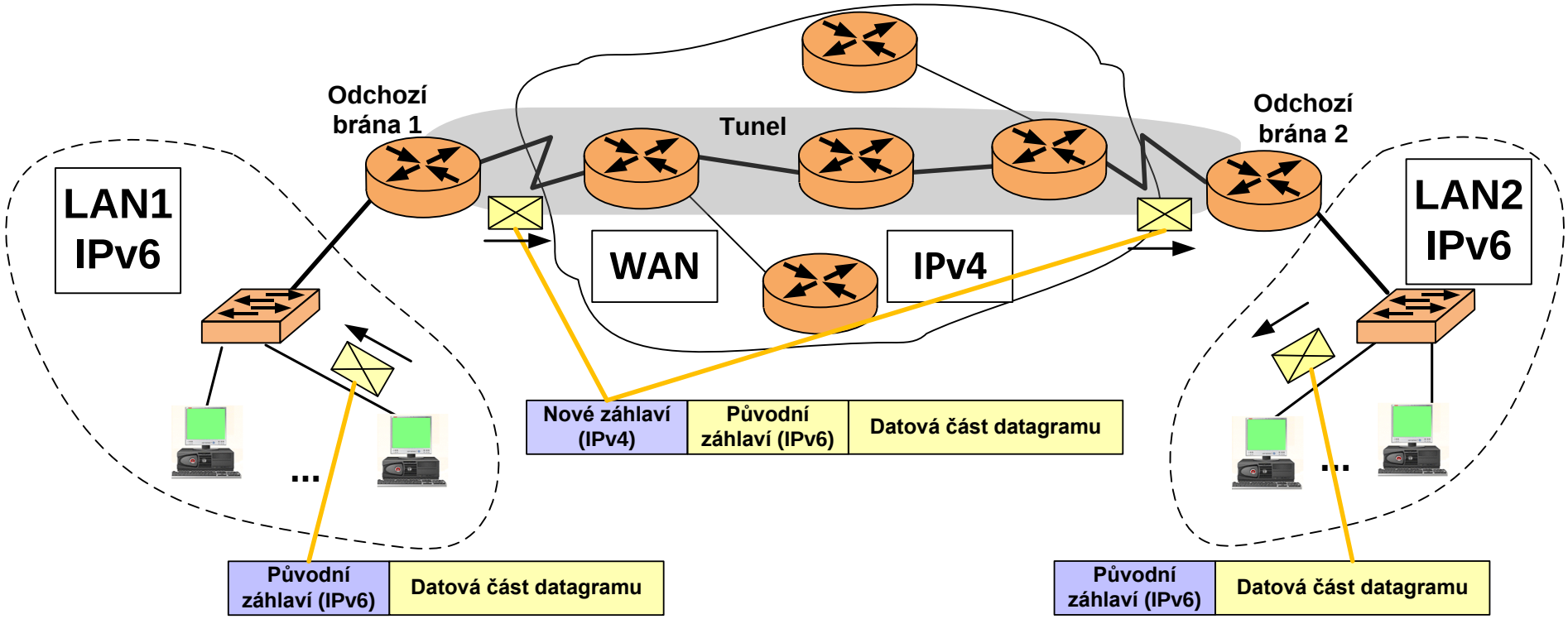


Tunelování paketů s IPsec



Tunelování mezi verzemi IP protokolu

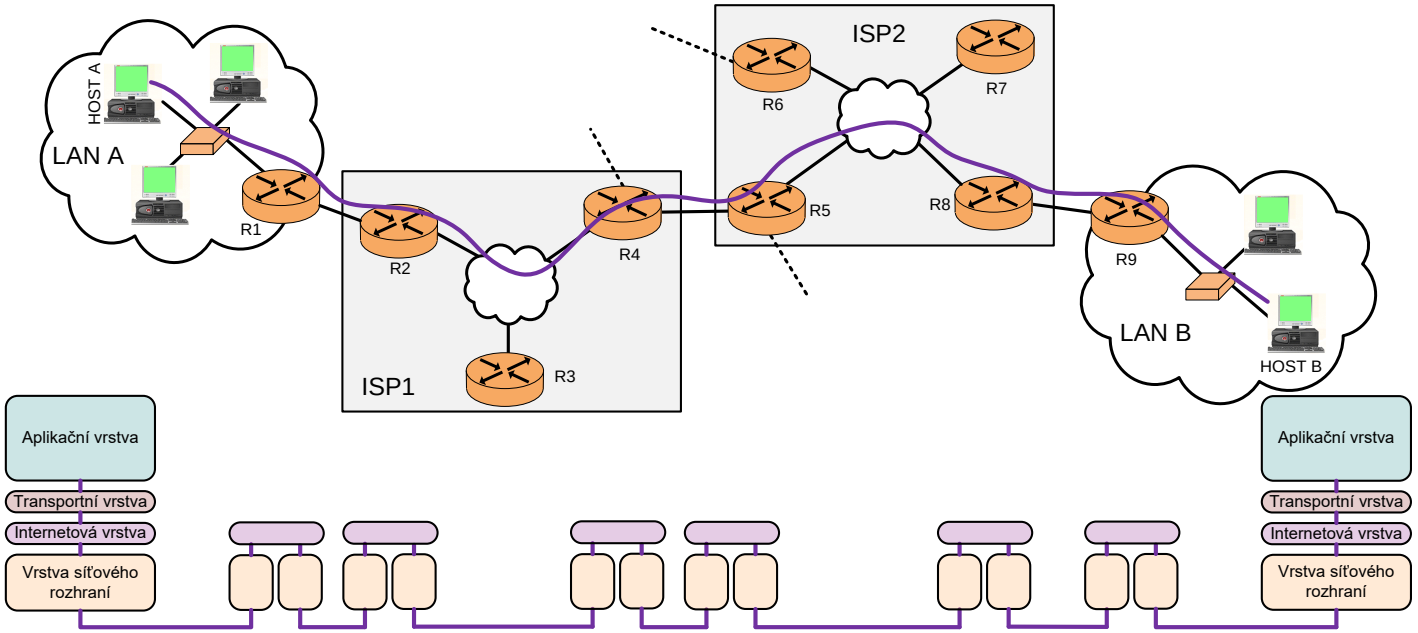
- užitečné v situaci, kdy existuje v síti **více verzí IP protokolu** (IPv4 a IPv6), jeden z přechodových mechanizmů



NÁVAZNOST NA ADRESY NIŽŠÍ ÚROVNĚ

Návaznost na adresy nižší úrovně

- IP adresy – abstrakce na úrovni síťové vrstvy – představa jednotné virtuální sítě
- dílčí sítě – různé mechanizmy skutečné (fyzické) adresace, různé formáty adres
- IP adresy musí být vždy převáděny na skutečné adresy, aby bylo možné vytvořit rámec



Návaznost na adresy nižší úrovně

- **základní způsoby řešení převodu IP adresy na fyzickou adresu**
  - **pomocí přímého převodu**
    - transformační funkce nebo matematický převod síťových a fyzických adres
    - lze někdy využít, aplikováno např. u multicastu
    - volitelné fyzické adresy; pouze malé sítě
    - není třeba udržovat tabulku odpovídajících si adres, na základě IP adresy je ihned známá i fyzická adresa
    - nevýhodou lidské chyby, přečíslování, jiné změny
    - př.: 8 bitové fyzické adresy = poslední byte IP adresy

Návaznost na adresy nižší úrovně

- **pomocí dynamické vazby**
  - „pevné“ fyzické adresy síťových adaptérů, IP adresy nemusí být pevné; žádná přímá vazba
  - každá stanice musí zjišťovat fyzickou adresu druhé strany dynamicky (proměnné prostředí)
  - např. u Ethernetu (48-bit adresy od výrobce) x IP adresa
  - každá stanice si může tvořit převodní tabulku odpovídajících si adres
  - výhodou menší riziko chyb
  - musí existovat mechanizmus (protokol), který to bude umožňovat (ARP × ICMPv6)

Address Resolution Protocol (ARP)

- **address resolution problem**
  - problém transformace adres vyšší úrovně na adresy nižší úrovně
  - nejčastěji nalezení odpovídající fyzické adresy k IPv4 adrese
  - řešeno formou lokální tabulky, obsahující seznam vzájemně si odpovídajících adres
  - spojeno s četnými problémy
    - kdo a jak zajistí počáteční naplnění tabulky
    - kdo ji bude udržovat a přizpůsobovat momentálnímu stavu sítě
    - kdo zajistí, aby její velikost nepřesáhla únosnou mez atd.
    - **protokol ARP,** pracuje s **tabulkou** dočasných záznamů (*cache*)

Address Resolution Protocol (ARP)

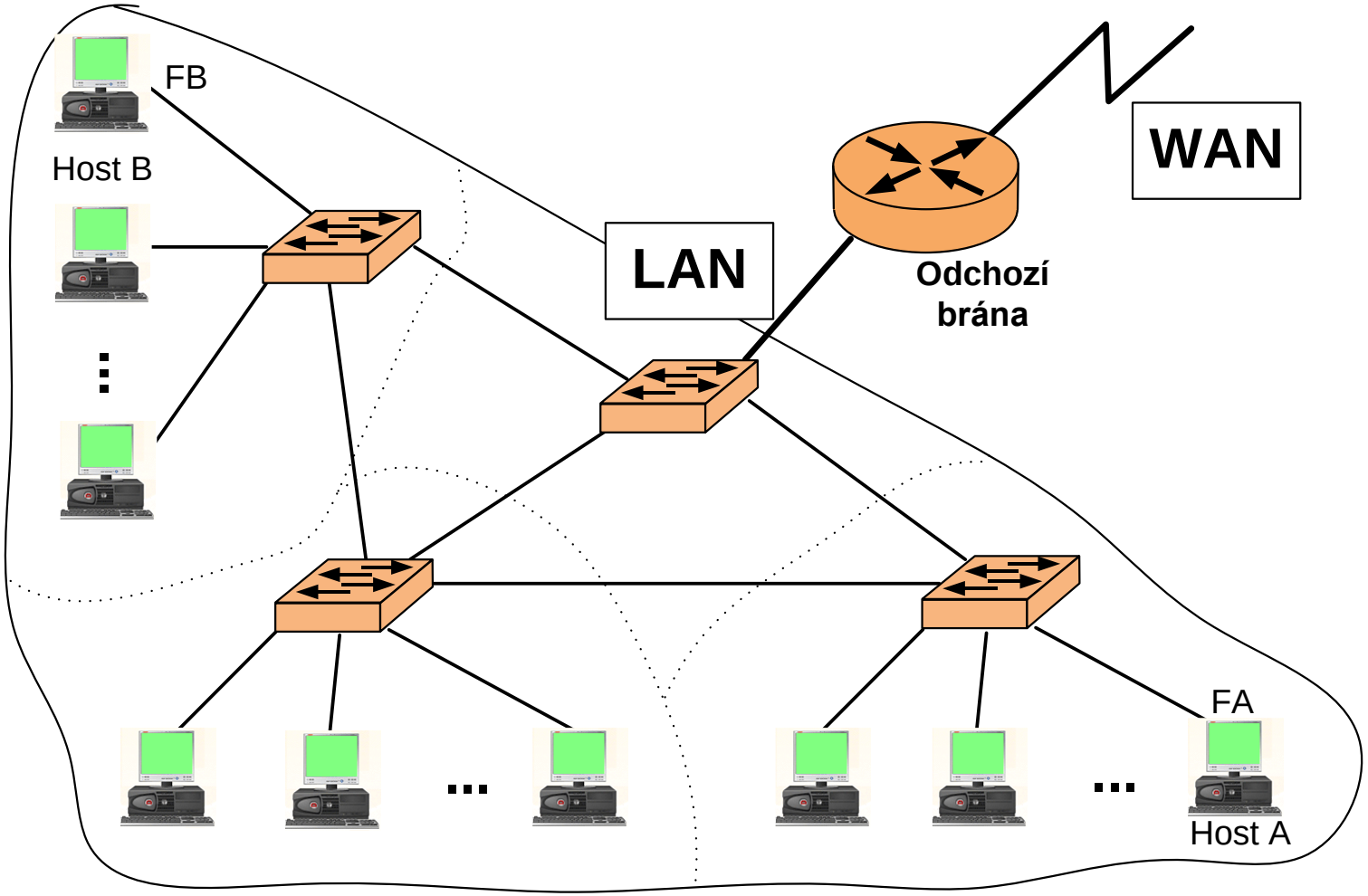
- **základní vlastnosti ARP**
  - dynamický, distribuovaný protokol, schopný reagovat na změny v síti
  - **určen primárně ke hledání neznámé linkové adresy na lokální síti, v situaci kdy známe adresu IP**
  - obecně ke zjištění adresy druhé úrovně na základě znalosti adresy třetí úrovně
  - informace ukládány do tabulky
    - podle potřeby se obnovují
    - položky jsou zpravidla uloženy pouze dočasně na několik minut a pak vymazány (mohly se stát neaktuální či nejsou třeba)
  - ARP pracuje mezi spojovou a síťovou vrstvou, používá rámce linkové

Struktura ARP paketu

Struktura ARP paketu

- **Typ média**
  - indikuje typ použitého média, např. pro Ethernet je hodnota 0x0001, ATM má 0x0010
- **Typ protokolu**
  - typ vyššího protokolu, v rámci něhož se logická adresa používá, pro IP je hodnota 0x0800
- **Délka fyzické adresy**
  - délka fyzické adresy v bajtech, pro Ethernet 0x06
- **Délka logické adresy**
  - délka logické adresy v bajtech, pro IPv4 adresu 0x04
- **Operace**
  - specifikuje operaci, kterou odesilatel paketu provedl
  - hodnota 0x0001 pro požadavek na zjištění fyzické adresy
  - hodnota 0x0002 na odpověď
- **Fyzická adresa zdroje / hledaná**
- **Logická adresa zdroje / hledaná**

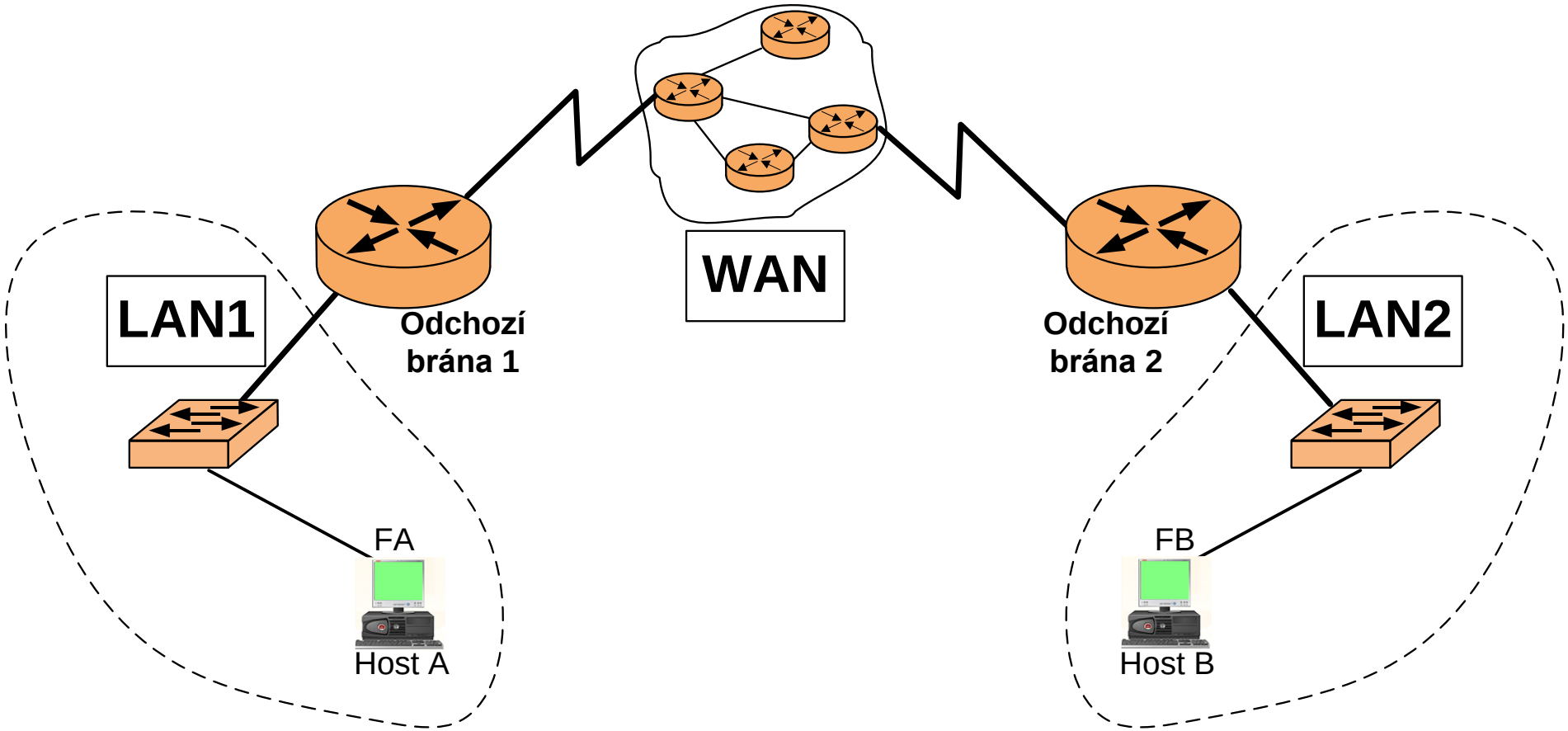
Příklad na fungování ARP – hledaná stanice je v rámci stejné sítě



Příklad na fungování ARP – hledaná stanice je v rámci stejné sítě

- dva hostitelské počítače A a B, IP adresy IA a IB
- **uzly téže (dílčí) sítě,** mohou mezi sebou komunikovat přímo
- fyzické adresy FA a FB
- síťová vrstva počítače A chce poslat něco na počítač s IP adresou IB
  - musí být schopna zajistit převod IP adresy (IB) na fyzickou adresu (FB)
  - potřeba pro vytvoření rámce
- řešení
  - stanice A prozkoumá svoji ARP *cache* [záznam nenalezen]
  - vyšle všem stanicím ARP žádost s hledanou IP adresou (IB)
  - žádost přijmou všechny stanice v síti
  - odpověď odešle pouze stanice B (oznámí svoji FB), ostatní rámec zahodí
  - současně stanice B zkontroluje obsah své ARP *cache*, zda ji nedoplnit o dvojici adres (IA a FA)

Příklad na fungování ARP – hledaná stanice není v rámci stejné sítě



Příklad na fungování ARP – hledaná stanice není v rámci stejné sítě

- **stejná situace, jen uzly různých sítí,** nemohou mezi sebou komunikovat přímo
- síťová vrstva počítače A odesílá rámec na výchozí bránu
- zjišťuje stejným způsobem fyzickou adresu, ale výchozí brány, ne stanice
- obdobně pak řešeno v dalších sítích po trase

Ukázka ARP tabulky

- uloženy známé překlady získané dynamicky i vypočtené staticky
- časové údaje nejsou standardně zobrazovány (řádově minuty)

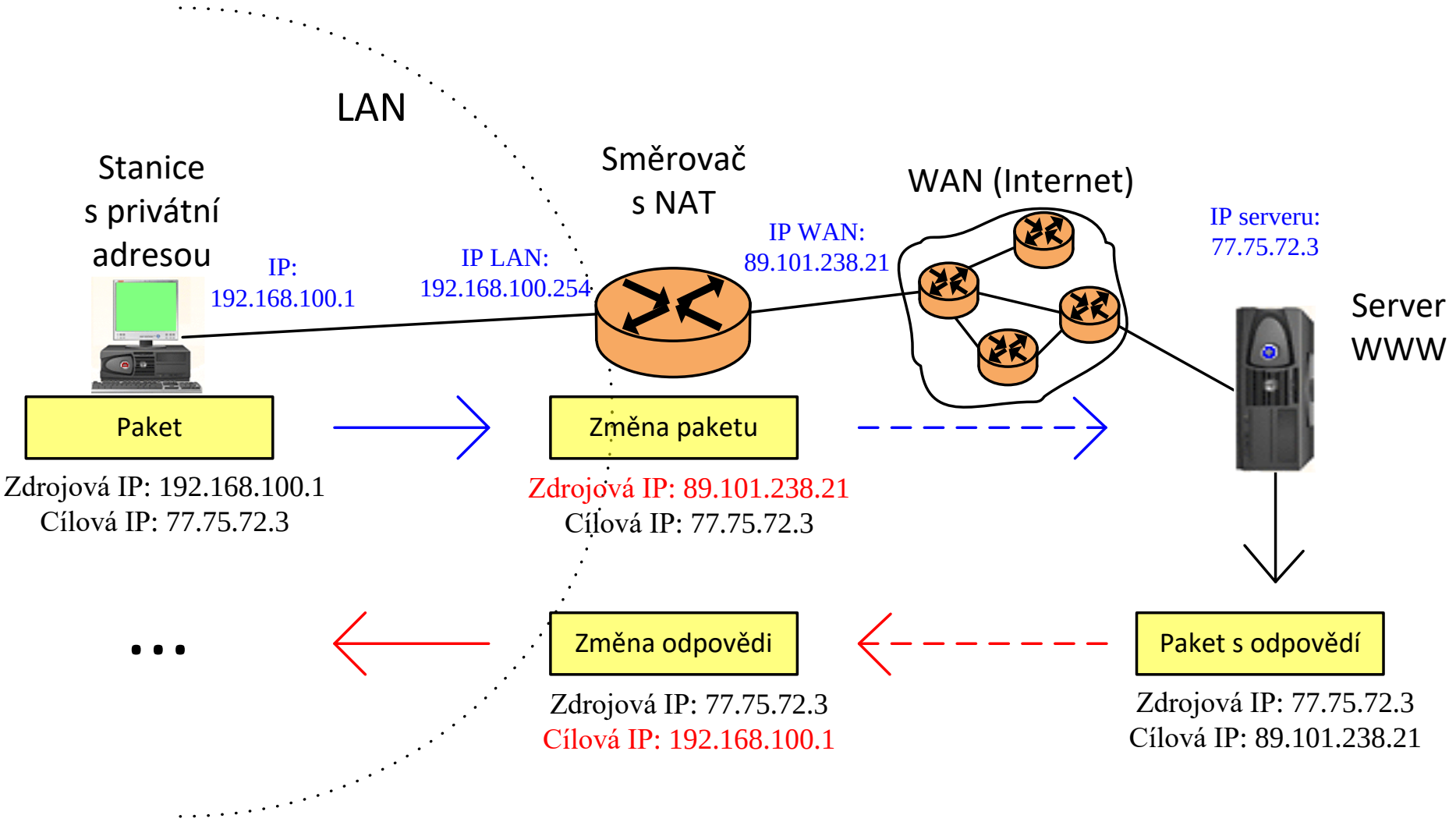
```
C:\>arp -a

Rozhraní: 100.100.100.55 --- 0xa
  internetová adresa     fyzická adresa         typ
  100.100.100.1          00-17-a4-c2-09-00      dynamická
  100.100.100.192        50-e5-49-35-6b-e2      dynamická
  100.100.100.152        50-e5-49-3c-61-bb      dynamická
  224.0.0.252            01-00-5e-00-00-fc      statická
```

PŘEKLAD SÍŤOVÝCH ADRES = NETWORK ADDRESS TRANSLATION (NAT)

Network Address Translation (NAT)

- překlad síťových adres
- změna IP adresy v záhlaví paketu, na směrovači
  - zpravidla mezi různými rozsahy
  - změna původce paketu (vnitřní × vnější síť, oddělení)
  - běžně podporováno a používáno
- směrovač
  - udržuje tabulku překladů (odlišení provozu jednotlivých stanic)
  - typicky
    - jedna veřejná IP (WAN)
    - více privátních IP (LAN)
    - využívá i transportní adresy (porty)
  - lze použít různými způsoby
    - i vícekrát
    - nelze detekovat vzdáleně
    - PT (*Protocol Translation*), IPv4 × IPv6; × tunelování

Network Address Translation (NAT) – příklad



Dva základní druhy překladu adres

- mnoho technik založených či podobných NATu, různé dělení
- základní druhy
  - SNAT (*Source NAT*)
    - prvotně je prováděn překlad zdrojové IP adresy a případně transportní adresy
    - uvedený příklad
  - DNAT (*Destination NAT*)
    - prvotně prováděn překlad cílové IP adresy a případně opět transportní adresy
    - DNAT se primárně používá ke „zveřejnění“ služby z interní sítě na veřejně přístupnou IP adresu
  - často kombinovány

Výhody a nevýhody NATu

- nevýhody
  - ztráta modelu end-to-end, přímočaré spojení omezeno
  - problém pro některé protokoly
  - vícenásobné použití nejproblematičtější
  - časové zpoždění překladu
- výhody
  - bezpečnost SNATu, komunikace začíná uvnitř
  - úspora veřejného adresního prostoru IP

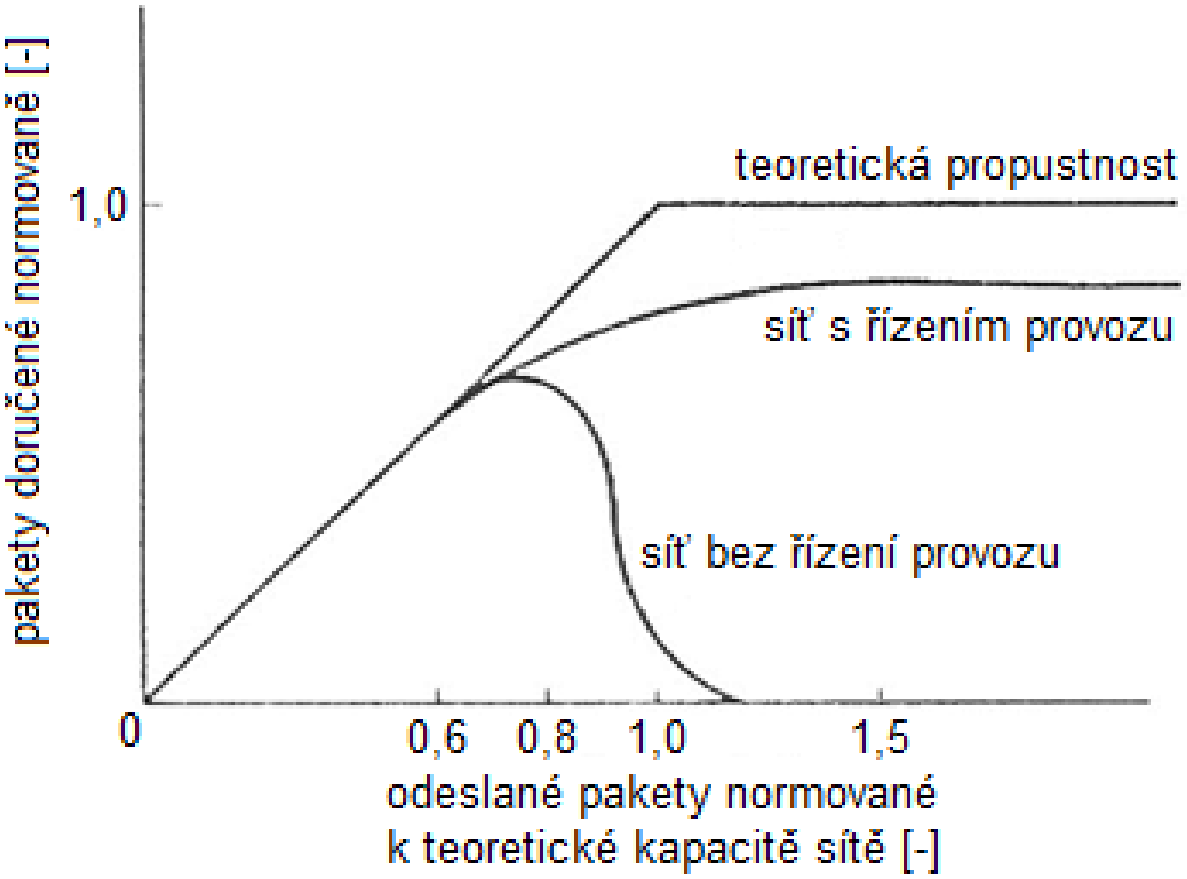
MECHANIZMY ŘÍZENÍ PROVOZU V SÍŤOVÉ VRSTVĚ

Mechanizmy řízení provozu v síťové vrstvě

- **řízení provozu**
  - diskutováno již v rámci spojové vrstvy
  - existuje i na síťové vrstvě
  - komunikace přes sítě, dílčí řízení toku jednotlivých linek na nižší vrstvě nemusí být dostatečné
  - snahou řízení přenosu paketů aby nedocházelo k zahlcení mezilehlých uzlů sítě anebo k zahlcení přijímací strany
  - **tři oblasti**
    - **řízení toku dat** (*flow control*)
      - regulace přenosu paketů mezi dvěma uzly
    - **předcházení zahlcení či uváznutí sítě** (*congestion avoidance*)
      - stav kdy většina uzlů sítě je zahlcena
    - **směrování s přerozdělováním zátěže** (*load balancing*)
      - umožňuje např. rozdělit pakety do více tras a tím snížit zátěž mezilehlých uzlů a linek

Propustnost sítě v různých situacích

- reálná propustnost od určité míry zatížení klesá (bez řízení) či neroste (s řízením)



Řízení toku dat v síťové vrstvě

- omezení rychlosti generování datových jednotek ve vysílači
- cílem zamezení zahlcení přijímače, vliv i na zahlcení celé sítě
- tři metody
  - **úprava rychlosti generování datových jednotek**
    - realizována změnou prodlevy časovače, který řídí generování paketů
    - lze využít tzv. škrtících paketů (*choke packets*), které vysílá přijímač
    - vysílač pak sníží rychlost a zároveň startuje časovač
    - po uplynutí opět rychlost zvýší
    - *choke packet* lze zasílat opakovaně
  - **odmítnutí paketu přijímačem**
    - přijímač pakety nad jeho možnosti neuloží do paměti, dojde k jejich zahazování (*discard*)
    - přijímač o této skutečnosti může informovat vysílač a ten může reagovat
  - **povolení k vysílání**
    - založeno na explicitním povolení vysílání přijímačem

Předcházení zahlcení sítě

- lze použít jednoduchou metodu spočívající ve **snížení existující zátěže**
  - založeno na zahazování určitého množství paketů tak, aby se snížil jejich celkový počet v síti
- lze zahazovat pakety
  - které jsou už příliš dlouho v síti
  - prošly příliš mnoha uzly
  - všechny pakety vstupující do uzlu po překročení přednastavené hladiny
  - používáno běžně v datagramových sítích
  - zahození paketu je napravitelné transportní vrstvou
    - opakování přenosu (problém cyklického zahlcování sítě)

Předcházení uváznutí sítě

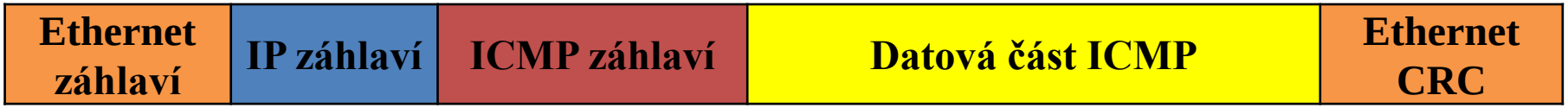
- uváznutí sítě když uzly nejsou schopny posílat pakety směrem k adresátovi, např. následující uzel má zaplněnu vyrovnávací paměť
- důležité stavu předcházet
  - vytvořit strukturovanou vyrovnávací paměť
    - organizována hierarchickým způsobem na několika úrovních
    - hlavní část vyrovnávací paměti je použitelná bez omezení (většina paměti)
    - dále jeden nebo více bloků vyrovnávací paměti, které jsou určitým způsobem rezervovány pro pakety vyšší důležitosti
    - běžný provoz nemůže nikdy zcela zahltit síťový prvek a způsobit uváznutí sítě
  - opatřit pakety hodnotou definující maximální dobu životnosti paketu TTL (*Time to Live*), resp. *Hop limit*
    - standardně využíváno
    - po vypršení tohoto počtu je paket zahozen
    - pakety nepřenášeny nekonečně (při chybě směrování)

Internet Control Message Protocol (ICMPv4)

- IP protokol
  - základní protokol síťové vrstvy, přenos paketů
  - neobsahuje žádné mechanizmy hlášení chyb či oprav chyb, ke kterým dojde při komunikaci na síťové vrstvě
  - občas k chybě dojde
    - např. směrovač musí zahodit paket
    - vhodné upozornit původce zprávy na vzniklý problém
  - neumožňuje testovat dostupnost určité stanice či zobrazit aktuální zvolenou přenosovou trasu
- Protokol ICMP (*Internet Control Message Protocol*)
  - protokol služebních hlášení, servisní protokol
  - nepřenáší žádná uživatelská data
  - aplikace formátu komunikace klient-server
  - součástí sady TCP/IP protokolů
  - slouží IP protokolu k vyřešení výše uvedených nedostatků

Internet Control Message Protocol (ICMPv4)

- Protokol ICMP (*Internet Control Message Protocol*)
  - umožňuje
    - signalizaci mimořádných událostí v síti
    - testování konektivity
  - přenášen přímo v IP datagramech



  - dělení zpráv na dvě základní skupiny
    - první určena k hlášení chyb (*error-reporting messages*)
    - druhá skupina je určena k dotazování, typicky pak k testování konektivity (*query messages*)

Vybrané typy zpráv ICMPv4 protokolu

Kategorie	Typ	Zpráva
Hlášení chyb	3	nedoručitelný IP datagram (*destination unreachable*)
	4	snížení rychlosti odesílání (*source quench*)
	5	přesměrování (*redirection*)
	11	vypršení doby života (*time exceeded*)
	12	problém s parametry (*parameter problem*)
Dotazování	8	žádost o odpověď (*echo request*)
	0	odpověď na žádost o odezvu (*echo reply*)
	13	požadavek na časové razítko (*timestamp request*)
	14	odpověď na časové razítko (*timestamp reply*)

Obecný formát ICMPv4 zprávy

- pole typ rozlišuje základní typ ICMP zprávy
- část kód využita ke specifikaci důvodu použití konkrétního typu či bližší specifikaci typu
- kontrolní součet počítán z celé ICMP zprávy včetně záhlaví

Bity 0-7	8-15	16-31
Typ	**Kód**	**Kontrolní součet**
Část záhlaví závislá na typu zprávy		
Datová část ICMP zprávy		

Vybrané typy zpráv pro hlášení chyb

- **ICMP protokol**
  - umí chyby hlásit, ne opravovat
  - oprava je (volitelně) ponechána na jiných mechanizmech
  - chybová hlášení
    - vždy odesílána z místa, kde se chyba objeví
    - adresována původnímu zdroji paketu
- **pět základní chyb**
  - **nedoručitelný datagram**
    - paket nebude dále směrován, byl zahozen
    - zpráva informuje odesilatele
    - důvodem vzniku této situace např.
      - směrovač neví, kam má paket dále směrovat
      - nelze jej dále směrovat např. v souvislosti s fragmentací nebo bezpečnostními pravidly

Vybrané typy zpráv pro hlášení chyb

- **potřeba snížení rychlosti odesílání**
  - jednoduchý mechanizmus řízení toku a předcházení zahlcení sítě
  - zpráva odesilatele informuje o tom, že paket byl zahozen z důvodu zahlcení
  - směrovač ve stavu blížícímu se zahlcení odesílá tuto zprávu, na kterou by měl zdroj daného paketu reagovat zpomalením odesílání paketů
  - fungování problematické, směrovač standardně nepozná, kdo ho zahlcuje, bere každý paket jako samostatnou jednotku a nesleduje od koho je kolik paketů
- **potřeba přesměrování**
  - pro řešení směrování ven z lokální sítě, kde se nachází více směrovačů (výchozích brán)
  - směrovač paket nezahazuje, jen informuje odesilatele, že by bylo výhodnější využít jinou výchozí bránu
- **vypršení doby života**
  - při každém skoku se snižuje hodnota TTL
  - snížení na nulu, paket zahozen
  - informace pro odesilatele, že došlo k zahození z tohoto důvodu

Vybrané typy zpráv pro hlášení chyb

- **problém s parametry**
  - nejednoznačná informace v záhlaví IP paketu (neplatná hodnota)
  - paket zahozen a odesilatel informován
- Každé chybové hlášení má v datové části záhlaví původního IP paketu
  - slouží k identifikaci paketu, kterého se chyba týká
  - plus i prvních 8 bajtů datové části původního paketu (typicky záhlaví transportních protokolů)

Vybrané typy zpráv pro dotazování

- určeny k diagnostice některých síťových problémů
- základem komunikace pouze protokolem ICMP a režim dotaz-odpověď
- **žádost o odezvu a odpověď**
  - k ověření, zda dvě síťové vrstvy vzdálených uzlů jsou spolu schopny komunikovat
  - iniciátor komunikace odešle žádost o odezvu na IP adresu testovaného uzlu
  - ten (pokud k němu zpráva dorazí a není aplikováno nějaké omezení) odpoví
  - základní využití aplikace *ping*
- **požadavek na časové razítko a odpověď**
  - primárně určeno k synchronizaci časů dvou stanic či měření zpoždění na přenosové trase v režimu RTT (*round-trip time*; tam a zpět)

Aplikace ICMP zpráv ke zjišťování trasy

- tracert či traceroute
  - využívány zprávy žádost o odezvu a odpověď
  - zobrazení informací o trase mezi dvěma uzly
  - přenosová trasa od zdroje k cíli, doba odezvy uzlů
  - pouze uzly pracující na IP vrstvě
  - technické řešení
    - využití zpráv žádost o odezvu v kombinaci s nastavením hodnoty TTL v záhlaví IP paketu
    - stanice zašle žádost o odezvu cílové stanice, TTL=1
    - první směrovač po trase paket zahodí a zareaguje chybovou zprávou o vypršení časovače
    - tím odesilatel získá adresu prvního směrovače
    - nová žádost o odezvu cílové stanice, TTL=2
    - paket projde prvním směrovač, zahozen na druhém směrovači
    - obdobně dále

```
C:\>tracert 217.31.205.50

Výpis trasy k 217.31.205.50

  1     1 ms     147.229.146.1
  2     1 ms     147.229.252.137
  3     1 ms     147.229.252.201
  4     1 ms     147.229.253.233
  5     1 ms     147.229.252.17
  6     4 ms     91.210.16.13
  7     4 ms     217.31.205.50

Trasování bylo dokončeno.
```

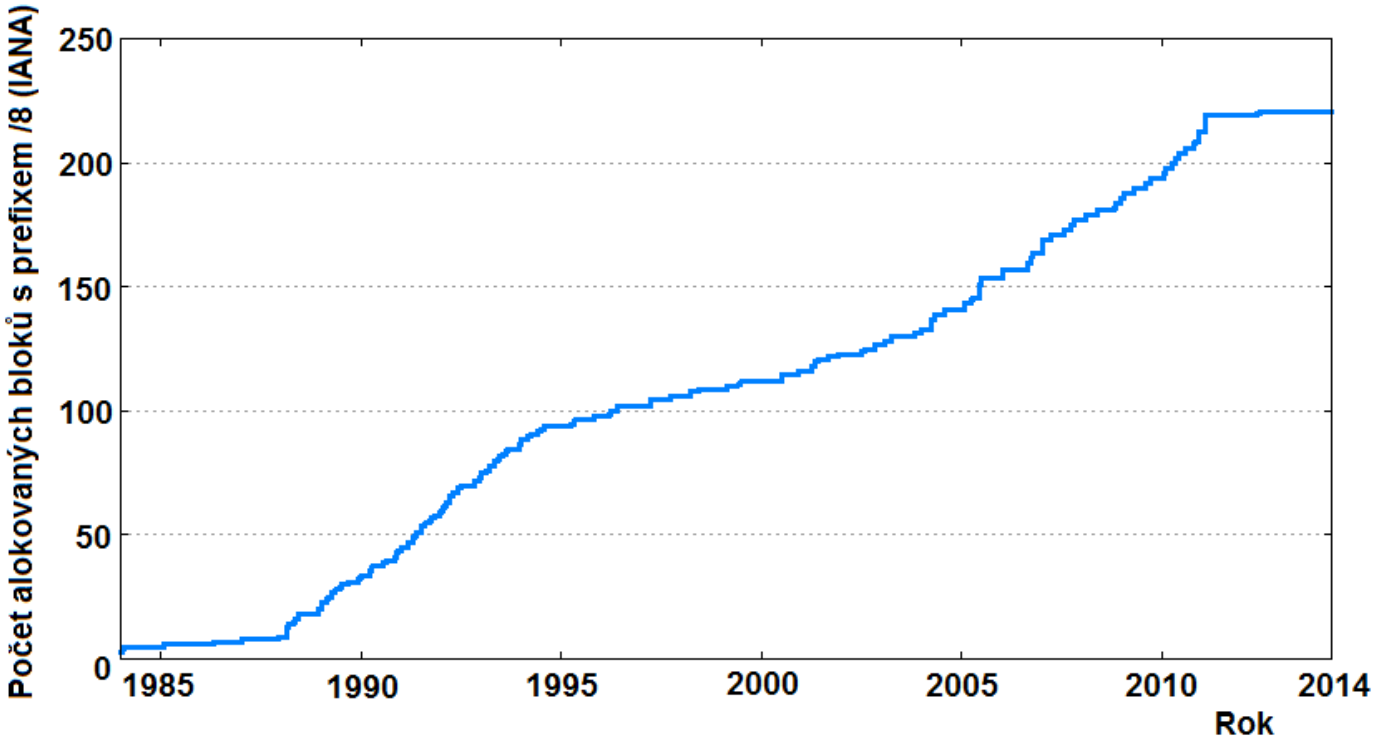
INTERNET PROTOKOL VERZE 6 (IPV6)

Motivace zavádění nového protokolu

- rozšiřitelnost sítí a vzrůstající počet zařízení s potřebou konektivity (mobilních) vyžaduje
  - dostatek IP adres
  - vylepšení dalších parametrů síťové vrstvy
- od poloviny 90. let a později zvolna problém s
  - budoucím vyčerpáním adresního prostoru
  - rozsahem internetových směrovacích tabulek
  - neexistence skutečného end-to-end modelu komunikace (NAT)
- začalo se uvažovat o náhradě IPv4
- vyústěním IP protokol verze 6 (IPv6)
  - celá sada protokolů, především úkoly síťové vrstvy
  - náhradní protokol síťové vrstvy
  - zvýšené množství adres
  - efektivnější záhlaví protokolu

Motivace zavádění nového protokolu

- v současné době stále dominantní IPv4
  - není v ohrožení, stále aktuální
  - bude koexistovat s IPv6, časem nahrazeno
- Současní i budoucí síťoví odborníci nuceni pracovat s IPv4 i IPv6



Základní vlastnosti IPv6

- nekompatibilní s IPv4
- zjednodušení formátu záhlaví – méně povinných položek
- snaha o zredukování velikosti směrovacích tabulek globální úrovně ve směrovačích
- malé snížení hodnoty zpoždění při zpracování ve směrovačích
  - nepřepočítává se CRC paketu
  - žádná fragmentace paketu v průběhu cesty
- nové podpůrné protokoly, zejména ICMPv6
- jednotné adresní schéma pro celý Internet i vnitřní sítě
- tři druhy adres
  - individuální (unicast)
  - skupinové (multicast)
  - výběrové (anycast)
- a již zmiňované rozšíření adresního prostoru
  - z 32 bitů na 128 bitů; z 2^{32} adres na 2^{128} adres

Historie a současnost IPv4 a IPv6

- Základní myšlenkou Internetu možnost přímočaré komunikace dvou libovolných koncových stanic
  - v současné době v IPv4 v souvislosti s masivním nasazením NATu znesnadněno
  - uživatelé často využívají služby, které koncové spojení mezi stanicemi potřebují
    - např. komunikační systémy pro přenos zpráv
    - internetová telefonie
    - videokonferenční systémy
    - sítě pro výměnu dat
- zavedení IPv6, plán vrátit Internet do původně zamýšleného stavu, bez NATu
  - nepříliš reálné vzhledem k tomu, jak je NAT zakořeněn v síťových technologiích i myšlení síťových odborníků
- reálné nasazení IPv6 běží, hotovo jen v některých sítích, tempo zrychluje
  - do konce roku 2010 díky mnoha vylepšením IPv4 stále konkurenceschopné a uspokojovalo většinu současných požadavků

Historie a současnost IPv4 a IPv6

- IPv4 adresování má velké rezervy
  - v počátcích se přidělovaly adresy po velkých blocích (třída A), které nejsou zcela využity
  - pouze cca 70% rozdělených adres je ve směrovacích tabulkách,
    - globálně dostupných
    - otázkou kolik adres je reálně použito
  - experimentální třída IP adres označována jako E
    - rozsah od 240.0.0.0/8 po 255.0.0.0/8
    - není a nebude využita
- i kdyby se všechny tyto adresy podařilo využít, znamenalo by to pouze
  - oddálení problému s vyčerpáním adres
  - další problémy IPv4 by zůstaly nevyřešeny
- K očekávanému vyčerpání adresního prostoru IPv4 (na globální úrovni) došlo počátkem roku 2011

× volné veřejné IPv4 adresy

Historie a současnost IPv4 a IPv6

- IPv6 přináší i nevýhody
  - dvě souvisí s obrovským adresním prostorem
    - z pohledu správce nelze adresní prostor jedné sítě (v rozumném čase) testovat a zjistit tak (ne)přítomnost určitých IPv6 adres (lze považovat i za výhodu)
    - spousta nových L2 problémů
  - předpokládá se, že dlouhou dobu poběží dvě paralelní sítě
    - fyzicky nebo spíše logicky
    - všechny aspekty komunikace řešeny dvakrát
    - náročné udržet obě tyto sítě funkční stejným způsobem (pro koncového uživatele irelevantní, zda komunikuje přes IPv4 nebo IPv6)
  - × jeden hlavní protokol a speciální mechanizmy zprostředkování komunikace mezi verzemi

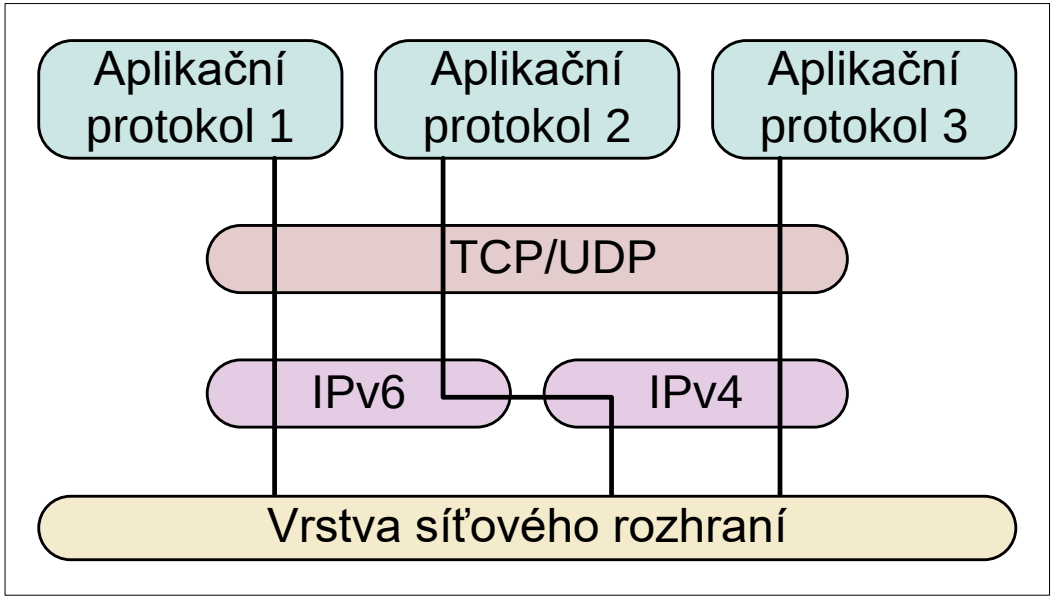
Historie a současnost IPv4 a IPv6

- IPv6 realitou
  - existují funkční globální, regionální poskytovatelské i lokální IPv6 sítě
  - v operačních systémech je podpora již delší dobu standardem
  - bez znalosti IPv6 se již neobejdeme (ani v čistě IPv4 síti)
  - velkým problémem existence obrovského množství software a hardware vytvořeného na míru pro konkrétní použití, typicky bez podpory IPv6
  - IPv6 day: 6.6.2011, 6.6.2012
  - podpora od velkých hráčů

Zavádění IPv6

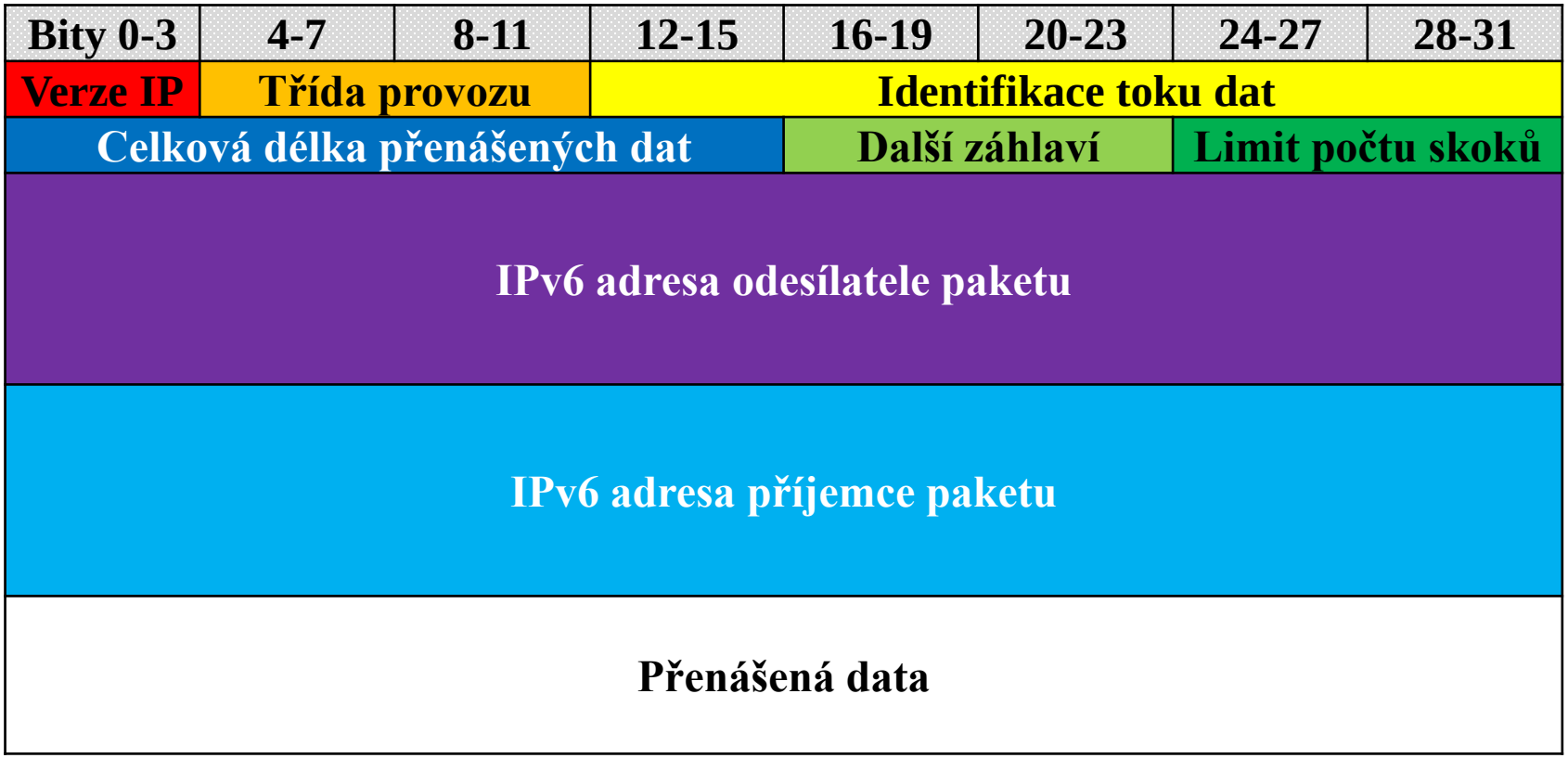
- překážkou v rychlém zavádění IPv6 je především jeho nekompatibilita s IPv4
- proto navrženo **několik mechanizmů** umožňujících hladký přechod od IPv4
  - **Souběh Internetových protokolů IPv6 a IPv4** (*dual stack*)
    - software a hardware podporuje plně oboje
    - zvýšení nákladů na vývoj
    - cesta pro nejbližší roky a sítě s dostatkem veřejných IPv4 adres
    - problémem neustávající potřeba adres IPv4
  - **Tunelování**
    - zapouzdření IPv6 paketu do IPv4
    - technika umožňuje komunikaci přes sítě s odlišnou verzí protokolu IP
  - **Překlad adres**
    - podobný technice NAT, při překladu se zaměňuje IPv4 adresa za IPv6 adresu
    - obecně se technika nazývá NAT-PT (*Network Address Translator - Protocol Translator*)

Zavádění IPv6



- Aplikační protokol
  - 1 přes IPv6
  - 2 přes IPv6 tunelované IPv4
  - 3 přes IPv4

IPv6 datagramy



IPv6 datagramy

- **Verze**
  - zajišťuje správné rozpoznání jednotlivých polí záhlaví paketu (hodnota 6)
- **Třída provozu**
  - nastavení priority paketu, minimální využití
- **Identifikace toku dat**
  - označení toku dat, umožňuje zjednodušené směrování, experimentální
- **Celková délka přenášených dat**
  - délka dat, bez záhlaví, maximum 64 kB, tj. v bajtech
- **Další záhlaví**
  - specifikuje typ vnořeného záhlaví, často TCP, UDP
- **Limit počtu skoků**
  - odpovídá TTL u IPv4
- **IPv6 adresa odesílatele/příjemce**

IPv6 datagramy

- délka základního záhlaví = 40 B (× 20 B u IPv4)
- vyřazení nadbytečných položek, či přesun do rozšiřujících záhlaví
  - rozšiřující volby
  - délka záhlaví
  - kontrolní součet
  - fragmentace
- **Fragmentace**
  - málo častý jev
  - komplikuje směrování
  - přesunuto do speciálního rozšiřujícího záhlaví
- **Kontrolní součet**
  - nepočítán, zbytečné zpomalení (přepočítání v každém uzlu)
  - důvěra v kontrolu na spojové vrstvě, případně na vyšších vrstvách

Adresní prostor

- IPv6 adresní prostor 2^{128}
  - ~ $3{,}4 \cdot 10^{38}$ adres
  - ~ $7 \cdot 10^{23}$ IPv6 adres na 1 m^2 povrchu Země
  - ~ $7 \cdot 10^{17}$ IPv6 adres na 1 mm^2
- IPv4 adresní prostor 2^{32}
  - ~ $4{,}3 \cdot 10^{9}$ adres
  - ~ 8 na 1 km^2
- podstatnou změnou v IPv6 že jedno rozhraní běžně využívá více než jednu IPv6 adresu

Základní druhy IPv6 adres

- **individuální** (*unicast*)
  - adresy identifikující jednotlivá síťová rozhraní, tak aby na ně mohly být zasílány pakety
- **skupinové** (*multicast*)
  - jsou určeny pro adresování skupin
  - pakety odeslané na tuto adresu doručeny všem členům skupiny
  - zastupují i **všesměrové** (*broadcast*) adresy z IPv4
  - zahrnuje i speciální skupiny
- **výběrové** (*anycast*)
  - také skupina adresátů
  - pakety se posílají pouze jedinému jejímu členu, zpravidla tomu nejbližšímu
  - existují i v IPv4

Zápis IPv6 adres

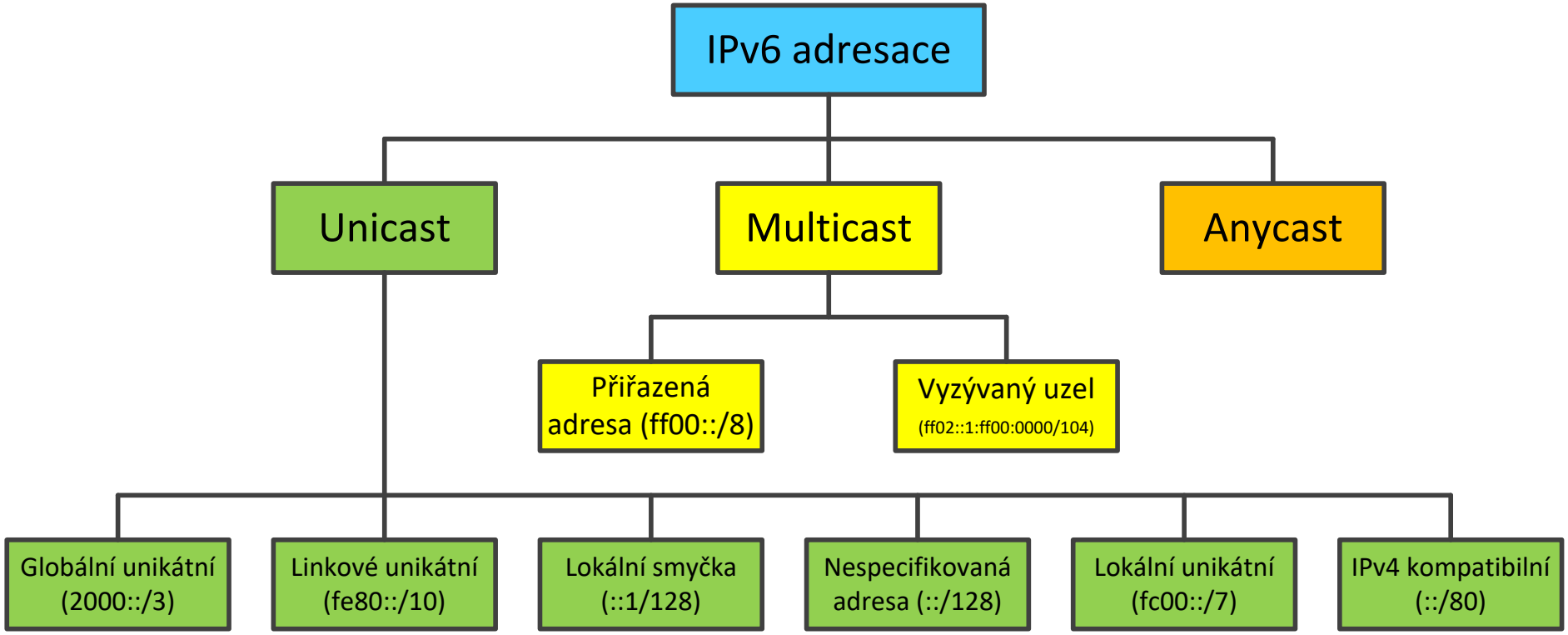
- binární zápis nepoužitelný, desítkový ± také ne

  ↓

- používá se hexadecimální – osm 16-ti bitových bloků oddělených znakem „:“
  - `8000:0000:0000:0000:0ABC:DEF1:2345:789A`
- mnoho nul – zkrácený zápis
  - `8000::0ABC:DEF1:2345:789A`
- první nuly bloku – zkrácený zápis
  - `8000::ABC:DEF1:2345:789A`
- délka prefixu stejný význam jako u IPv4
  - `8000::ABC:DEF1:2345:789A` **/ 64**
  - polovina adresa sítě, druhá polovina adresa stanice

Typy IPv6 adres

- definovány speciální typy a podtypy adres
- zabývat se budeme pouze Globálními unikátními adresami
  - zastupují IPv4 adresy veřejného typu



Globální individuální adresy

- přiděluje IANA prostřednictvím RIRů
- hierarchické přidělování rozsahů (snadnost agregace)
- *pevná* struktura adresy

48 bitů	16 bitů	64 bitů
Globální směrovací prefix	**Identifikátor podsítě**	**Identifikátor rozhraní**
Veřejná topologie	Místní topologie	Lokální síť

- **Globální směrovací prefix**
  - ~ adresa sítě v IPv4
  - celkem těchto prefixů může být ~ 2^{48}, tedy 2,8 . 10^{14}
  - odpovídá přibližně 43 000 globálním sítím na jednoho obyvatele Země

Globální individuální adresy

- **Identifikátor podsítě**
  - rozlišení jednotlivých podsítí v rámci celé sítě
  - rozdělení na podsítě je důležité např. z pohledu rozdělení celé sítě na o něco menší a lépe spravovatelné jednotky
  - v rámci každé sítě může být až 2^{16} podsítí, tedy celkem 65 536 podsítí
  - Plně v kompetenci organizace
- **Identifikátor rozhraní**
  - slouží k odlišení koncových stanic v rámci lokální sítě
  - v jedné podsíti pak může být až 2^{64} stanic ($1{,}8 \cdot 10^{19}$)

Internet Control Message Protocol verze 6 (ICMPv6)

- režijním (servisním) protokolem pro IPv6
- nepřenáší žádná uživatelská data
- implementace v uzlech s podporou IPv6 povinná
  - bez ICMPv6 je IPv6 nefunkční
- využití
  - ohlašování chybových stavů
  - testování dostupnosti síťové vrstvy
  - výměna určitých provozních informací
  - objevování sousedů (obdoba ARP)
  - podpora správy multicastových skupin
  - překladu adres
  - zajištění mobility
- detaily jsou nad rámec tohoto kurzu

Směrování v IPv6 sítích

- totožné principy jako v IPv4 sítích, pouze *delší* adresy
- IGP IPv6 protokoly
  - **RIPng** (*Router Information Protocol Next Generation*)
  - **EIGRP for IPv6** (*Enhanced Interior Gateway Routing Protocol*) – směrovací protokol firmy Cisco ve verzi pro IPv6
  - **OSPFv3** (*Open Shortest Path First*)
  - **IS-IS for IPv6** (*Intermediate System to Intermediate System*)
- EGP IPv6 protokol
  - **BGP4+** (*Border Gateway Protocol*)

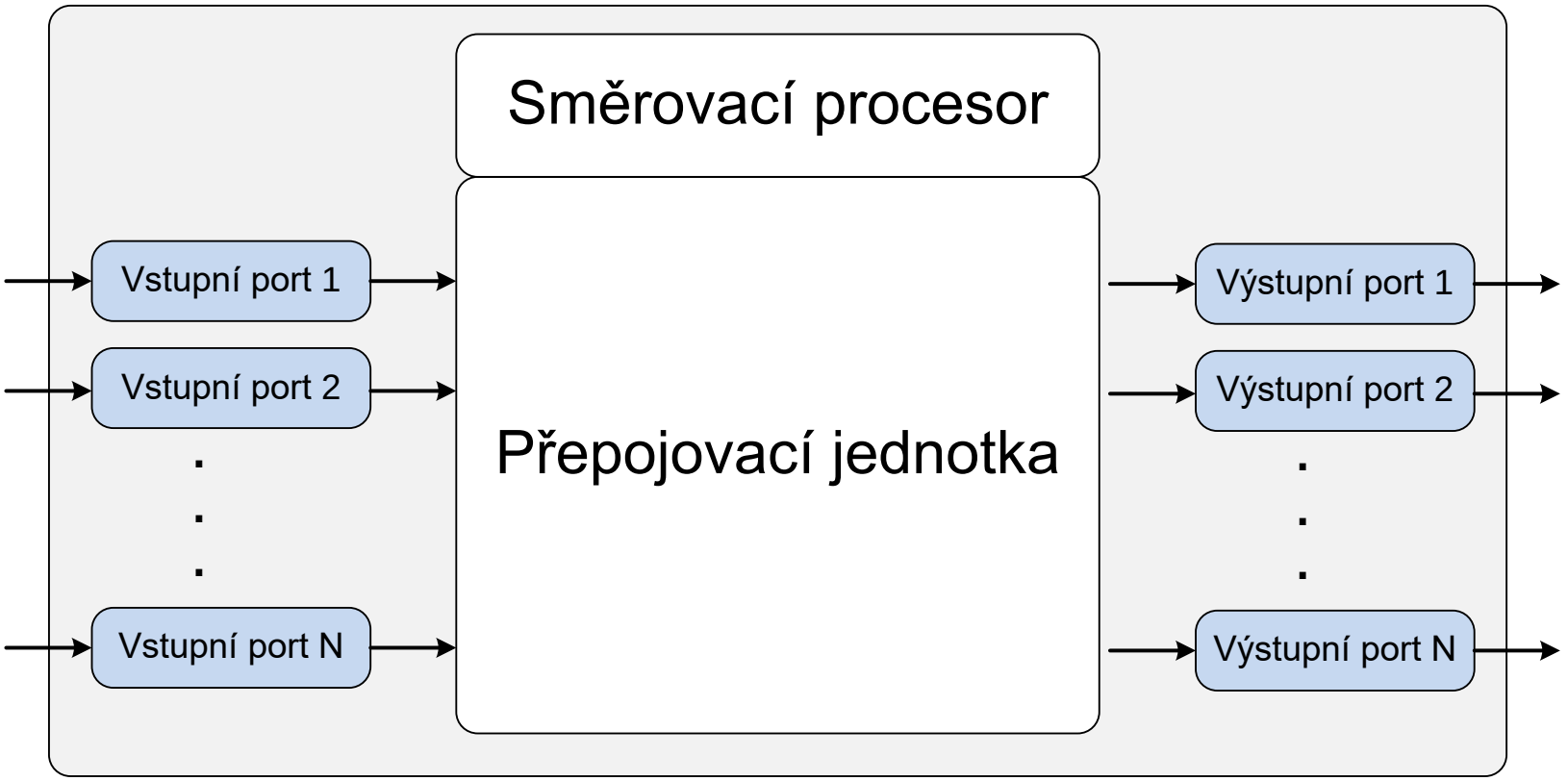
Zařízení síťové vrstvy

- **směrovač**
  - základním zařízením síťové vrstvy, slouží především k propojení sítí
  - pracuje zejména s pakety, ty předává a doručuje podle obsahu jejich záhlaví
  - základní úlohou směrování
  - pracuje zpravidla se směrovacími protokoly
    - umožňují zjišťovat směrovací informace od sousedů
    - následně vybudovat a udržovat směrovací tabulku
  - typicky dvě a více síťových rozhraní (každé vlastní IP adresa)
  - pracuje vždy i s ICMP protokolem
    - sám původcem zpráv (paketů s informacemi o chybě)
- **funkce směrování**
  - realizováno primárně v hardware nebo v software
  - hardwarový směrovač bývá často označován jako L3 přepínač
  - směrovač lze vytvořit i pomocí vhodného software na běžné pracovní stanici
    - za předpokladu existence více síťových rozhraní a nižších požadavků na propustnost

Zařízení síťové vrstvy

- směrovače běžně podporují i další mechanizmy
  - zajištění kvality služeb
  - určité bezpečnostní mechanizmy (filtrování nežádoucího provozu)
  - …
- základní struktura směrovače
  - vstupní porty slouží k přijetí paketu
  - výstupní porty k odeslání
  - v případě plně duplexní komunikace
    - fyzicky vstupní a výstupní totožné, z hlediska směrování jsou to oddělené jednotky
  - přepojovací jednotka
    - na základě řízení procesorem funkce směrování
    - klíčová funkce, řada technik
    - nad rámec textu

Zařízení síťové vrstvy – základní struktura směrovače



Zařízení síťové vrstvy – základní struktura směrovače

- vstupní port
  - musí disponovat fyzickou vrstvou, spojovou vrstvou a typicky i frontou
- každý výstupní port
  - stejné komponenty
  - pouze v opačném pořadí
- fronta
  - slouží k ukládání požadavků či zpráv při přijetí nebo před odesláním do času, kdy bude možné provést zpracování či odeslání
  - tvoří tak určitý vyrovnávací mechanizmus pro situace, kdy směrovač nestíhá zpracovávat všechny pakety ihned

Zařízení síťové vrstvy – základní struktura směrovače