



Katedra softwarového inženýrství,
Matematicko-fyzikální fakulta,
Univerzita Karlova, Praha



Lekce 4: Rodina protokolů TCP/IP

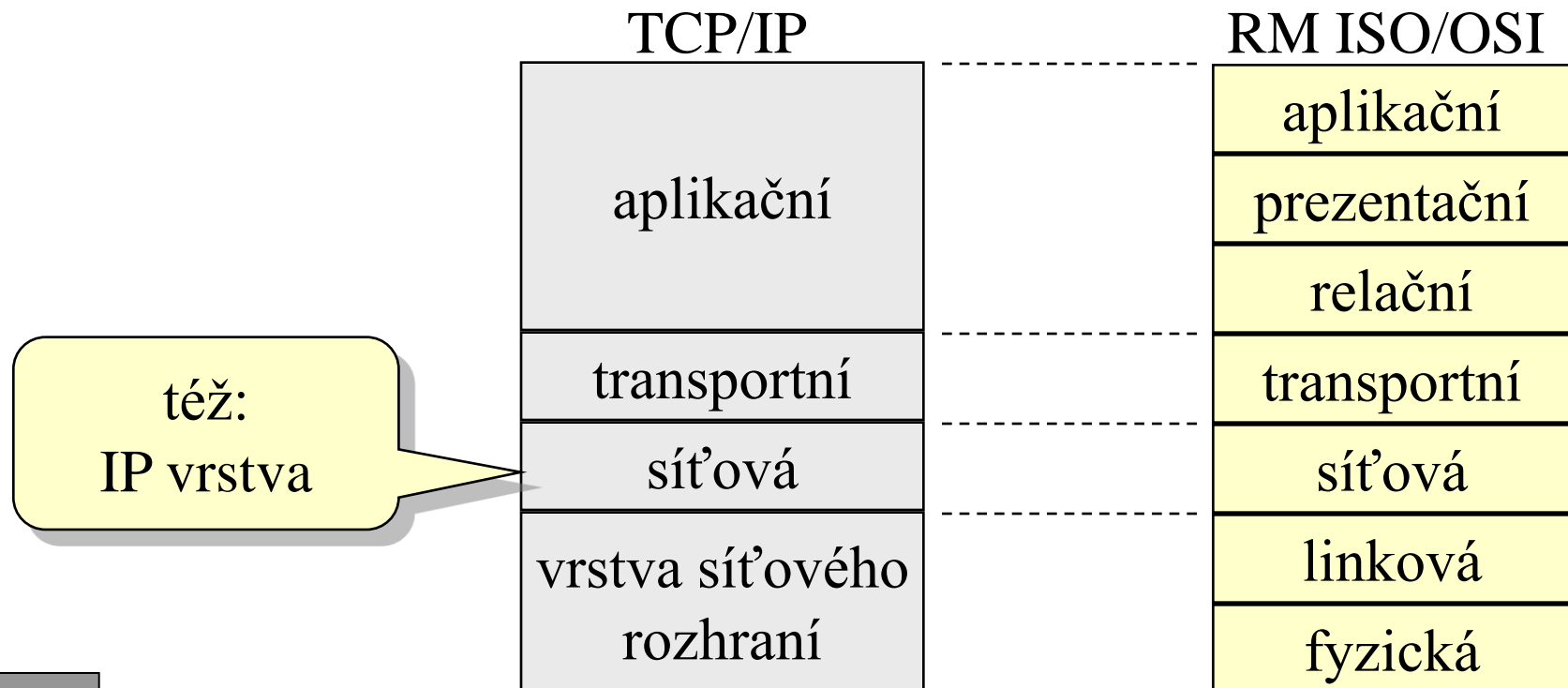
Jiří Peterka, 2010

srovnání RM ISO/OSI

Motto:

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

Nevíš-li, ani sedm ti jich nepomůže



co je TCP/IP?

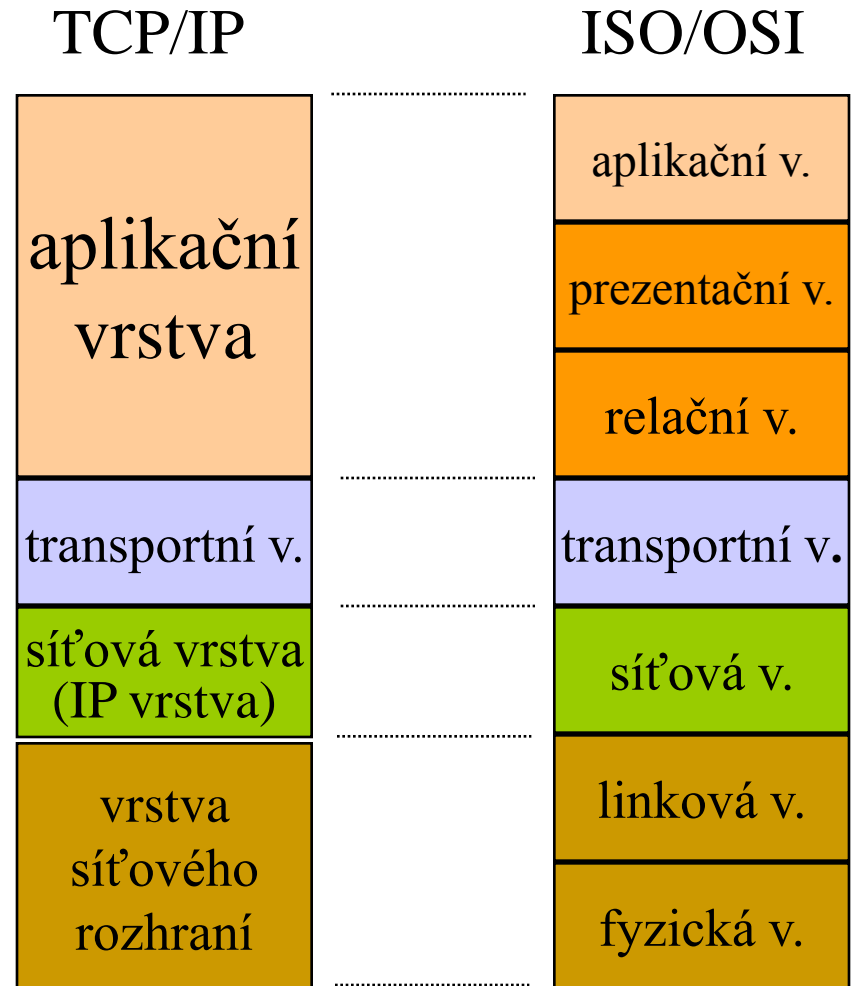
- síťová architektura:
 - obsahuje ucelenou představu o počtu a úloze vrstev
 - obsahuje i konkrétní protokoly
- obvyklé označení:
 - **TCP/IP protocol suite** (rodina protokolů TCP/IP)
 - součástí je více jak 100 protokolů
- postup vzniku:
 - nejprve: protokoly
 - teprve potom: vrstvy
 - TCP/IP vzniklo v akademickém prostředí
 - prosadilo se i v komerčním prostředí
 - od svého vzniku se změnilo jen relativně málo
 - nikoli zásadně – změny jsou „aditivní“
- dnes:
 - **nejpoužívanější síťová technologie**
 - nejrozšířenější síťová architektura
 - prosadila se lépe než cokoli jiného (RM ISO/OSI, IPX/SPX atd.)
 - funguje „nad vším“
 - **IP over Everything**
 - protokoly TCP/IP dokáží fungovat nad každou (linkovou) přenosovou technologií
 - „všechno“ funguje nad IP
 - **Everything over IP**
 - snad všechny aplikace již byly implementovány (portovány) i nad protokoly TCP/IP a dokáží nad nimi fungovat
- neznamená to že TCP/IP je ideální!!
 - má také řadu nevýhod, nedostatků ...

v čem se liší TCP/IP a ISO/OSI?

- v celkovém přístupu autorů
 - **ISO/OSI:** všechno musíme vymyslet sami (nebo alespoň převzít to, co vymysleli jiní, a udělat z toho vlastní standard)
 - příklad: ISO vydává Ethernet jako svůj standard ISO 8802.3
 - **TCP/IP:** to co je rozumné převezmeme a využijeme
 - soustředí se na "provázání" vlastních řešení s cizími
 - řeší např. jak provozovat IP nad Ethernetem
- ve způsobu tvorby nových řešení:
 - **ISO/OSI:** od složitého k jednoduššímu
 - řešení vznikají od začátku jako "dokonalá"
 - nejprve navymýšlí vzdušné zámky, pak musí slevovat
 - nejprve vznikne standard, pak se zkoumá praktická realizovatelnost
 - **TCP/IP:** od jednoduššího ke složitějšímu
 - řešení vznikají nejprve jako "skromná", postupně se obohacují
 - nejprve se řešení ověří, a teprve pak vzniká standard

konkrétně

- v pohledu na počet vrstev a způsob jejich fungování
 - jaké služby mají být nabízeny
 - a na jaké úrovni mají být poskytovány
 - kde má být zajišťována spolehlivost
 - jak mají služby fungovat
 - spolehlivost/nespoehlivost, spojovanost/nespojovanost, princip maximální snahy vs. garance kvality služeb, ...
 - zda má být ponechána možnost volby
 - mají aplikace právo si vybrat např. mezi spolehlivým a nespoehlivým přenosem?

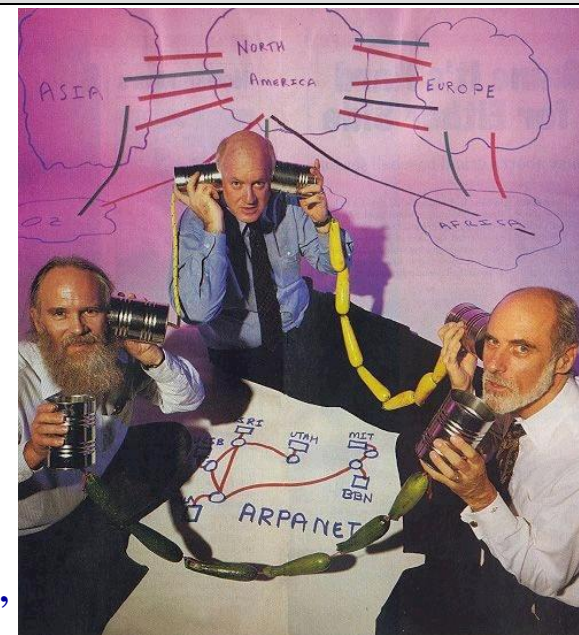


historie vzniku TCP/IP

- souvisí s Internetem (ARPANETem)
 - bylo potřeba v praxi ověřit životaschopnost paketové technologie
 - přepojování paketů
 - byla postavena velká testovací síť
 - ARPAnet (zárodek pozdějšího Internetu)
 - pro zárodečnou síť byl vyvinut "prozatímní" protokol:
 - NCP (Network Control Program)
 - ten ale nebyl vhodný pro rutinní používání
 - vše financoval DoD (Department of Defense), skrze grantovou agenturu (D)ARPA
 - proto: ARPANET
- další vývoj:
 - když si DoD ověřil životaschopnost paketové technologie ...
 - rozhodl se testovací síť nezrušit,
 - ale předat ji akademické sféře do rutinního používání
- vývoj:
 - na zárodečný ARPANET se nabalovaly další sítě
 - postupně vznikl Internet
 - pro rutinní provoz ARPANETu/Internetu bylo třeba vyvinout nové "rutinní" protokoly
- protokoly TCP/IP byly vyvíjeny jako „definitivní“ řešení pro vznikající Internet
 - peníze na vývoj protokolů TCP/IP poskytl DoD (ministerstvo obrany USA)
 - specifikace jsou „volné“ (volně dostupné)
 - (v USA): když už daňoví poplatníci jednou zaplatí, nemusí to platit podruhé
 - vlastní návrh vznikl zejména v akademickém prostředí



lidé kolem TCP/IP



- ústřední postavou byl **Vinton G. Cerf**
 - do r. 1972 postgraduální student na UCLA
 - od r. 1972 docent na Stanfordu
 - pořádá síťové semináře (účastní se např. Robert Metcalfe, Jack Haverty a další)
 - na těchto seminářích se pod vedením Vintona Cerfa a Roberta Kahna postupně zrodily protokoly TCP/IP
- později se stal zakladatelem a šéfem Internet Society
 - pracoval také (jako senior vicepresident) v MCI a Worldcom-u
 - byl šéfem organizace ICANN (chairman of the board)
- dnes:
 - spolupracuje s NASA na "InterPlanetary Internet-u"
 - od září 2005 pracuje pro Google (jako "Chief Internet Evangelist")



historie vzniku TCP/IP

- **1973:** představa TCP/IP poprvé prezentována veřejnosti (konference v UK)
- **1974:** koncepce TCP/IP publikována v IEEE Transactions on Computers (Cerf, Kahn)
- **1977:** první praktické zkoušky
- **1978-9:** TCP/IP získává dnešní podobu
- **1980:** DoD akceptuje protokoly TCP jako perspektivní
- **1982:** DoD přikazuje použití TCP/IP u všech sítí, nově připojovaných k Internetu
- **1.1.1983:** celý Internet přechází na protokoly TCP/IP
 - směrování „protokolu“ NCP bylo ukončeno/zastaveno
- **1983-1986:** nástup protokolů TCP/IP do praxe
 - DoD (ARPA) nechává implementovat protokoly TCP/IP u komerční firmy
 - BBN (Bolt, Beranek& Newman)
 - DoD (ARPA) financuje začlenění TCP/IP do BSD Unixu, který je distribuován (zdarma) americkým univerzitám
 - Berkeley Software Distribution
 - protokoly TCP/IP jsou postupně implementovány i v dalších operačních systémech ...

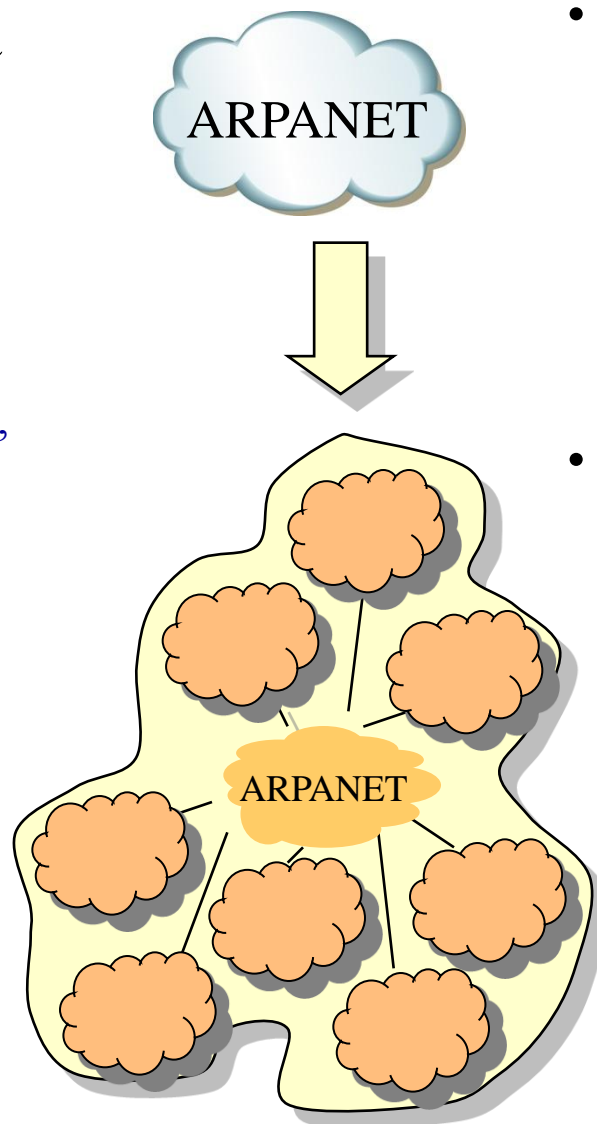
přibližně ve stejné době vzniká i RM ISO/OSI

filosofie, uplatněná při vzniku TCP/IP

- co bylo požadováno ještě po původním ARPANETu:
 - nesmí to mít žádnou centrální část
 - tu by nepřítel zničil jako první
 - důsledek: bude to mít decentralizovaný charakter, dnes naplněno existencí providerů a autonomním charakterem jejich sítí
 - musí to být velmi robustní
 - tak aby to aspoň nějak fungovalo, když nepřítel část sítě odstřelí
 - důsledek: preferují se nespolehlivé a nespojované přenosové mechanismy
 - protokol IP funguje nespolehlivě a nespojovaně
- co bylo požadováno po "rutinních" protokolech (TCP/IP):
 - internetworking
- co **nebylo** požadováno ani po TCP/IP:
 - zabezpečení
 - nebyl požadavek na zajištění důvěrnosti dat
 - jen velmi malé požadavky na identifikaci a autentizaci uživatelů
 - mobilita
 - v době vzniku byly počítače "nepřenosné"
 - (různá) kvalita služeb
 - aby různé přenosy mohly mít různou prioritu, různé parametry přenosu atd.
 -

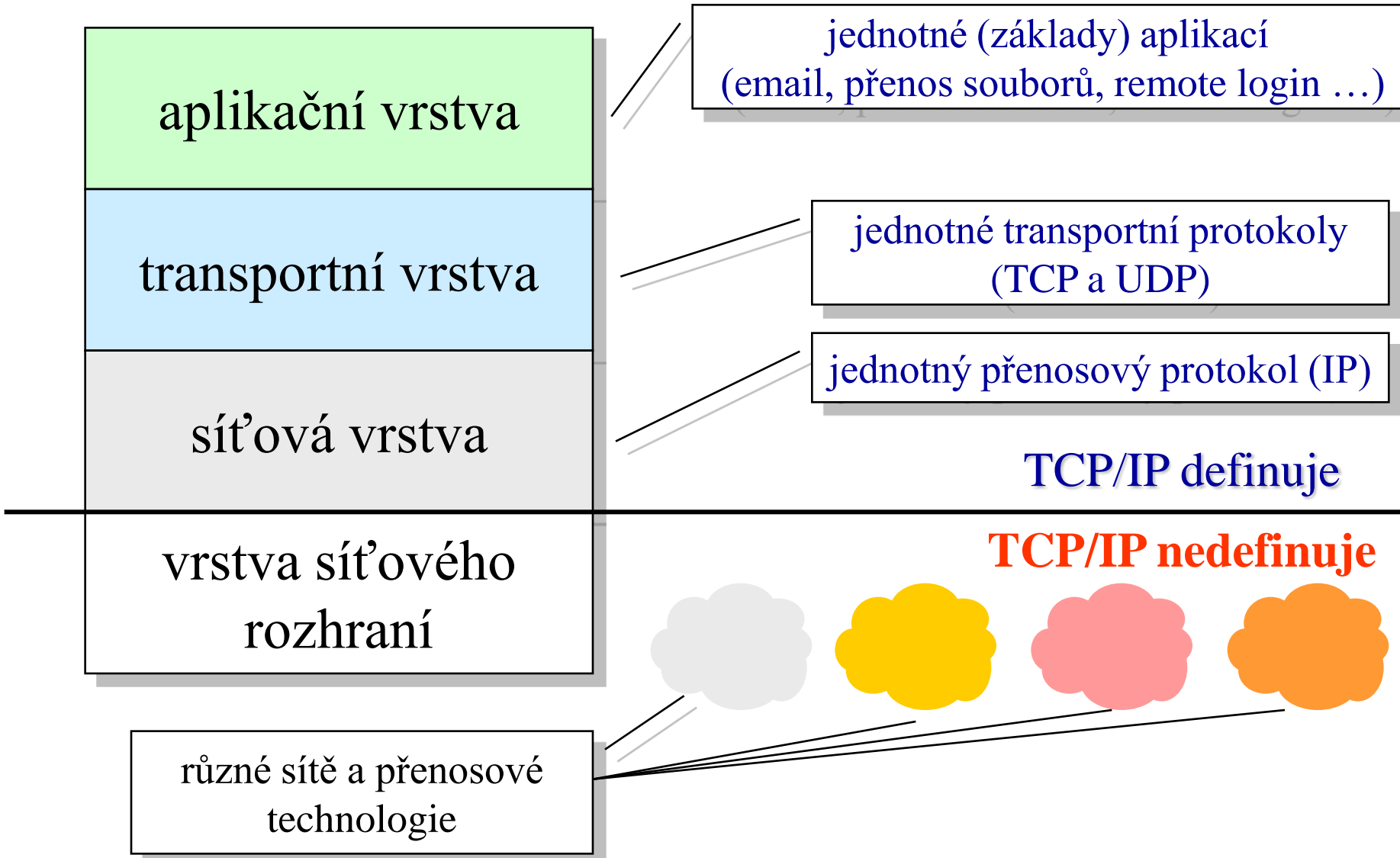
důraz na internetworking

- proč byl položen důraz na „internetworking“?
 - **internetworking** = vzájemné propojování sítí
 - když TCP/IP vznikalo, ARPANET už existoval, a byl velký zájem o připojení k němu
 - o připojení k ARPANETu usilovaly sítě různého typu (s různými síťovými technologiemi)

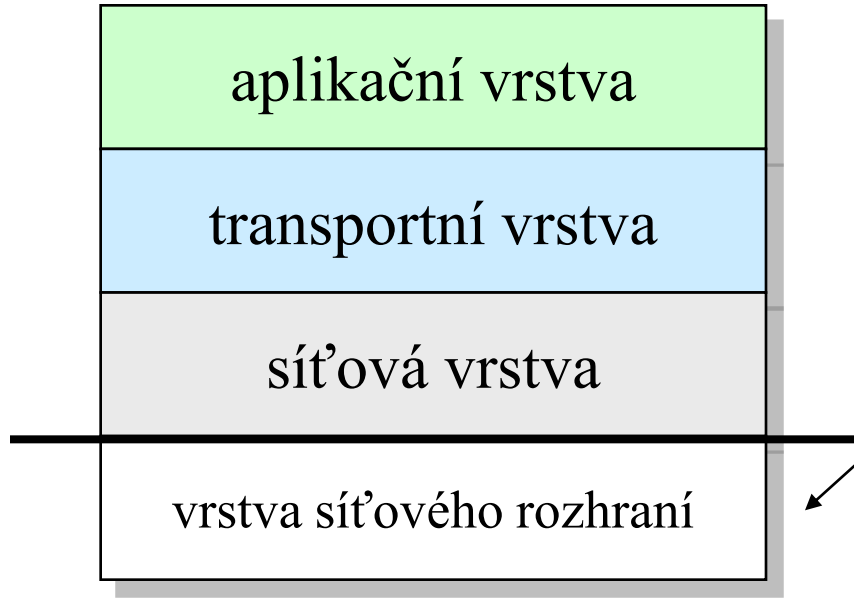


- TCP/IP je řešeno tak, aby:
 - šlo snadno připojovat dříve samostatné sítě
 - bylo možné propojit i sítě fungující na různých (odlišných) linkových technologiích
- postupným připojováním dalších sítí k zárodečnému ARPANETu vzniká vlastní Internet!!!
 - ještě později (1. polovina 90. let) se Internet otevírá komerčnímu světu

vrstvy TCP/IP



vrstva síťového rozhraní (Network Interface Layer)



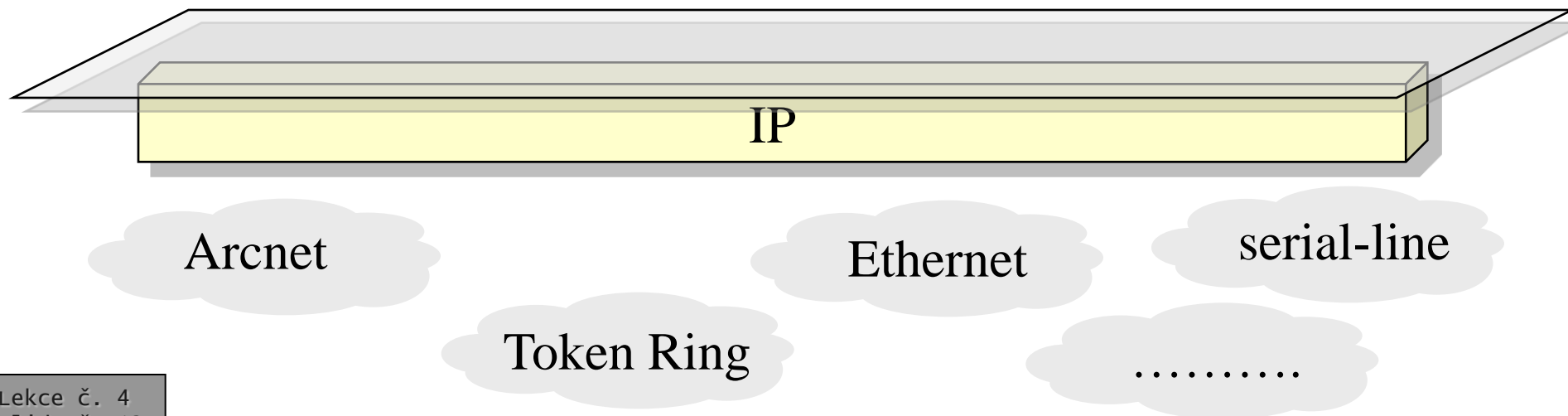
- zahrnuje „vše pod síťovou vrstvou“
- TCP/IP tuto vrstvu samo nijak nenaplnjuje
 - tj. nespecifikuje svoje vlastní přenosové technologie na nejnižších vrstvách!!!!

- proč?
 - předpokládá, že zde se použije to, co vznikne někde jinde (mimo rámec TCP/IP), například:
 - Ethernet
 - Token Ring
 - ATM
 - nepovažuje za potřebné znovu vyvíjet řešení, která již existují a fungují
 - byť je vyvinul "někdo jiný"
 - TCP/IP se zabývá pouze tím, jak tyto již existující technologie co nejlépe využít
 - jak nad nimi provozovat protokol IP
 - výjimka: protokoly SLIP a PPP (pro 2-bodové spoje)

pro srovnání: RM ISO/OSI považuje za potřebné převzít "cizí" řešení a přijmout je jako vlastní standardy!!!

filosofie TCP/IP – síťová vrstva

- přenosové technologie (z vrstvy síťového rozhraní) mají svá specifika
 - různé způsoby adresování, různou velikost přenášených rámců, různých charakter poskytovaných služeb
- síťová vrstva všechny tyto přenosové technologie "zastřešuje"
 - vytváří nad nimi "pokličku"
- "pokličku" tvoří protokol IP
 - hlavní přenosový protokol síťové vrstvy v TCP/IP
- otázka:
 - jak má tato poklička vypadat?
 - jaký má být protokol IP?

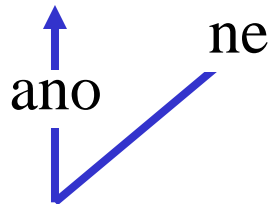


dilema pokličky

Autoři TCP/IP se museli rozhodnout, zda:

– vytvoří jednotnou nadstavbu nad soustavou vzájemně propojených sítí

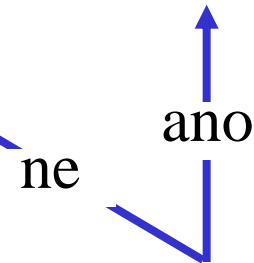
- přenosový protokol na úrovni síťové vrstvy (IP protokol), který bude mít všude stejné vlastnosti a poskytovat stejné služby
- stejné adresování
-



vyšší vrstvy mohou být jednotné, nemusí se zabývat odlišnostmi

– nebo zda nadstavba nebude všude stejná

- tj. protokol IP bude mít v různých sítích různé vlastnosti, resp. nabízet různé služby
-



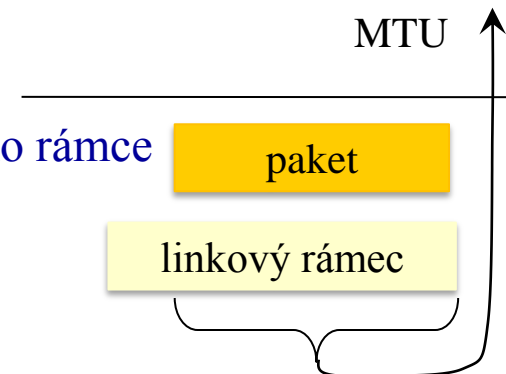
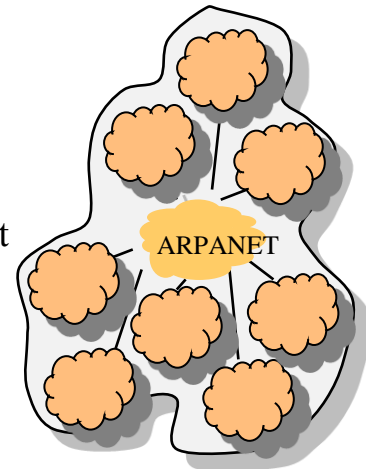
umožňuje to dosahovat maximální možné efektivity, přizpůsobením se specifickým vlastnostem přenosových mechanismů

dilema pokličky – další otázky

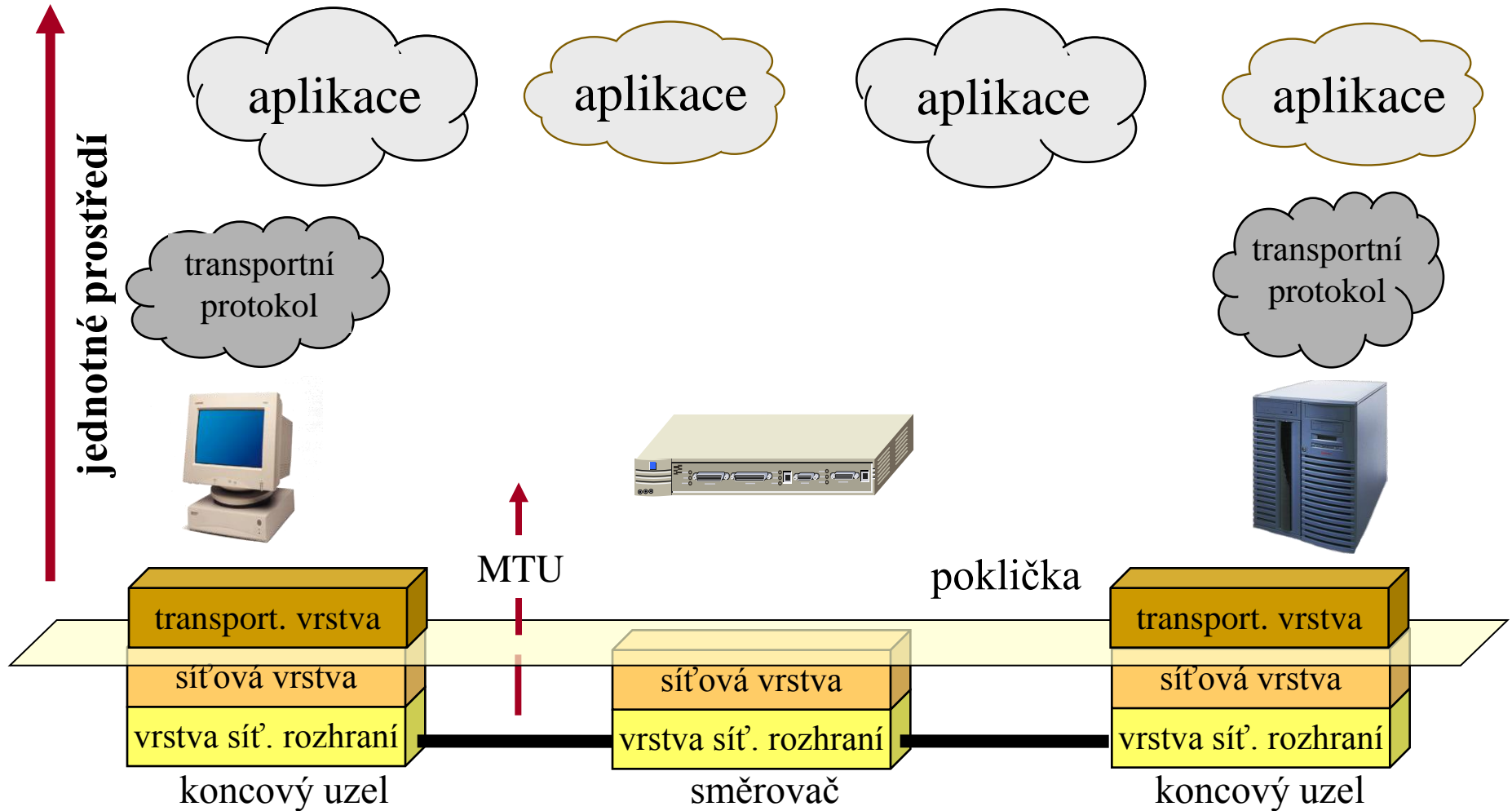
- jak by měla vypadat "jednotná poklička" nad přenosovými protokoly nižších vrstev?
 - z hlediska adresování (charakteru a logiky používaných adres)?
 - z hlediska spojovaného/nespojovaného způsobu fungování?
 - z hlediska spolehlivého/nespolehlivého způsobu fungování
 - z hlediska garance kvality služeb?
- výchozí předpoklady/úvahy:
 - přenosová část by měla hlavně přenášet data
 - a ne se starat o další věci
 - je výhodnější, když inteligence bude soustředěna až do koncových uzlů
 - a nikoli do přenosové části sítě
 - řešení by mělo být decentralizované a maximálně robustní
 - řešení by mělo maximálně podporovat internetworking
 -

výsledek – zvolená koncepce

- autoři TCP/IP se rozhodli pro "jednotnou pokličku", která zastírá konkrétní specifika jednotlivých IP sítí
- fakticky jde o jednotnou nadstavbu, kterou tvoří:
 - přenosový **protokol IP**, který má všude stejné vlastnosti a všude poskytuje stejné služby
 - je nespojovaný, nespolehlivý, funguje na principu maximální snahy
 - **jednotné adresování**
 - virtuální 32-bitové adresy (nemají žádný reálný vzor), tzv. **IP adresy**
 - tyto adresy by měly vyhovovat "pohledu na svět", který má TCP/IP – že svět je tvořen (vzájemně propojenými) dílčími sítěmi →
 - IP adresy mají "sít'ovou část", identifikující síť jako celek, a dále "uzlovou část", identifikující uzel v rámci sítě
 - **převodní mechanismy, které překládají mezi fyzickými (linkovými) adresami a virtuálními IP adresami**
 - protokoly ARP, RARP,
- existuje ale jedna výjimka:
 - IP protokol i vyšší vrstvy "vidí" maximální velikost linkového rámce (skrz parametr MTU, Maximum Transfer Unit) a měli by jej respektovat
 - tak aby nedocházelo ke zbytečné fragmentaci při přenosech

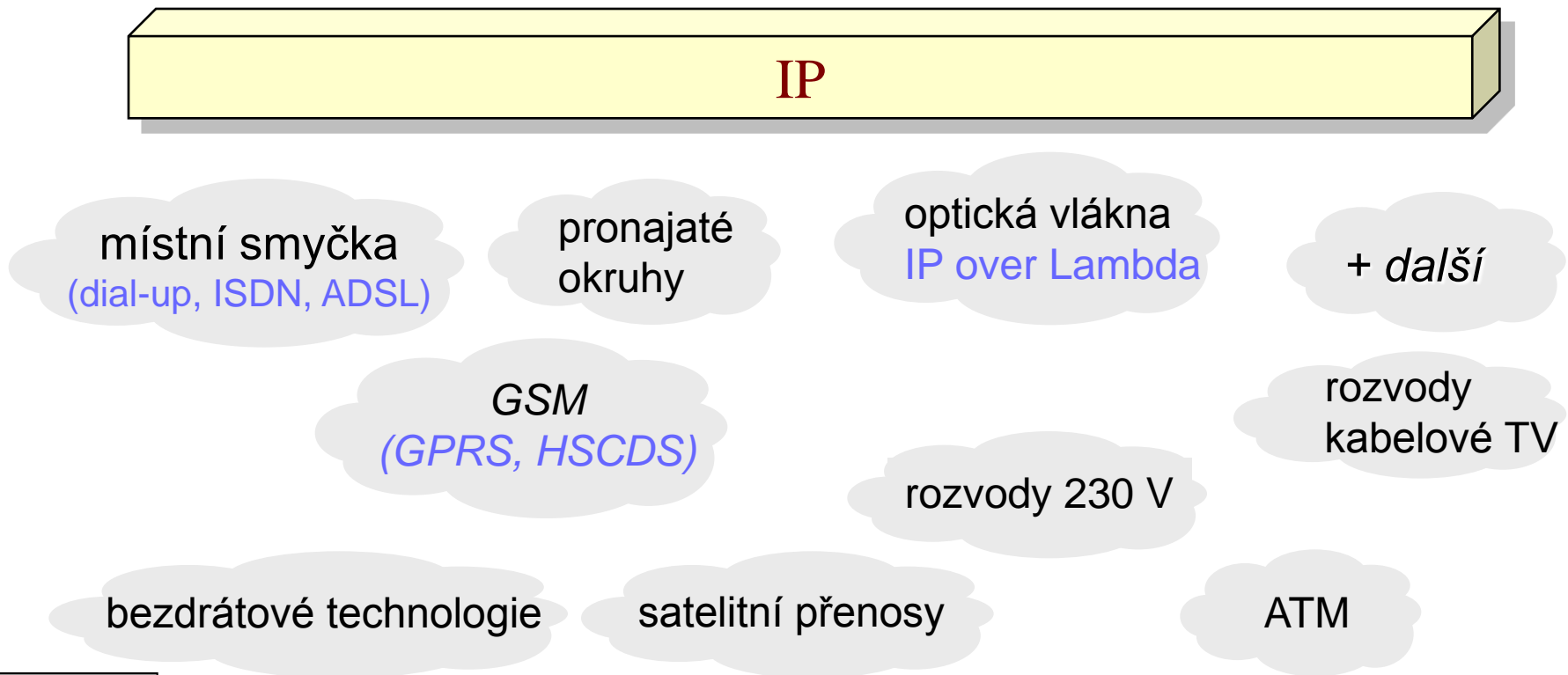


představa pokličky



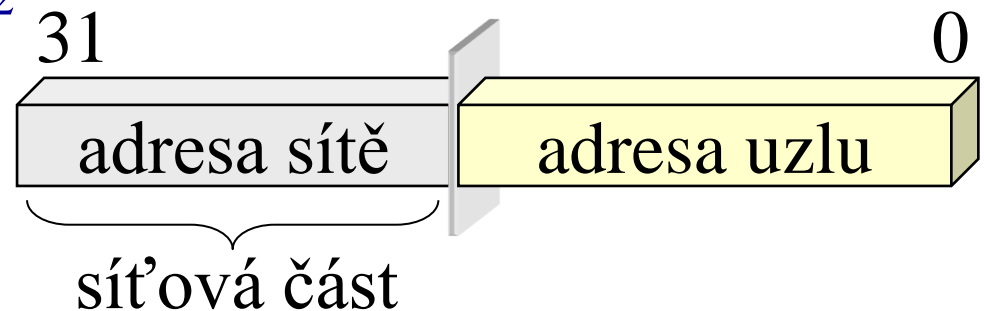
dnešní stav: IP over Everything

- protokol IP (protokol síťové vrstvy) dokáže fungovat "nad čímkoli"
 - nad jakýmkoli přenosovým mechanismem, který dokáže (fyzicky) přenášet data
- protokolům vyšších vrstev vytváří jednotné prostředí pro jejich fungování



IP adresy

- problém:
 - přenosové technologie nižších vrstev používají značně různorodé adresy
 - např. Ethernet používá 48-bitové adresy, ARCnet 8-bitové atd.
 - protokol IP nepřejímá žádnou a koncepcí adresování na úrovni nižších vrstev.
 - protokol IP zavádí vlastní (ryze abstraktní) adresy v rozsahu 32 bitů
 - tzv. IP adresy
 - nemají bezprostřední vzor v žádném systému adresování na nižší úrovni
- IP adresy jsou logicky dvousložkové
 - obsahují síťovou část
 - adresu dílčí sítě
 - a relativní část
 - relativní adresu uzlu v rámci sítě
- dvousložkový charakter vychází z představy tzv. katenetového modelu
 - směrování probíhá primárně podle síťové části adresy
 - a teprve v rámci cílové sítě podle (relativní) adresy uzlu



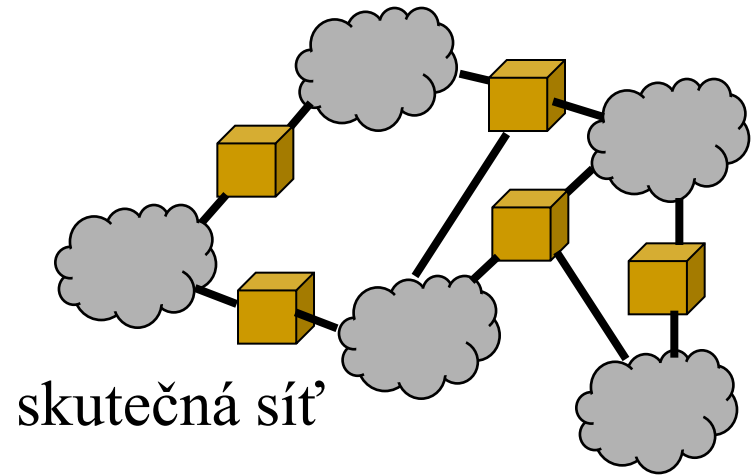
katenetový model

- TCP/IP předpokládá že "svět" je tvořen soustavou dílčích sítí
 - chápaných jako celky na úrovni síťové vrstvy, tzv. IP sítí
 - dílčí sítě jsou vzájemně propojeny na úrovni síťové vrstvy
 - pomocí směrovačů (dříve nazývaných IP Gateways, dnes: IP Routers)
 - toto propojení může být libovolné
 - může být stylem "každý s každým", nebo "do řetězce" apod.

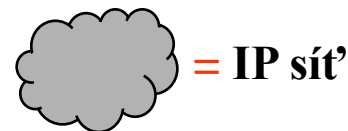
"katenet" je "řetězec" – ten je podmínkou pro souvislost celé soustavy sítí



představa katenetu

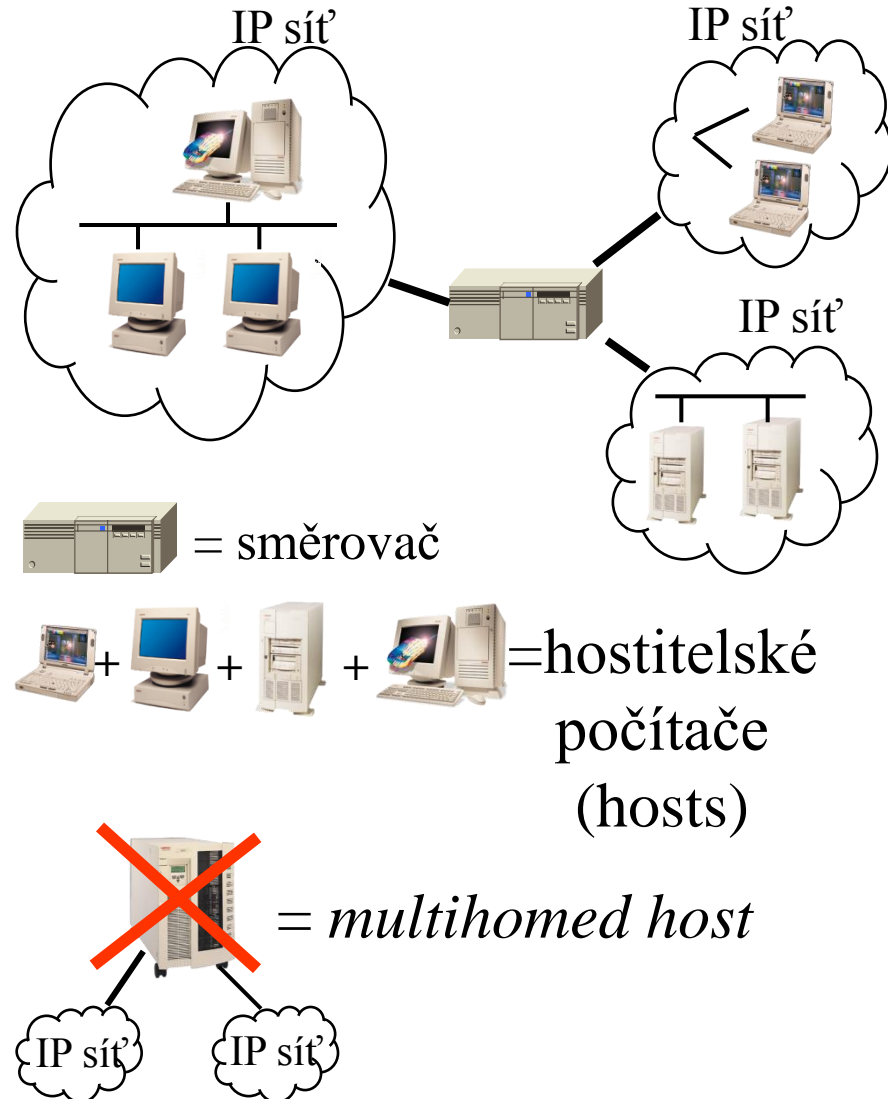


skutečná síť



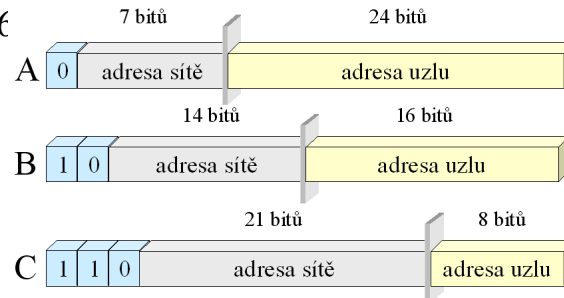
hostitelské počítače vs. směrovače

- TCP/IP předpokládá, dva typy uzlů v síti:
 - **hostitelské počítače (host computers)**
 - tj. koncové uzly, např. servery, pracovní stanice, PC, různá zařízení (tiskárny, ...)
 - jsou připojeny jen do jedné IP sítě (mají jen jednu síťovou adresu)
 - **směrovače (IP Routers)**
 - jsou připojeny nejméně do dvou IP sítí
 - zajišťují "přestup" (směrování)
- teze:
 - každý uzel by měl mít přiřazenu celosvětově unikátní síťovou adresu
 - tzv. **IP adresu**
 - **přesněji**: každé rozhraní by mělo mít vlastní adresu
 - směrovač má nejméně 2 IP adresy (podle počtu svých rozhraní)



původní "hospodaření" s IP adresami

- autoři TCP/IP vyšli z předpokladu že bude existovat:
 - malý počet opravdu velkých sítí
 - vyžadují malou síťovou část, a naopak velkou část pro relativní adresu uzlu
 - střední počet středně velkých sítí
 - měly by mít srovnatelně velkou síťovou i relativní část
 - velký počet malých sítí
 - vyžadují velkou síťovou část, stačí jim malá část pro relativní adresy
- tomu uzpůsobili i velikost síťové části IP adresy
 - 3 možné varianty, které odpovídají 3 třídám adres
 - **třída A**
 - pro velmi velké sítě, poloha hranice 8:24 (rozděluje 32bitů na 8 a 24)
 - **třída B**
 - pro středně velké sítě, 16:16
 - **třída C**
 - pro malé sítě, 24:8

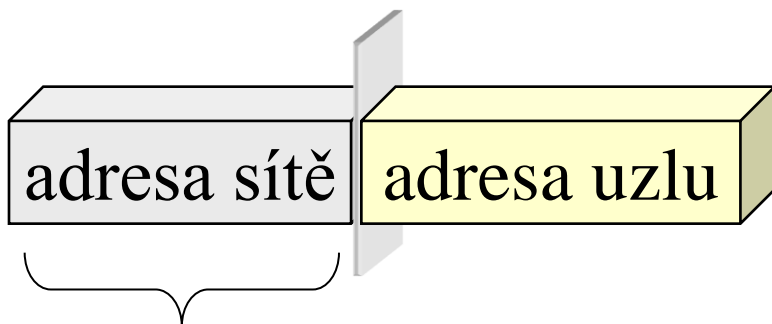


- (původní) způsob přidělování IP adres:
 - vždy se přidělila celá třída adres
 - např: 1x B:
 - fakticky 65536 (2^{16}) různých IP adres (se stejnou síťovou částí)
 - např. 1x C:
 - fakticky 256 (2^8) různých IP adres
 - pokud takto přidělené adresy nebyly využity, nešlo je už "vzít zpět" a přidělit někomu jinému!!
- důsledek: vedlo to k plýtvání IP adresami
 - příklad: když někdo chtěl 1000 IP adres, dostal 1xB (65 536 adres)
 - později: dostal 4-8x C (4-8x256 IP adres, ale to zase způsobovalo jiné problémy
 - se směrovacími tabulkami

problém s IP adresami

- původně navržený systém tříd A, B a C nepočítal s dnešní velkou poptávkou po IP adresách
 - docházelo k plýtvání IP adresami
 - nejmenší "kvantum" je 256 IP adres (1x třída C)
 - a ke značné roztržitosti přidělených IP adres
 - komplikace při směrování a udržování směrovacích tabulek
- začalo hrozit nebezpečí vyčerpání všech IP adres

- objevila se dočasná řešení, která zmírňují problém
 - subnetting
 - umožňuje "dále dělit" již jednou přidělené třídy IP adres
 - CIDR (Classless Inter-Domain Routing)
 - umožňuje přidělovat IP adresy po libovolně velkých kvantech (2^n)
 - privátní IP adresy
 - umožňují opakované použití stejných IP adres
 - například v privátní síti schované za firewallem
- vzniklo i definitivní řešení celého problému:
 - nová verze protokolu IP
 - IP verze 6, s IP adresami velikosti 128 bitů



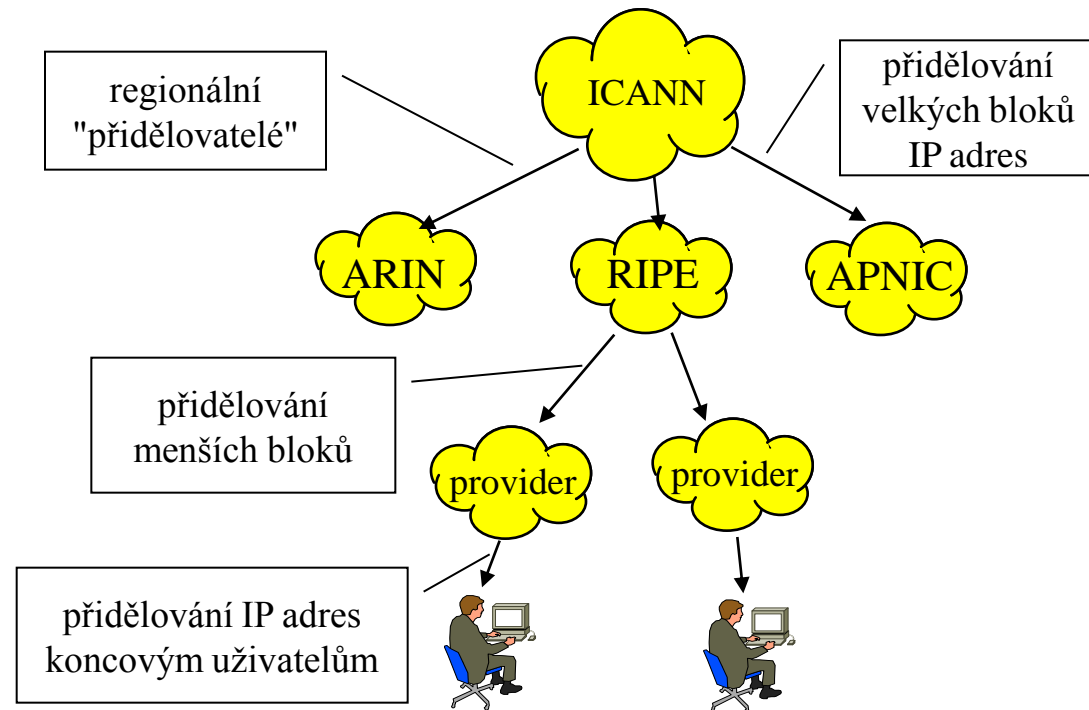
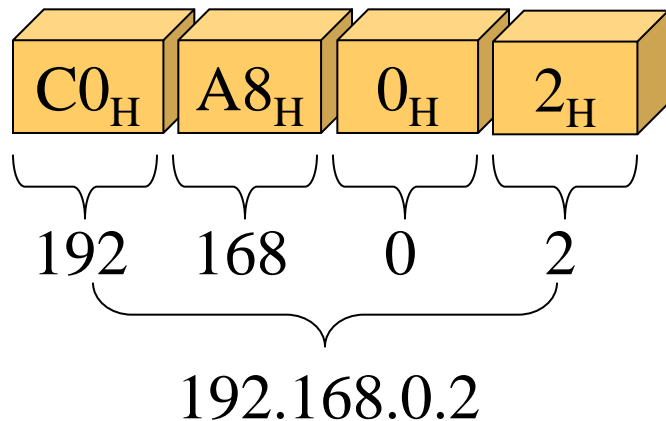
tzv. CIDR prefix

(říká, kolik bitů tvoří síťovou část)

jedna z velmi mála zásadnějších změn v TCP/IP

IP adresy – distribuce a zápis

- IP adresy jsou 32-bitové
 - lze je chápat jako jedno velké (32-bitové) binární číslo
 - ale to se špatně zapisuje i čte
- používá se jednotný způsob zápisu:
 - obsah každého bytu je vyjádřen jako desítkové číslo
 - jednotlivé části jsou spojeny tečkou
 - příklad: 193.84.57.34
 - příklad: 147.3.1.3
- původně:
 - IP adresy se koncovým uživatelům přidělovaly centrálně
 - bez ohledu na způsob jejich připojení
- dnes:
 - IP adresy přiděluje svým zákazníkům provider
 - IP adresy jsou závislé na způsobu připojení, při změně providera se musí měnit



filosofie TCP/IP

– spolehlivost, nebo nespolehlivost?

- spolehlivá přenosová služba
 - když zjistí že nějaká data jsou poškozena/ztracena, považuje za svou povinnost postarat se o nápravu
 - typicky: vyžádá si nový přenos již jednou přenesených dat, v očekávání že opakovaný přenos již dopadne dobře
 - se zajištěním spolehlivosti je spojena určitá režie
 - přenosová režie: spotřebovává se další přenosová kapacita
 - časová režie: nějakou dobu to trvá, způsobuje to zpoždění v přenosu, nerovnoměrnosti v doručování
 - výpočetní režie: uzly musí mít dostatečnou inteligenci na zajištění všeho potřebného
- nespolehlivá přenosová služba
 - sama z vlastní iniciativy nezpůsobuje žádná poškození/ztráty dat
 - vyvíjí maximální snahu o korektní přenos
 - jakmile ale zjistí, že došlo k nějaké chybě/poškození/ztrátě, nepovažuje za svou povinnost postarat se o nápravu
 - předpokládá, že pokud bude náprava zapotřebí, postará se o ni někdo jiný
 - vyšší vrstvy
 - má právo zahodit poškozená data (ignorovat ztrátu) a pokračovat dál
 - není s tím spojena žádná režie
 - je to rychlé, efektivní ...

filosofie TCP/IP – protokol IP

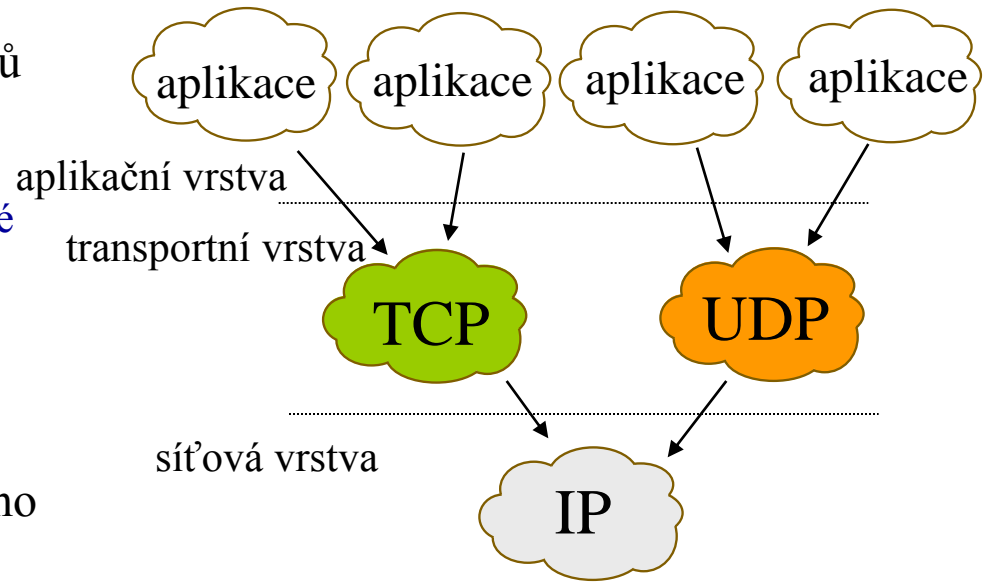
- otázka:
 - má IP fungovat spolehlivě, nebo nespolehlivě?
- výchozí úvaha:
 - přenosová část by měla hlavně přenášet data
 - a ne se starat o další věci
 - je výhodnější, když si spolehlivost zajistí až koncové uzly
 - a nikoli přenosová část sítě
 - proč?
 - někdo (některé aplikace) nemusí spolehlivost potřebovat, a dá přednost rychlému a pravidelnému přenosu
 - protože k zajištění spolehlivosti je třeba výpočetní kapacita, a ta je lacinější v koncových uzlech než „uvnitř“ sítě
 - spolehlivost je vždy relativní (nikoli 100%), někomu by nemusela postačovat míra „zabudované“ spolehlivosti a musel by si ji zajišťovat sám a znovu
 - a to by bylo neefektivní, protože režie spojená se zajištěním spolehlivosti na každé vrstvě by se sčítala, či dokonce násobila!
- řešení v rámci TCP/IP:
 - přenosová část (síťová vrstva, protokol IP) funguje pouze nespolehlivě
 - mechanismy zajišťující spolehlivost jsou implementovány až v transportní vrstvě
 - ale jako volitelná možnost (tj. není povinnost je využívat!!!)
 - aplikace si mohou vybrat, zda chtějí spolehlivý či nespolehlivý přenos

protokol IP je

- nespolehlivý
- nespojovaný

filosofie TCP/IP – transportní vrstva

- řeší komunikaci koncových účastníků (end-to-end communication)
 - sama využívá nespojovaný a nespolehlivý přenos na úrovni síťové vrstvy
- sama alternativně nabízí:
 - spojovaný a spolehlivý přenos
 - nespojovaný a nespolehlivý přenos
- aplikace si mohou vybrat dle vlastního uvážení!!!



- protokol **UDP** (User Datagram Protocol)
 - zajišťuje nespojovaný a nespolehlivý přenos
 - je jen „lehkou nadstavbou“ nad síťovou vrstvou, nemění povahu přenosových služeb síťové vrstvy
- protokol **TCP** (Transmission Control Protocol):
 - zajišťuje spolehlivý a spojovaný přenos
 - „tváří se“ jako proud (stream), který přenáší jednotlivé byty

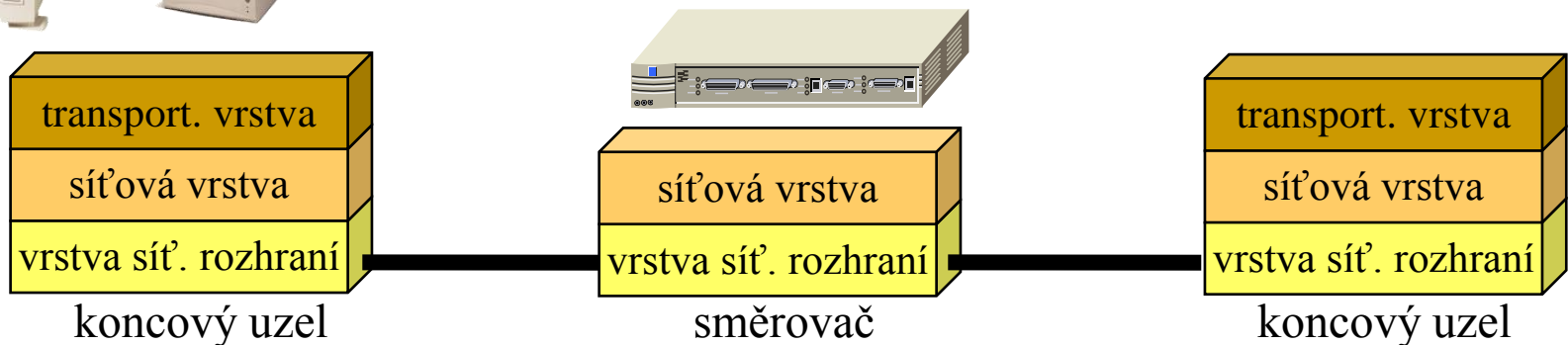
SMTP FTP Telnet HTTP RPC rlogin ... DNS SNMP TFTP BOOTP DHCP RPC NFS XDR ...

TCP

UDP

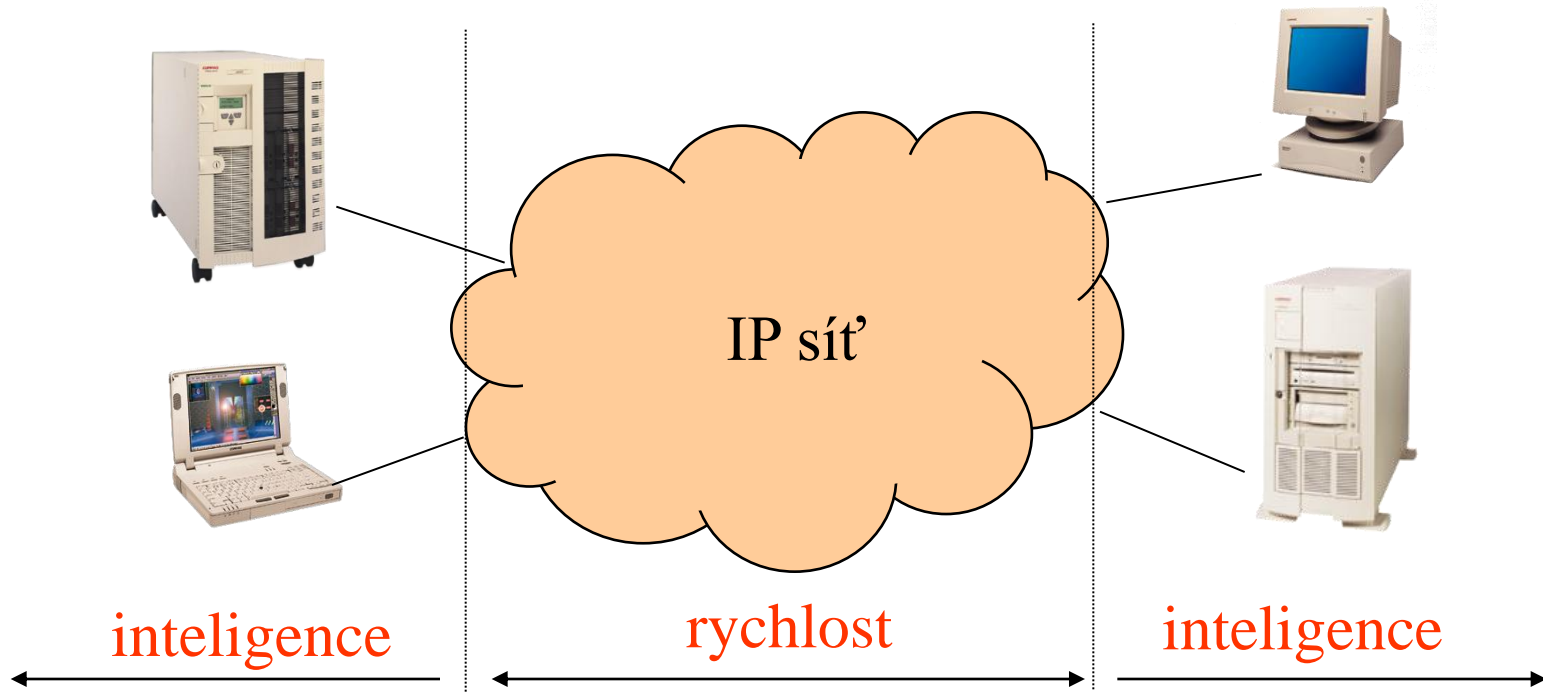
jiný pohled na spolehlivost

- způsob zajištění spolehlivosti je také o tom, kde v síti má být umístěna "intelligence"
 - výpočetní kapacita, logika implementující zajištění spolehlivosti
 - připomenutí: síťová vrstva je ještě ve všech uzlech, transportní již jen v koncových uzlech
- ISO/OSI:
 - **intelligence má být v síti**
 - spolehlivost musí být řešena na úrovni síťové vrstvy
 - intelligence je ve směrovačích
 - je to drahé a nepružné
 - nedává to možnost výběru
- TCP/IP:
 - **intelligence má být v koncových uzlech**
 - spolehlivost je řešena až v transportní vrstvě
 - je to lacinější, pružnější
 - umožňuje to, aby si aplikace vybíraly zda spolehlivost chtějí či nechtějí



hloupá síť vs. chytré uzly

- jiná interpretace:
 - přenosová část sítě (IP síť) má být "hloupá"
 - ale efektivní, má co nejrychleji a nejefektivněji plnit své základní úkoly
 - "chytré" mají být koncové uzly
 - inteligence má být soustředěna do koncových uzlů

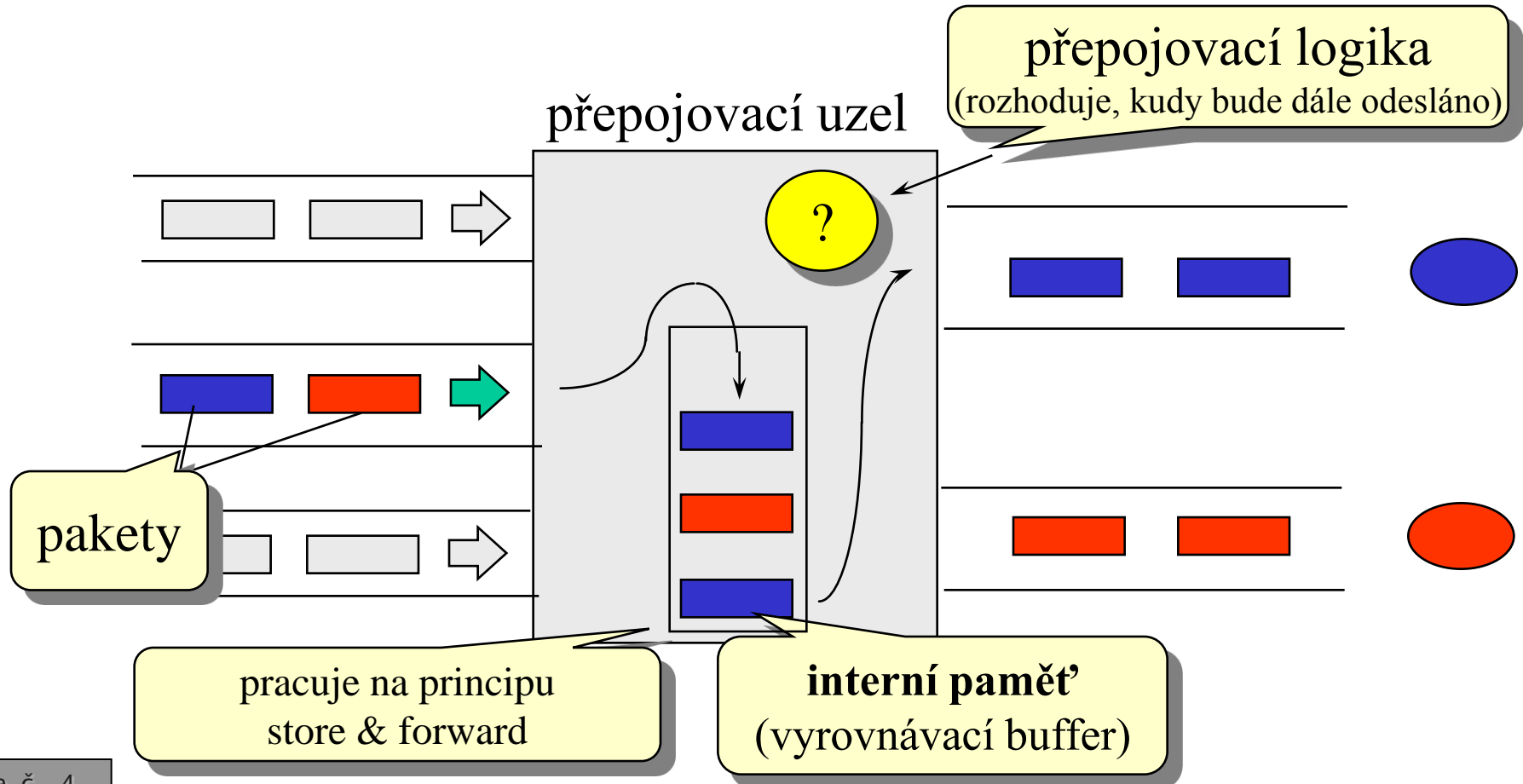


princip maximální snahy

- anglicky "best effort"
 - přenosová část sítě se maximálně snaží vyhovět všem požadavkům, které jsou na ni kladeny
 - pokud se jí to nedaří, má právo krátiť požadavky (limitovat, ignorovat je, nevyhovět jim, ...)
 - např. pozdržet přenášené pakety do doby, než je bude moci zpracovat
 - může i zahazovat pakety, které vůbec nedokáže zpracovat
 - dělá to rovnoměrně vůči všem požadavkům
 - "měří všem stejně", nepracuje s prioritami
- je to celková filosofie TCP/IP
 - je praktickým důsledkem použití paketového přenosu a přístupu ke spolehlivosti
- alternativa:
 - garance služeb (QoS, Quality of Service)
 - QoS nabízí telekomunikační sítě
- výhoda:
 - sítě fungující na principu "best effort" jsou mnohem efektivnější (i ekonomicky) než sítě nabízející QoS
 - **kdyby Internet poskytoval QoS, byl by mnohem dražší než dnes a méně rozvinutý**
- nevýhoda:
 - vadí to multimediálním přenosům

příčina – princip paketového přenosu

- problém: kapacita přepojovacího uzlu i "odchozích směrů" je omezena. Pokud součet požadavků překročí dostupnou kapacitu, má uzel právo zahazovat pakety které nedokáže zpracovat!!!!

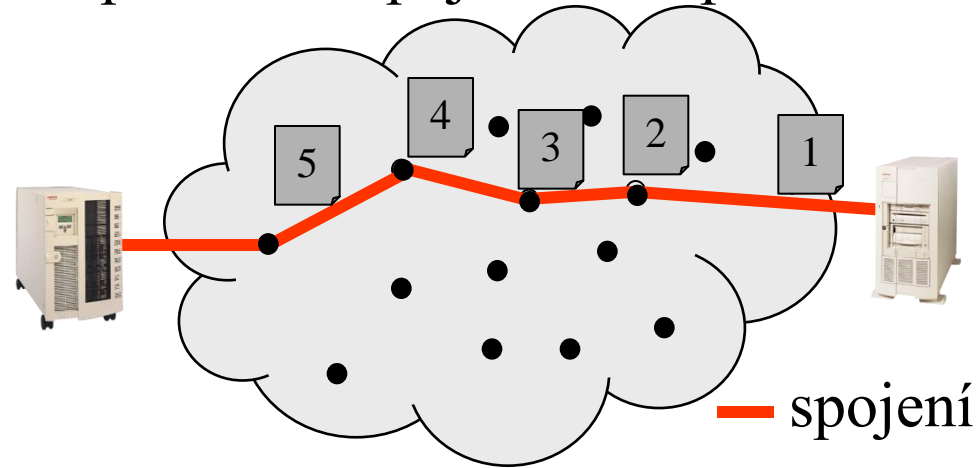


filosofie TCP/IP

- spojovanost nebo nespojovanost?

- spojovaný způsob přenosu
 - před samotným přenosem dat dojde k navázání spojení mezi příjemcem a odesilatelem
 - včetně vytyčení trasy spojení
 - všechna data pak cestují stejnou trasou
 - pořadí přenášených paketů se nemění
 - odesílatel má jistotu, že příjemce existuje a je ochoten přijímat data
 - v případě výpadku/změny topologie musí být spojení detekována změna, poté ukončeno existující spojení a navázáno nové

představa spojovaného přenosu

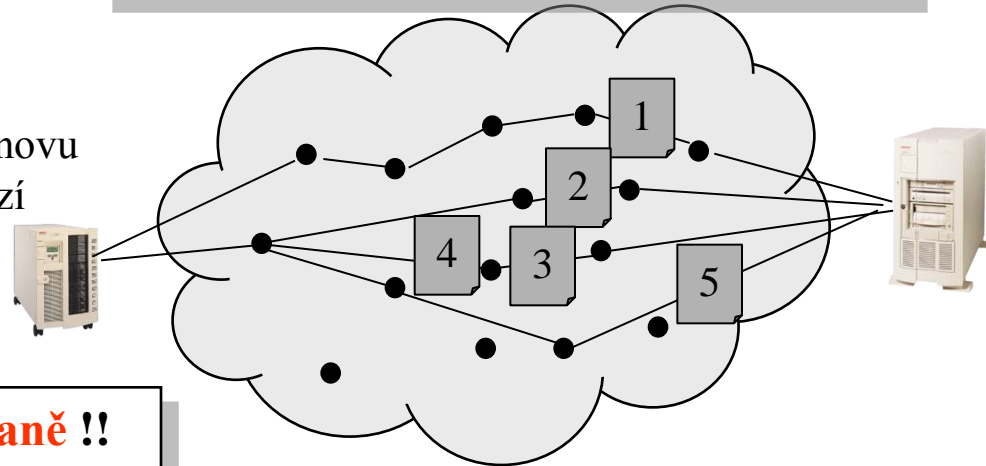


- je to výhodné pro nárazové přenosy větších objemů dat
- není to vhodné při častějších změnách v topologii či stavu sítě
 - kdy je nutné explicitně ošetřovat tyto změny
- jde o stavový způsob fungování
 - mění se stav komunikujících stran

filosofie TCP/IP - nespojovanost

- nespojovaný způsob přenosu
 - datové pakety (tzv. datagramy) jsou přenášeny bez toho, že by se navazovalo jakékoli spojení s příjemcem
 - odesílatel ani neví, zda příjemce existuje a je ochoten data přijmout
 - každý paket (tzv. datagram) je přenášen samostatně, nezávisle na ostatních
 - vždy se pokaždé znovu hledá jeho cesta k cíli
 - provádí se tzv. směrování, vždy znovu v každém uzlu kudy paket prochází
 - není zaručeno pořadí doručování paketů
- je to výhodné tam, kde dochází k častějším změnám v síti
 - nebo je lze očekávat
- je to vhodnější pro méně intenzivní přenosy více rozložené v čase
 - kde se mohou více uplatnit změny v síti

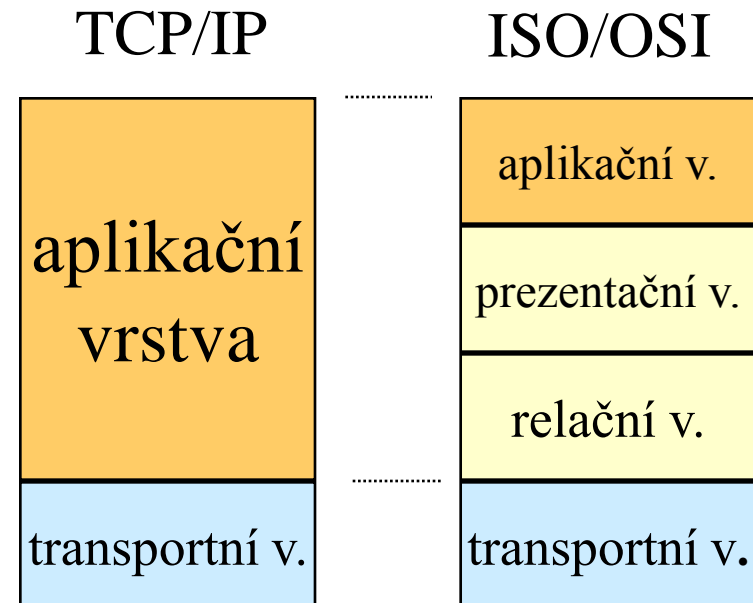
protokol **UDP** funguje **nespojovaně**,
TCP **spojovaně** (emuluje spojovaný
způsob fungování) !!



protokol **IP** funguje **nespojovaně** !!

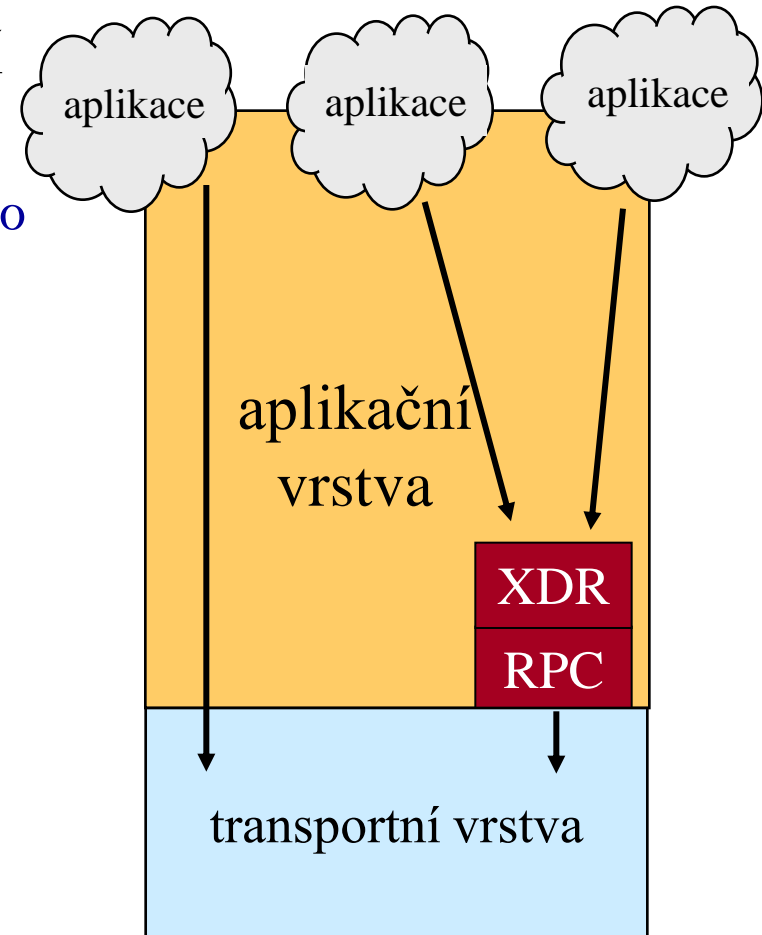
filosofie TCP/IP - sdílení mechanismů

- když se někde musí implementovat nějaké mechanismy, jak mají být řešeny?
 - například mechanismy pro vedení relací, konverze apod.
- **RM ISO/OSI**: tak, aby je měli všichni k dispozici
 - sdíleně, tj. jako samostatné vrstvy
 - a režii těchto mechanismů pak ponese všichni (i ti, kdo je nepoužívají)
- **TCP/IP**: tak, aby režii nenesli ti, kdo je nechtějí používat
 - ne-sdíleně, tj. zabudovávají se přímo a pouze do těch aplikací, které je skutečně potřebují
 - režii nese ten, kdo mechanismy nepotřebuje
- důsledek:
 - **ISO/OSI má samostatnou prezentační a relační vrstvu**
 - vychází z předpokladu že prezentační a relační služby budou potřebovat všechny aplikace
 - pak mají samostatné vrstvy smysl
 - **TCP/IP nemá samostatné vrstvy**
 - vychází z předpokladu, že prezentační a relační služby budou potřebovat jen některé aplikace
 - pak nemá smysl dělat samostatné vrstvy
 - aplikace, které tyto služby potřebují, si je musí realizovat samy



výjimka: RPC a XDR

- aplikační protokol NFS používá ke svému fungování prezentační a relační služby
 - protokol RPC (Remote Procedure Call) pro relační služby
 - protokol XDR (eXternal Data Representation) pro prezentační služby
- tyto protokoly jsou implementovány jako vícenásobně využitelné
 - jako samostatné moduly, jejichž služby může využívat každá aplikace která chce
 - a naopak nemusí ta aplikace, která nechce (a v tom případě nenese jejich režii !!!!)

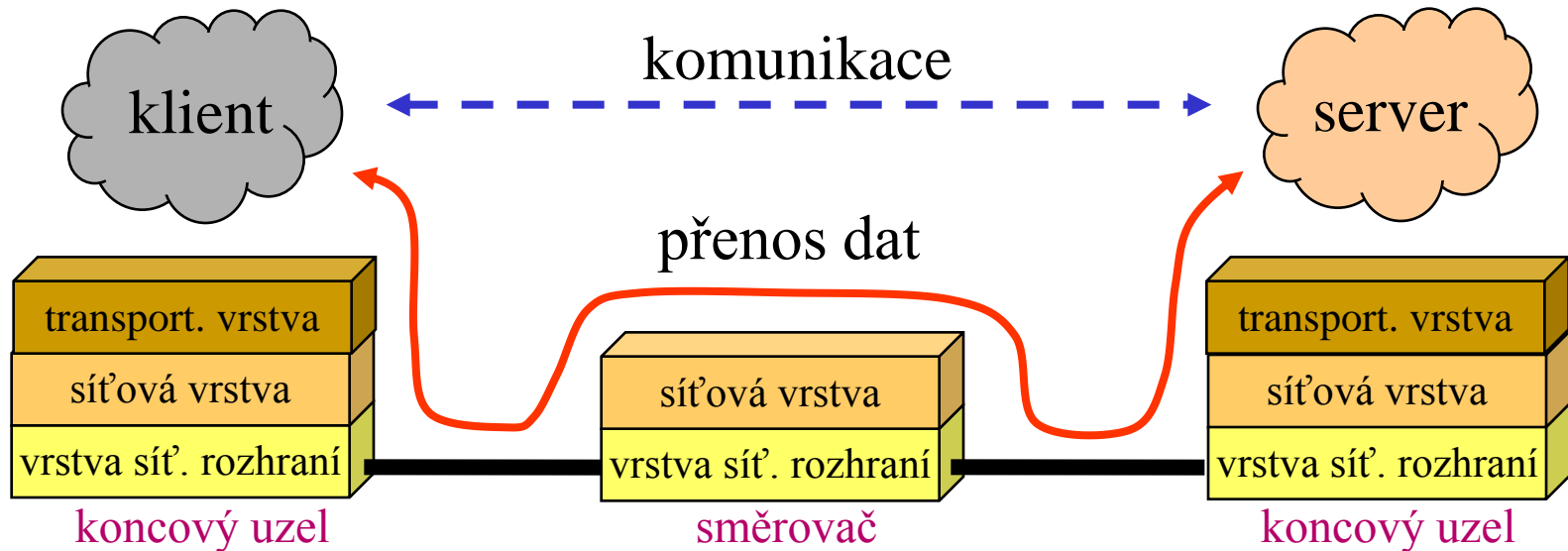


aplikace v TCP/IP

- původně:
 - elektronická pošta (SMTP, RFC 822)
 - přenos souborů (FTP)
 - vzdálené přihlašování (TELNET, rlogin)
 - těmto aplikacím dobře vyhovovalo fungování sítě "na principu maximální snahy, ale nezaručeného výsledku"
- později se objevily a prosadily nové aplikace:
 - news
 - sdílení souborů (NFS)
 - Web (HTML, HTTP,)
 - on-line komunikace (IRC, chat, ..)
 - pro tyto aplikace princip "maximální snahy" není optimální, ale ještě postačuje, důležitá je hlavně disponibilní přenosová kapacita
- dnes se prosazují také aplikace "multimediálního" charakteru, např.:
 - VOIP (Voice over IP)
 - internetová telefonie, "hlas přes IP"
 - IPTV
 - Internet Protocol TV
 - VOD (Video on Demand)
 - přenos obrazu na vyžádání
 - AOD (Audio on Demand)
 - on-line hry
 -
 - pro tyto aplikace je princip "maximální snahy" velmi nevhodný, potřebovaly by zajistit kvalitu služby (QoS)

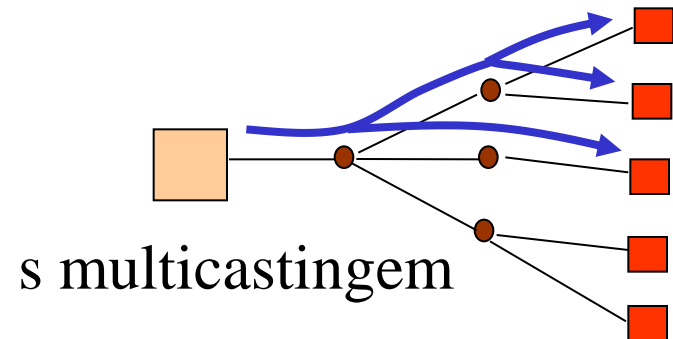
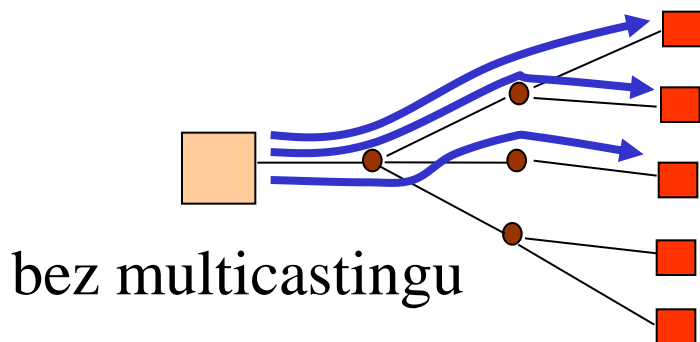
aplikace v TCP/IP

- prakticky všechny (tradiční) aplikace v rámci TCP/IP jsou založeny na architektuře client/server
 - servery poskytující "veřejné" služby jsou dostupné na tzv. dobře známých portech (well-known ports)
 - přenosové mechanismy TCP/IP jsou uzpůsobeny komunikaci stylem 1:1 (mezi 1 serverem a 1 klientem)



problém distribučních aplikací

- s postupem času se objevily i takové aplikace, pro které je fungování přenosových mechanismů TCP/IP principiálně nevhodné
- "**distribuční služby**" = videokonference, vysílání rozhlasu a TV,
 - potřebují dopravovat stejná data od 1 zdroje k více příjemcům současně
 - tzv. **multicasting** (event. broadcasting)
 - přenosové mechanismy TCP/IP to neumí !!!
 - přenosové mechanismy počítají s přenosem 1:1 (od jednoho zdroje k jednomu příjemci)
 - pokus: služba MBONE (nepříliš úspěšná)
 - řeší se až v rámci IPv6 a IP Multicast Initiative



problém multimedialních aplikací

- potřebují dostávat svá data:
 - s malým zpožděním (latence)
 - s pravidelným zpožděním (jitter)
 - s pravidelnými odstupy mezi sebou
- týká se to například přenosu živého obrazu či zvuku
 - aplikace VOIP, IPTV, rozhlas, video-on-demand,
- problém je s fungováním přenosových mechanismů TCP/IP na principu "*maximální snahy, ale nezaručeného výsledku*"
 - byla by zapotřebí podpora QoS (kvality služeb)
 - QoS je v zásadě "protipólem" principu maximální snahy
- možná řešení:
 - "**kvantitativní**": zvyšování disponibilní kapacity
 - fungování na principu "maximální snahy ..." zůstává
 - zlepšení je statistické
 - je menší pravděpodobnost, že bude muset dojít ke krácení požadavků
 - týká se:
 - přenosových kapacit (tj. linek)
 - "přepojovacích kapacit" (směrovačů, switchů)
 - "**kvalitativní**": zavedení podpory QoS
 - fungování na principu "maximální snahy ..." je nahrazeno jiným způsobem fungování
 - zlepšení je garantované
 - ale drahé a obtížné

QoS v TCP/IP – možné přístupy

- prioritizace
 - různým druhům přenosů se přiřadí různé priority a je s nimi nakládáno odlišně
 - přenosy s vyšší prioritou dostávají "kvalitnější obsluhu" (a přiděl zdrojů) na úkor přenosů s nižší prioritou
 - příklady řešení:
 - DiffServ (Differentiated Services)
- rezervace
 - pro potřebu konkrétních přenosů si lze vyhradit (rezervovat) požadované zdroje a ty pak využívat
 - týká se i vyhrazení přenosové kapacity, přepojovací kapacity atd.
 - příklady řešení:
 - IntServ (Integrated Services)
 - vyžaduje: RSVP (Resource Reservation Protocol)
 - » zajišťuje "vyhrazení" zdrojů na úrovni síťové vrstvy, na úkor protokolu IP

podporu QoS lze poskytovat:

- "per flow": pro každý jednotlivý jednosměrný tok dat mezi dvěma aplikacemi
- "per aggregate": pro celé skupiny toků

problém bezpečnosti

- přenosové mechanismy TCP/IP neposkytují žádné zabezpečení
 - nebylo to "v původním zadání"
 - přenášená data nejsou žádným způsobem chráněna proti "odposlechu"
 - nejsou šifrována ani jinak kódována či chráněna
 - nejsou ani chráněna proti ztrátě
 - u nespolehlivých přenosů
- předpoklad:
 - pokud nějaká aplikace potřebuje určitou míru zabezpečení, musí si ji zajistit sama
- jde o stejný "kompromis" jako u spolehlivosti:
 - buďto poskytnout zabezpečení všem (i těm kteří jej nepotřebují), nebo si jej bude muset každý zájemce udělat sám
 - teze: přenosové mechanismy by měly hlavně přenášet data, ne se starat o další funkce ...
- důsledek:
 - přenosová infrastruktura je jednodušší, rychlejší a také lacinější
 - oproti stavu, kdy by fungovala zabezpečeným způsobem
- praxe:
 - zabezpečení se řeší na aplikační úrovni
- IPSEC:
 - framework (rámec) pro zajištění bezpečnosti na úrovni síťové vrstvy

IPv6, mobilita

- IPv6
 - řeší problém nedostatku IP adres
 - pracuje se 128-bitovými adresami
 - podporuje řadu dalších vlastností/funkcí
 - např. QoS
 - zabezpečení
 - autokonfigurace
 - směrování (source routing, ...)
 - místo broadcastu má multicast a anycast
- mobilita
 - IP adresy nejsou "mobilní"
 - nelze je přenášet mezi sítěmi
 - řešení mobility:
 - přidělení nové IP adresy v nové síti
 - DHCP atd.
 - skrze agenty a tunely
 - "na původním místě" zůstane agent, který vše přeposílá "skrze tunel" tam, kde se uzel právě nachází
 - je vůbec mobilita zapotřebí?

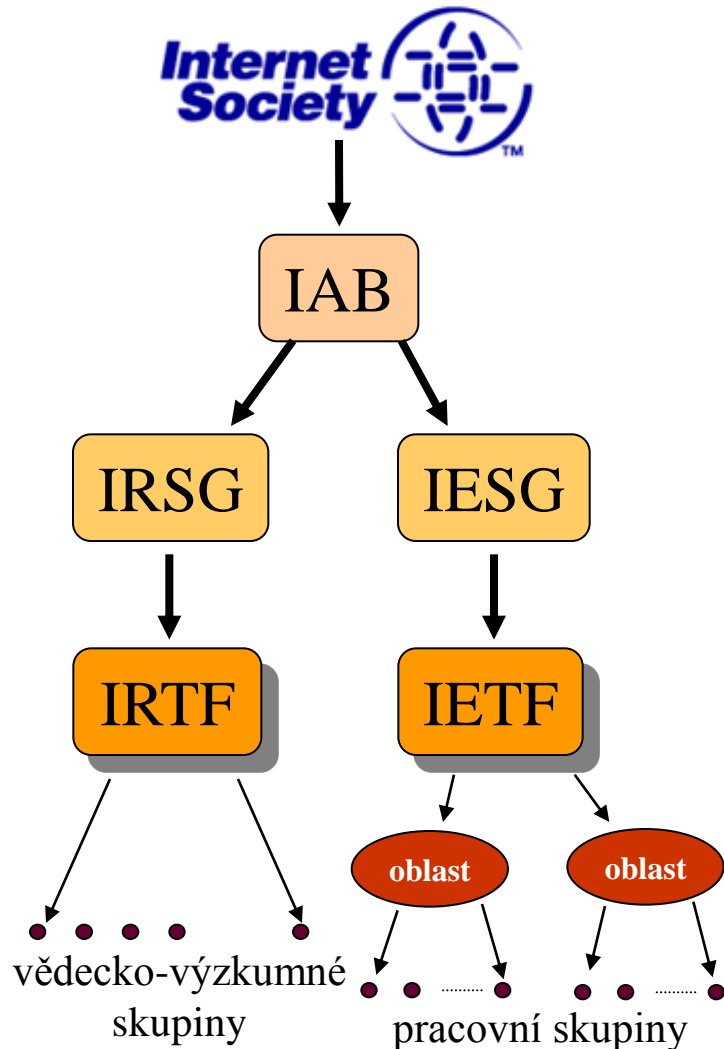
filosofie "vývoje" TCP/IP

- schopnosti služeb a přenosových protokolů TCP/IP se vyvíjí stylem "od jednoduššího ke složitějšímu"
 - postupným zdokonalováním
 - začíná se s minimem funkcí, teprve postupně se přidávají další schopnosti a vlastnosti, pokud se ukáže jejich potřeba a realizovatelnost
- tomu je přizpůsoben i standardizační proces – než se něco stane standardem, musí to prokázat
 - reálnou implementovatelnost
 - alespoň 2 nezávislé implementace
 - funkceschopnost
 - musí existovat provozní zkušenosti s pilotním nasazením
- příklad: elektronická pošta
 - vznikla jako jednoduchá služba pro přenos čistě textových zpráv
 - postupně byla obohacena o další možnosti (přílohy, formátování, národní abecedy atd. – standard MIME)

standardizace TCP/IP

- standardy TCP/IP jsou skutečně otevřené
 - i když nikdo pořádně neví, co to přesně znamená
 - nejsou „v rukou“ jediné firmy
 - vznikají (jsou přijímány) na základě všeobecného konsensu
- specifikace těchto protokolů jsou veřejným vlastnictvím
 - za jejich využití se neplatí žádné licenční poplatky
 - texty specifikací mají povahu volně šiřitelných dokumentů (dokumentů RFC)
- technická řešení, která jsou předmětem standardů, vznikala původně v rámci „sdružení“ **IETF** (Internet Engineering Task Force)
 - dosti volné společenství odborníků, zainteresovaných na vývoji TCP/IP
- dnes tato řešení vznikají u komerčních firem, které je předkládají ke standardizaci
 - snaží se je prosadit jako internetový standard
 - IETF je nyní pouze posuzuje a vybírá mezi nimi

standardizační orgány pod ISOC



- ISOC: (<http://www.isoc.org>)
 - zastřešuje, reprezentuje vůči jiným organizacím a orgánům
- IAB: (<http://www.iab.org>)
 - řídí standardizační práci, přijímá strategická rozhodnutí, formálně vydává dokumenty RFC
- IESG,IRSG:
 - "Steering Groups", řídí práci IETF a IRTF, které mají velmi "volnou organizaci"
 - "vnáší řád do chaosu" (kompenzují to, že samotné IETF a IRTF nemají žádné řádné formální členství)

shrnutí standardizačního procesu



<http://www.isoc.org>

- standardy vydává ISOC
 - formálně IAB
- ISOC nemá statut standardizační organizace
 - její standardy nemají statut standardů **de jure**
 - jde o standardy **de facto**
 - přesto jsou v praxi velmi důsledně dodržovány
 - standardy týkající se TCP/IP jsou publikovány formou dokumentů RFC (STD)



<http://www.w3c.org>

- výjimkou jsou standardy týkající se WEB-u
 - např. k HTML, XML, CSS, PICS, PNG
 - ty vydává konsorcium W3C jako svá doporučení
 - candidate recommendation
 - proposed recommendation
 - recommendation
 - je dohoda o tom, že relevantní doporučení W3C budou publikovány též jako dokumenty RFC

srovnání TCP/IP a RM ISO/OSI

- ISO/OSI a jeho součásti vznikají stylem „od složitého k jednoduššímu“
 - nejprve se požaduje hodně, a pak se musí ubírat
 - vznikají problémy s kompatibilitou „podmnožin“
- k přijetí standardu není nutné ověření praktické realizovatelnosti
- standardy ISO jsou prodávány a jsou opravdu hodně drahé
 - uplatňuje se strategie: *„chci, abys dodržel moje standardy. Nejprve mi ale musíš hodně zaplatit, abych ti vůbec řekl, co po tobě chci ...“*
 - výsledek tomu odpovídá ☹
- TCP/IP vzniká stylem „od jednoduchého ke složitějšímu“
 - nejprve se přijme jednodušší řešení, pak se ev. přidává
 - existuje záruka kompatibility alespoň na úrovni „společného minima“
- pro přijetí standardu je nutné ověření praktické realizovatelnosti
 - dokonce i praktické provozní zkušenosti
- standardy TCP/IP (i související dokumenty) jsou dostupné volně a zdarma
 - uplatňuje se strategie: *„když chci něco prosadit, musím k tomu maximálně usnadnit přístup“*
 - tato strategie funguje ☺