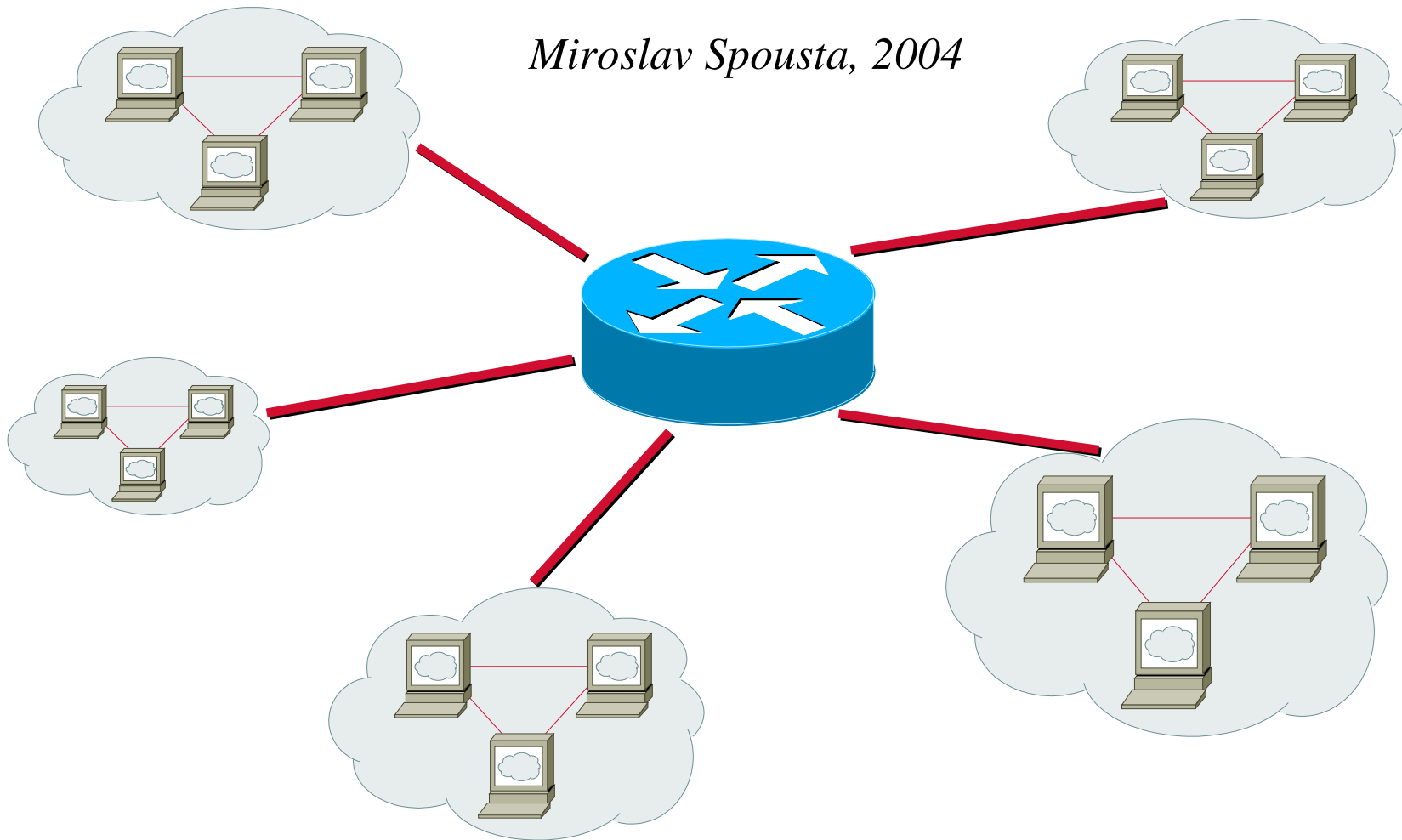


Počítačové sítě I

2. Síťové modely

Miroslav Spousta, 2004



Síťový model

Jak postavit počítačovou síť?

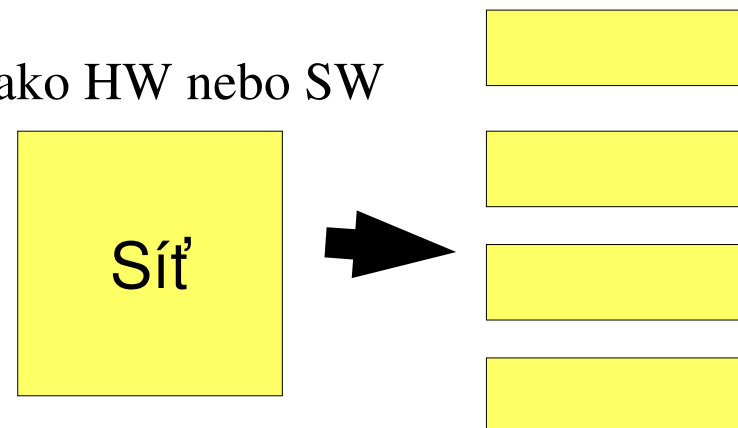
- složitý problém, je vhodné ho rozložit na podproblémy
- nabízí se možnost dekomponovat na několik úrovní podle funkce

dobře odpovídá opravdovým implementacím

umožňuje to do jisté míry zaměnitelnost implementací

v praxi: zaměňujeme hlavně nejnižší vrstvy

- jednotlivé vrstvy mohou být řešeny jako HW nebo SW
- kolik má být vrstev?
- co má která za úkol?



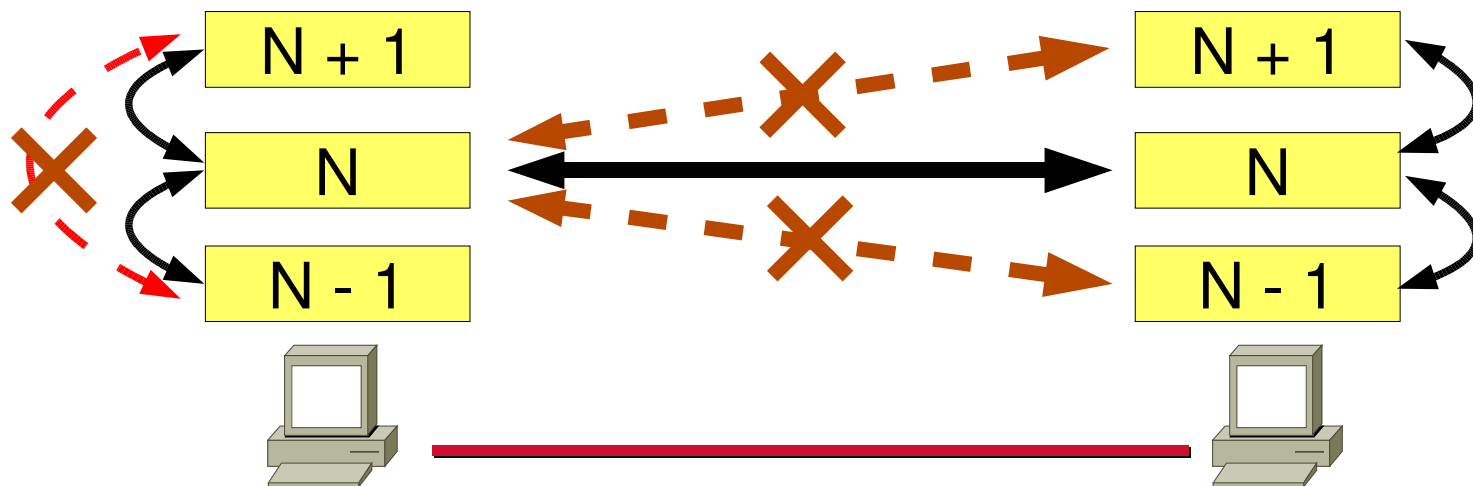
Síťový model

- Jak spolu budou vrstvy provázané?
- vždy budou komunikovat jen sousední vrstvy (vertikální komunikace)

vrstva dostává požadavky od vyšší a využívá služeb nižší vrstvy

- vrstvy komunikují „po síti“ s protilehlou vrstvou *stejně* úrovně

horizontální komunikace



Protokol

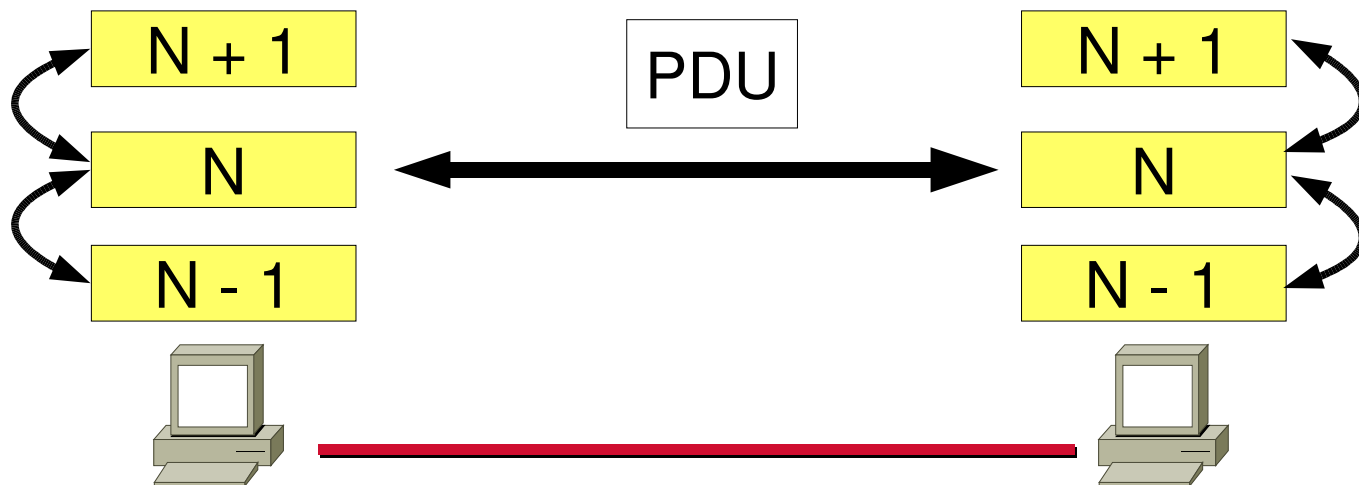
- definiuje pravidla komunikace odpovídajících si vrstev

každý protokol patří do některé z vrstev

v jedné vrstvě může koexistovat několik protokolů

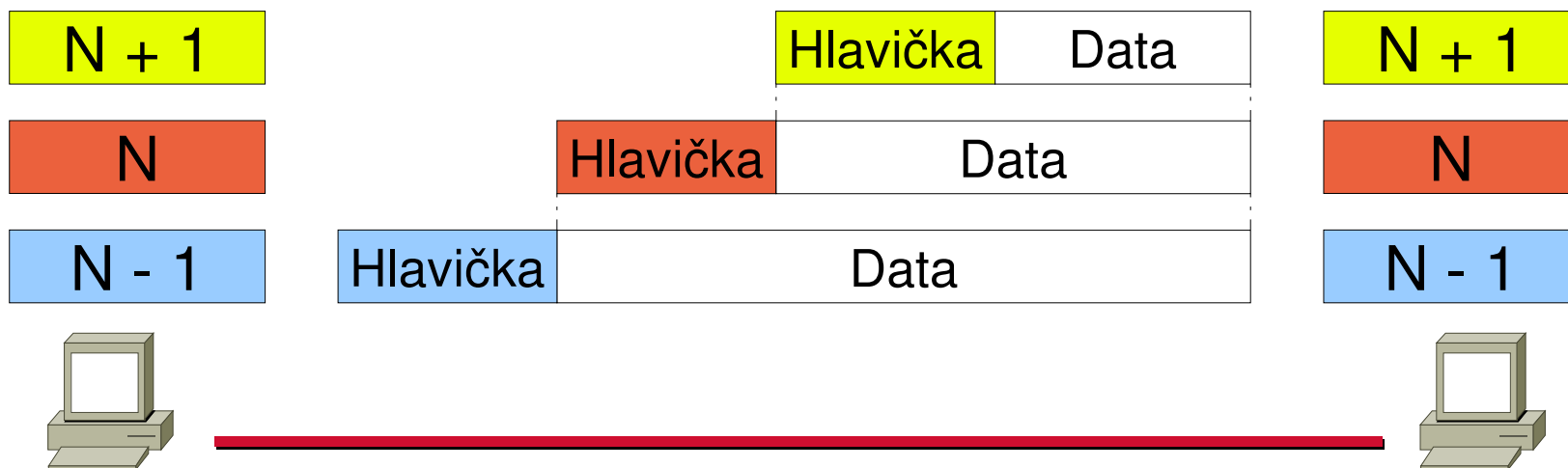
- data se předávají po PDU (Protocol Data Unit)

PDU se liší podle vrstvy

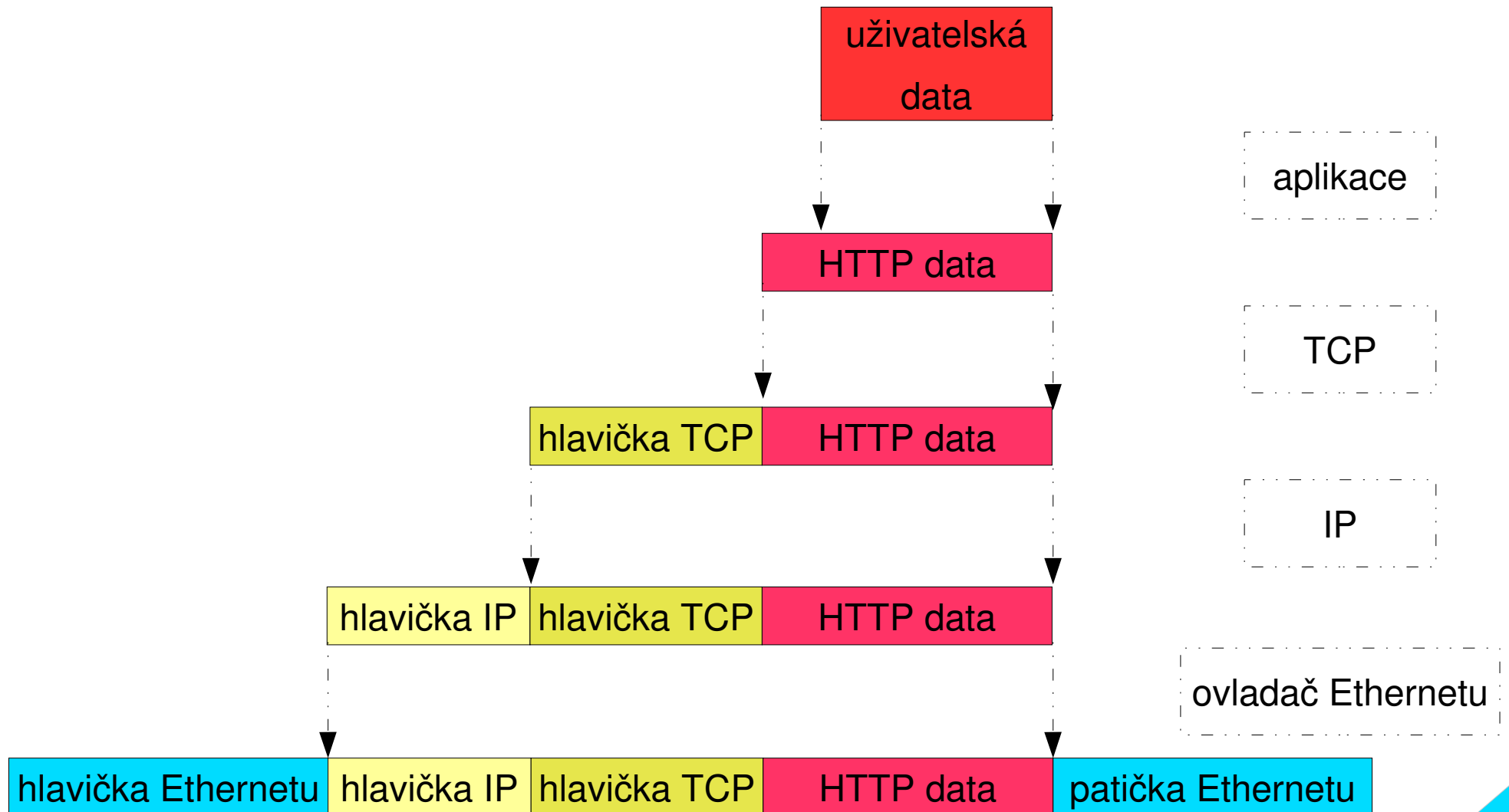


Zapouzdření

- Data se předávají od vyšší vrstvy k nižší
- postupně se „obalují“, přibývají řídicí informace jednotlivých vrstev
- nižší vrstva nerozumí struktuře, bere vše jako data
- po přijetí se data opět postupně vybalují



Příklad zapouzdření



Architektura a model

- Model = představa o tom, jak má síť vypadat

kolik má vrstev, které vrstvy mají co za úkol

např. referenční model ISO/OSI

- Architektura

konkrétní naplnění jednotlivých vrstev

konkrétní protokoly pro jednotlivé vrstvy

např. TCP/IP, IPX/SPX

Referenční model ISO/OSI

- původně mělo jít o síťovou architekturu (tedy včetně implementace)
- velmi obecný
 - snažil se obsáhnout všechny možnosti síťové komunikace
 - vše, co by se „někdy mohlo hodit“
 - příliš složitý na implementaci (vznikal jako teoretický základ)
- mezinárodně standardizován
- dnes slouží především pro srovnávání jednotlivých architektur
- nakonec bylo zvoleno 7 vrstev jako ideální

Referenční model ISO/OSI

- podobné činnosti patří do stejné vrstvy
- rozdělení na vrstvy by mělo minimalizovat tok dat mezi nimi (režii)
- práce by měla být mezi vrstvy rozdělena stejnoměrně
- rozdělení by mělo zohledňovat stávající standardy
- není sedm vrstev zbytečně mnoho?

TCP/IP má čtyři



Fyzická vrstva

- jejím úkolem je přenos bitů po fyzickém médiu
nabízí příjem a odesílání bitů
- kódování, modulace, časování, synchronizace
- elektrické parametry signálů
- mechanické parametry (konektory, rozhraní)
- paralelní, sériový přenos
- synchronní, asynchronní, arytmičtý

Aplikační

Prezentační

Relační

Transportní

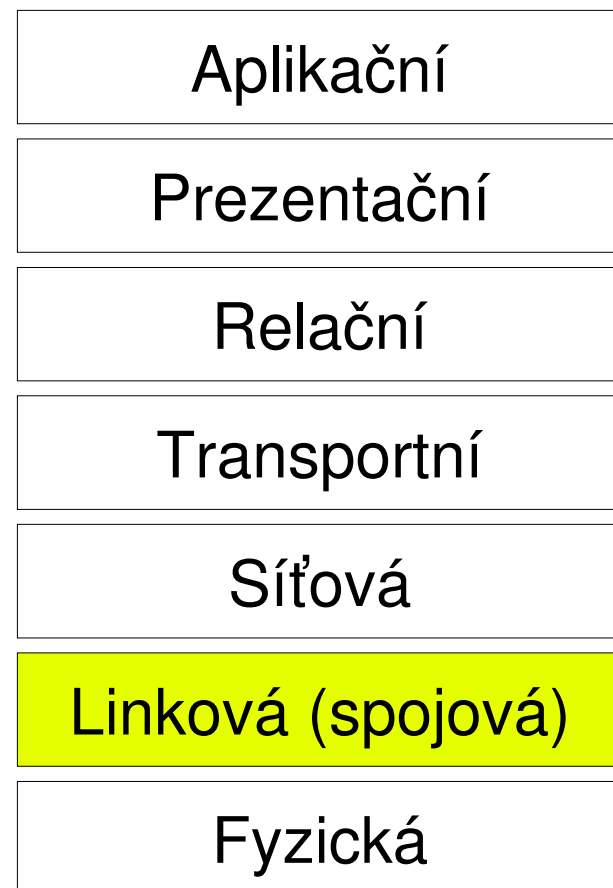
Síťová

Linková (spojová)

Fyzická

Linková vrstva

- přenáší bloky dat: rámce (frame)
- přenáší data jen v přímém spojení (jen k blízkým sousedům, ne přes hranici sítě)
- využívá různé implementace fyzické vrstvy
- synchronizace rámců (začátek, konec, ...)
- řízení přístupu ke sdílenému médiu
- detekce a náprava chyb
- řízení toku (ochrana před zahlcením)

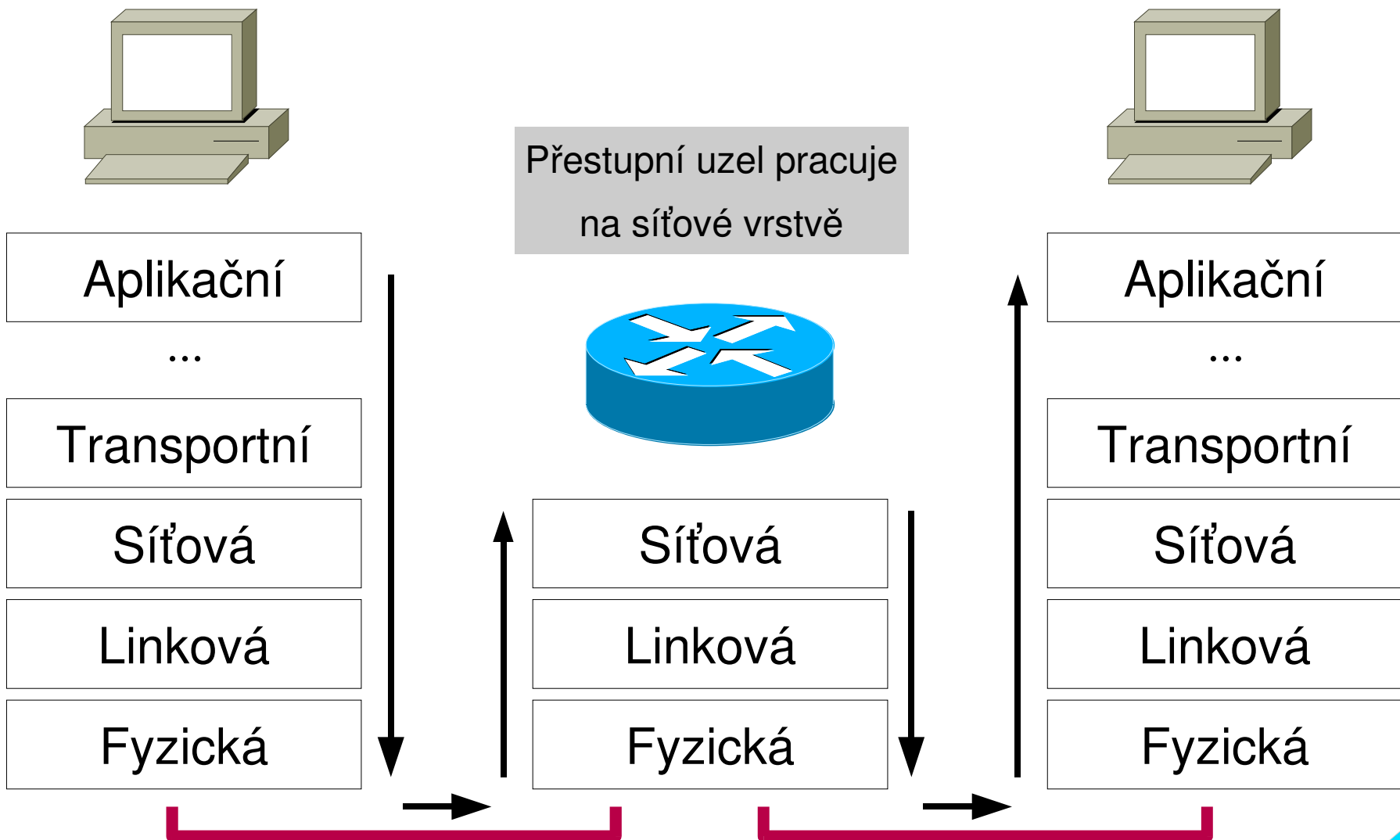


Síťová vrstva

- zajišťuje přenos paketů (ty se vkládají do linkových rámců)
- pakety se přenášejí od zdrojového uzlu k cílovému, mohou procházet přes různé přestupní uzly v mezilehlých sítích
- zajišťuje směrování jednotlivých paketů v síti podle různých algoritmů
- nejvyšší vrstva přenosové infrastruktury tedy nejvyšší, která musí být přítomna na přestupních uzlech



Směrovač (spojuje sítě)



Transportní vrstva

- Nabízí a zajišťuje spolehlivý přenos dat
- dvě varianty:
 - transportní služba bez spojení (přenos bloků)
 - transportní služba se spojením (navázání, přenos dat a ukončení spojení)
- zakrývá rozdíly nižších vrstev
 - vyšší vrstvy mohou vyžadovat něco, co nižší vrstvy nenabízí
 - spojení \Leftrightarrow bez spojení. spolehlivost \Leftrightarrow nespolehlivost
- řízení toku dat

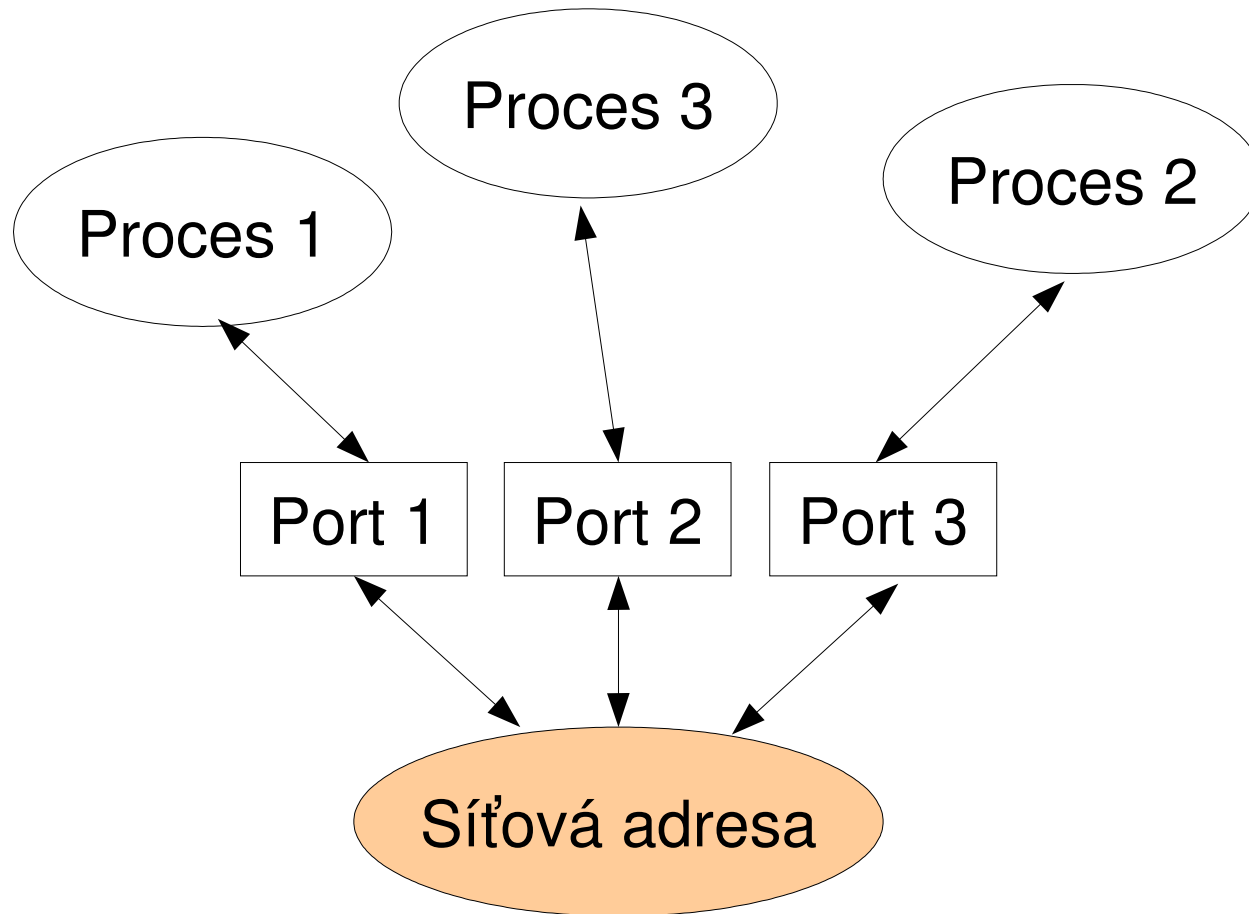


Transportní vrstva

- až do síťové vrstvy se uzly chápou jako nedělitelné, mají jednu adresu
- transportní služba umožňuje rozlišit jednotlivé entity (např. procesy, služby)
- obvykle jsou rozlišeny pomocí portů, se kterými se procesy asociují
- příklad: TCP port 80 se používá pro HTTP protokol (World Wide Web)



Transportní vrstva



Relační vrstva

- Úkolem je synchronizace dialogu vyšších vrstev
- navazuje spojení
něco jako operátorka v manuální telefonní ústředně
- řídí tok dat (prioritní data, ...)
- není příliš jasné, co má dělat v počítačových sítích
- v TCP/IP úplně chybí



Prezentační vrstva

- zabývá se strukturou zpráv, jejím zápisem (*syntaxí*)
- přizpůsobuje strukturu zprávy aplikaci
- převod kódů a abeced, modifikace grafického uspořádání dat
- poskytuje:
 - dohodu o syntaxi, transformace syntaxe
 - šifrování, dešifrování
 - komprese, dekomprese



Prezentační vrstva

Nižší vrstvy se snaží přenést data přesně bit po bitu

Prezentační vrstva naopak do dat může zasahovat:

- změna kódování dat:

převod mezi různými typy čísel s plovoucí řádovou
čárkou (floating point)

převod mezi architekturami Big a Little Endian

celá čísla se mohou ukládat dvěma způsoby

převod kódování (ASCII, EBCDIC)

formát dat, struktur



Aplikační vrstva

- zpřístupnění komunikace aplikacím a procesům
- poskytuje:
 - přenos zpráv
 - identifikaci komunikujících stran (číslem, adresou, jménem)
 - dohoda o ochraně přenášených zpráv
 - určení kvality používané služby
 - synchronizace aplikací (klient – server)



Problémy modelu ISO/OSI

- příliš složitý, objemný, těžkopádný
- maximalistický
- vznikl na papíře (s malým ohledem na dosavadní praxi v *počítačových* sítích)
- vhodnější pro rozsáhlé sítě (pro lokální zbytečně složitý)
- upřednostňuje spolehlivé a spojované služby

vznikl na popud lidí „od spojů“, tam je to přirozené

původně tam byl jen spolehlivý spojovaný přenos

klade velké nároky na infrastrukturu, zbytečně složité, pomalé a drahé

v počítačových sítích se mohou o spolehlivost postarat koncové body

- některé části vrstev plní stejnou funkci

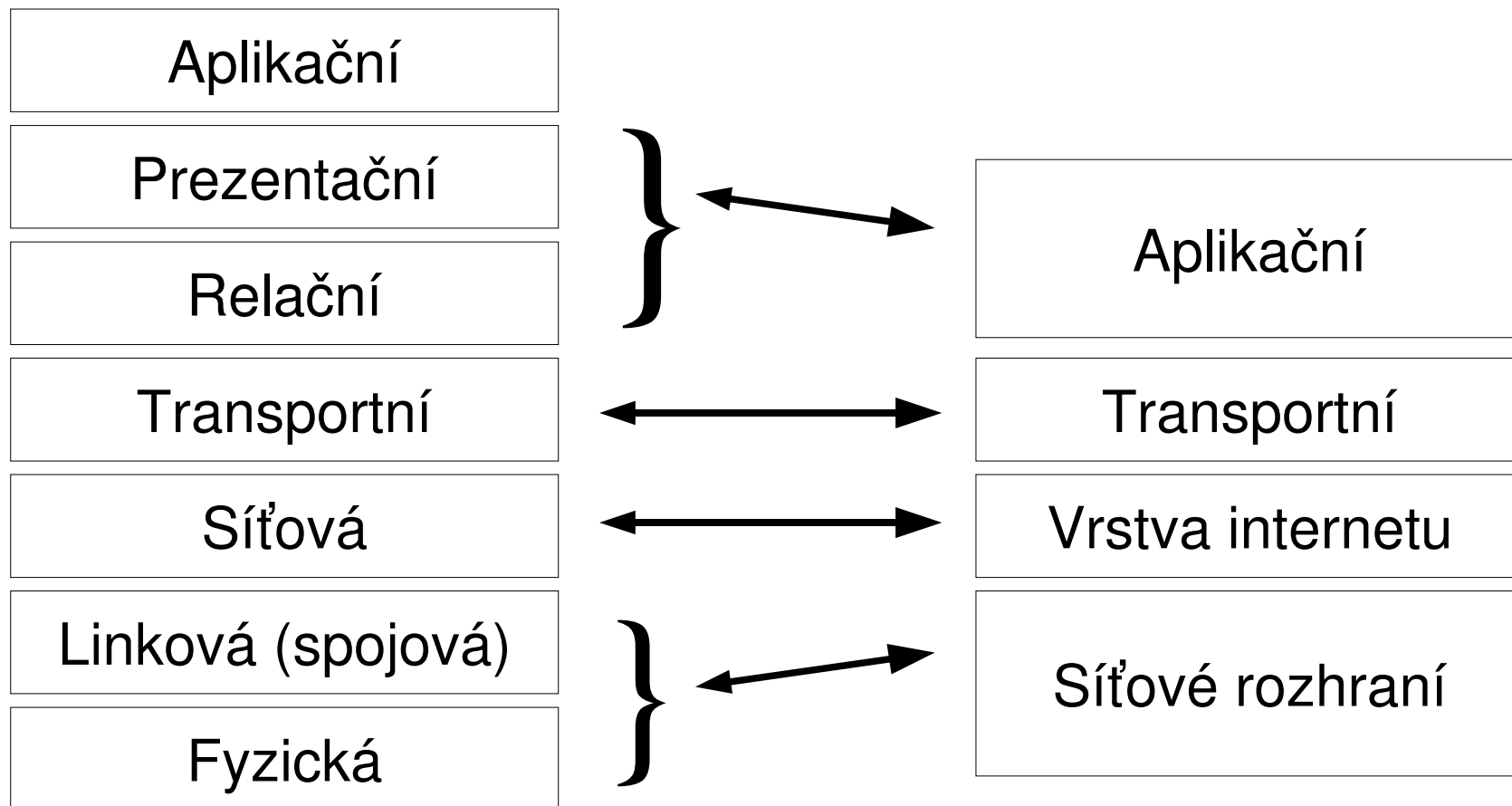
TCP/IP

- Internet Protocol, Transmission Control Protocol
- celá architektura, neodpovídá přesně RM ISO/OSI
- rodina protokolů TCP/IP (protocol suite, zahrnuty i další protokoly)
- čtyři vrstvy:
 - síťového rozhraní: fyzická a linková, TCP/IP pouze používá, nedefinuje
 - mezisíťová: služba bez spojení, nespolehlivá
 - transportní: spolehlivá, spojovaná komunikace
 - aplikační: uživatelské úlohy i podpůrné procesy pro TCP/IP
- celý Internet je jedna síť (spojení sítí do jedné velké sítě)

Historie Internetu

- vznik: nejprve protokoly, pak vznikaly vrstvy
- historie: těsně svázáno s rozvojem Internetu
- ARPANET: protokol NCP
 - měl ověřit použitelnost paketové technologie
 - postupně nahrazen protokolem IP (1973, praxe: 1977, v Internetu od 1.1. 1983)
- financování zajistilo DoD USA
 - vlastnosti: robustnost proti výpadkům části sítě, bez centrálních prvků
 - specifikace volně k dispozici, daňoví poplatníci už vývoj zaplatili
 - vznikal především v akademické sféře (na univerzitách v USA)

TCP/IP a RM ISO/OSI



Víš-li jak na to, čtyři vrstvy ti plně stačí.

Nevíš-li, ani sedm ti jich nepomůže

Fyzická vrstva

- TCP/IP fyzickou vrstvu nedefinuje

předpokládá se použití různých technologií (Ethernet, FDDI, ATM, ...)

IP over everything

- důsledek: IP se spokojí s libovolnou službou, která poskytuje nějakou službu pro přenášení dat

- IP zakrývá rozdíly použité přenosové technologie

spojovaná/nespojovaná

spolehlivá/nespolehlivá

(Mezi)síťová vrstva

Výchozí požadavky pro síťovou vrstvu:

- síť má hlavně přenášet data
- je dobré, aby „intelligence“ byla zabudovaná do koncových uzlů
 - podstatně zjednoduší návrh sítě (a sníží cenu)
- řešení má být decentralizované a maximálně robustní
- co z toho plyne pro síťovou vrstvu:
 - používáme nespolehlivé a nespojované služby
 - jsme dobře připraveni na výpadky
 - případné další požadavky na spojení řeší vyšší vrstvy

Adresování IP

IP nepoužívá žádné adresy fyzické vrstvy (adresy jsou velmi rozdílné)

- IP adresy: dvousložkové

adresa sítě	adresa uzlu
-------------	-------------

číslo sítě a počítače v rámci sítě

dohromady 32 bitů, zapisují se (v4) pomocí čtyř dekadických čísel

např. 192.168.32.4

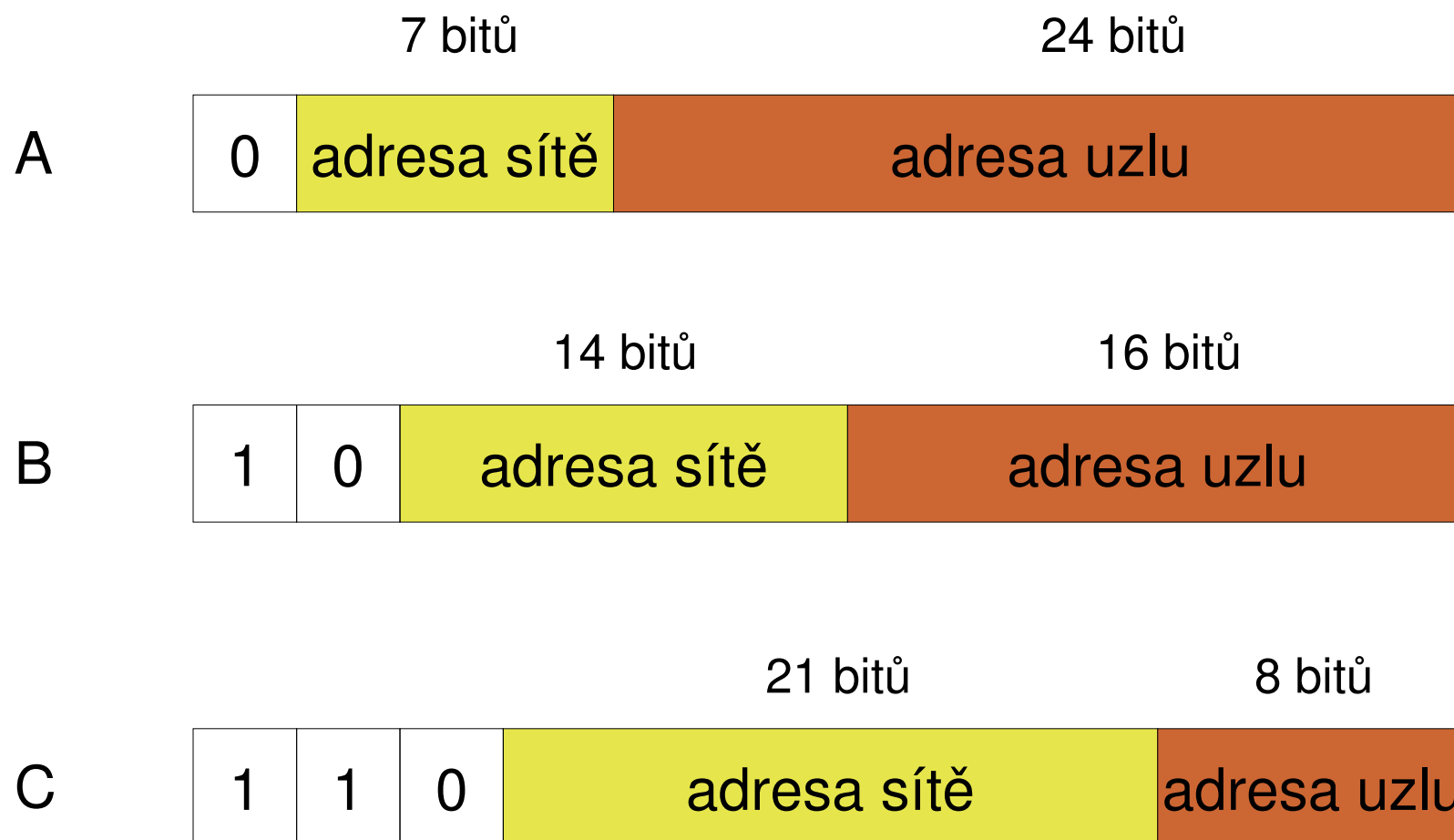
- je potřeba více adres uzlů než adres sítí. Kde zvolit hranici?
- výsledné rozdělení:

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)

Třídy IP adres



Propojení sítí

- TCP/IP rozlišují dva druhy uzlů v síti

koncové uzly (běžné počítače zapojené do sítě)

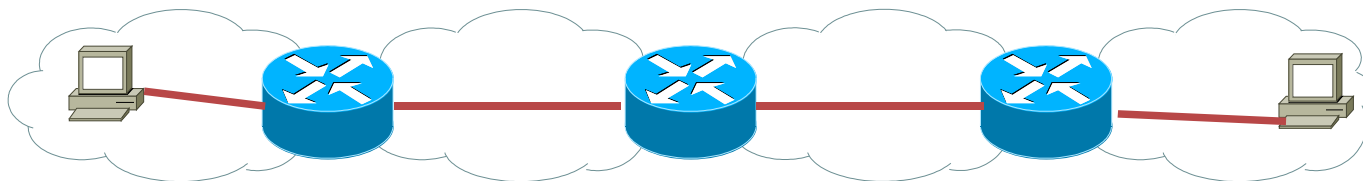
směrovače (uzly připojeny do více než jedné sítě)

směrovače předávají data z jedné sítě do jiné sítě

- řetězcový model

spojení sítí, sítě jsou spojeny na síťové vrstvě

každé dva uzly v síti jsou připojeny přes řetězec sítí a směrovačů



Vyčerpání IP adres

- obrovský zájem o Internet způsobil postupné vyčerpání adres
 - přidělují se vždy celé **adresy sítí**
- řešení dočasné:
 - jemnější dělení rozsahu (neuvažují se třídy A, B, C, adresa se dělí na síťovou a koncovou část v libovolném místě)
 - CIDR (Classless Inter-Domain Routing)
 - používání speciálních privátních rozsahů síťových adres
 - vyhrazené adresy, které se mohou používat pouze v privátních sítích, nesmí se dostat za brány lokální sítě (do Internetu)
- řešení definitivní: IP verze 6

Síťová vrstva: otázka spolehlivosti

Má být spolehlivá nebo nespolehlivá?

- spolehlivá:

pokud dojde ke ztrátě/poškození dat, vrstva to musí napravit (nový přenos dat)

vyžaduje to režii přenosovou (přenáší se více dat), časovou, výpočtení

- nespolehlivá:

sama od sebe nepoškozuje ani nezahazuje data

má právo zahazovat poškozená data (případně ignorovat ztrátu dat) a pokračovat dál

není navíc žádná režie, ale o opravy se musí starat vyšší vrstva (pokud to vyžaduje)

Síťová vrstva: spolehlivost

Síťová vrstva má hlavně přenášet data

- je výhodnější, když si spolehlivost zajistí koncové uzly

některé služby spolehlivost nevyžadují, navíc spolehlivost není nikdy 100%

výpočetní výkon je levnější v koncových uzlech než v síťových prvcích

Síťová vrstva (IP) je pouze **nespolehlivá**, na principu maximální snahy

- spolehlivost řeší až vrstva transportní

ale aplikace jich nemusí využívat, může si vybrat:

protokol TCP je spolehlivý

protokol UDP je nespolehlivý

Best effort

- maximální snaha
- síť se snaží maximálně vyhovět požadavkům
- pokud se jí to nedaří, může (spravedlivě – všem stejně) ignorovat požadavky, pozdržovat data, dokonce data zahazovat
- důvod: paketový systém přenosu dat:

kapacita odchozí linky může být menší, než kapacita příchozí

směrovač může pakety uchovávat, ale jen po omezenou dobu (než mu dojde paměť)

pak další pakety musí zahodit!

Síťová vrstva: otázka spojovanosti

Má být spojení spojované (telefon) nebo nespojované (pošta)?

- původní požadavek byl na robustnost (odolnost proti výpadku částí sítě)

výpadky mohou nastávat i při běžném provozu – síťová topologie se dynamicky mění

- IP funguje **nespojovaně**

výhodné pro méně intenzivní přenosy dat rozložené v čase

neexistuje spojení, které by bylo možné útokem přerušit

pakety jsou přenášeny nezávisle jeden na druhém, každý může putovat jinou cestou

odesílatel ani neví, jestli příjemce existuje

Transportní vrstva

- řeší komunikaci koncových uzlech
 - je přítomna pouze na koncových uzlech
- využívá služeb IP, tedy nespojované, nespolehlivé služby
- TCP (Transmission Control Protocol)
 - spolehlivý, spojovaný
 - přenáší proud dat (typ telefon)
- UDP (User Datagram Protocol)
 - nespolehlivý, nespojovaný (k IP nepřidává v tomto ohledu nic navíc)
 - jen nadstavba nad IP, doručují se jednotlivé zprávy (typ pošta)

Aplikační vrstva

- základní část aplikací
- služby relační a prezentační vrstvy RM ISO/OSI jsou v TCP/IP součástí aplikační vrstvy
 - mohou je tvořit knihovny funkcí
- původní služby aplikační vrstvy:
 - elektronická pošta, přenos souborů, vzdálené přihlašování
- novější služby:
 - WWW, sdílení souborů
 - správa sítě

Protokoly TCP/IP

HTTP

SMTP

DNS

SNMP

DHCP

TCP

UDP

Internet Protocol (IP)

ARP

RARP

Ethernet, Token ring, FDDI, ...

RFC: standardy Internetu

- Internet: od začátku postaven na otevřených standardech
- vznikal na univerzitní půdě (financován armádou)
- jeví se jako jediná síť
- RFC (Request For Comment)

původně opravdu návrhy, které se komentovaly

veřejně dostupné

<http://www.rfc-editor.org/>

několik typů: standards track (STD), best current practice (BCP), informational (FYI), experimental, historic

Kritika TCP/IP: zabezpečení

- protokol vznikl v akademickém prostředí, zabezpečení nebylo v zadání
- důraz byl kladen na efektivitu
- postupnou komercializací Internetu se zabezpečení stává velkým problémem
- jak na to?

zabezpečení na aplikační úrovni (aplikací)

zabezpečené tunely

filtrování paketů (firewall)

Kritika TCP/IP

Filosofie TCP/IP nepočítá s mobilitou uživatelů

- nelze s jednou adresou cestovat po světě
- IP adresy jsou vázány na topologii sítě
- problém při využívání mobilního připojení

Negarantovaný charakter přenosu

- nemáme zaručeno, kdy vyslaná data dorazí (a pokud vůbec)
- vhodné pro poštu, přenos souborů (nárazový charakter)
- vadí při multimediálních přenosech

data se vysílají a spotřebovávají pravidelně