



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



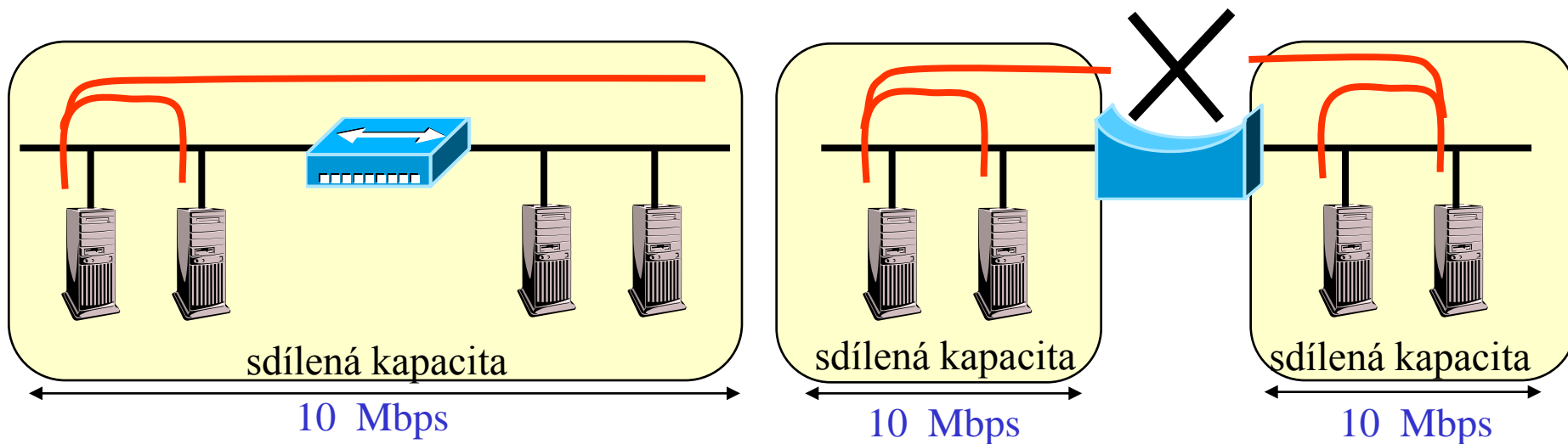
Lekce 2: internetworking - II.

J. Peterka, 2010

základní otázka (internetworking-u)

- jak rozčlenit lokální síť?
 - nechat ji jako jednu "velkou a plochou" síť?
 - rozdělit ji na více dílčích sítí/segmentů?
 - kdy použít opakovač, kdy most či switch, a kdy směrovač?
 -
- neexistuje jednoznačný návod, záleží na konkrétní situaci ...
 - jaká je síť
 - jak je velká, kolik je počítačů, jaké jsou servery a jaké stanice, jaké aplikace se používají
 - co je cílem
 - zda zvýšení propustnosti, propojení, ochrana proti neoprávněnému přístupu, optimalizace toků v síti či něco jiného
 - významnou roli hrají i faktory typu: styl práce uživatelů, způsob nakonfigurování aplikací, výpočetní model
 - např. zda jsou MS Windows a základní aplikace nainstalovány lokálně, nebo centrálně (na file serveru), případně používány na dálku
- rozhodování mezi opakovačem a mostem (či switchem) hodně závisí na rozdílu mezi sdílenou a vyhrazenou přenosovou kapacitou
 - opakovače zachovávají sdílený charakter dostupné přenosové kapacity
 - mosty nezachovávají sdílený charakter, snaží se alespoň nějakou část přenosové kapacity vyhradit
 - prepínače (switche) mohou dosahovat poměrně vysokého stupně „vyhrazení“ přenosové kapacity
- důležité otázky:
 - co je sdílená co vyhrazená kapacita?
 - jaký je rozdíl mezi mostem a prepínačem?
 - jaké jsou trendy "segmentace" lokálních sítí
 - co jsou virtuální LAN?
 -

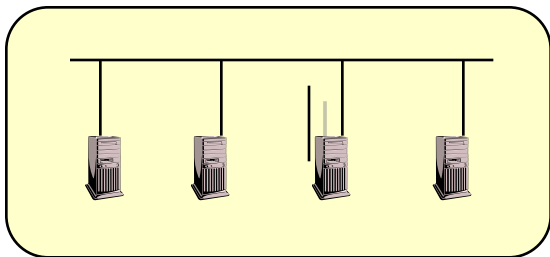
sdílená vs. vyhrazená přenosová kapacita



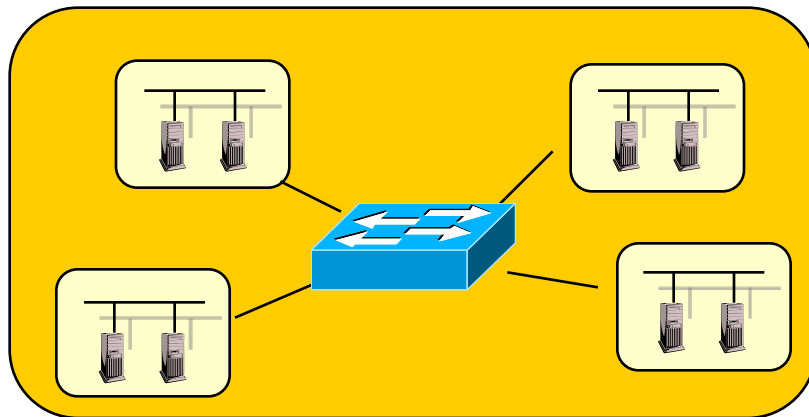
- opakovač šíří veškerý provoz do všech směrů
 - vše, co je propojeno opakovači, má k dispozici celkovou přenosovou kapacitu odpovídající 10 Mbps (v Ethernetu) - tato kapacita je všemi uzly sdílena
 - pro celkovou propustnost to (obvykle) není optimální
- most (ani přepínač) nešíří veškerý provoz do všech směrů
 - díky „lokalizaci“ provozu v jednotlivých částech mohou mít komunikující dvojice „celou“ přenosovou kapacitu jen pro sebe (tato je pro ně vyhrazena)
 - v ideálním případě!!!!

jak zvýšit propustnost sítě?

- přístup "hrubou silou"
 - nezmění se princip fungování
 - sdílená přenosová kapacita
 - jen se zvýší nominální přenosová rychlost
 - např. 10x u 100 Mbps Ethernetu
- pak stačí použít propojení pomocí opakovačů
 - lze zůstat u sdílené přenosové kapacity
 - ale ani to nelze dělat "příliš dlouho", kvůli kolizím v Ethernetu

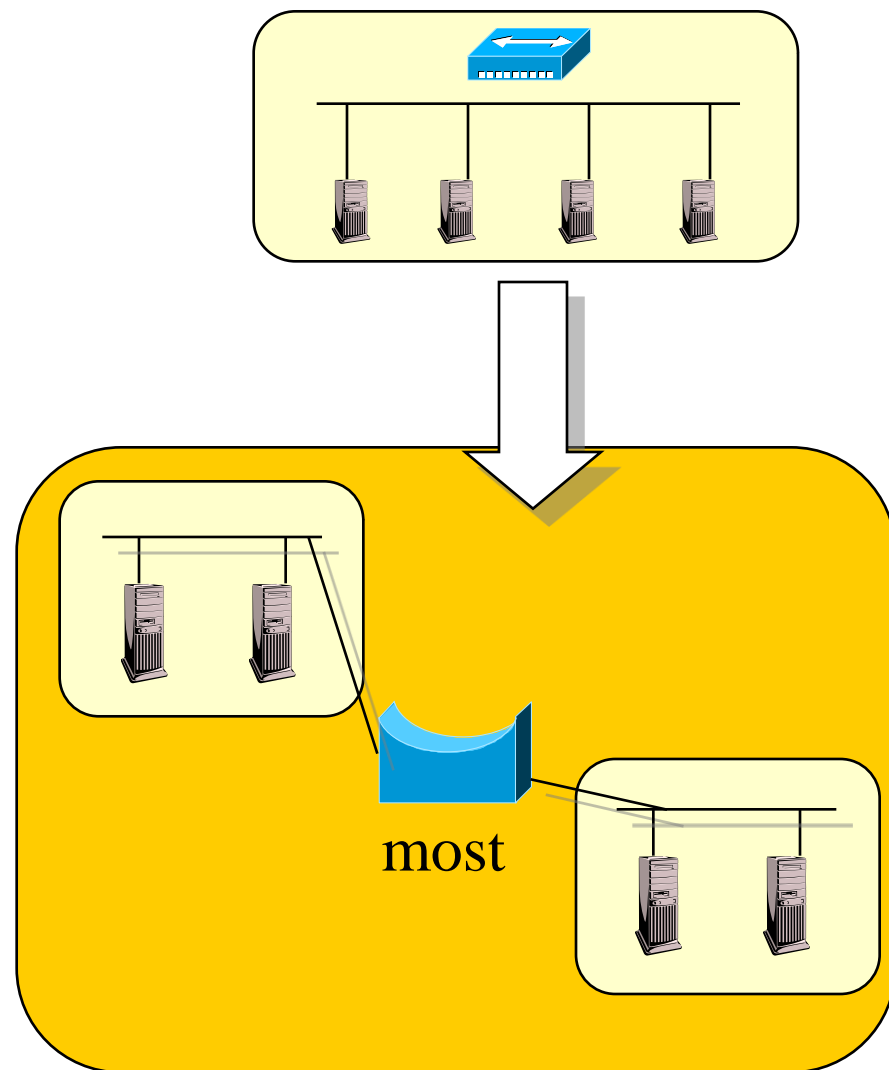


- "inteligentní" přístup
 - snaha rozčlenit síť tak, aby se lokalizoval "místní provoz" a maximálně využil efekt vyhrazené přenosové kapacity
 - aby byly optimalizovány toky v síti
 - např. tzv. přepínaný Ethernet
 - Switched Ethernet
- využívá se propojení pomocí přepínačů



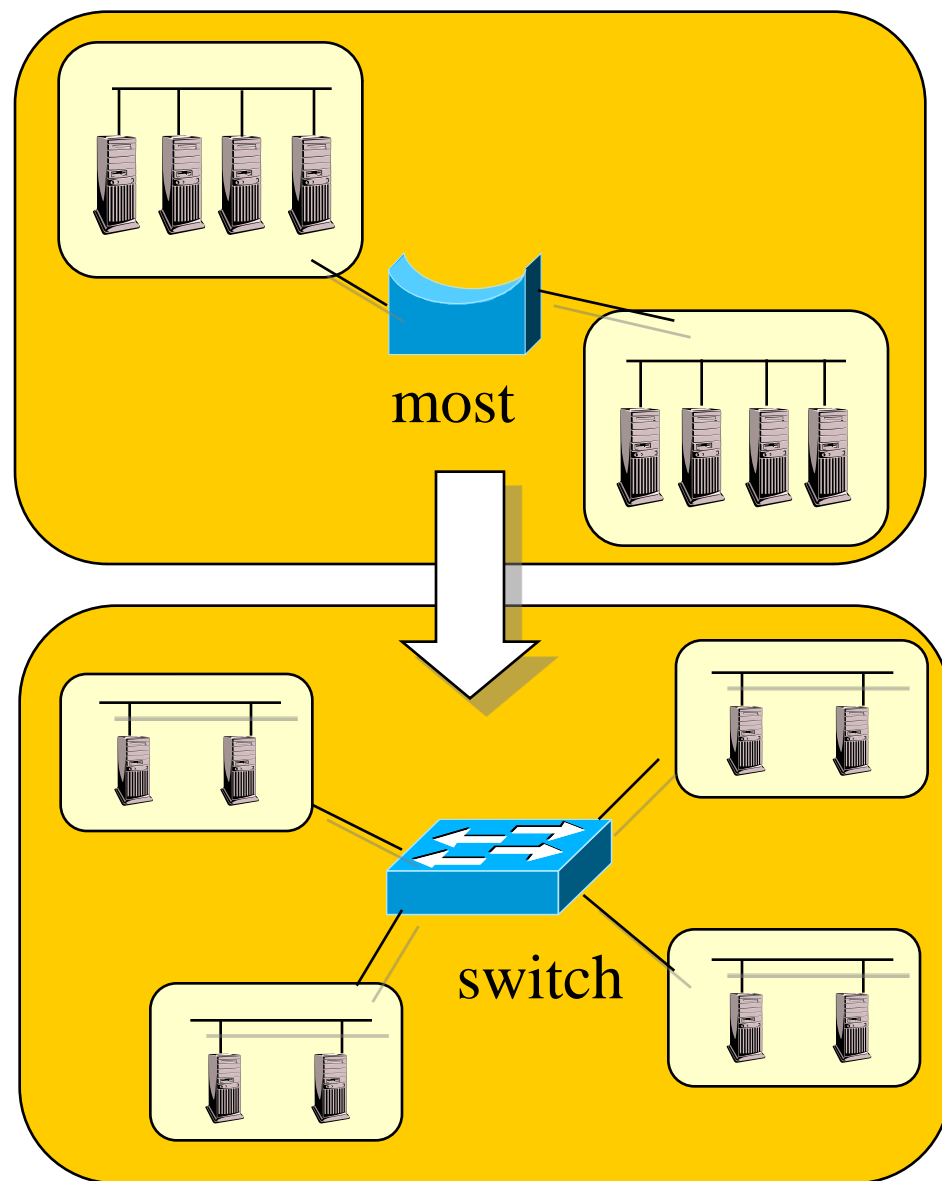
techniky pro zvýšení propustnosti: segmentace

- princip:
 - jeden souvislý segment (představující sdílenou přenosovou kapacitu a kolizní doménu) se rozdělí na dvě části (dva segmenty)
 - případně více segmentů
 - využívá se efektu lokalizace provozu
 - místní provoz v dílčím segmentu není šířen do ostatních segmentů
 - pro realizaci stačí most (bridge)
 - hlavní důraz je kladen na schopnost filtrovat
 - zablokovat přenos dat do jiného segmentu
 - **výkonnost cíleného předávání (forwardingu) není tolik důležitá!!**
 - proto stačí klasický most (bridge)



techniky pro zvýšení propustnosti: segmentace

- pozorování:
 - čím budou dílčí sdílené segmenty menší, tím menší bude "lokální provoz"
 - a naopak tím větší bude provoz mezi dílčími segmenty
 - tím současně porostou nároky na přepojovací kapacitu mostu
 - bude se méně využívat "filtering" a více "forwarding"
 - místo mostu (bridge) se musí použít takové zařízení, které je na to lépe dimenzováno:
 - **přepínač (switch)**

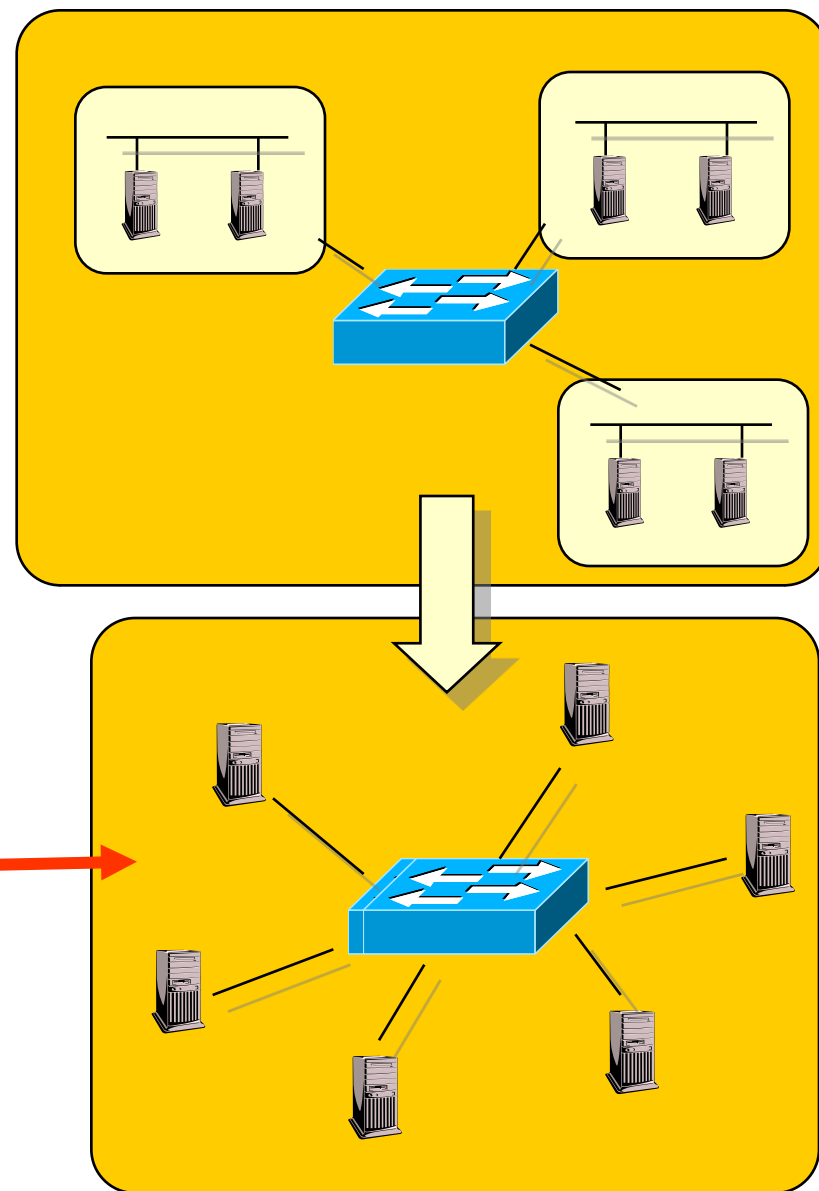


rozdíl most – přepínač (bridge – switch)

- neliší se:
 - principem fungování
 - oba fungují na úrovni linkové vrstvy
 - oba se rozhodují podle informací dostupných na linkové vrstvě
 - linkových adres a znalosti bezprostředního okolí
 - oba zajišťují filtering i forwarding
- **most** (bridge) je starší typ zařízení
 - má méně portů pro připojení dílčích (sdílených) segmentů
 - není u něj důraz na výkonnost
 - na rychlost provádění forwardingu
 - jeho vnitřní fungování je často řešeno programovými prostředky
 - pokud je na něco optimalizován, pak na jednoduchost
- **přepínač** (switch) je novější typ zařízení
 - má více portů než typický most
 - původně byly switche označovány také jako "multiportové bridge"
 - je optimalizován na výkonnost a celkovou propustnost
 - pro potřeby forwardingu
 - jeho "přepojovací stroj" (switching engine) je typicky realizován v hardwaru
 - pomocí zákaznického obvodu (ASIC), šitého na míru dané funkci
 - přináší efekt vyhrazené přenosové kapacity
- je stále "plug-and-play"
 - v Ethernetu funguje na principu samoučení
 - i když kvůli optimalizaci může pracovat i se statickou konfigurací

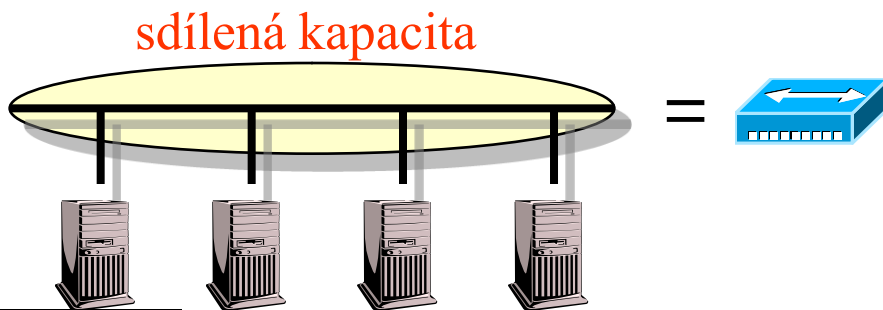
techniky pro zvýšení propustnosti: mikrosegmentace

- mikrosegmentaci si lze představit jako segmentaci dotaženou do dokonalosti:
 - každý dílčí (sdílený) segment bude "obydlen" jen jedním uzlem
 - pak nebude existovat žádný lokální provoz
 - nebude žádný filtering
 - veškerý provoz bude třeba cíleně forwardovat do příslušného cílového segmentu
- dosáhne se tak maximálního možného efektu vyhrazené přenosové kapacity
 - ale klade to největší nároky na přepojovací kapacitu přepínače !!!

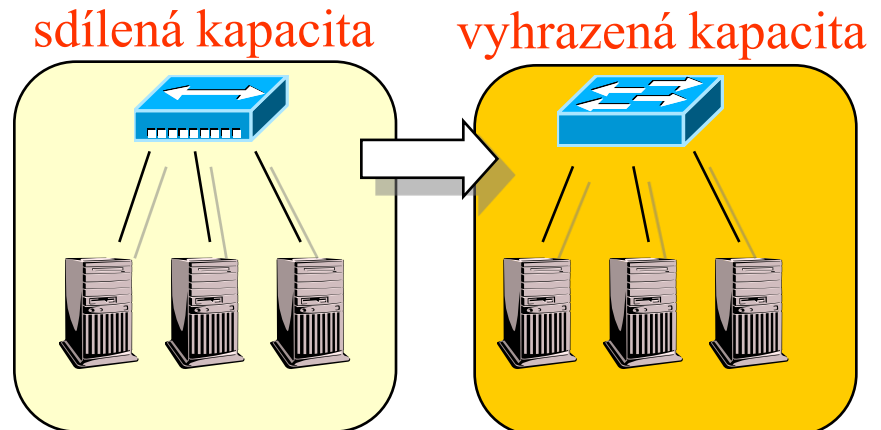


mosty vs. přepínače

- jiné vysvětlení rozdílu mezi mosty a přepínači (v Ethernetu):
 - mosty vznikly v době, kdy Ethernet používal koaxiální kabely a měl skutečně sběrnicovou topologii
 - tj. byl technologií se sdíleným přenosovým médiem
 - segmenty měly typicky více uzlů
 - mosty se snažily udělat maximum pro využití dostupné kapacity
 - segmenty s jedním uzlem neměly smysl

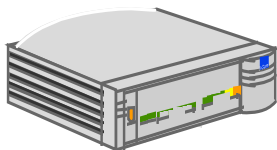


- později Ethernet přešel na použití kroucené dvoulinky, která není sdíleným médiem
 - topologie se ze sběrnicové změnila na stromovitou !!
 - ale Ethernet se k ní stále choval jako kdyby měla charakter sdíleného média
- přepínač (switch) je vlastně řešením, které naplno využívá možnosti stromovité topologie
 - zrodil se tzv. "přepínaný Ethernet"
 - Switched Ethernet

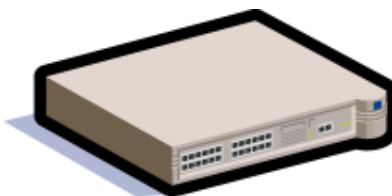


v čem se liší přepínače?

- v tom, kolik uzlů je možné připojit ke každému segmentu (portu)
 - kolik MAC adres si přepínač zvládne pamatovat na každém segmentu (portu)
 - 1 uzel na segment = ideální stav (mikrosegmentace)
 - více uzlů na segment = méně-nej-ideální stav
 - počet je omezen kvůli efektivnosti
 - kvůli velikosti forwardovací tabulky a složitosti jejího prohledávání
- v celkové přepojovací kapacitě
 - zda postačuje pro ideální stav
- v režimu fungování
 - store&forward přepínač
 - přepínač nejprve načte celý rámec a uloží jej do svého bufferu (store), pak se rozhodne co s ním a event. ho předá dál (forward)
 - má větší průchozí zpoždění
 - cut-through přepínač
 - přepínač načeká na načtení rámce ale rozhodne se ihned po načtení jeho hlavičky (a začne rámec přeposílat okamžitě dál)
 - má menší zpoždění (tzv. latenci)



?

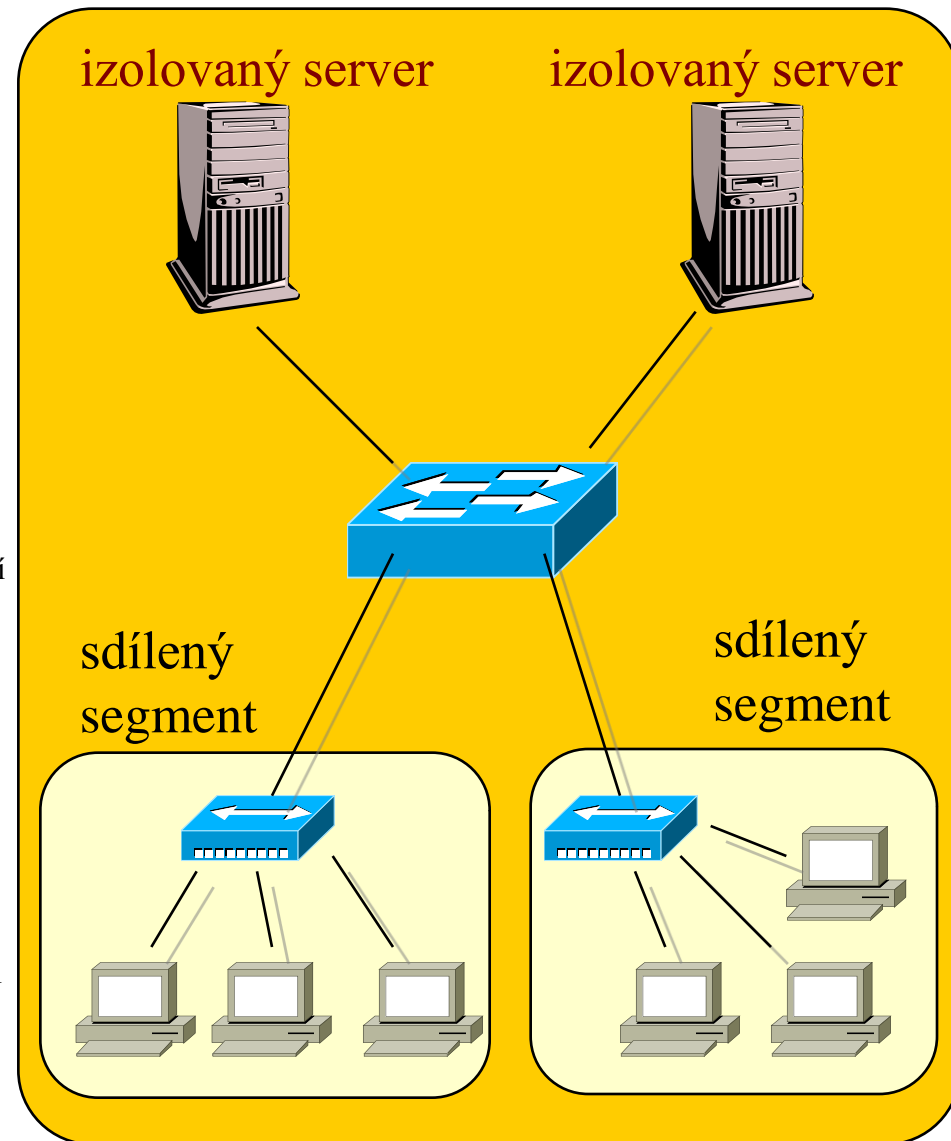


?



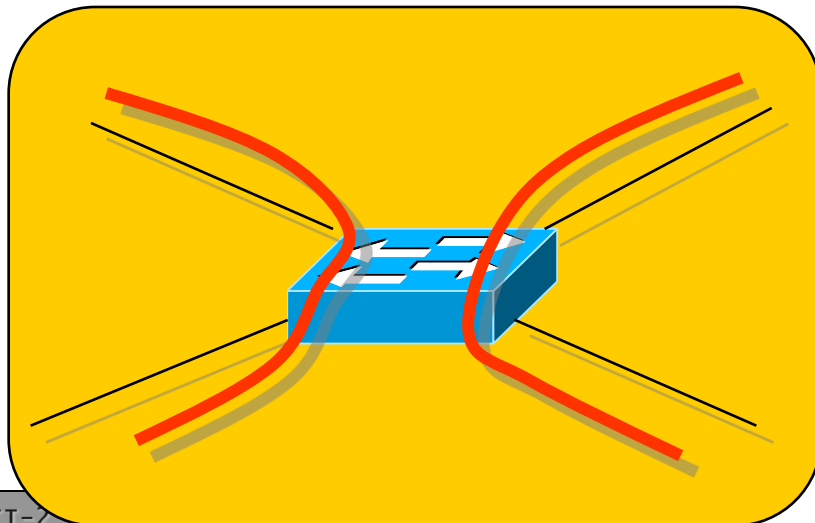
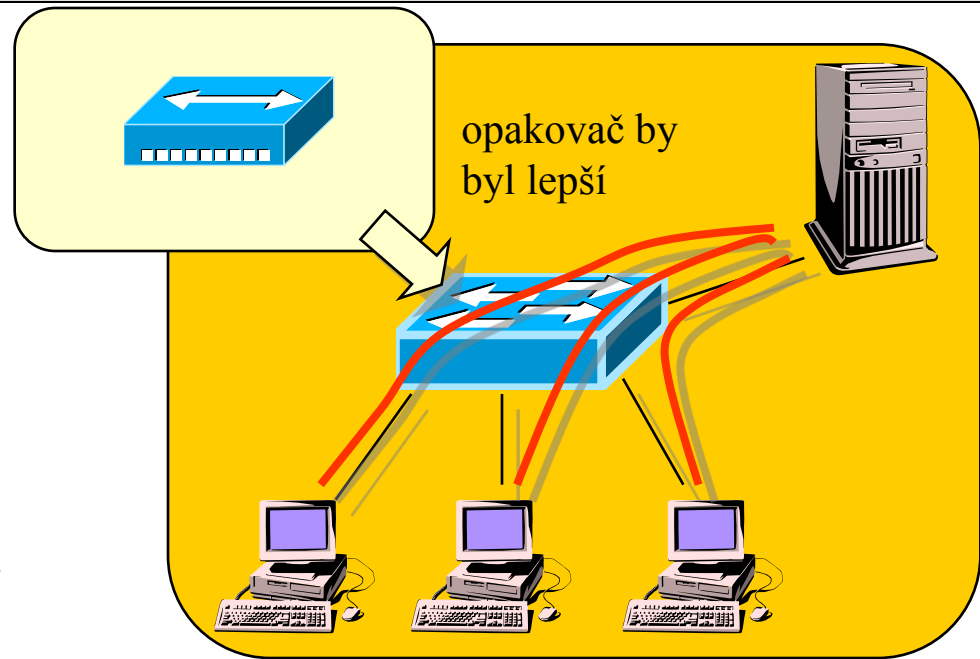
další techniky pro zvýšení propustnosti: izolace serverů

- mikrosegmentace nebývá v praxi (vždy) vhodným řešením
 - porty přepínačů jsou relativně drahé, nevyplatí se připojovat k nim jednotlivé pracovní stanice
 - které ani nevyužijí dostupnou přenosovou kapacitu
- častější řešení:
 - nejvíce zatížené uzly se připojí přímo k portům switche
 - tj. na principu mikrosegmentace, neboli jako 1-uzlové segmenty
 - méně zatížené uzly se připojí ke sdíleným segmentům
 - a teprve tyto sdílené segmenty se jako celky připojují k portům switche
- efekt "izolovaných serverů" lze dále zvýšit použitím přepínačů s různými rychlostmi na portech
 - např. ethernetové switche 10/100 Mbps
 - izolované servery s velkou zátěží se připojují na rychlejší porty
 - pracovní stanice (event. celé sdílené segmenty) se připojují na pomalejší porty
- připadá to v úvahu jen u přepínačů (switchů) fungujících na principu store&forward
 - nikoli cut-through
 - ty musí mít všechny porty stejně rychlé



použití opakovačů vs. přepínačů

- přepínače nejsou univerzálně výhodnější oproti opakovačům
 - vyhrazená kapacita nemusí být výhodnější oproti sdílené
 - v případě že se vyhrazená kapacita nemůže uplatnit



- například pokud veškerý provoz směřuje z/do jednoho segmentu
 - například když jde o pracovní stanice, které nekomunikují mezi sebou ale pouze se serverem
 - pak je výhodnější opakovač
 - kvůli ceně i latenci

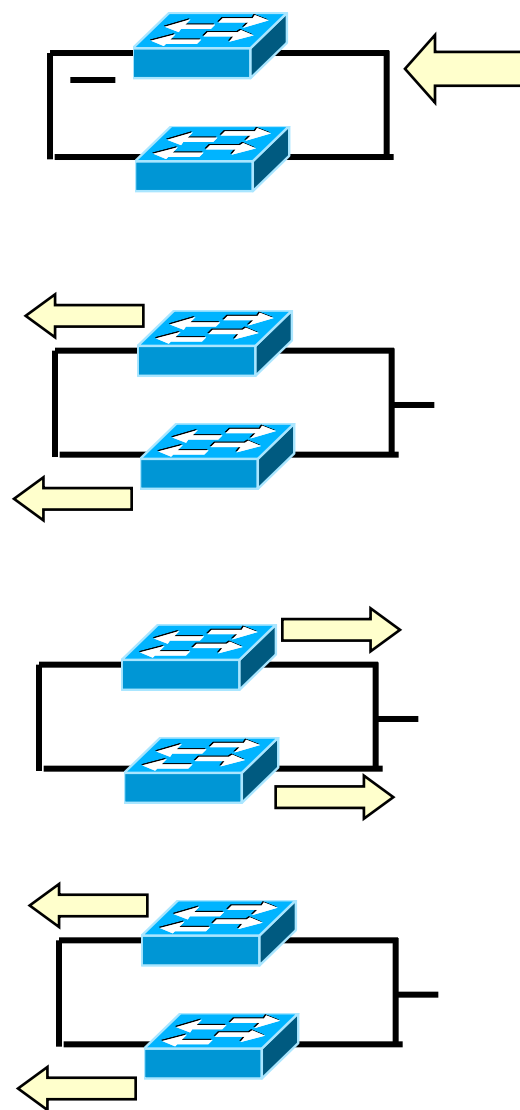
nevýhody mostů/přepínačů

- musí zkoumat obsah všech rámců
 - a ne pouze rámců které mu jsou adresovány přímo
 - což nejsou žádné, když jsou mosty/přepínače transparentní
 - viz promiskuitní režim fungování
- musí šířit všesměrové vysílání
 - připomenutí: co je propojeno na úrovni linkové vrstvy, tvoří tzv. **broadcast doménu**
 - problém: mnohé služby využívají broadcast ke svému fungování
 - např. pro hledání serverů, pro překlad IP adres na linkové atd.
- fungují na principu "forward-if-not-local"
 - forwardují kdykoli nějaký rámec není lokální
 - nezkontrolují zda příjemce existuje
 - mohou forwardovat zbytečně
- některé situace vyžadují „oddělení“ na úrovni síťové vrstvy
 - např. připojení k Internetu
- nepodporují redundantní cesty (cykly)
 - dokonce to vadí jejich řádnému fungování
- propojením pomocí přepínače (obecně na linkové úrovni) vzniká tzv. “plochá síť”
 - z hlediska síťové vrstvy a síťových adres (např. IP adres) je to jedna síť
 - musí propagovat všesměrové vysílání do všech svých částí
 - které je u dnešních aplikací dosti běžné
 - nebezpečí tzv. broadcast storms (laviny, způsobené chybným všesměrovým vysíláním)
 - mohou být problémy s přidělováním adres (např. IP adres)
- neumožňují aplikovat přístupová omezení, ochranu
 - informace související s přístupovými právy a ochranou jsou typicky vztaženy až k síťové vrstvě
 - postavení všech uzlů (z hlediska přístupových práv) je identické

směrovače pracují na obráceném principu: směřují dál jen když vědí kam

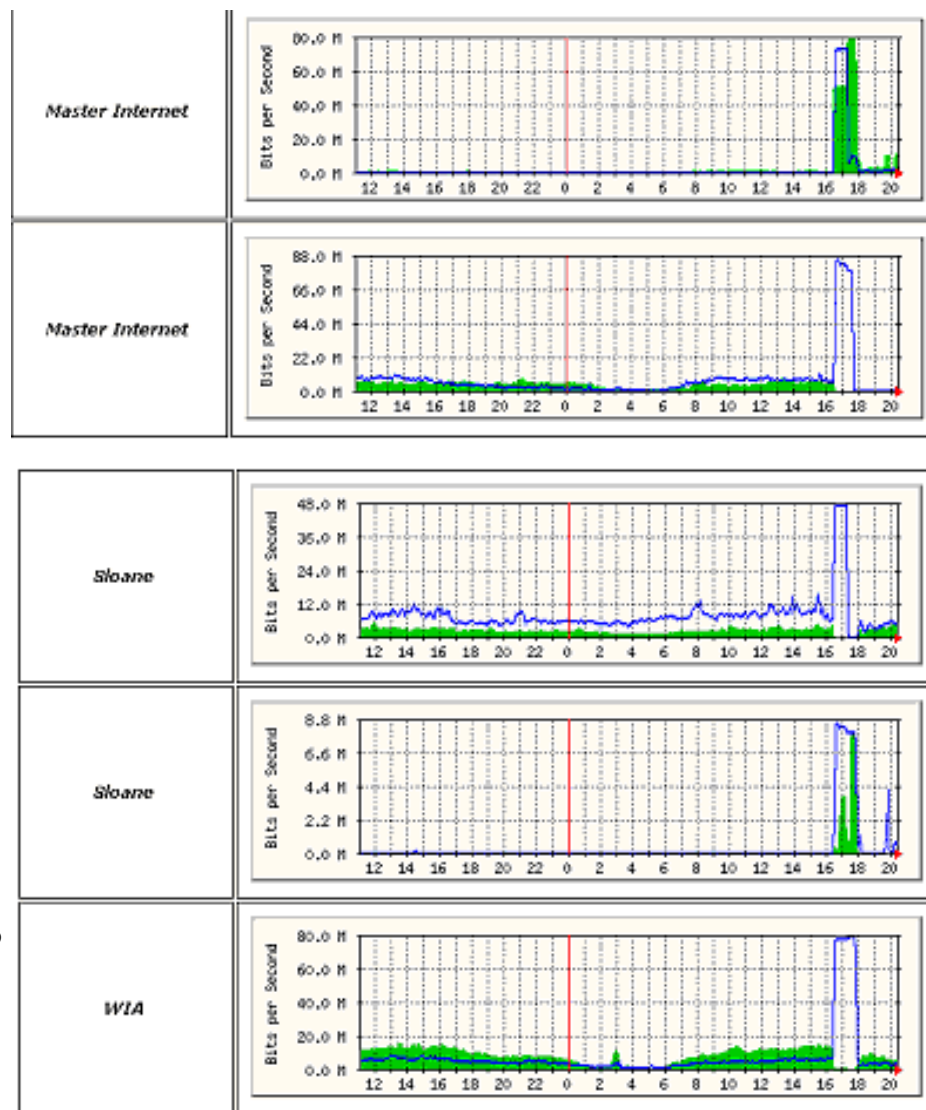
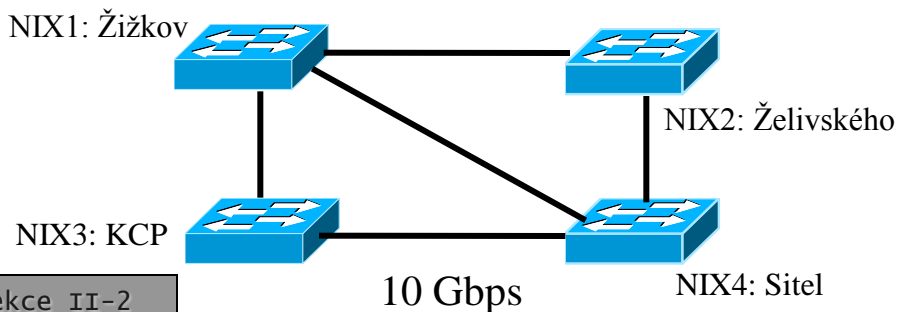
co je "broadcast storm"?

- je to stav, kdy si přepínače (event. mosty) nekontrolovaným způsobem vzájemně posílají rámce, které příjemce dále šíří do všech směrů (jako broadcast), a tyto rámce se nezastavují ale lavinovitě šíří dál a dál
 - ...
 - jde o řetězovou reakci
 - často eskaluje až do zahlcení dostupné kapacity
 - typické příčiny:
 - chyba jednoho či více zařízení
 - neošetřený cyklus na úrovni linkové vrstvy
 - obrana:
 - dokonalejší přepínače
 - umí řešit cykly,
 - menší "přepínané" celky
 - oddělení menších částí pomocí směrovačů



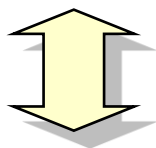
příklad z praxe

- NIX.CZ zažil broadcast storm 11.5.2004
 - důvodem byla (zřejmě) závada na jednom z přepínačů
 - významná část CZ Internetu byla na určitou dobu bez peeringu
 - občas se to stává i v jiných peeringových střediscích
 - 1x za ... let
- řešení peeringu v rámci NIX-u:
 - jedna "broadcast doména", vše propojeno jen pomocí přepínačů
 - tj. na úrovni linkové vrstvy
 - dnes:
 - celkem 4 lokality, přímé propojení na úrovni linkové vrstvy
 - v každé lokalitě jen přepínaný segment



důsledek

- celkový důsledek:
 - soustavy segmentů propojené pomocí mostů/přepínačů by neměly být příliš velké!
 - jinak se příliš projeví jejich záporné vlastnosti



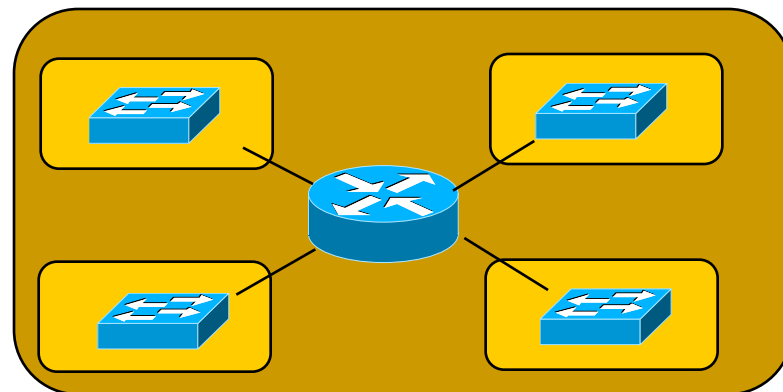
rozpor!

- pro dosažení co nejvyšší (vyhrazené) přenosové kapacity je tendence dělat soustavy propojené přepínači co největší



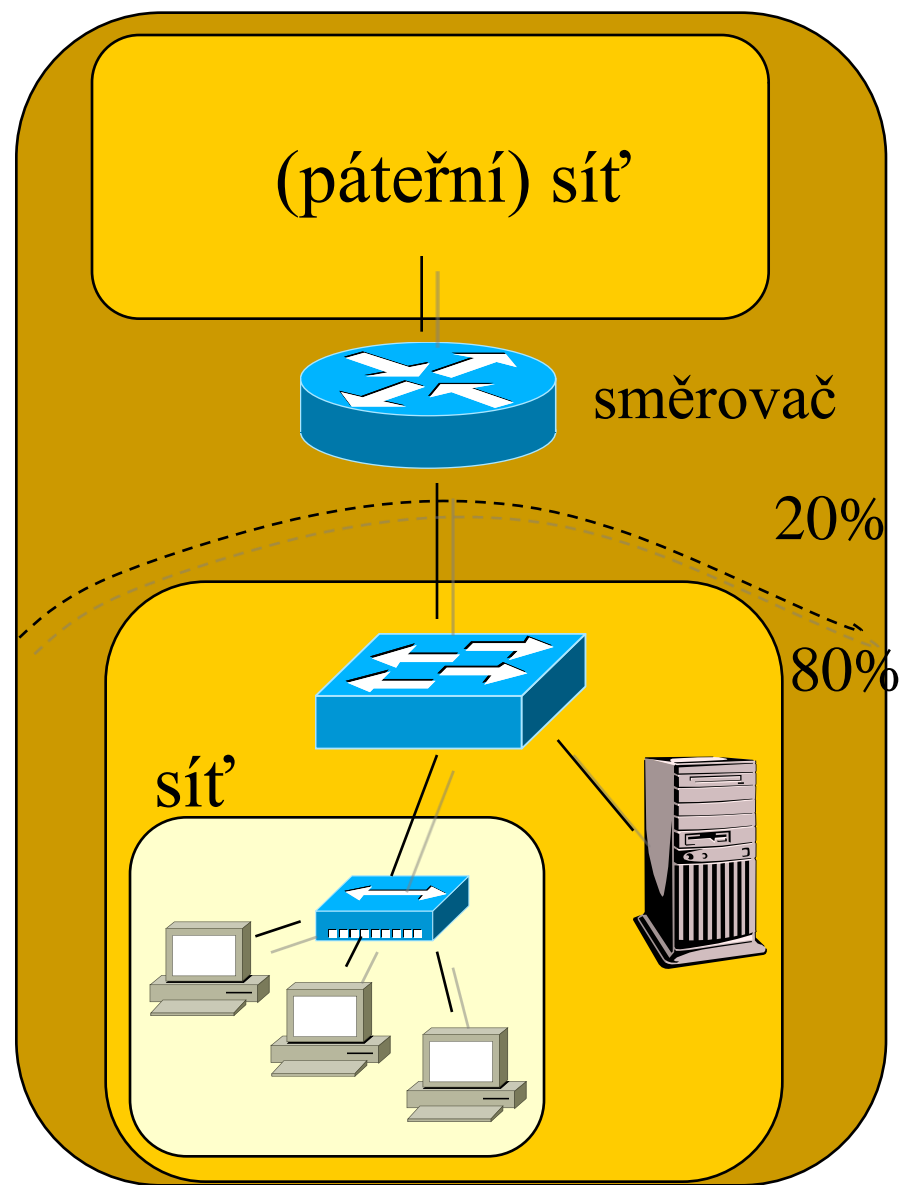
řešení: oddělit pomocí směrovačů

- obvyklé řešení:
 - přepínače se používají „uvnitř“ lokálních sítí, pro zvýšení jejich průchodnosti
 - ale velikost těchto sítí by neměla překračovat určité meze
 - kvůli broadcasting-u, adresám, přístupovým právům, managementu atd.
 - navzájem se tyto sítě propojují na úrovni síťové vrstvy, tj. pomocí směrovačů
 - nebo se prostřednictvím směrovačů připojují na páteřní síť

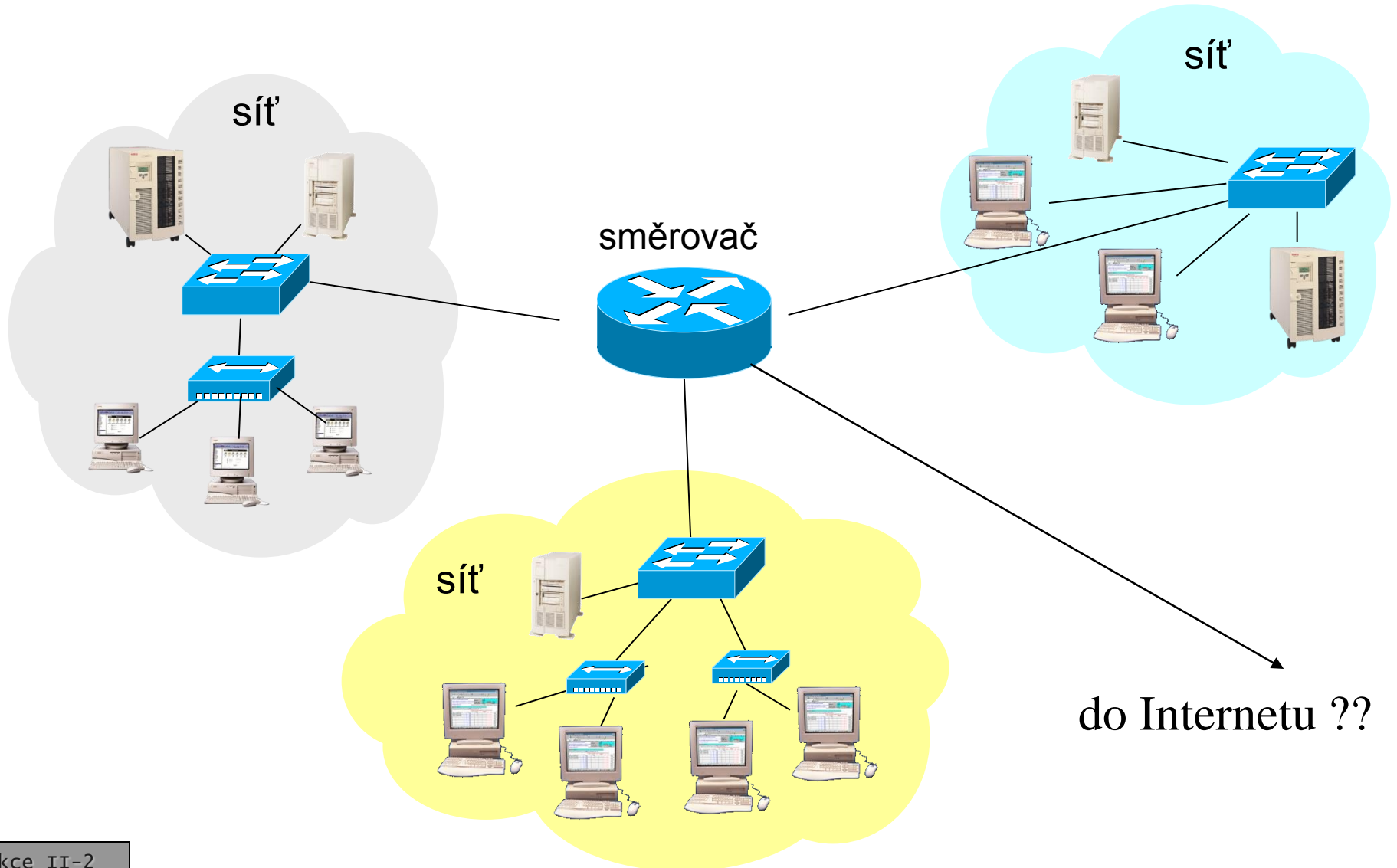


techniky pro zvýšení propustnosti: hierarchické členění

- snaha:
 - rozdělit celou soustavu segmentů na sítě (uvnitř propojené pomocí přepínačů), a ty propojit směrovači, tak aby:
 - maximum provozu bylo lokální
 - a využívalo vyhrazenou kapacitu poskytovanou přepínači
 - minimum provozu vedlo mimo danou síť a procházelo přes směrovač
- pozorování: **pravidlo 80:20**
 - v klasických sítích LAN má cca 80 procent provozu místní charakter
 - a může zůstat v dané síti
 - a cca 20 procent provozu je "vnější" a vede z dané sítě ven do jiné
- dnes již toto pravidlo mnohdy neplatí!!!
 - například kvůli používání vzdálených aplikací ("hostovaných" aplikací)
 - kvůli používání Internetu

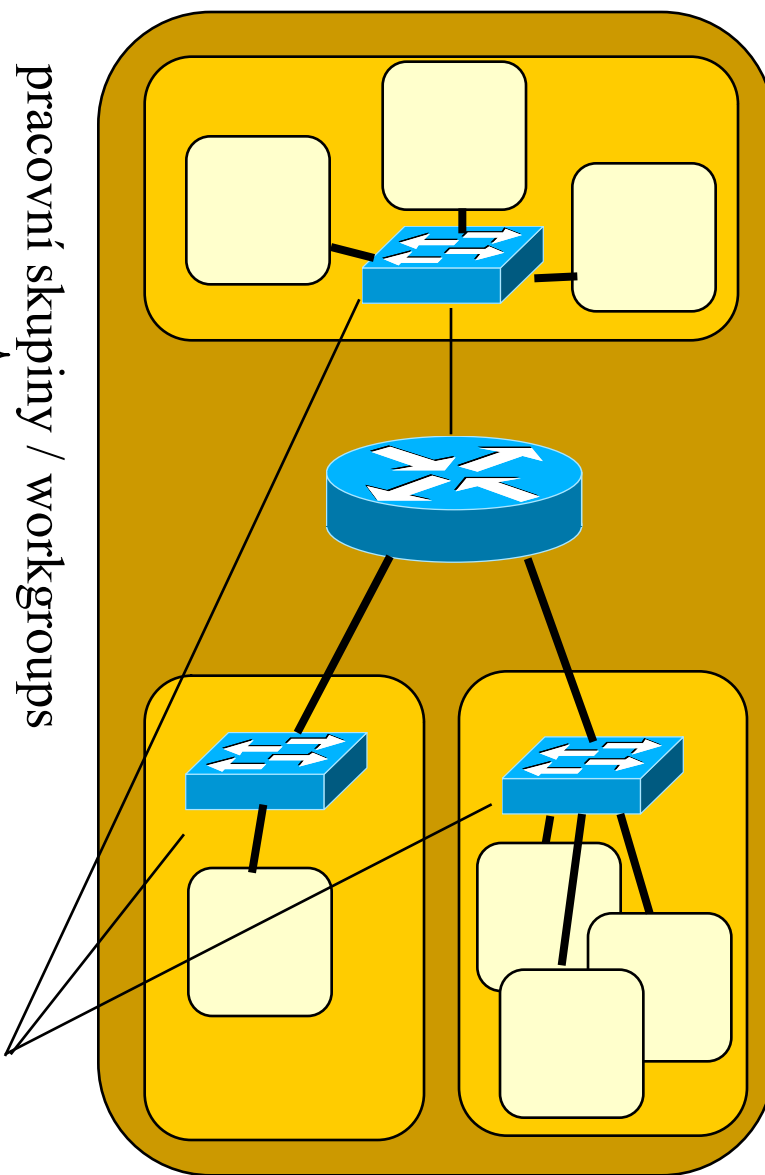


představa typického řešení



shrnutí („klasického“) řešení

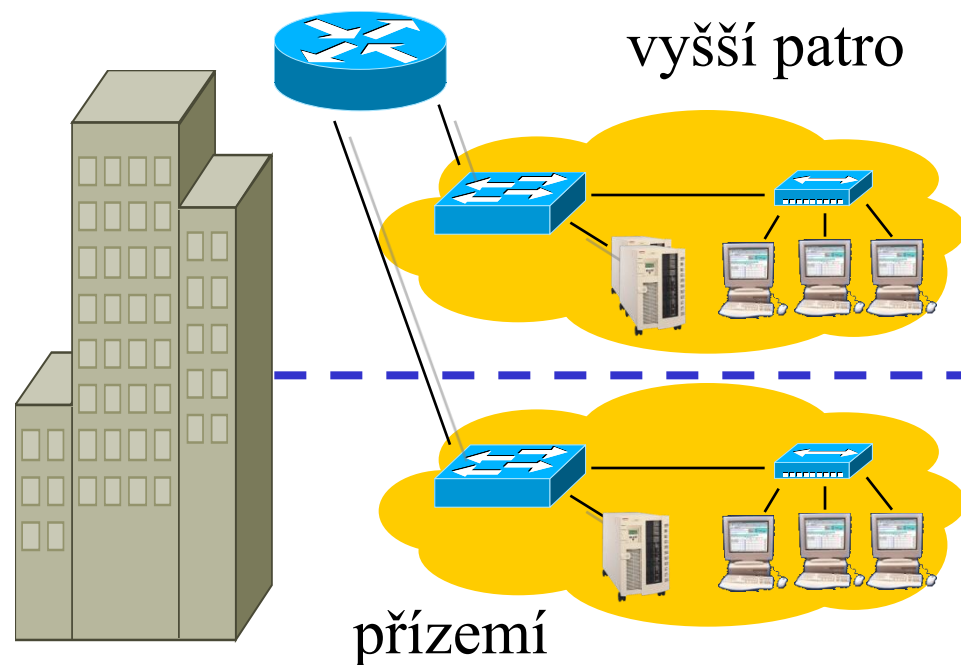
- celá soustava uzlů se rozdělí na takové celky, které jsou:
 - "vhodně velké"
 - neexistuje na to jednoznačný "must"
 - homogenní z hlediska přístupových práv
 - například pracovníci jednoho oddělení ve firmě apod.
 - komunikují co možná nejvíce mezi sebou
 - základem bylo pravidlo 80:20, dnes ale již (tolik) neplatí !!!!
- tyto celky se stanou samostatnými sítěmi
 - uvnitř jsou propojeny na úrovni linkové vrstvy
 - pomocí přepínačů a event. opakovačů (hub-y)
 - mezi sebou jsou propojeny na úrovni síťové vrstvy
 - pomocí směrovačů
 - platí i pro připojení "ven"



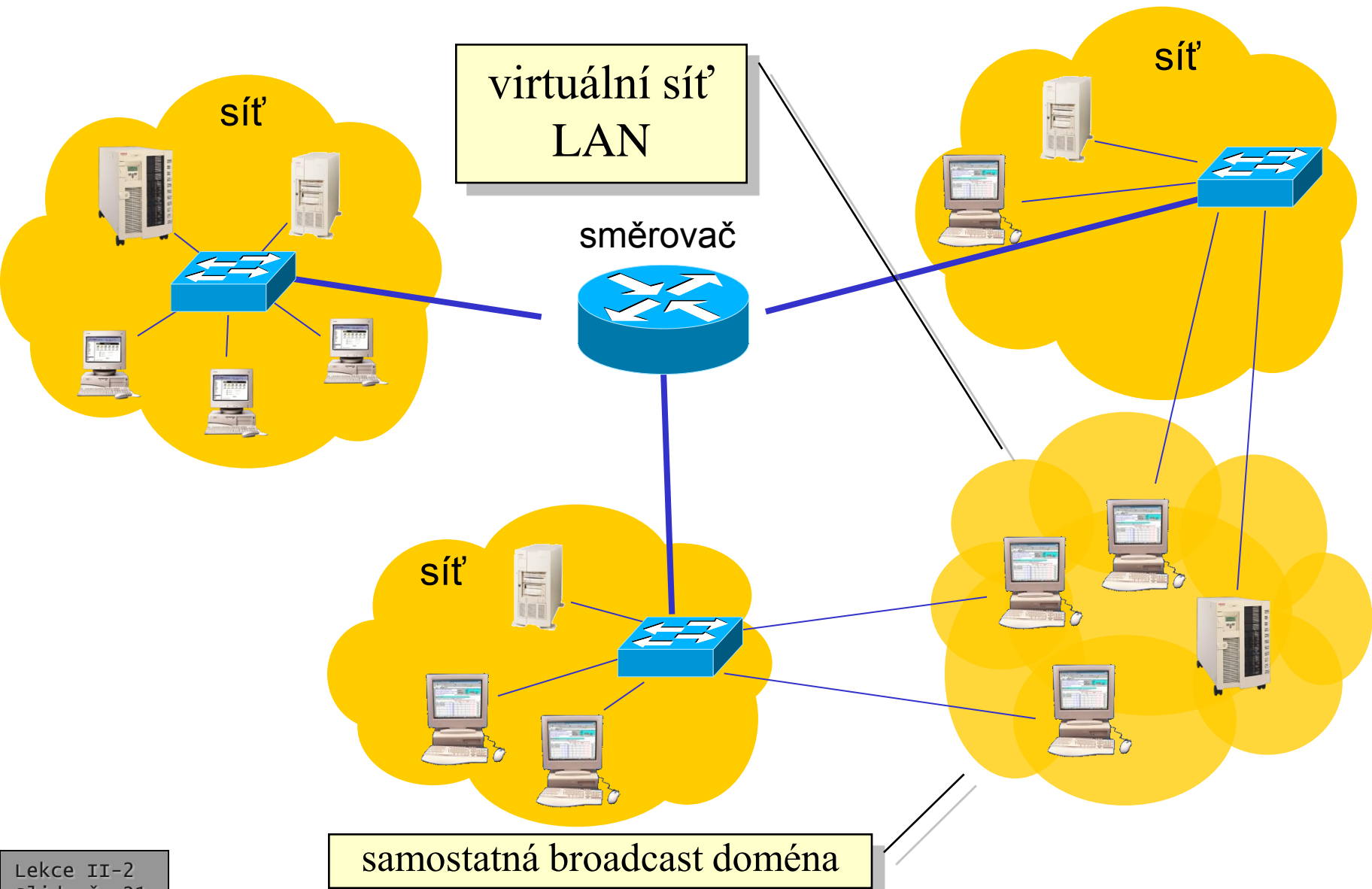
odbočení: virtuální sítě LAN

- jednotlivé sítě by měly odpovídat pracovním skupinám (workgroups)
 - které mají společné zájmy, chování (i data)
- ale:
 - rozdělení do jednotlivých sítí je také ovlivněno fyzickými dispozicemi
 - vzdáleností, umístěním
 - fyzické dispozice nemusí korespondovat s „logickými“
 - například s příslušností k určité skupině, která by měla mít stejná přístupová práva

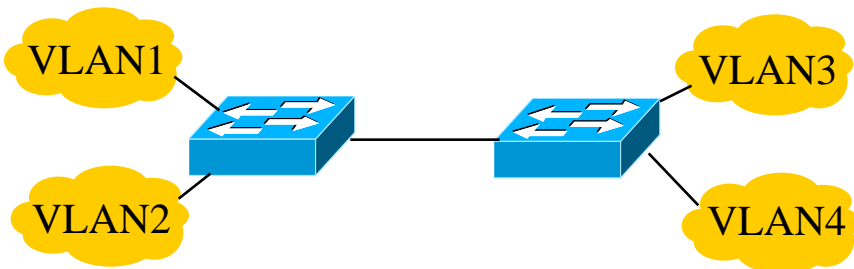
- Myšlenka virtuálních sítí LAN (VLAN):
 - udělat to tak, aby začlenění jednotlivých uzlů do konkrétních sítí mohlo být nezávislé na jejich fyzickém umístění



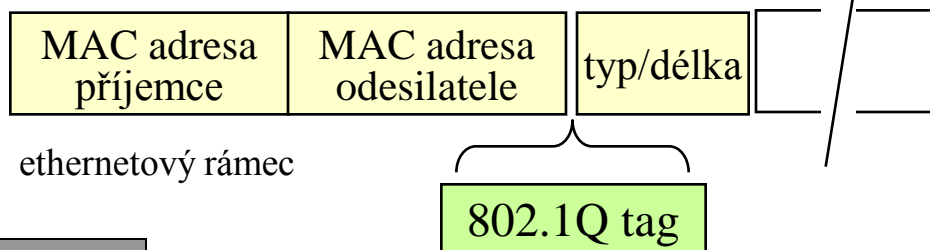
představa sítě VLAN



jak jsou sítě VLAN implementovány?

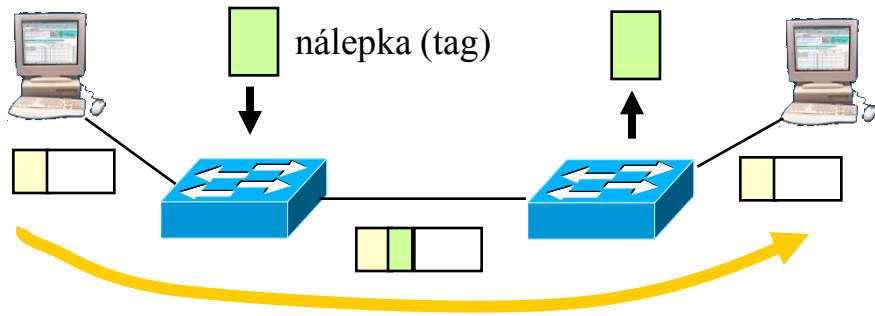


- sítě VLAN musí být "rozpoznávány" již na úrovni linkové vrstvy, v přepínačích !!
 - přepínač musí např. vědět, kam má přenášet broadcast a kam už nikoli
 - podle sítí VLAN
- jak přepínače rozpoznávají, pro kterou VLAN je určen konkrétní rámec?
 - "individuálně", podle linkové adresy nebo typu obsahu z L3
 - "podle nálepky"
 - tzv. tagging, linkový rámec je opatřen nálepkou určující VLAN

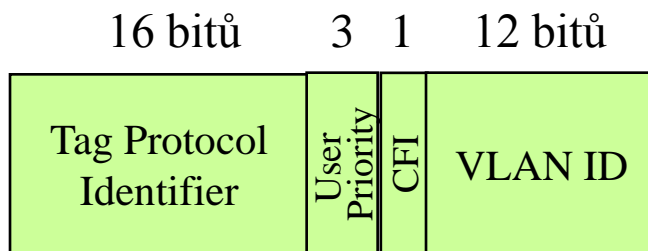


- standard IEEE 802.1Q definuje fungování sítí VLAN
 - preferuje nálepky (frame tagging)
 - každý rámec je ve své VLAN opatřen nálepkou
 - zpracování podle nálepky má přednost přes ostatním zpracováním
 - filtrování, forwarding, šíření broadcastu atd.
- možnosti implementace VLAN
 - "port VLAN"
 - příslušnost do konkrétní VLAN je dána portem na přepínači
 - všechny uzly, připojené k danému portu, jsou ve stejné VLAN
 - "static VLAN"
 - příslušnost do konkrétní VLAN je dána kombinací portu, linkové (MAC) adresy a síťového protokolu,
 - příslušnost do VLAN je na přepínačích pevně (staticky) nastavena
 - "dynamic VLAN"
 - příslušnost do VLAN je nezávislá na portu
 - je dána linkovou adresou a síťovým protokolem

jak jsou sítě VLAN implementovány?



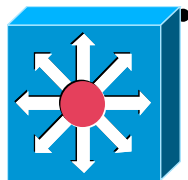
- většina síťových karet (NICs) nepodporuje VLAN ani nálepky
 - nálepky přidává a odebrává "první", resp. "poslední" přepínač na cestě mezi dvěma uzly
 - pro koncové uzly je existence VLAN neviditelná
- formát "nálepky" (tag-u):
 - Tag Protocol Identifier
 - 0x8100 pro Ethernet
 - VLAN ID: 4096 různých VLAN



- sítě VLAN mohou být "překlenuty" přes více přepínačů
 - uzly, spadající do stejné VLAN, mohou být fyzicky připojeni k různým sítím VLAN
- přepínače potřebují mít k dispozici mechanismy, kterými se budou vzájemně informovat o existenci VLAN, příslušnosti uzlů do VLAN atd.
 - definováno v IEEE 802.1P
 - GARP
 - Generic Attribute Registration Protocol
 - přenáší informace o příslušnosti k sítím
 - GVRP
 - GARP VLAN Registration Protocol
 - přenáší informace o existenci sítí VLAN

alternativa k VLAN: multilayer switching

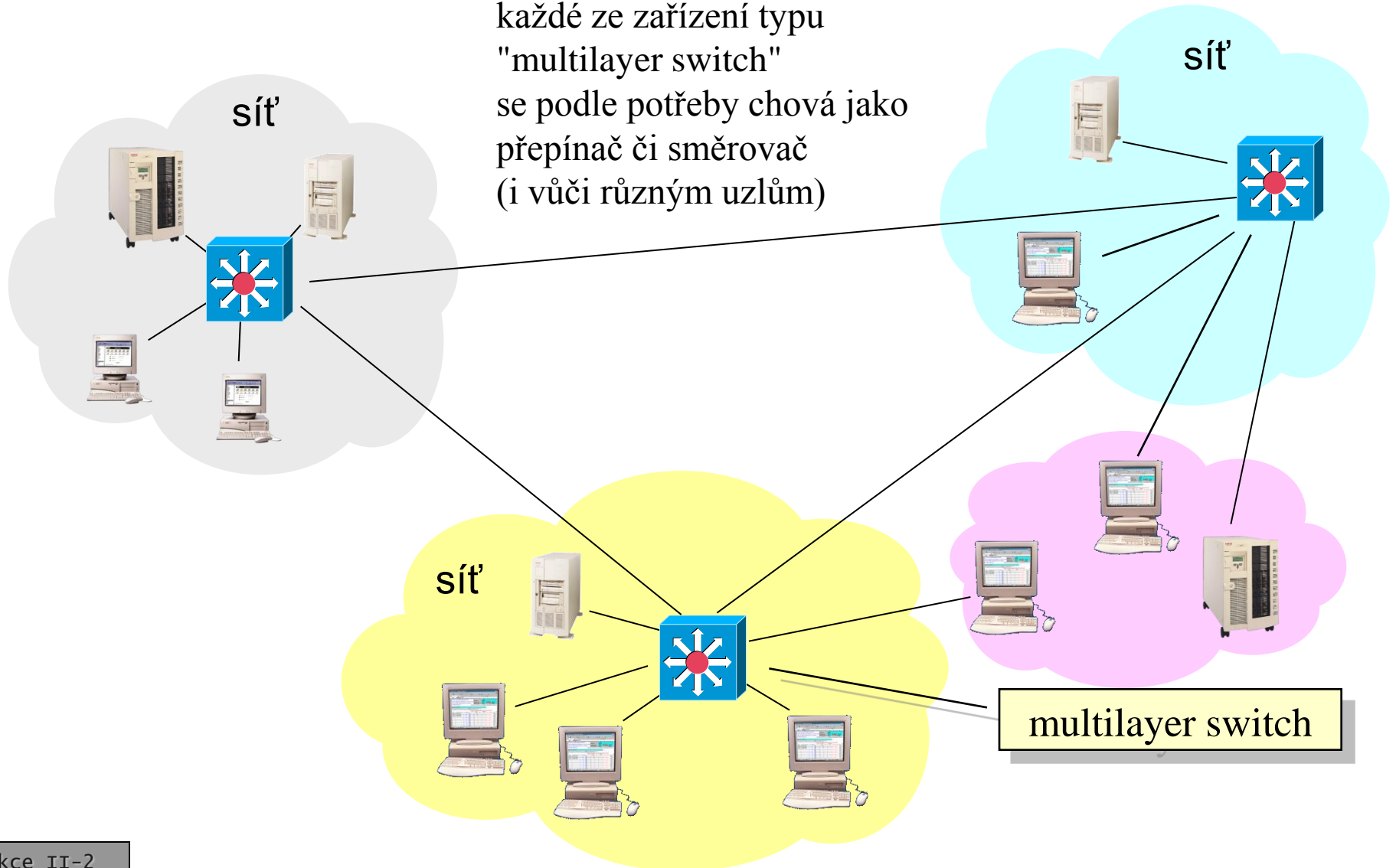
- v praxi je žádoucí, aby začlenění jednotlivých počítačů do konkrétních sítí bylo velmi pružné
 - aby bylo pouze logickou záležitostí, neovlivněnou fyzickými faktory
- virtuální sítě LAN tuto pružnost nabízí
 - ale jsou velmi drahé
 - možná i zbytečně univerzální
 - jsou řešením na úrovni linkové vrstvy
- existují i alternativní řešení, využívající
 - distribuované směrování
 - route servery



- základní myšlenka: použijí se zařízení, která v sobě kombinují funkci mostu/přepínače i směrovače
 - tzv. **multilayer switch**
 - jde vlastně jen o rozdíl v SW, zda umí přepojovat i na síťové vrstvě
- schopnost směrování (i přepínání) se tak dostává do všech propojovacích uzlů
- výhoda:
 - je větší volnost v rozdělování uzlů do jednotlivých sítí (ale ne úplná)
- nevýhoda:
 - velmi vzrůstají nároky na konfiguraci, správu a management směrovacích informací

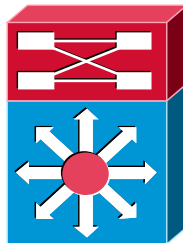
představa využití multilayer switch-ů

každé ze zařízení typu
"multilayer switch"
se podle potřeby chová jako
přepínač či směrovač
(i vůči různým uzlům)

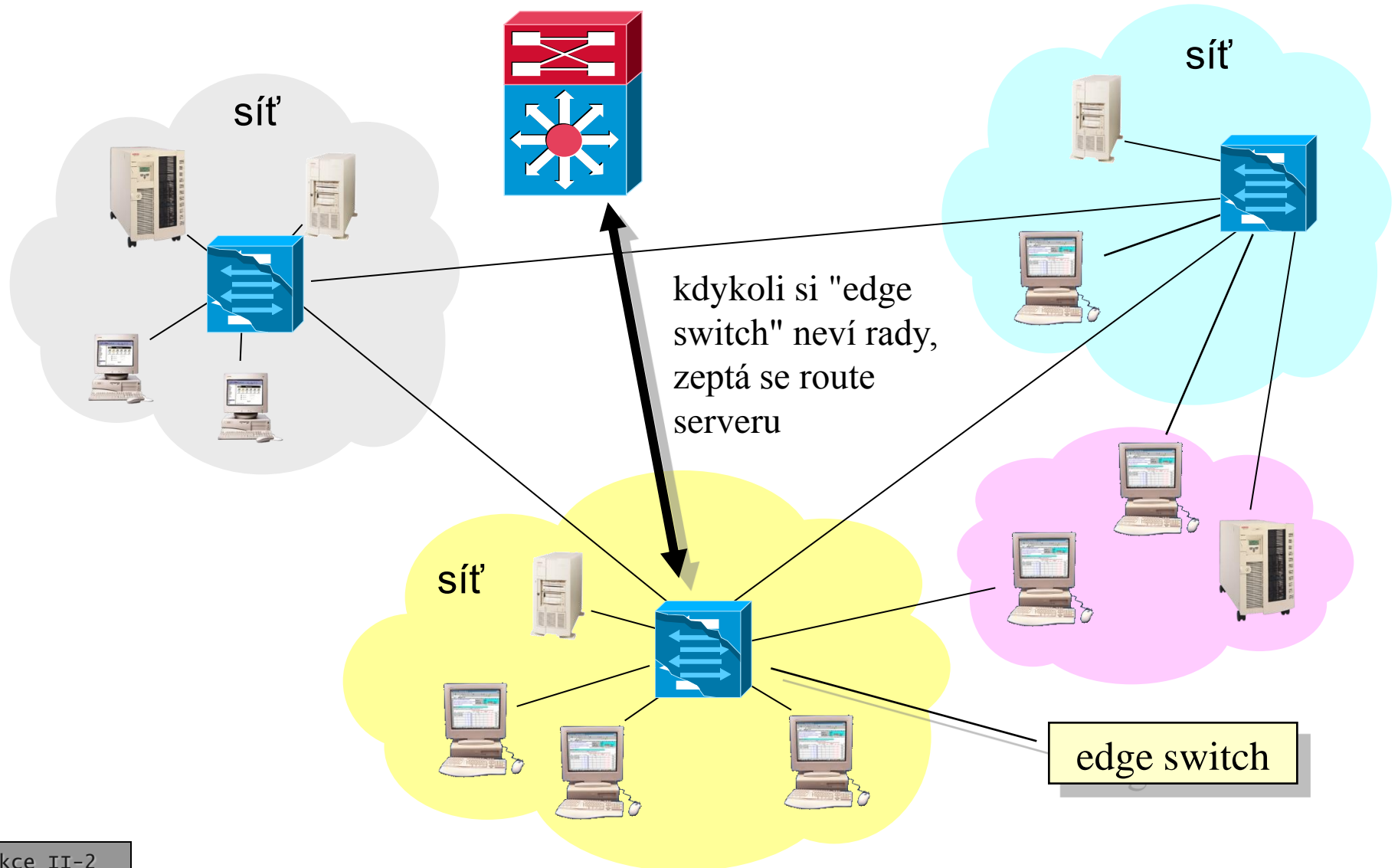


route servery

- hlavním problémem distribuovaného směrování je složitost
 - to, že se směrovací informace vyskytují na mnoha místech
 - navíc ve značně „rozmělněné“ podobě
- myšlenka route serverů:
 - soustředit směrovací informace do jednoho místa
 - kde se budou lépe spravovat
 - zde: včetně informací o rozdělení uzlů do jednotlivých VLAN
- bude existovat jeden centrální route server
 - disponující potřebnými informacemi pro rozhodnutí o směrování/přepínání
- v „okrajích“ sítě budou „okrajová zařízení“
 - tzv. edge switch
 - fakticky multilayer switch
 - když si neví rady, zeptá se centrálního route serveru co a jak mají udělat !!!!!

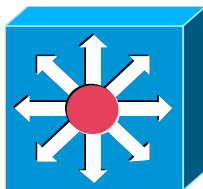


představa route serverů



Layer 3 Switching

- pravidlo 80:20 dnes již (tak úplně) neplatí
 - zejména kvůli internetovým službám, kvůli ASP službám
 - podstatně více provozu směřuje ven z dané sítě a prochází skrz směrovač
 - nelze již sestavovat sítě tak, aby většina provozu zůstala lokální
- důsledek: přes směrovače prochází podstatně více provozu
 - a na směrovače jsou tudíž kladeny zvýšené nároky na propustnost, latenci atd.
 - v zásadě stejné nároky jako na switche
- řešení: **Layer 3 Switch**
 - zařízení, které funguje jako klasický směrovač na 3. vrstvě
 - ale je optimalizováno na rychlost a dokáže fungovat srovnatelně rychle jako přepínač (switch)
- podstata L3 switchingu
 - základní logika fungování zůstává stejná jako u směrovačů
 - nebo je trochu zjednodušená
 - zařízení se rozhoduje podle síťových adres
 - rozhodování je kvůli rychlosti "zadrátováno"
 - realizováno v HW
 - i ostatní parametry jsou voleny s ohledem na rychlost a výkonnost



content switching

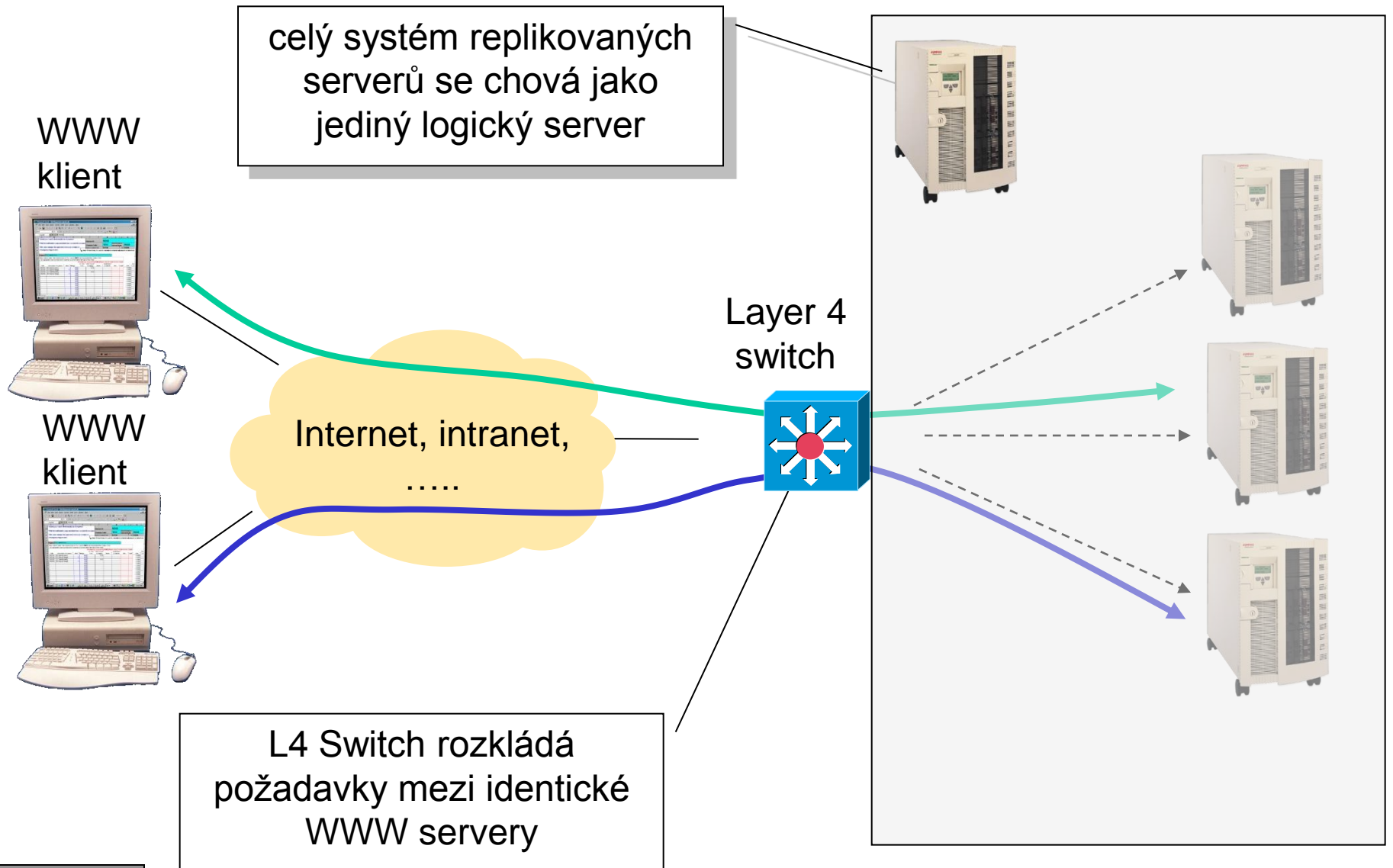
- směrování na základě informací dostupných na úrovni 3. vrstvy nemusí být postačující
 - například při snaze poskytnout různým službám různé zpracování
- příklad:
 - na zatížené lince se přenáší pošta a WWW stránky. Směrovač by chtěl dát přednost přenosu WWW stránek (pošta může počkat)
 - problém: směrovač nepozná, která data patří které službě
 - nepozná to z údajů na 3. vrstvě
- příklad:
 - existuje redundantní spojení, směrovač se snaží rozkládat provoz mezi alternativní cesty podle typu požadavku
 - např. přenosy zvuku a obrazu po jedné cestě, vše ostatní po jiné cestě
 - opět problém: klasický směrovač nepozná, o kterou službu se jedná

řešení: nechat směrovač, aby se podíval i na údaje patřící vyšším vrstvám

Layer 4 Switching

- možné řešení:
 - dát přepojovacímu uzlu schopnost pracovat s údaji které patří na 4. vrstvu
 - tj. rozpoznávat čísla portů
 - současně se řídí i informacemi z nižších vrstev – například síťovými adresami
 - takovýto propojovací uzel pak dokáže rozpoznat o jaký druh služby se jedná
 - WWW, el. pošta, přenos souborů atd.
- takovýto přepojovací uzel bývá optimalizován na rychlost
 - proto se o něm hovoří jako o "Layer 4 Switch"
- další možné využití L4 Switche: Load Balancing
 - podle charakteru požadavku jej směruje různým způsobem, například na jeden ze vzájemně alternativních serverů které nabízí stejnou službu
 - a sám mezi nimi vybírá například na základě jejich vytížení

představa load balancingu



Layer 7 Switching

- Layer 4 Switching nemusí být postačující pro korektní Load Balancing
 - ani pro další účely
- například Load Balancing pro WWW by měl respektovat průběh relace mezi klientem a serverem
 - např. HTTP 1.1 relace
 - SSL relace
 -
- podobně při snaze distribuovat obsah mezi různé servery
 - je třeba podrobněji rozumět požadavku, který má být někam nasměrován
- řešení: Layer 7 Switching
 - přepojovací uzel bude moci vycházet i z informací dostupných na aplikační vrstvě a podle nich volit svá rozhodnutí
 - bude rozumět aplikacím a jejich datům – například požadavkům na WWW
- umožňuje to například realizovat farmy WWW serverů, různé clustery, řešení pro distribuci obsahu
 - CDN, Content Distribution Network

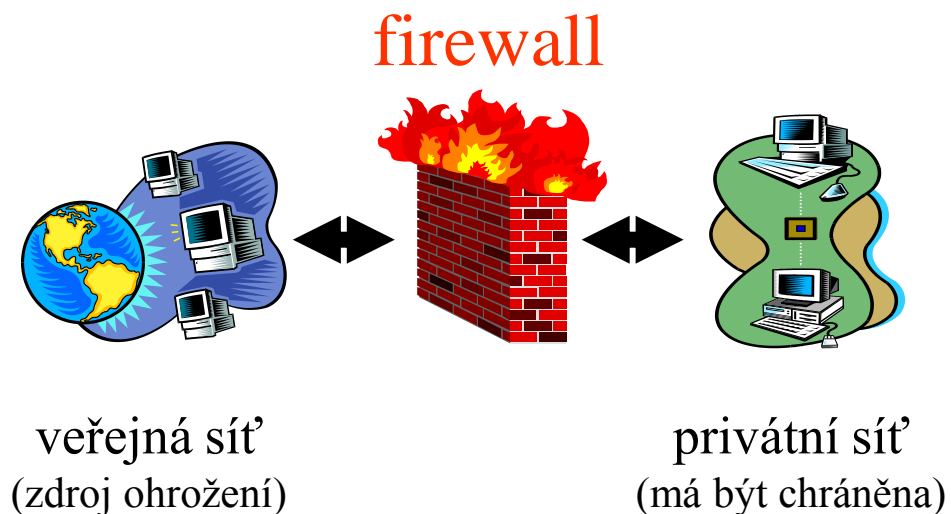
další otázky internetworking-u

- vzájemné propojování sítí se týká také
 - zajištění bezpečnosti
 - tzv. firewally, demilitarizované zony
 - jde o celou rozsáhlou problematiku bezpečnosti, zde se omezíme jen aspekty související s oblastí internetworking-u
 - zajištění prostupnosti
 - aplikační (proxy) brány
 - zajištění efektivnosti
 - cachující servery



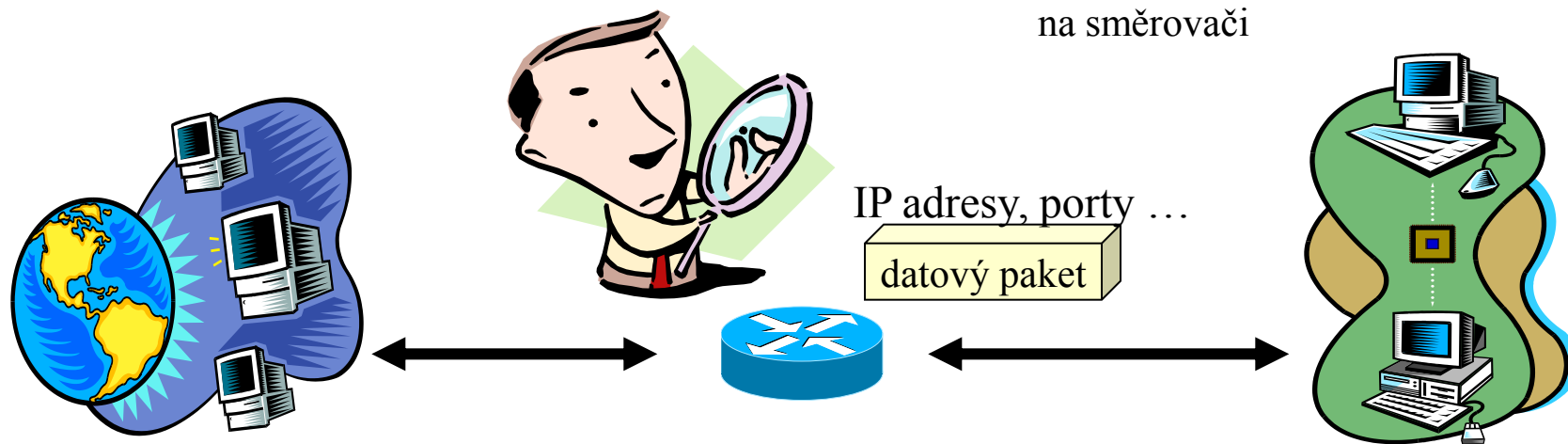
firewall

- jde o obecné označení řešení, které sleduje zajištění bezpečnosti
- firewall může být realizován různými způsoby, např.
 - pouze organizačními opatřeními
 - jen v SW
 - vhodným nakonfigurováním směrovačů
 - kombinací SW a HW
 - nejčastěji
- každý firewall obecně má:
 - část zajišťující blokování
 - zabraňující v přístupu
 - část zajišťující prostupnost toho, co má být povoleno



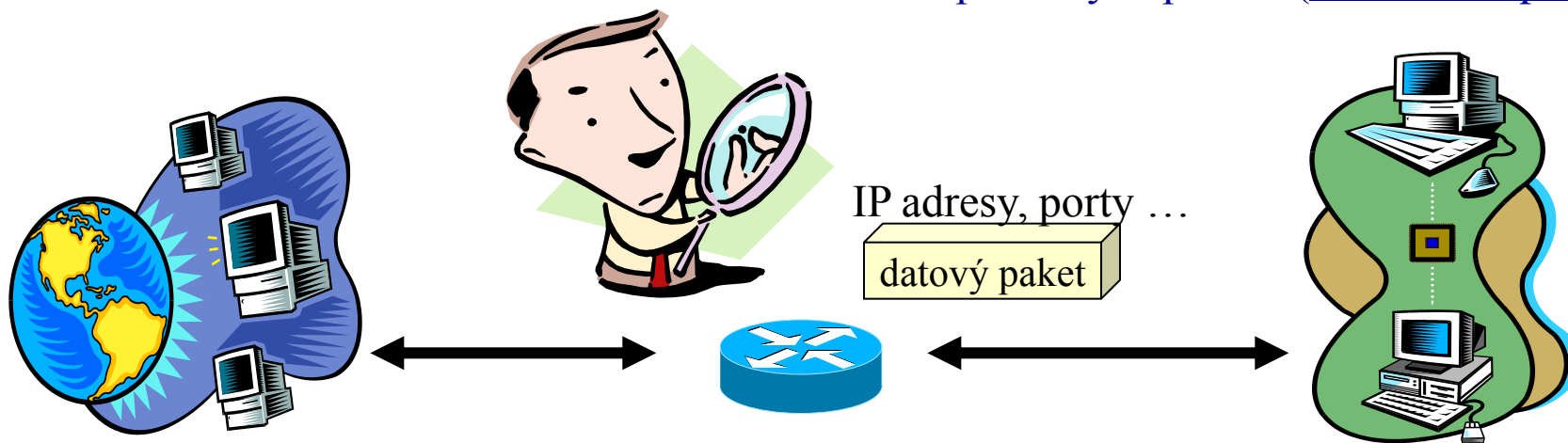
možnosti blokování

- lze realizovat například nakonfigurováním směrovačů
 - tak aby nepropouštěly určitý druh provozu, resp. nepropouštěly nic kromě explicitně povoleného provozu
 - problém: ne všechny běžné směrovače dávají takové možnosti, aby bylo možné nakonfigurovat vše co je třeba
- existují specializované produkty, tzv. **paketové filtry**
 - které mají výrazně posíleny nejrůznější „povolovací“ a „blokující“ možnosti, v závislosti na mnoha různých faktorech
 - mohou to být řešení na bázi vlastního HW a SW
 - nebo i řešení čistě SW
 - běžící na normálním počítači nebo i na směrovači

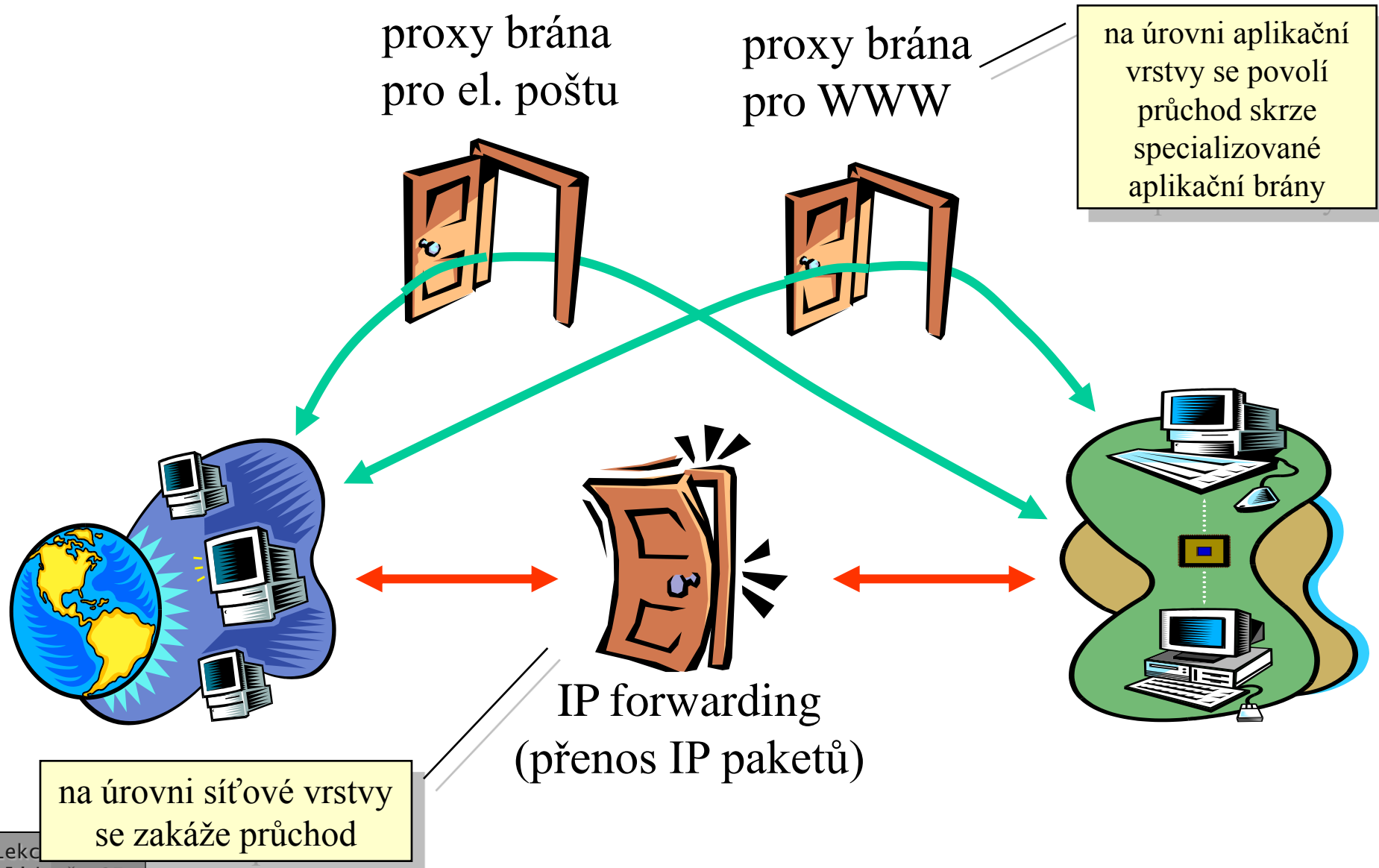


paketové filtry

- Výhody:
 - relativně laciné a snadné řešení
- Nevýhody:
 - fungují na úrovni síťové vrstvy, eventuálně i transportní
 - nefungují na úrovni aplikační vrstvy
 - musí se rozhodovat na základě síťových adres a čísel portů
 - jejich možnosti rozpoznání útoku jsou omezené
 - kvůli tomu že "nevidí" až na aplikační úroveň
- paketové filtry mohou být "statefull" nebo "state-less"
 - podle toho zda každý paket posuzují bez uvážení historie (state-less inspection) nebo s uvážením historie a předešlých paketů (statefull inspection)



princip řešení na aplikační úrovni



možné řešení na aplikační vrstvě

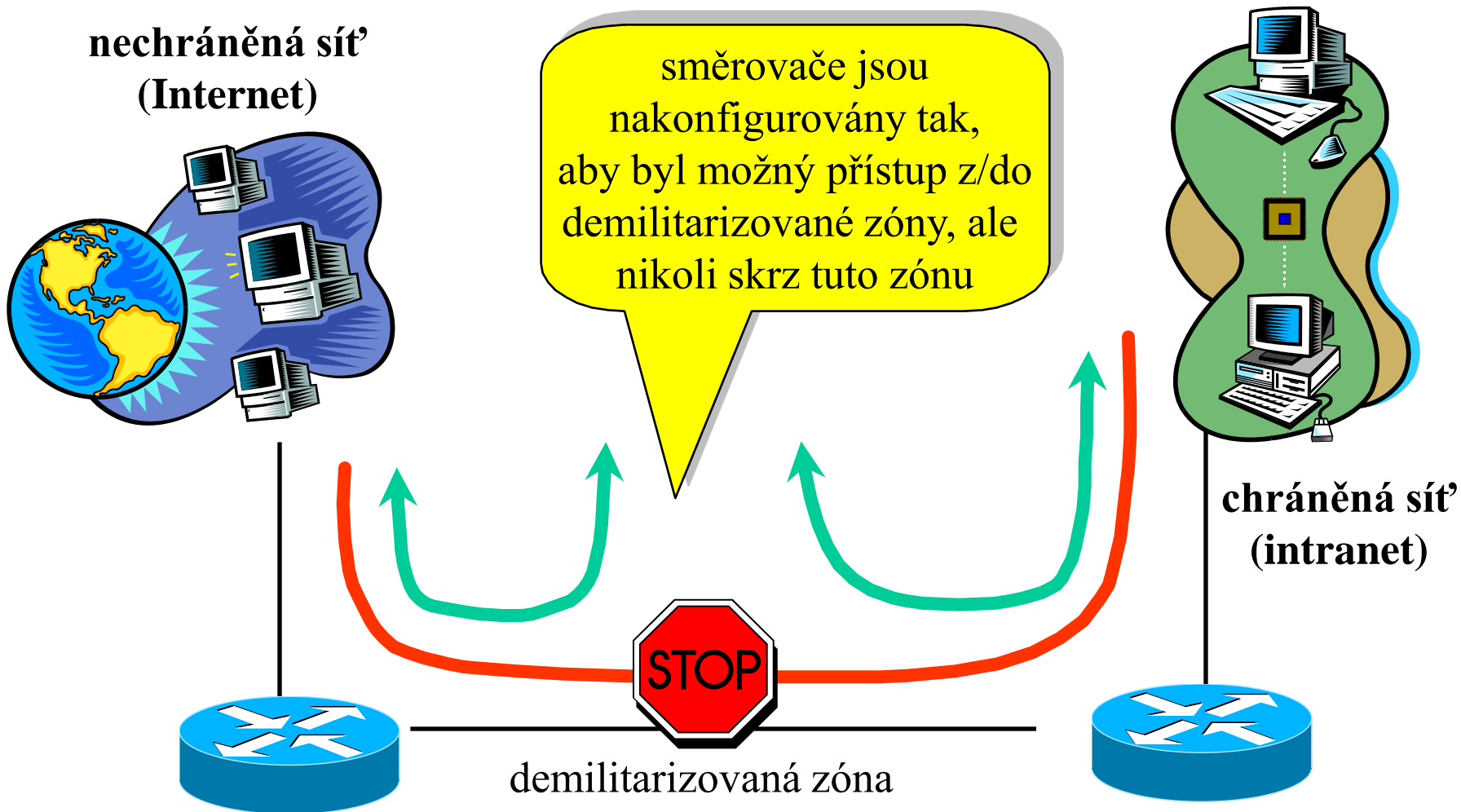
- vše může být implementováno čistě softwarovými prostředky
 - zákaz IP forwardingu (dual-homed host nefunguje jako směrovač)
 - aplikační (proxy) brány běží na daném uzlu jako aplikace
 - dnes již součástí některých operačních systémů, např. MS Windows
- relativně laciné řešení
 - ve formě "kompaktních" aplikací, např. WINROUTE



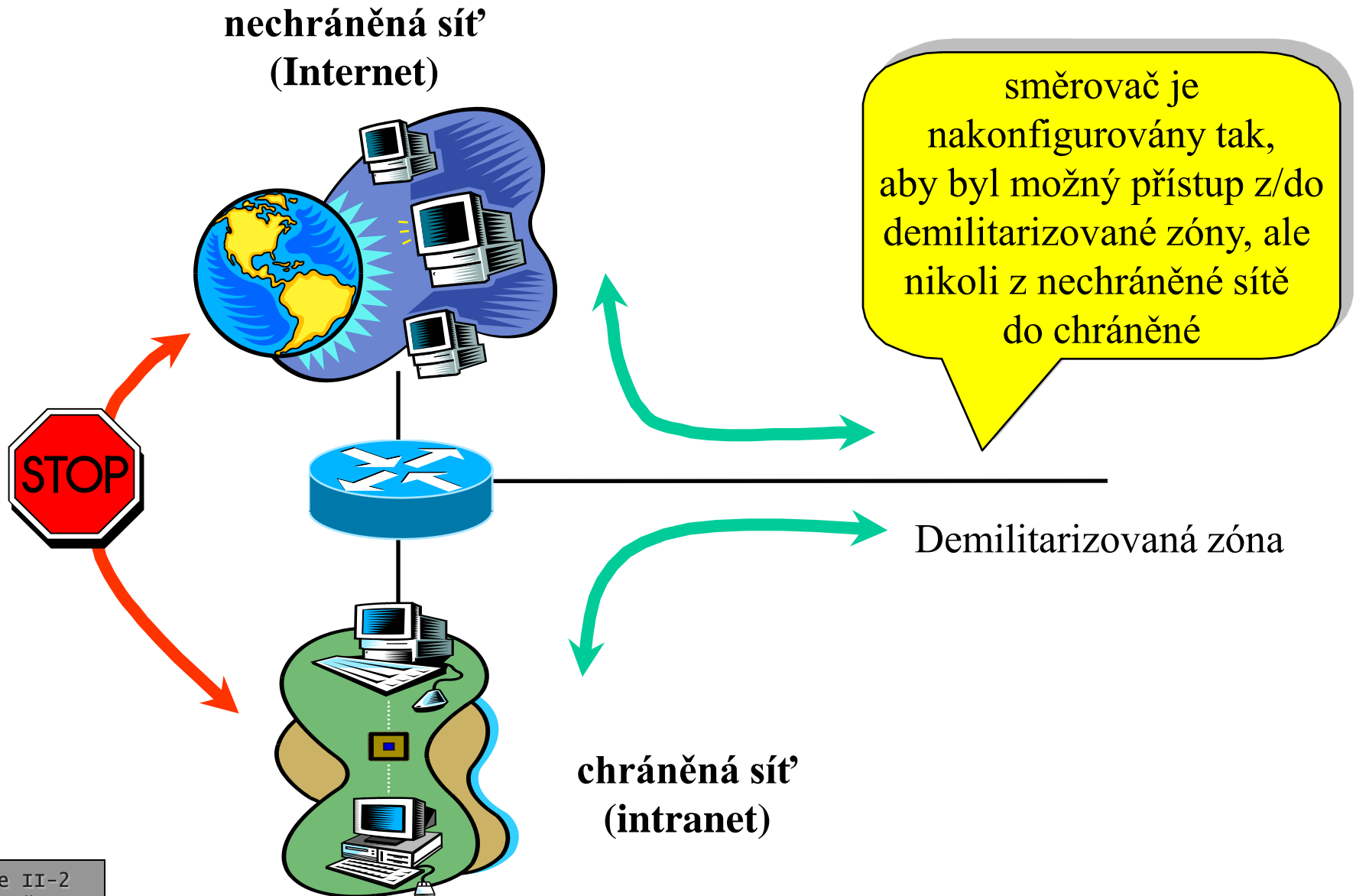
počítač v roli firewallu



řešení s tzv. demilitarizovanou zónou (se 2 směrovači)

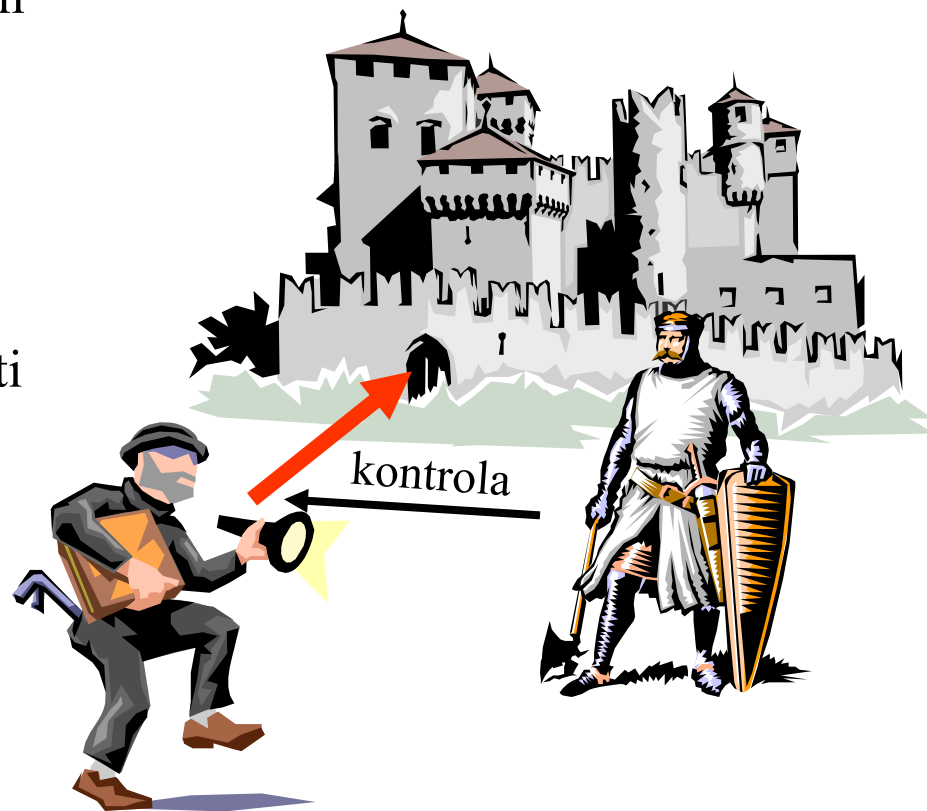


řešení s tzv. demilitarizovanou zónou (s 1 směrovačem)

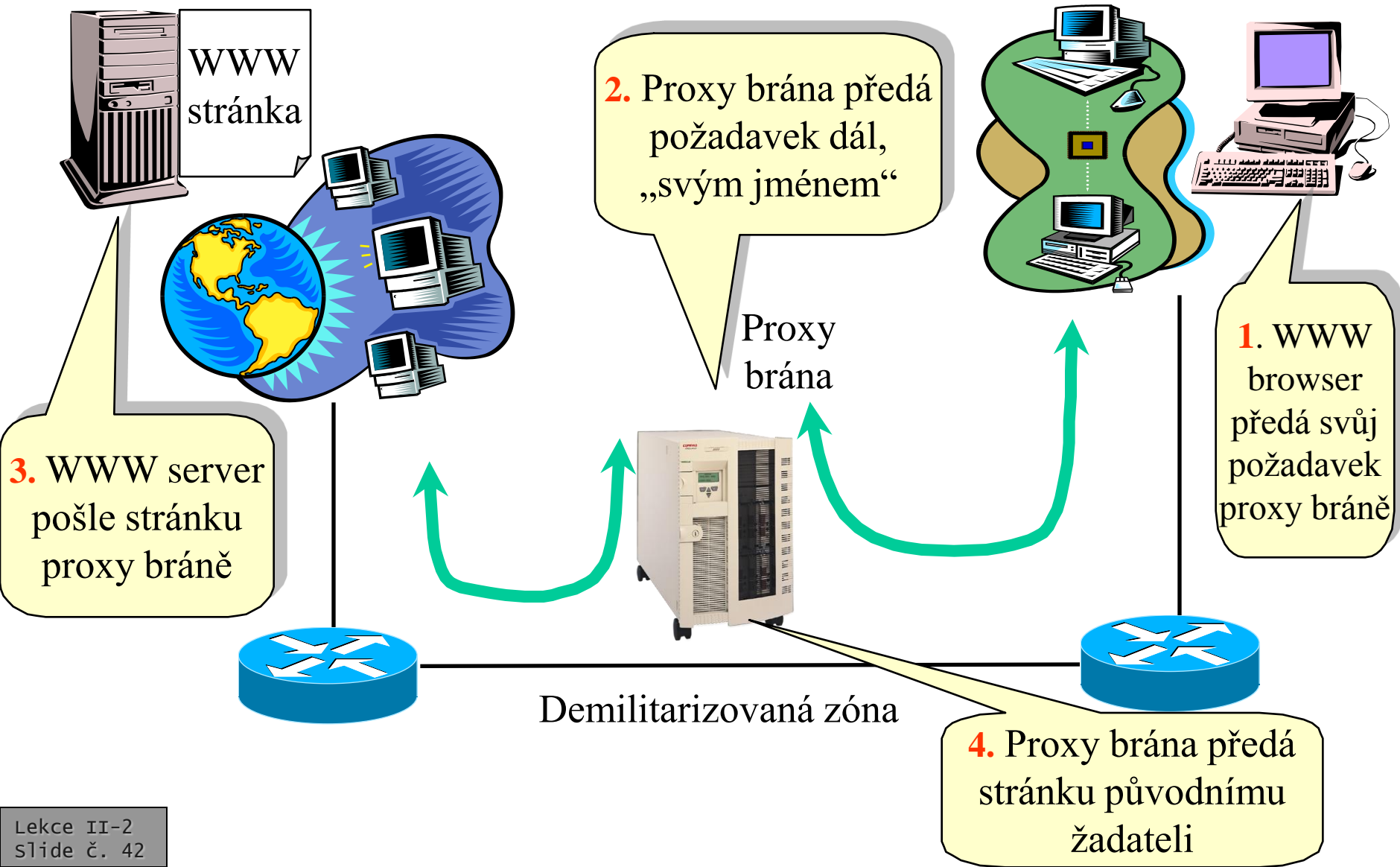


využití demilitarizované zóny

- veškerý provoz skrz DMZ je zablokován
 - idea: do DMZ se umístí „přestupní stanice“, přes které půjde veškerý provoz který má být povolen
 - a přestupní stanice jej dokáže účinně kontrolovat
- „přestupní stanice“ budou ve skutečnosti aplikační brány
 - specializované na určitý druh provozu, který dokáže dobře kontrolovat, například poštu, WWW apod.
 - jsou to tzv. proxy brány
- jde o stejný princip, jaký byl využíván již u středověkých hradů
 - vodní příkop měl bránit tomu, aby se do hradu dostal někdo jinou cestou než hlavní branou
 - u hlavní brány stál hlídač a ten každého zkontroloval



fungování WWW proxy brány



využití demilitarizované zóny

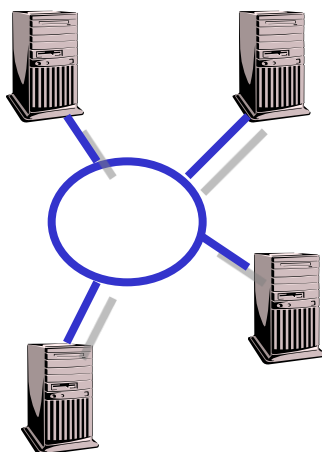
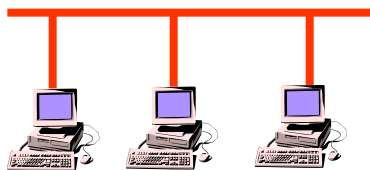
- demilitarizovaná zóna je “vidět” z obou stran, ale není “průhledná skrz”
 - z nechráněné sítě (Internetu) jsou “vidět” pouze uzly přímo v DMZ
 - celá chráněná síť za DMZ je z vnějšku neviditelná
 - může dokonce používat adresy, které by “venku” byly nepřipustné
 - do DMZ se umístí takové servery, které mají být „vidět“
 - WWW, FTP server
 - (přestupní) poštovní server, DNS, ...
 - ostatní (chráněné) servery mohou být „schovány“ v chráněné síti
 - např. (skutečný) poštovní server
- na stejném principu jako WWW proxy brána mohou fungovat i brány pro Gopher a FTP
 - pro některé jiné služby je to problém
 - např. Telnet, IRC
- do DMZ se umísťuje také poštovní server
 - který funguje pouze jako přestupní stanice
 - faktický (hlavní) poštovní server je v chráněné síti
 - kde není zvenku viditelný
- a server DNS
 - který ale „zná“ jen uzly v DMZ, nikoli uzly uvnitř chráněné sítě

propojování různých síťových segmentů

- otázka:

- je možné propojit mezi sebou takové segmenty (sítě), které používají různé přenosové technologie na úrovni linkové vrstvy?

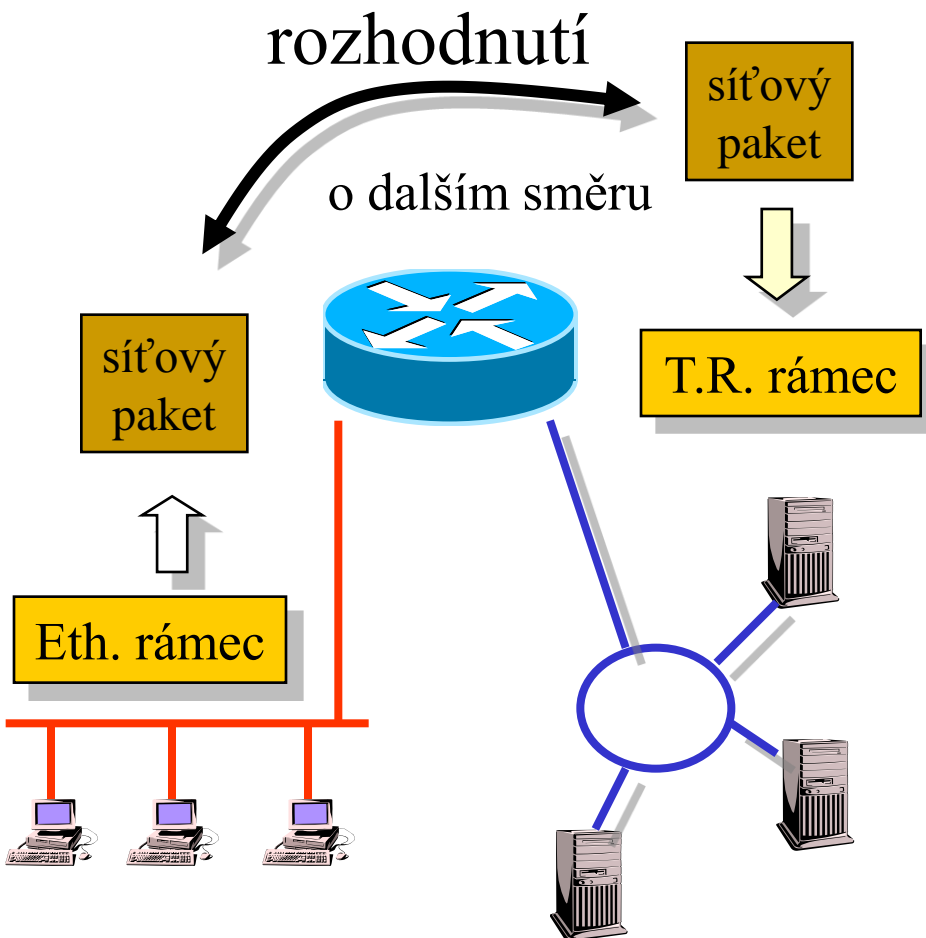
- např. Ethernet, Token Ring, FDDI, ATM,



- odpověď:

- pomocí opakovačů:
 - nelze
 - např. kvůli různým přenosovým rychlostem (ale i kvůli dalším odlišnostem)
- pomocí mostů/přepínačů:
 - někdy ano, někdy ne
 - je to komplikované
- pomocí směrovačů:
 - ano,
 - jde o standardní řešení

propojení různých segmentů pomocí směrovačů



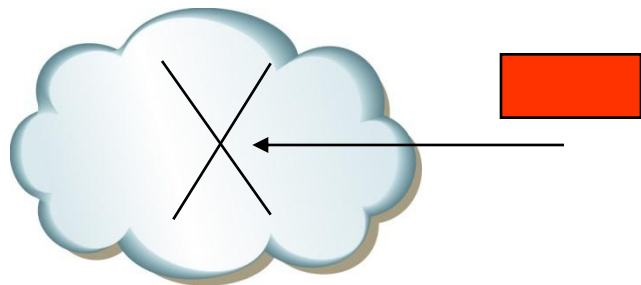
- při propojení různých segmentů na úrovni síťové vrstvy nevznikají "kvalitativní" problémy
 - síťový paket je vybalen z jednoho typu linkového rámce a vložen do jiného typu linkového rámce
 - mohou ale vznikat problémy "kvantitativní"
 - např. tzv. fragmentace
 - když se paket nevejde do max. velkého linkového rámce a musí být sám rozdělen
 - ale na to síťové protokoly pamatují
 - protokol IP je na to připraven a dokáže fragmentaci řešit

problémy při propojování různých segmentů pomocí mostů/přepínačů

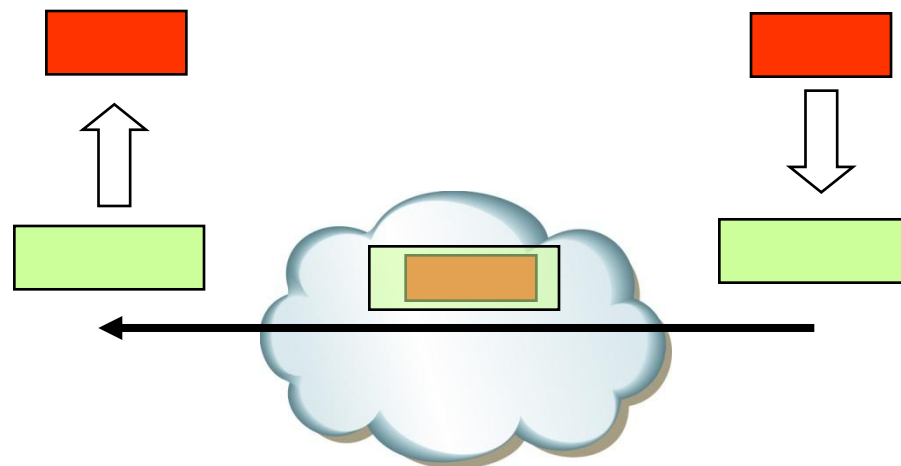
- příklad: Ethernet a Token Ring
 - problémy jsou:
 - v rozdílné povaze informací o topologii
 - Ethernetový most chce znát adresy sousedních uzlů, Token Ring-ový most chce znát cesty v síti
 - v různém způsobu vyjádření stejných informací
 - status rámce, adresy a zabezpečení jsou vyjádřeny jinak
 - v neexistenci ekvivalentů
 - např. v Token Ring-u mohou mít některé rámce vyšší prioritu, v Ethernetu neexistuje analogie
 - v rozdílné max. velikosti rámců
 - Ethernet připouští max. 1500 bytů, Token Ring 4000 až 17800 bytů
 -
- možné řešení:
- **„překlad“**
 - angl: translation
 - data obsažená v rámci jednoho typu se „přeloží“ do jiného tvaru (odpovídajícího jinému typu rámce)
 - ne vždy je to možné, např. kvůli velikosti
 - může se tím něco ztratit (např. priorita)
 - musí se přijmout některá omezení
 - například při propojení Ethernet-Token Ring se Token Ringu omezí velikost rámce na maximum z Ethernetu
 - nejsou k dispozici mechanismy pro řešení fragmentace
 - **„zapouzdření“, "tunelování"**
 - angl: encapsulation, tunnelling
 - rámec jednoho typu se vloží (jako data) do rámce jiného typu, přenesení, a opětně „vybalí“
 - lze použít jen pro „průchozí“ konfigurace
 - může to být neefektivní

zapouzdřování (encapsulation)

- jde o obecně použitelnou techniku, lze ji aplikovat na různých úrovních
 - lze vkládat rámce do rámců, rámce do paketů, pakety do paketů ...
 - dokonce i buňky do rámců (cells over frames)
- umožňuje řešit situace, kdy určitá část sítě není průchodná pro určitý druh provozu



síť není průchozí pro určitý druh paketů/rámců

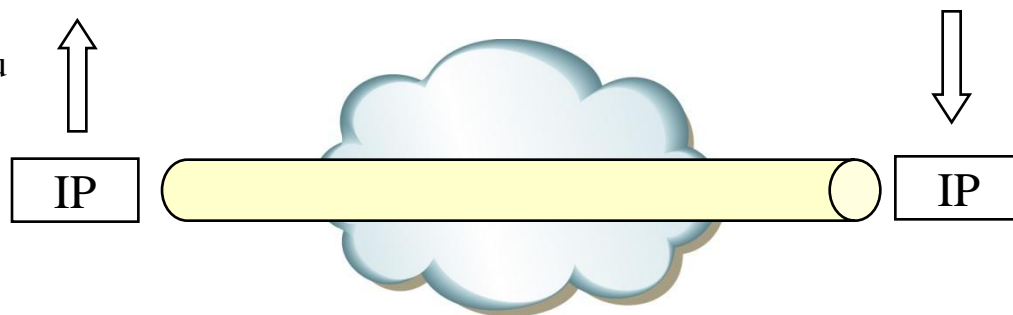


rámce/pakety, které samy sítí neprojdou, jsou vloženy (zapouzdřeny) do takových rámců/paketů, pro které je síť průchozí

příklad (využití techniky zapouzdřování)

- existují takové protokoly (soustavy protokolů, technologie), které nelze směrovat
 - proto, že neobsahují síťovou vrstvu, resp. nepočítají s její existencí, nemají síťové adresy, neznají pojem sítě
 - jejich autoři zřejmě nepočítali s možností internetworking-u
 - s tím, že by docházelo k propojování dílčích segmentů - vidí svět jako jednu „velkou a plochou“ síť
- jde o protokoly
 - LAT (firmy DEC)
 - už se skoro nepoužívá
 - NetBIOS
 - stále hojně používané, jsou „nativním“ síťovým řešením
- tyto protokoly nemohou „projít“ přes směrovač
 - ani multiprotokolový
 - protože ten neví jak s nimi naložit

- řešení:
 - zapouzdření nesměrovatelných protokolů do jiných (směrovatelných) protokolů
 - nejčastěji:
 - do IP paketů (IP tunelování, IP tunel)



jiné řešení:

brouter (bridging router) je kombinace směrovače a mostu

- když ví jak, chová se jako směrovač a směruje
- když neví jak (resp. když to nejde), chová se jako most