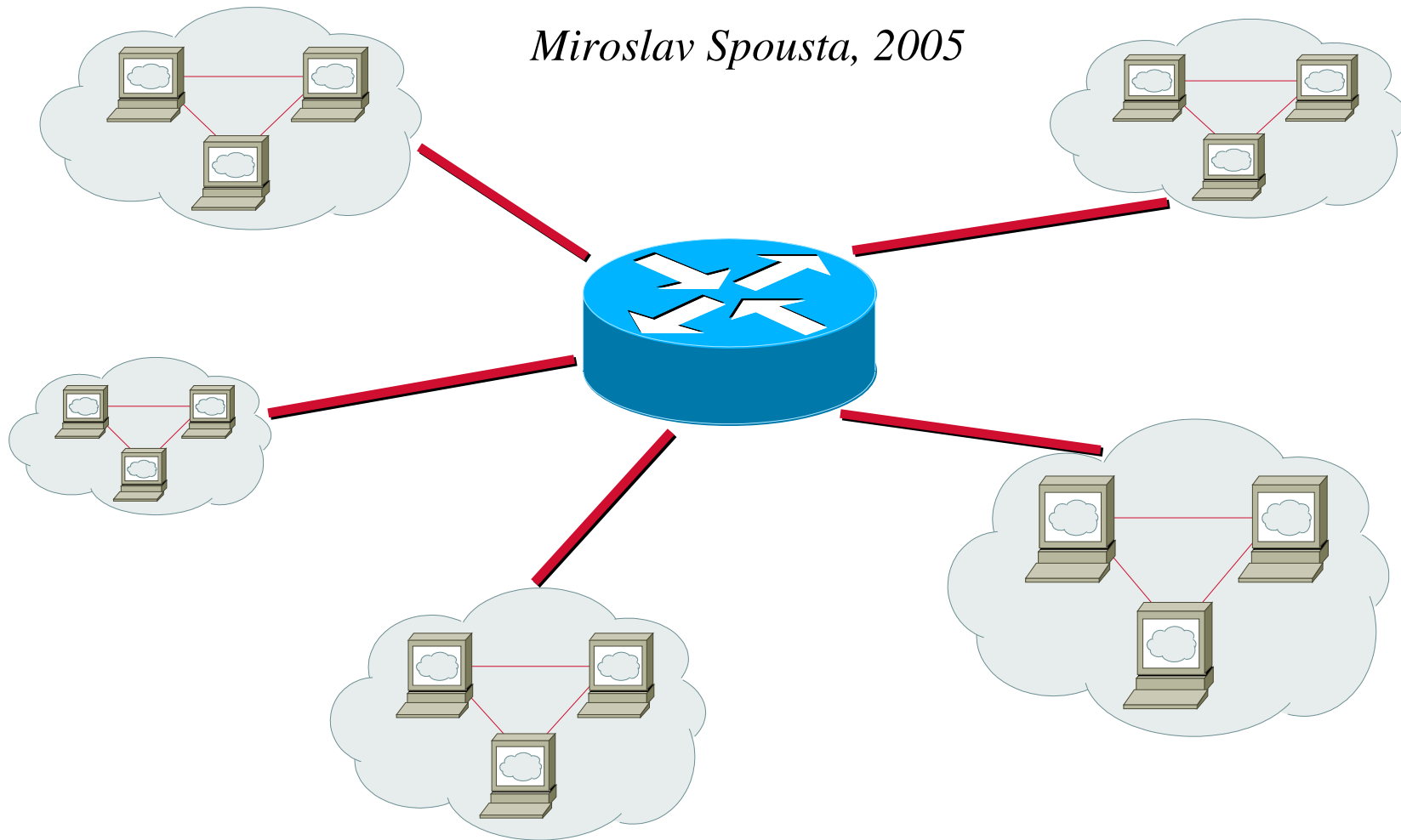


# Počítačové sítě II

## 11. IP verze 4, adresy

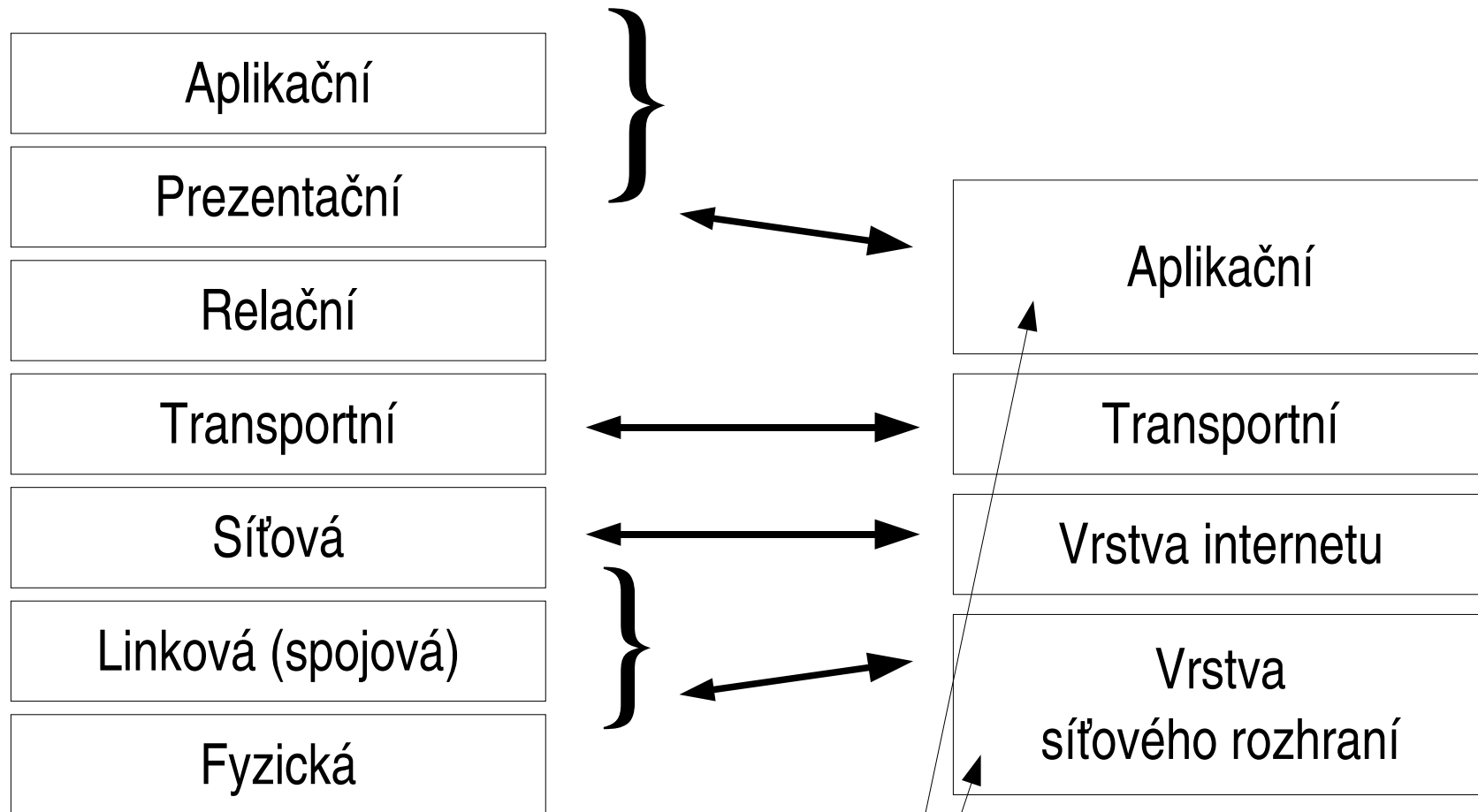
*Miroslav Spousta, 2005*



# IP verze 4

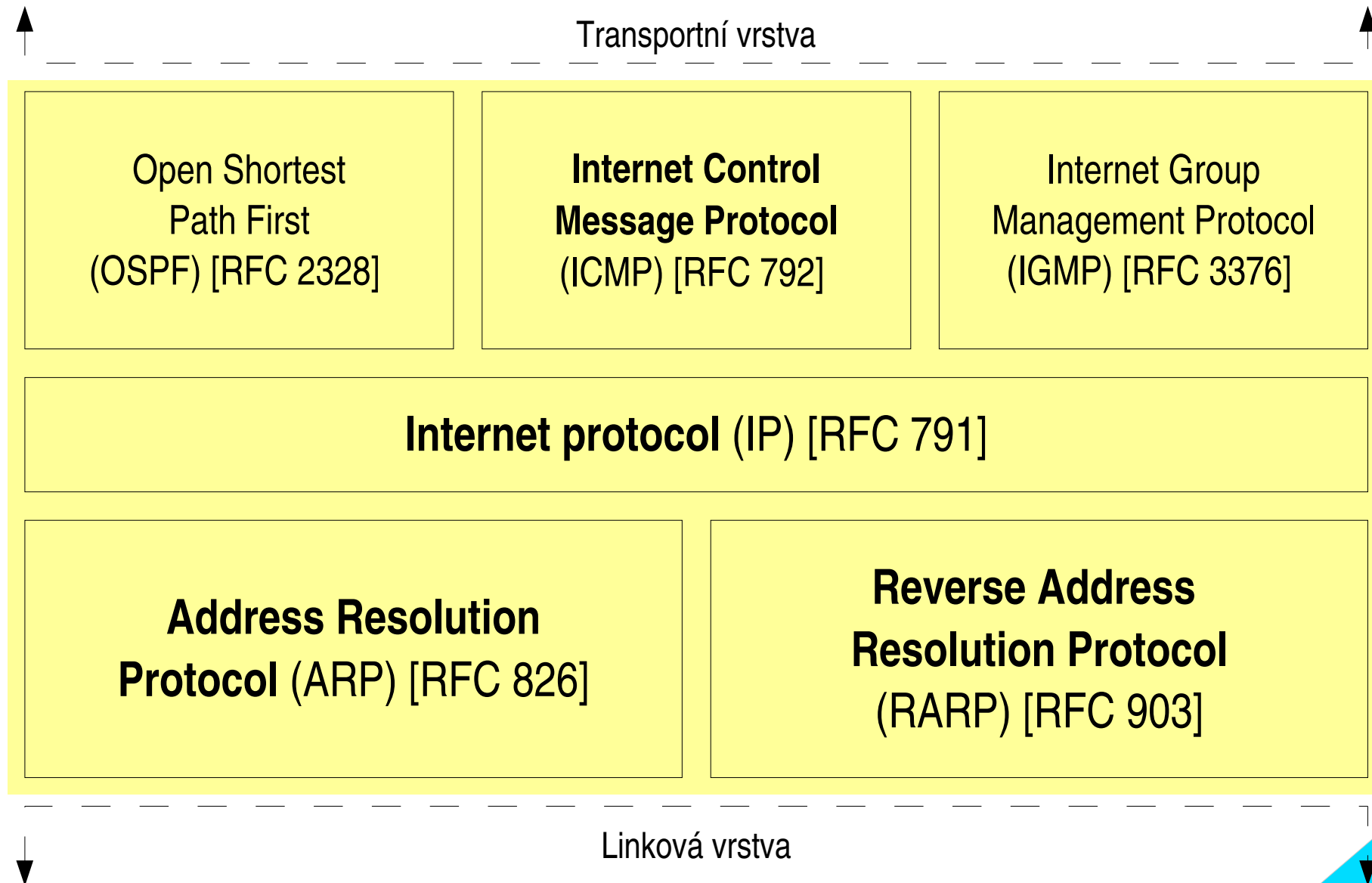
- základní protokol Internetu, RFC 791
- v současnosti nejrozšířenější síťový protokol
  - součást síťové vrstvy architektury TCP/IP
- první verze (1, 2, 3) se používaly během vývoje v letech 1977 – 1980
- v budoucnu se počítá s nasazením IP verze 6 (IPv6)
  - dnes experimentální sítě, pomalu se prosazují
  - volny.cz
- IPv5 byl streamovací protokol, neujal se
- existují i další verze protokolu IPv7 a IPv8
  - neujaly se

# Vrstvy TCP/IP



TCP/IP neřeší

# Síťová vrstva TCP/IP



# IP: Nespojovanost

- IP je nespojovaný protokol (není třeba předem navazovat spojení)
  - obrovská výhoda: bezstavovost: jednodušší architektura síťových prvků
  - vhodné pro řídké přenosy (většina datových přenosů)
  - spojovaný přenos mohou zajišťovat vyšší vrstvy
- každý datagram (paket) je samostatná jednotka
  - k cíli cestuje nezávisle na ostatních
  - po cestě může vzniknout potřeba paket rozdělit (pokud to linková vrstva vyžaduje)
  - jednotlivé fragmenty se stávají pakety a opět cestují nezávisle na sobě
  - sestavení fragmentů provede cílový uzel

# IP: Nespolehlivost

- IP je nespolehlivý protokol
  - není zaručeno dodání ani zachování obsahu paketů
  - pakety mohou přijít v jiném pořadí, než byly odeslány, případně mohou přijít vícekrát
  - spolehlivost není nikdy 100%, bývá spojena s nemalou reží
- nespolehlivost umožňuje jednodušší přenosovou architekturu
  - nespolehlivost vadí u multimédií, jinak lze poškozená data poslat znovu
  - spolehlivost mohou zajišťovat vyšší vrstvy (TCP)
  - IP protokol nekontroluje korektnost dat (kontrolní součet je jen pro IP hlavičku)

# Maximální snaha

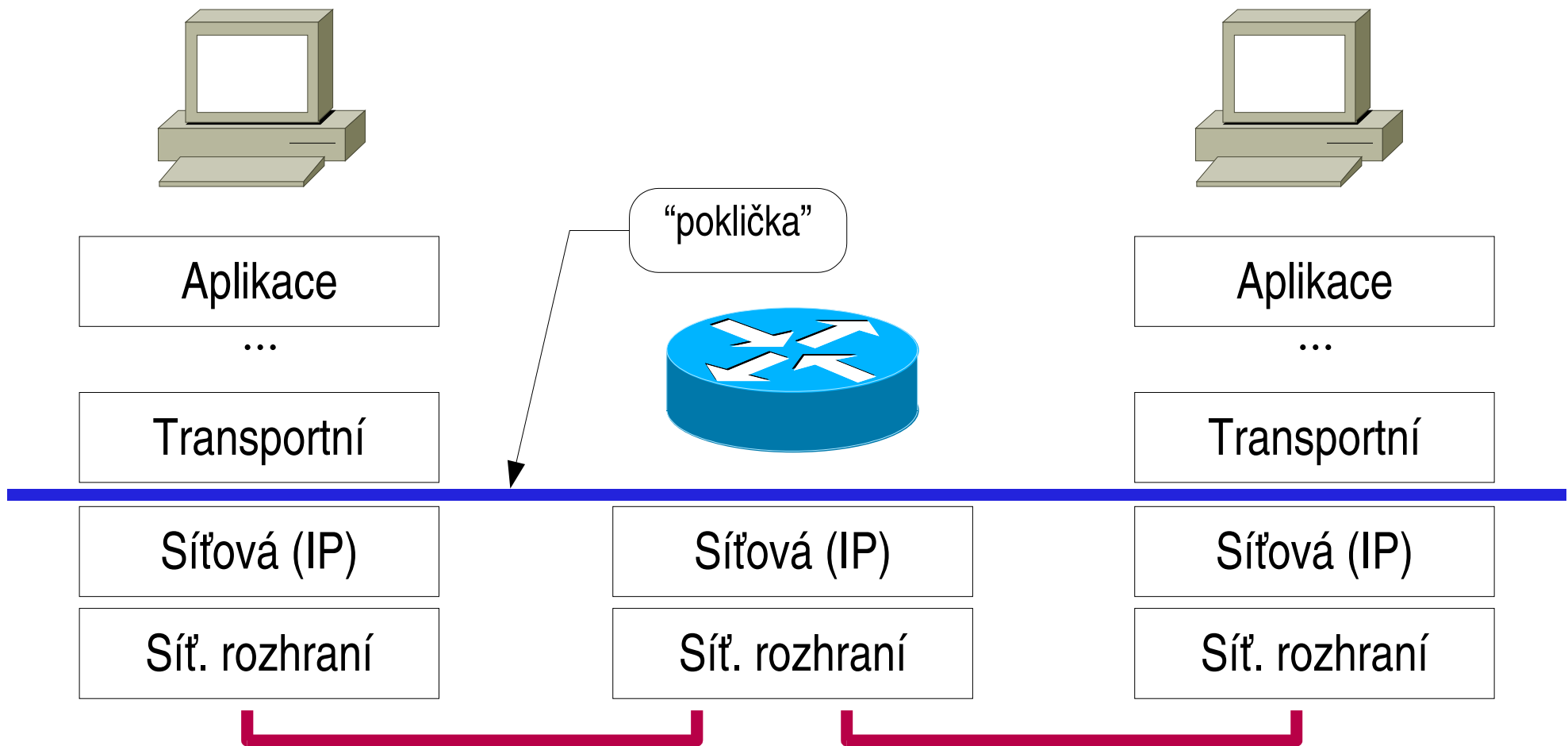
- princip maximální snahy (best effort)
  - ale nezaručeného výsledku
  - snaha vyhovět všem požadavkům, pokud je to možné
  - není-li, může s daty nakládat jak uzná za vhodné
  - ale musí se ke všem chovat stejně
  - problém s multimediálními přenosy, částečné řešení je navýšení přenosové kapacity
- alternativní k QoS (Quality of Service)
  - zajišťují, že služba bude mít předem určené vlastnosti
  - vhodné pro multimediální přenosy

# Poklička

- IP bylo vyvinuto jako jednotná nadstavba nad síťovými technologiemi
  - umožňuje fungovat nad mnoha rozličnými síťovými technologiemi
  - od Ethernetu po ATM
  - IP protokol tvoří „pokličku“, pod kterou není vidět
  - výjimka: síťová vrstva bere ohled na maximální velikost linkového rámce
- důsledek: IP používá adresy nezávislé na linkových adresách
  - musí existovat převodní mechanismy (protokoly ARP, RARP)
  - adresy vyjadřují pohled na svět skrz brýle TCP/IP:
  - skládají se z adresy sítě a adresy počítače v rámci sítě

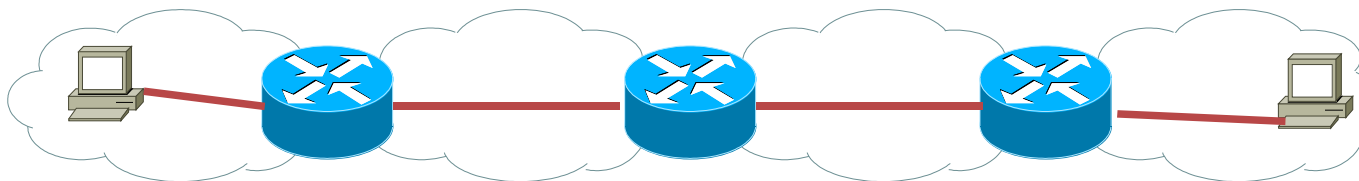


# Představa pokličky



# Adresace

- každý uzel má právě jednu unikátní adresu
  - v ideálním případě, směrovač má více adres, některé počítače nemají unikátní adresu
- adresy jsou abstraktní, všude stejné (nezávislé na linkových adresách)
- adresy mají 32 bitů, zapisují se desítkově po bajtech
- skládají se z části označující síť a z části označující uzel v dané síti
  - vychází z pohledu TCP/IP na propojení sítí
  - každé dva uzly jsou propojeny přes řetězec sítí a směrovačů



# Adresace

- směrovače se rozhodují na příslušnosti cílové adresy daného paketu k síti
  - tedy ne na základě celé adresy cílového uzlu
  - zmenšuje směrovací tabulky, zjednodušuje směrování
- je třeba umožnit z adresy extrahovat síťovou část a číslo počítače v síti
- adresy jsou fyzicky jednolitě (32 bitové), logicky dvojsložkové
- původně bylo z adresy možné zjistit přímo rozdělení
  - rozlišovaly se tzv. třídy adres
- dnes se rozlišení uvádí explicitně (maskou, příp. počtem bitů)
  - např 194.113.31.128/26 nebo 194.113.31.128/255.255.255.192

# Přidělování IP adres

- IP adresy nemohou být přidělovány nahodile
  - musí být respektováno rozdělení na sítě (celkovou topologií)
  - uzly ve stejné síti musí mít stejnou síťovou část adresy
  - uzly v různých sítích musí mít různou síťovou část adresy
- IP adresa patří rozhraní uzlu, ne celému uzlu
- IP adresy se musí přidělovat po celých blocích (po sítích)
- jak rozdělit adresu (po kolika bitech?)
  - raději více malých sítí nebo málo velkých sítí?
  - zamezit zbytečnému plýtvání IP adresami (musí se přidělovat po sítích)

# Přidělování IP adres

- je potřeba více adres uzlů než adres sítí. Kde zvolit hranici?
- pevná hranice (např. 16 bitů) by nevyhovovala
  - pro síť s 200 počítači by bylo přiděleno 65534 adres
- výsledné rozdělení:
  - 126 sítí velkých, v každé z nich až 16 miliónů adres uzlů ( $2^{24}-2$ )
  - 16384 sítí středních, v každé z nich maximálně 65534 adres uzlů ( $2^{16}-2$ )
  - více než dva milióny sítí malých ( $2^{21}$ ), v každé maximálně 254 adres uzlů ( $2^8-2$ )
  - v dobách počátku Internetu se to zdálo rozumné
  - dneska nepoužitelné (došlo k vyčerpání rozsahů)

# Třídí adres IPv4

7 bitů

24 bitů

A

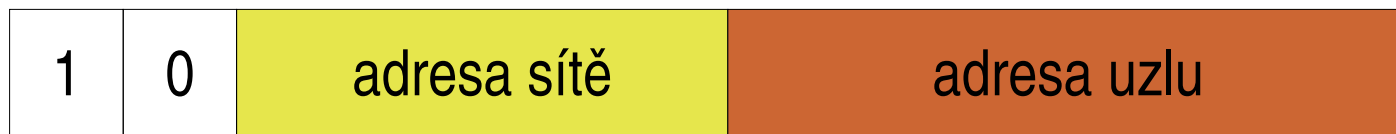


1.x.x.x – 126.x.x.x

14 bitů

16 bitů

B

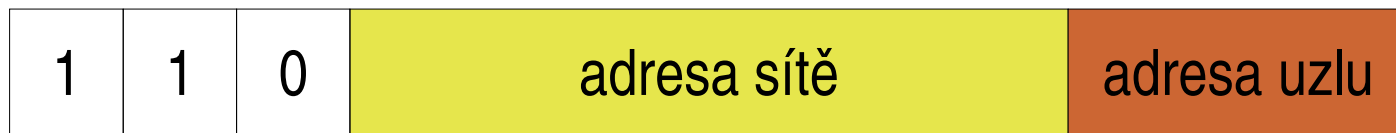


128.0.x.x – 191.255.x.x

21 bitů

8 bitů

C



192.0.0.x – 223.255.255.x

# Další třídy adres

- kromě tříd A, B, C existují ještě další speciální třídy adres
- třída D, která je určena pro multicasting
  - 224.0.0.0 – 239.255.255.255
- třída E, která je oficiálně určena pro budoucí použití
  - 240.0.0.0 – 255.255.255.255
- adresy D a E nejsou dvojsložkové (přidělují se po 1)
- v rámci sítě existují adresy se speciálním významem
  - adresující všechny počítače v síti, danou síť, atd.

# Speciální adresy

0	0
---	---

tento počítač

0	x
---	---

počítač v této síti

x	0
---	---

tato síť jako celek

x	1...1
---	-------

všechny počítače v síti (broadcast)

1...1	1...1
-------	-------

všechny počítače v této síti (broadcast)

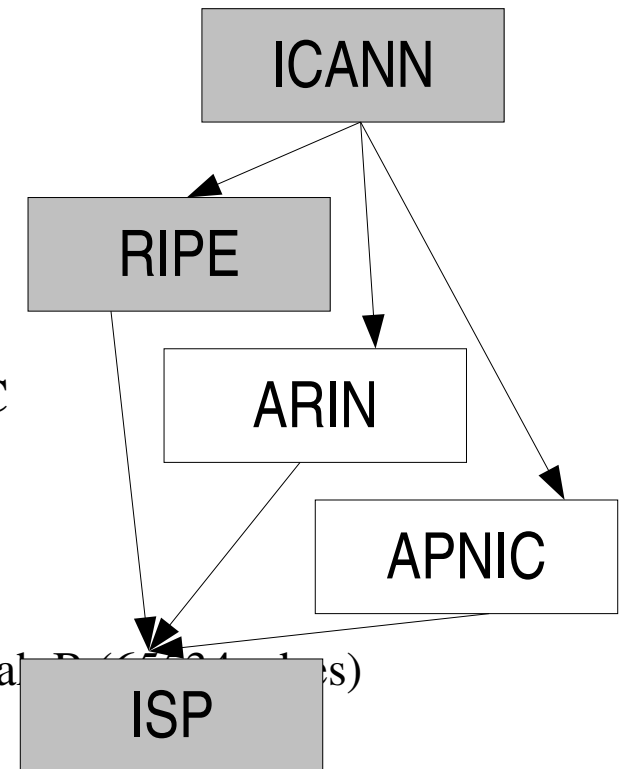
127	0.0.1
-----	-------

loopback (rozhraní, které nejde ven)



# Problém s vyčerpáním adres

- každá adresa je přidělena maximálně jednou
  - v Internetu nesmí existovat dva uzly se stejnou adresou
- adresy přiděluje centrální autorita
  - distribuce ICANN -> RIPE (ARIN, APNIC) -> ISP
  - ICANN přiděluje celé bloky, RIPE přiděluje adresy B a C
- došlo k velkému plýtvání
  - každý žadatel dostal aspoň rozsah C (254 adres)
  - kdokoliv potřeboval více dostal více rozsahů C nebo rozsah B (65 536 adres)
  - adresy začaly docházet, co s tím?



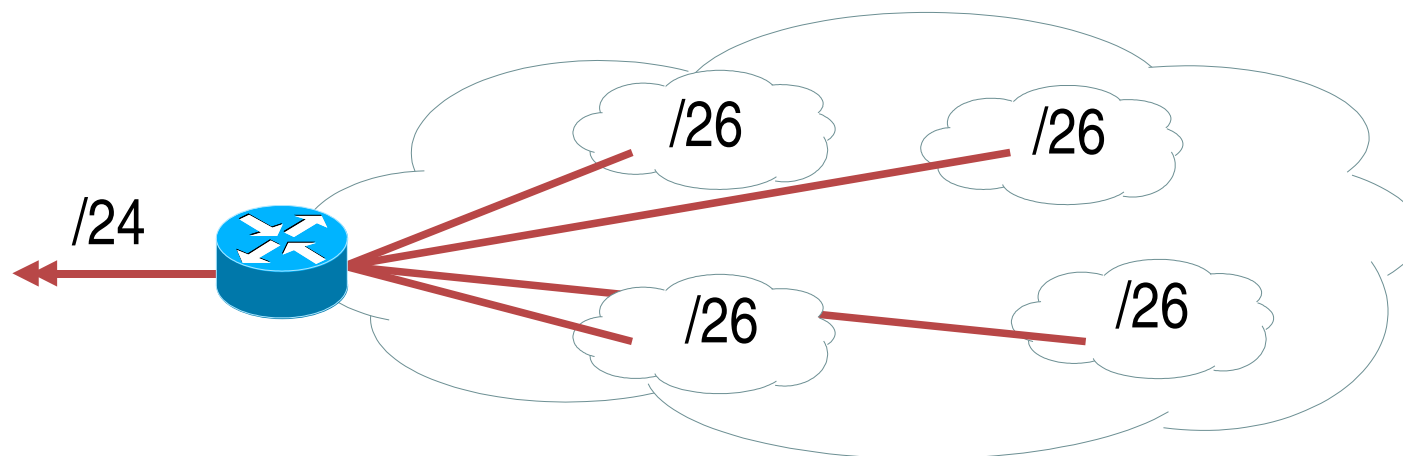
# Řešení vyčerpání adres

- zapomenout na třídy a hranici adresa sítě/adresa uzlu v síti posouvat libovolně (po bitech)
- původní mechanismy práce s adresami na to nebyly připravené
  - tedy spoléhaly na třídy adres
- je nutné zavést tzv. masku sítě
  - jednoznačně určuje rozhraní adresy sítě/uzlu
  - udává se buď počtem bitů nebo přímo jako maska (pro operaci AND)
  - např 194.113.31.128/26 nebo 194.113.31.128/255.255.255.192

$$194.113.31.129 \text{ AND } 255.255.255.192 = 255.255.255.128$$

# Subnetting

- rozdělení původního rozsahu sítě na několik částí
  - proto subnetting
  - např. jedna adresa třídy C na 4 podsítě (maska /26)
- rozdělení se provede v rámci jednoho subjektu
  - navenek se síť tváří jako jediná síť třídy C
  - je možné použít, pokud sítě mají jeden společný vstupní bod (např ISP)

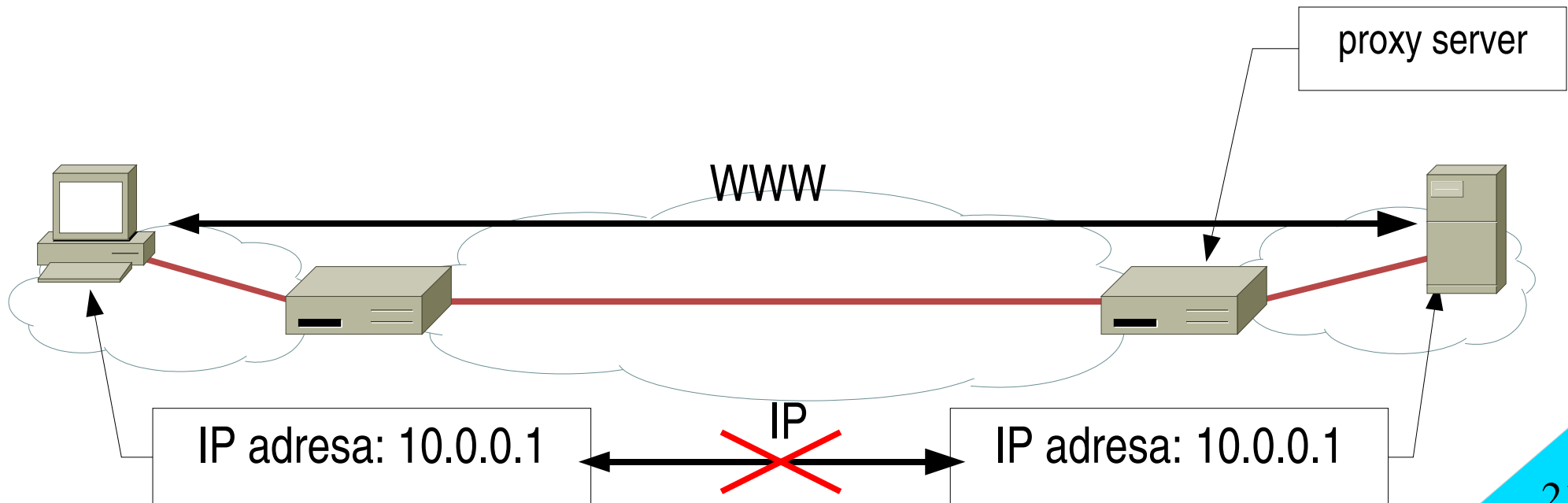


# Další metody

- dnes už se nepřidělují celé třídy, ale jen jejich části
- výrazně se omezila spotřeba adres IPv4
- principiální řešení to ale není (stále je shora omezen počet aktivních uzlů maximálním počtem adres IPv4)
- konečné řešení má přinést IPv6 (podstatně více adres)
- rozvinuly se i další metody vedoucí k úspoře adres:
  - CIDR (Classless InterDomain Routing)
  - použití privátních IP adres
  - NAT (Network Address Translation)

# Privátní adresy

- uzly v Internetu musí mít unikátní IP adresy, aby mohly komunikovat
  - směrovače musí mít jasno, kam mají pakety pro daný uzel přeposílat
- tam, kde není nutná přímá komunikace, je možné adresy opakovat
  - např. u počítačů za firewallem nebo aplikačním proxy serverem
  - takové uzly mohou mít speciální, tzv. privátní adresy



# Privátní adresy

- speciální vyhrazené adresy, které nepatří do Internetu (RFC 1597)
- smí se vyskytovat pouze uvnitř privátních sítí, nesmí projít skrz router
- router ani nesmí šířit směrovací informace o těchto adresách vně sítě
- teoreticky by v privátní síti bylo možné použít libovolné IP adresy
  - ale není to vhodné (nešlo by rozlišit, zda je cílový uzel uvnitř privátní sítě nebo vně)
- privátní adresy je vhodné použít i u sítě, která není připojena k Internetu

1 x třída A: 10.0.0.0 – 10.255.255.255

16 x třída B: 172.16.0.0 – 172.31.255.255

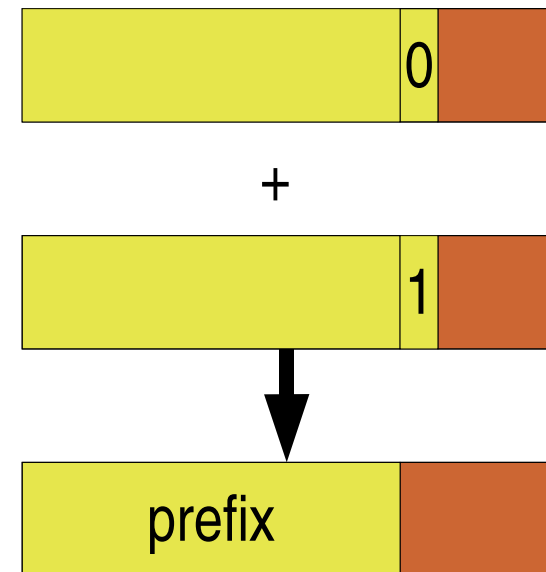
256 x třída C: 192.168.0.0 – 192.168.255.255

# CIDR

- Classless InterDomain Routing, také supernetting
- původně platilo: co jeden záznam v tabulce, to jedna adresa třídy A, B, C
- podobné jako subnetting, ale hranice se posouvá opačným směrem
  - je možné přidělit více podsítí najednou
- do směrovacích tabulek se zaznamenávají kromě adresy také masky sítě
- v podstatě se jedná o slučování „sousedních“ sítí
- síťová část je označena jako „prefix“
- tak vznikne tzv. CIDR blok
- IP adresy se dnes přidělují po CIDR blocích

# CIDR

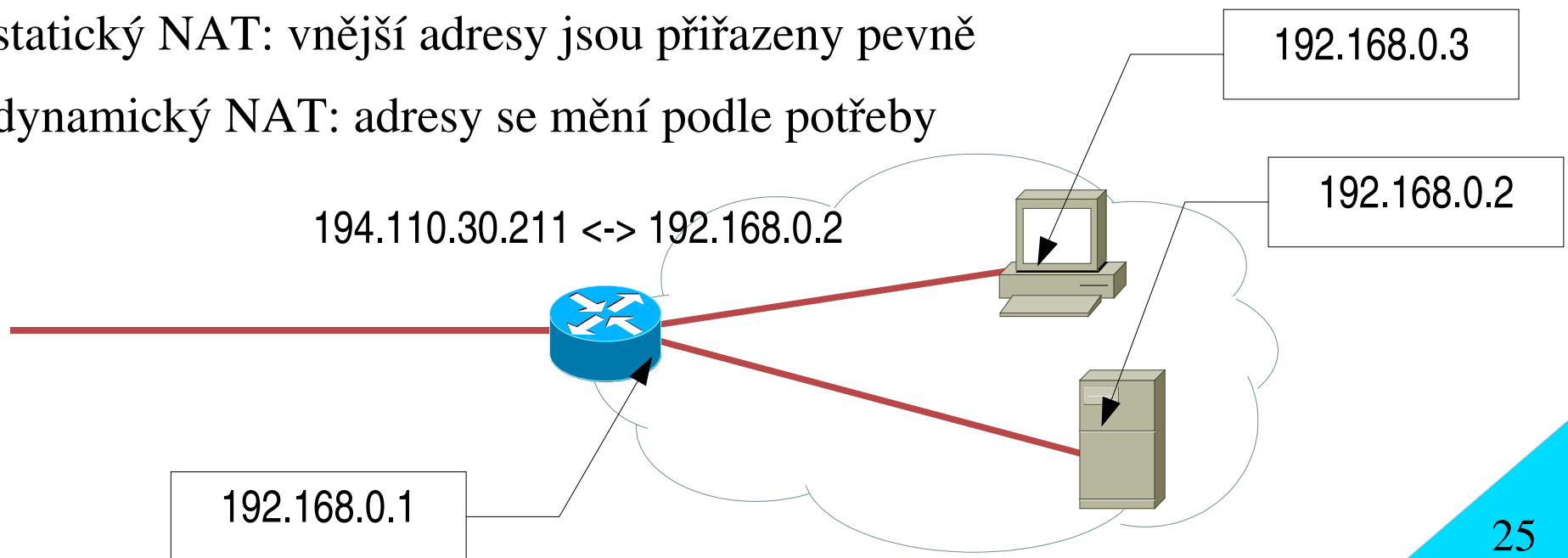
- dokonce CIDR umožňuje zmenšit objem směrovacích tabulek
  - zvláště u páteřních směrovačů, které by jinak musely obsahovat položku pro každou síť v Internetu
  - dochází ke sdružování záznamů se stejným prefixem
  - další zmenšení: autonomní systémy
- IP adresy se stávají závislými na připojení
  - neboli sítě již nemohou mít libovolné adresy
  - při změně ISP se změní IP adresa
- opět zamezilo velkému plýtvání s adresami





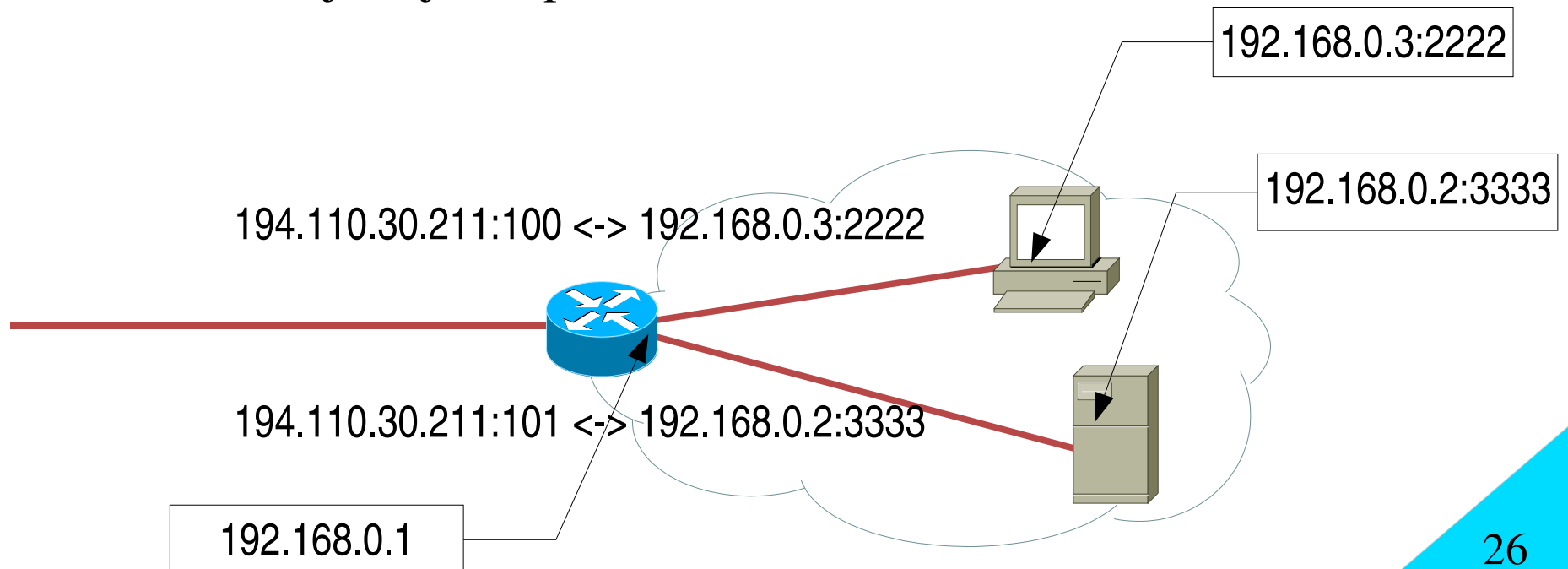
# NAT

- Network Address Translation neboli překlad adres
  - v privátní síti můžeme použít privátní adresy (vyhrazené rozsahy)
- brána přepisuje adresy v hlavičce IP na „vnější“ adresy Internetu (1:1)
  - pro pakety obráceným směrem musí přepsat adresy zpět
- pro počítače, které nekomunikují se světem nepotřebujeme vnější adresy
- statický NAT: vnější adresy jsou přiřazeny pevně
- dynamický NAT: adresy se mění podle potřeby



# PAT

- Port Address Translation neboli překlad portů
- podobné jako NAT, ale překládá se zpravidla na jednu vnější adresu (1:N)
- jednotlivé spojení se rozlišují číslem portu
  - na vyšší (transportní) úrovni
- celá síť se chová jako jeden počítač



# NAT/PAT

- **výhody:**
  - využívá jen jednu adresu/málo adres
  - bezpečnost(?): nelze navazovat spojení směrem dovnitř
- **problémy:**
  - nelze navazovat spojení směrem dovnitř (P2P)
    - FTP přenáší data směrem ke klientovi
  - problém se službami/protokoly, které přenáší adresy i jinde než v hlavičkách
    - např. IPSec
  - řešení: rozpoznávat provoz a snažit se měnit informace i v paketech
- NAT boří jeden ze základních principů fungování TCP/IP: *minimální intervence* (přenášející vrstva se nestará o to, co přenáší)

# Datagram IP

4b	4b	8b	16b
verze	délka záhlaví	typ služby P P P D T R C 0	celková délka paketu
identifikace		DF MF	ofset fragmentu
TTL	protokol		kontrolní součet hlavičky
zdrojová adresa			
cílová adresa			
volitelné rozšíření záhlaví			
data (max. 65535-délka hlavičky)			

# IP datagram

- verze: 4
- délka záhlaví: po 4B, typicky 20B (bez rozšíření), max. 60B
- typ služby (ToS – Type of Service): priority a kvality služby
  - různá kritéria, nedoporučuje se používat více než dvě najednou
  - dnes se používá pro QoS (Quality of Service) – kód DSCP
- celková délka: v bajtech (včetně záhlaví)
- identifikace: pro podporu fragmentace, jednoznačně identifikuje datagram
- flags: 3 bity 0 DF MF, DF = nefragmentovat, MF = následují fragmenty
- číslo fragmentu: pozice od začátku původního datagramu
- TTL (Time To Live): počítadlo, dekrementuje se po průchodu směrovačem, pokud dosáhne 0, datagram se zahodí. Brání nekonečnému bloužení datagramu sítě (např. při chybné konfiguraci)

# ToS

Aplikace	min. zpoždění	max. propustnost	max. spolehlivost	min. cena	hodnota (hex)
telnet	1	0	0	0	10
FTP příkazy	1	0	0	0	10
FTP data	0	1	0	0	08
SMTP příkazy	1	0	0	0	10
SMTP data	0	1	0	0	08
DNS dotaz	1	0	0	0	10
SNMP	0	0	1	0	04
BOOTP	0	0	0	0	00
NNTP	0	0	0	1	02

# IP datagram

- číslo protokolu: udává, který protokol se má použít na zpracování dat

Protokol	Popis	Číslo protokolu
ICMP	chybové zprávy IP	1
IGMP	řízení skupin	2
IP v IP	tunelování IP v IP	4
TCP	spolehlivý transportní protokol	6
UDP	nespolehlivý transportní protokol	9
ESP	IPSec šifrování	50
AH	IPSec integrita	51
OSPF	směrovací protokol	89

# IP datagram

- zabezpečení záhlaví: jedničkový doplněk hlavičky IP
- zdrojová, cílová adresa: IP adresy
- volitelné možnosti:
  - zdrojová cesta, zabezpečení
  - různá délka, ale v násobcích 4B (32bitů)
  - nepoužívá se (náročné na zpracování ve směrovačích), směrovače zahazují
- data: vlastní data vyšší vrstvy
  - nejsou zabezpečeny kontrolním součtem (je úkolem vyšší vrstvy!)



# Fragmentace

- velikost IP datagramu může být až 65535 bajtů
- ale linková vrstva může mít podstatně menší MTU (Maximum Transmission Unit) – maximální velikost rámce
  - např. u Ethernet je to 1500B (+ hlavička a patička Ethernetu)
- je nutné datagram rozdělit do několika menších, které je možné přenést linkovým rámcem
- potřeba rozdělit datagram může vzniknout i po cestě k cíli (při přechodu z jedné technologie na jinou)
- fragmentaci provádí po cestě směrovače
  - pokud to není zakázané nastavením bitu DF (Don't Fragment)
  - v IPv6 provádí fragmentaci pouze zdrojová stanice
- fragmenty sestavuje *vždy* až koncová stanice

# Fragmentace

- stanice i směrovač znají MTU jen pro lokální síť, nemohou vědět, jaká bude po cestě k cíli
- popsáný způsob umožňuje opětovnou fragmentaci fragmentů
- síť by měla přenést aspon 576B nefragmentovaných (512B užitečných)

