Směrovací protokoly v datových sítích



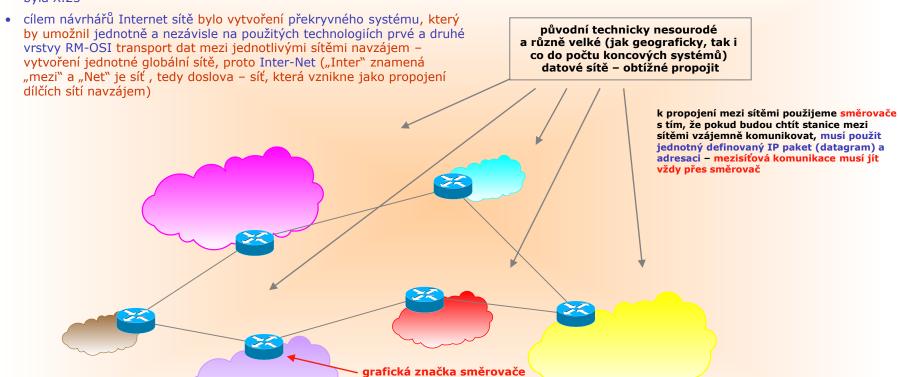
Co je směrování

- směrování je proces, který řeší nalezení optimální cesty v síti od zdrojové stanice k cílové
- proces směrování používá k výše uvedenému nalezení optimální cesty typicky informace obsažené v cílové síťové adrese koncové stanice
- směrovací proces patří do třetí vrstvy RM-OSI modelu
- směrovací proces v rozlehlých datových sítích s výhodou využívá hierarchické adresace koncových stanic
- hierarchická adresa v sobě integruje jak identifikátor sítě, do níž daná koncová stanice patří, tak i vlastní identifikátor koncové stanice v rámci uvažované sítě
- zařízení, které je zodpovědné za realizaci směrování v datové síti se nazývá směrovač (ROUTER)



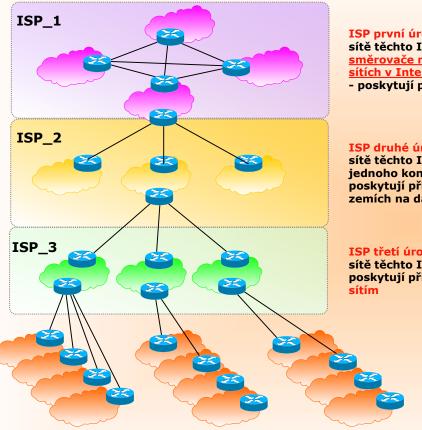
Koncept přenosu dat v Internetu

 v době vzniku Internetu se již rozvíjely a implementovaly různé technologie lokálních sítí, ale postupně i veřejných datových sítí jako byla X.25





Ideální topologie Internetu



ISP první úrovně (TIER 1) sítě těchto ISP pokrývají celou planetu, směrovače musí obsahovat informace o všech sítích v Internetu (default free zona)

- poskytují připojení ISP druhé úrovně



ISP druhé úrovně (TIER 2) sítě těchto ISP působí na rozloze jednoho kontinentu – např. Evropu a poskytují připojení pro ISP v jednotlivých zemích na daném kontinentu



ISP třetí úrovně (TIER 3)
sítě těchto ISP působí na rozloze jednoho států a
poskytují připojení jednotlivým zákaznickým
sítím

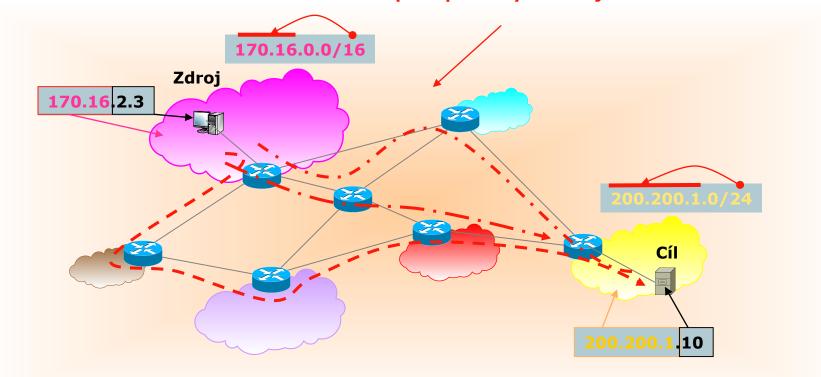


sítě jednotlivých zákazníků se připojují k ISP třetí úrovně, pro zvýšení spolehlivosti a rozložení zátěže se ve specifických případech může zákaznická síť připojit k jednomu stejnému ISP třetí úrovně ve více místech, nebo dokonce k různým ISP třetí úrovně ve více místech – tzv. "Multihoming. Většina těchto sítí získá veřejný adresový IP prostor od svého ISP3



Směrování – kudy vede cestička

? – kterou cestu v síti mám použít a jak následně zajistit, aby dané IP pakety po ní putovaly od zdroje k cíli





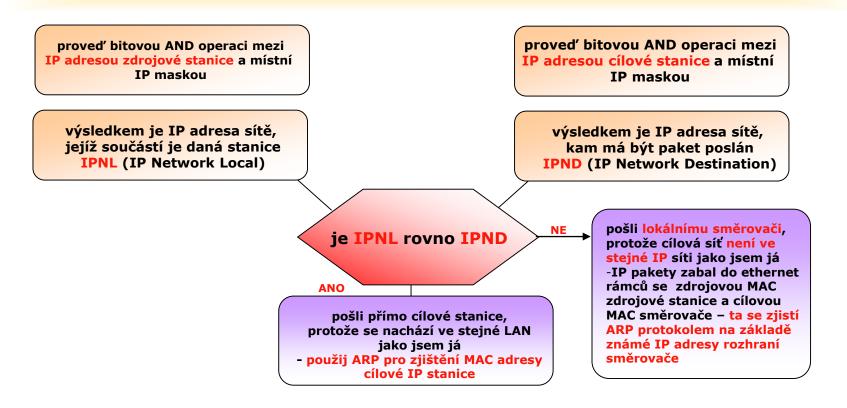
Směrování - komentář

- každý IP paket obsahuje cílovou IP adresu, kterou každý směrovač v síťové cestě používá k rozhodnutí, kam má být v dalším kroku poslán (přes jaké rozhraní a popř. jakému směrovači přes toto rozhraní)
- síťová část cílové IP adresy jednoznačně identifikuje fyzickou IP síť, která je dílčí částí celé větší globální sítě (např. Internetu nebo podnikové sítě)
- všechny koncové stanice a rozhraní směrovačů, které mají shodnou síťovou část své IP adresy jsou součástí jedné fyzické IP sítě, ve které mohou komunikovat přímo, bez nutnosti posílat IP pakety nejdříve směrovači toto je typicky nejnázornější u LAN, kde všechny koncové stanice mají společnou síťovou část IP adresy a mohou si tedy předávat IP pakety přímo použijí ARP protokol pro získání MAC adresy protější stanice s požadovanou IP adresou, viz předchozí přednáška)
- dvoubodové spojení mezi směrovači je většinou nutné v architektuře TCP/IP chápat též jako malou "LAN" síť, která nemá žádné koncové stanice. Jediné co je do této pomyslné sítě připojeno, jsou dvě IP rozhraní vzájemně spojovaných směrovačů
- směrovače propojují IP sítě a nepřímo potom stanice v nich obsažené



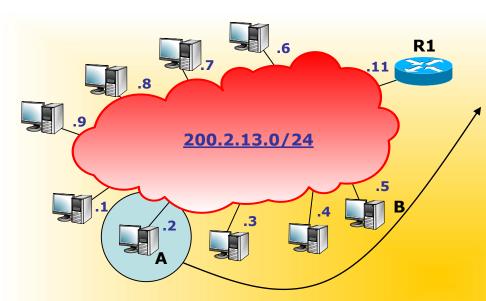
Kdy koncové zařízení stanice použije směrovač?

- koncová stanice použije pro doručení IP paketů směrovač, pokud cílová stanice leží mimo dosah lokální IP sítě
- <u>otázkou je, jak to pozná</u> -> k tomu slouží rozhodovací proces, který využívá IP adresu stanice, IP masku a IP cílovou adresu paketu





Příklad rozhodnutí



11001000.00000010.00001101.00000010 - 200.2.13.2 bitový AND

11111111.11111111111111111.00000000 - 255.255.255.0

11001000.00000010.00001101.00000000 - 200.2.13.0

stanice A teď ví, že leží v IP síti, jejíž adresa je 200.2.13.0

bitový AND

- tento výpočet se provede jen jednou při inicializace a dále se již neprovádí

Stanice A posílá IP pakety na adresu 200.2.13.5

11001000.00000010.00001101.00000101 - 200.2.13.5 bitový AND

11111111.111111111111111111.00000000 - 255.255.255.0

 $11001000.00000010.00001101.00000000 - \underline{200.2.13.0}$

stanice A teď ví, že cílová stanice
B s IP adresou 200.2.13.5 leží ve stejné
IP síti jako ona samotná, protože IP adresy
sítí jsou v obou případech shodné, tj.
200.2.13.0 – IP pakety se budou posílat
stanici B přímo v rámci LAN – nepůjdou přes
směrovač R1

Stanice A posílá IP pakety na adresu 147.32.192.2

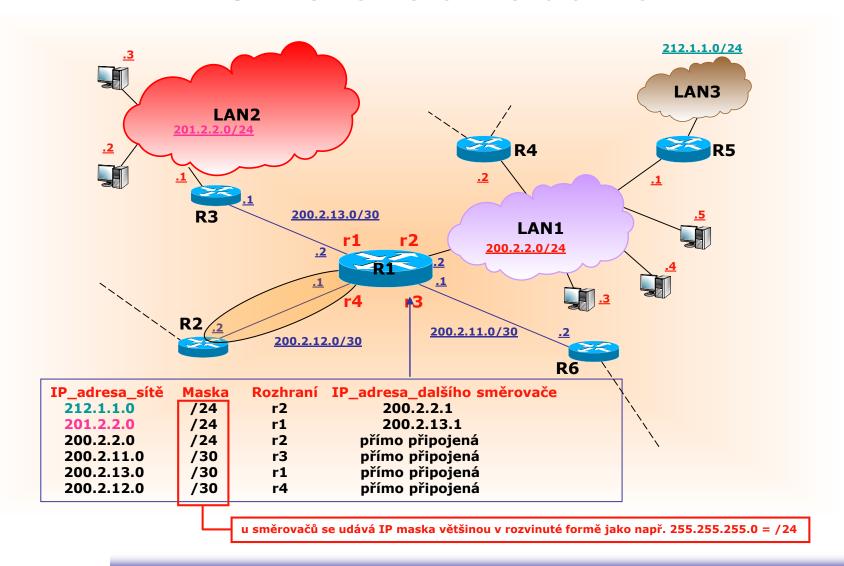
10010011. 00100000.11000000.00000010 - 147.32.192.2

10010011. 00100000.11000000.00000010 - 147.32.192.0

stanice A teď ví, že cílová stanice s IP adresou 147.32.192.2 neleží ve stejné IP síti jako ona samotná, protože IP adresy jsou rozdílné, v tomto případě je nutné dané pakety poslat LAN sítí ke směrovači R1, který se postará o jejich poslání dále do IP sítě



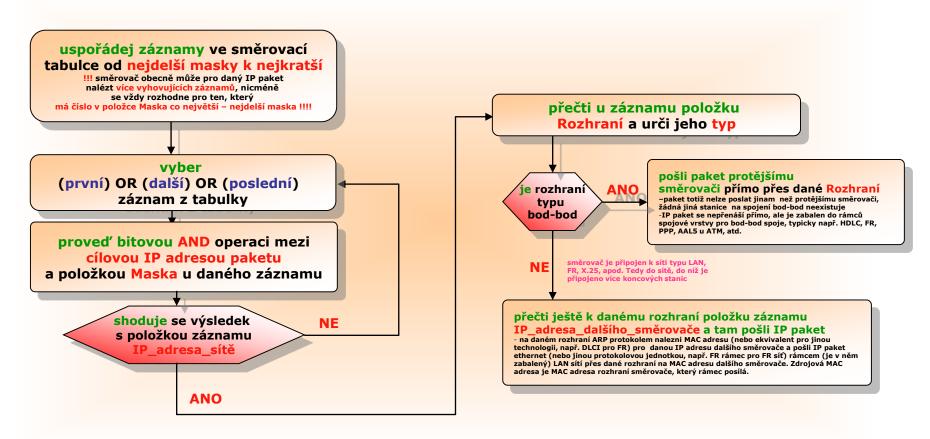
Směrovací tabulka





Základní rozhodovací proces směrovače

- klasický směrovač používá v procesu rozhodnutí kam má být právě přijatý IP paket do sítě poslán záznamy ve směrovací tabulce
- v nejjednodušším případě směrovač prochází celou tabulku jeden záznam po druhém a snaží se najít ten, který vyhovuje následujícímu pravidlu (moderní vysokorychlostní směrovače používají jiný algoritmus než sekvenční prohledávání – to by bylo příliš pomalé)





Výchozí směrovací záznam – "default route"

- směrovač nemusí mít nezbytně ve své směrovací tabulce záznamy o všech sítích v Internetu (nemusí to být Internet, ale třeba i podniková sít)
- stačí, když bude vědět, jak směrovat pakety jen k určité podmnožiny všech sítí
- všechny ostatní IP pakety, které nedokáže směrovač směrovat (není pro ně v tabulce relevantní záznam) lidově řečeno, "neví co s
 nimi má dělat" pošle jinému směrovači o němž se domnívá, že má více informací a že tedy dokáže IP pakety správně směrovat
- záznamu, který umožní všechny (kromě těch, pro které existuje v tabulce alespoň jeden relevantní záznam) IP pakety posílat k jinému směrovači se říká výchozí záznam (default route)
- pokud do směrovače přijde IP paket, k němuž nelze nalézt vyhovující záznam, paket je zahozen
- pokud existuje ve směrovači výchozí záznam, nemůže dojít k situaci, že by směrovač zahodil IP paket z důvodu neexistence odpovídajícího záznamu v tabulce – hledání záznamu vždy skončí právě tímto výchozím záznamem

203.100.1.0	255.255.255.0	Fa0	147.16.1.192
204.100.1.0	255.255.255.0	Se0	147.13.1.1
205.100.1.0	255.255.255.0	Se1	147.16.1.1
200.1.3.0	255.255.0.0	Fa0	147.16.1.192
201.2.1.0	255.255.0.0	Fa0	147.16.1.192
1.1.1.0	255.0.0.0	Fa0	147.16.1.192
0.0.0.0	0.0.0.0	Fa1	147.17.1.1

výchozí směrovací záznam (default route)

pokud cílové adrese v IP paketu nevyhovuje ani jeden z těchto explicitních záznamů, použij výchozí záznam (implicitní záznam) -> pošli je na rozhraní Fa1 směrovači s IP adresou 147.17.1.1



Kdo naplní směrovací tabulku?

- jakmile směrovač naplní směrovací tabulku platnými záznamy, může je okamžitě použít pro směrování IP paketů v síti
- záznamy do směrovací tabulky lze vložit ručně

manuálně a staticky

- v tomto případě vloží záznam do tabulky administrátor, daný záznam je statický, protože je v tabulce stále až to doby, než jej administrátor opět ručně zruší
- staticky definované záznamy nepotřebují směrovací protokol
- nevýhodou je, že při změně topologie sítě nelze záznam automaticky změnit a reagovat tak na případné výpadky v síti

ip route 200.1.1.0 255.255.240.0 147.32.1.10 route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 route add net 10.0.0.0 netmask 255.0.0.0 10.20.110.1

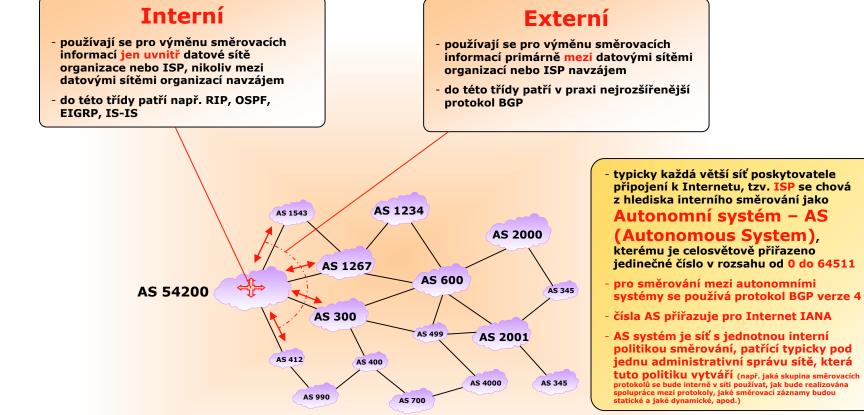
automaticky a dynamicky

- v tomto případě musí být na směrovači aktivován směrovací protokol, pomocí něhož se vzájemně směrovače v síti informují o dostupných (k nim připojených a funkčních) IP sítích. Na základě těchto informací určí směrovač optimální směrovací záznam pro konkrétní cílovou IP síť – jinými slovy, určí optimální další sekci v rámci celé cesty IP paketu v síti
- směrovací protokol sám vkládá směrovací záznamy do tabulky, bez zásahu administrátora sítě
- směrovací protokol je schopen automaticky reagovat na změněný stav sítě (např. přerušení okruhu, nefunkčnost směrovače nebo naopak přidání nové sítě) a opět optimálně upravit záznamy ve směrovací tabulce, aby doručení IP paketů k cíli zůstalo stále funkční



Směrovací protokoly

směrovací protokoly lze rozdělit podle použití v datové síti na:



síť, která vlastní veřejné IP adresy (např. ČVUT) nemusí mít nutně automaticky veřejné číslo autonomního systému



Směrovací protokoly a metrika

- pokud v datové síti existuje od zdrojové stanice více alternativních cest k cílové stanice, je nutné podle dnešní představy fungování přenosu dat vybrat typicky jen jedinou, po níž se budou pakety přenášet – existují určité výjimky pro rozdělení zátěže
- je však otázkou podle jakých kritérií se má daná cesta z <u>x</u> možných vybrat
- v praxi se to řeší tak, že se každé cestě přiřadí kvantifikující číselné veličina, která se častěji nazývá pojmem metrika
- poté se vybere ta cesta, jejíž metrika je v celém souboru s metrikami ostatních cest nejmenší – což koresponduje s obecnou představou, že je daná cesta nejkratší
- do výpočtu metriky lze zahrnout celou řadu kritérií, jako je počet směrovačů v
 cestě, výsledná přenosová rychlost, zpoždění průchodu paketu cestou, aktuální
 zatížení cesty (bráno často jako exponenciální klouzavý průměr), spolehlivost,
 apod. takto chápané metrice se říká kompozitní metrika (např. u EIGRP)
- některé protokoly však používají k výpočtu metriky jen jeden parametr cesty, např. počet směrovačů v cestě (tzv. "hop count") - RIP nebo přenosovou rychlost
 OSPF

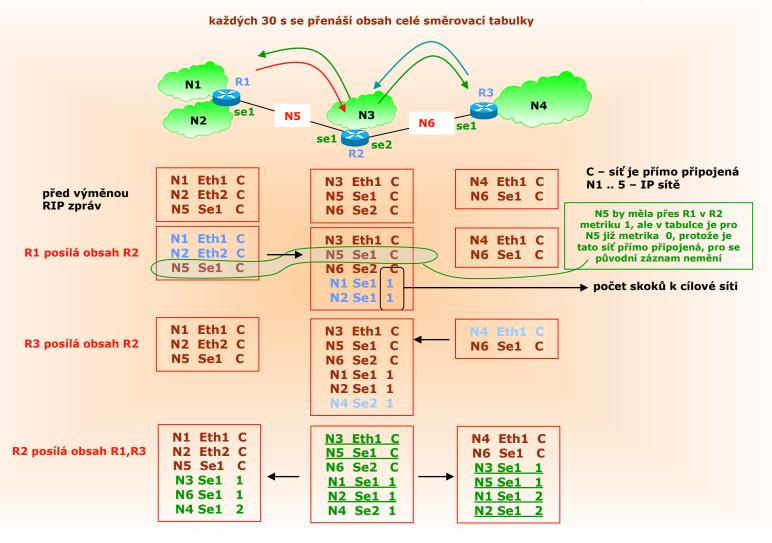


Směrovací protokol RIP(1)

- směrovací protokol **RIP** (Routing Information Protocol) je vektorově orientovaný (Distance Vector) distribuovaný směrovací protokol
- RIP je vnitřním směrovacím protokolem (viz dříve) standardizovaný pro architekturu sítí TCP/IP
- existuje ve dvou verzích RIP-1 a RIP-2, podle toho zda umožňuje přenášet informace o VLSM sítích (RIP2) či ne (RIP1),
 dnes se používá primárně verze RIP-2, u něhož se v záznamech o dostupných IP sítích vždy přenáší i příslušná její maska
- na každém směrovači v RIP doméně (část sítě, kde je použit RIP jako směrovací protokol) běží stejný algoritmus RIP protokol
 RIP je distribuovaný a decentralizovaný směrovací protokol
- vždy vzájemně sousedící směrovače si v RIP doméně mezi sebou neustále v pravidelných časových intervalech (ve výchozím stavu 30 s) vyměňují celé obsahy svých směrovacích tabulek
- pro transport směrovacích informací se používá UDP protokol a standardizovaný formát RIP protokolové datové jednotky (RIP PDU)
- RIP protokol je definován ve standardu RFC 1058 (RIP-1) a RFC 2453 (RIP-2) a je vůbec jedním z nejstarších směrovacích protokolů použitých v Internetu
- metrikou u RIP protokolu je počet směrovačů nacházejících se v dané cestě, tzv. "Hop count"
- směrovač k cílové síti vybere vždy tu z nabízených cest od svých sousedů, která obsahuje nejmenší počet směrovačů – nejmenší počet "skoků", kde skok=směrovač
- i když je RIP protokol velice jednoduchý ve své podstatě, jeho použití přináší určité úskalí:
 - pomalá rychlost konvergence, při změně v síti trvá dost dlouhou (i minuty v závislosti na rozsahu sítě a typu poruchy) než na danou změnu celá síť jako celek zareaguje - zprávy informující zbytek sítě, že došlo někde ke změně, se šíří velice pomalu
 - za určitých okolností může být RIP protokol extrémně pomalu konvergovat, což může vést ke vzniku dočasných směrovacích smyček v síti a ztrátě konektivity mezi některými sítěmi, z tohoto důvodu byly do RIP protokolu dodatečně implementovány pomocné algoritmy, které urychlují jeho konvergence (Split Horizon, Triggered updates, max hop count, Poison reverse, hold down timers)
- z důvodu rozumné doby konvergence, byl zvolen maximální limit, jak daleko (počet směrovačů v cestě) v doméně RIP mohou mezi sebou vzdálené IP sítě být, **tento limit je stanoven na max. 15 směrovačů**
- RIP protokol je dnes implementován v celé řadě i jednodušších zařízení pro svou snadnou implementaci a
 výpočetní nenáročnost, je však nutné podotknout, že jeho použití je omezené jen pro malé IP sítě pro sítě většího
 rozsahu je vhodné použít dokonalejší směrovací protokol jakým je např. OSPF, IS-IS nebo EIGRP (viz OSPF dále)



Směrovací protokol RIP(2)





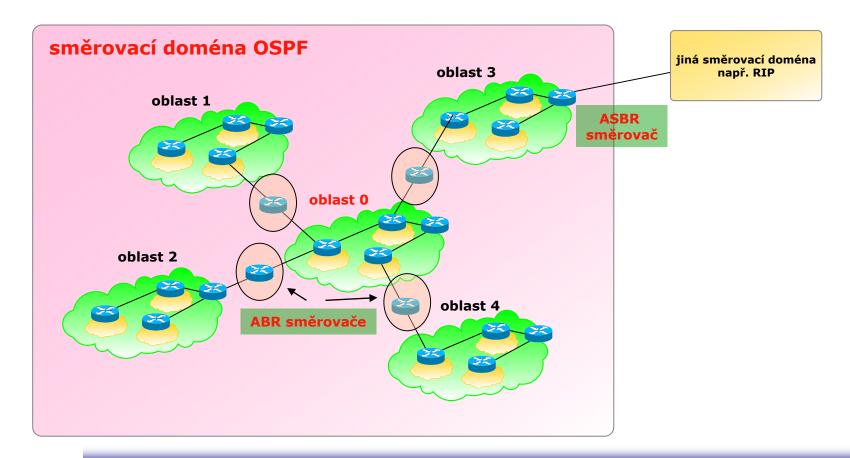
Směrovací protokol OSPF(1)

- směrovací protokol **OSPF (Open Shortes Path First)** je **stavově orientovaný a distribuovaný** směrovací protokol standardizovaný v **RFC 2328** a používaný v datových sítích s architekturou TCP/IP
- OSPF je jedním z vnitřních směrovacích protokolů, podobně jako RIP
- OSPF je **komplexní směrovací protokol**, který byl navržen **pro rozsáhlé sítě**, přičemž odstraňuje problémy se kterými se můžeme setkat u RIP protokolu rychlost konvergence sítě, nestabilita
- OSPF je navržen tak, aby byl snadno škálovatelný pro různě rozsáhlé datové sítě, cesta mezi sítěmi není limitována počtem směrovačů v cestě, jako u RIP
- OSPF používá koncept rozdělení celé velké IP sítě do menších celků, kterým se říká oblasti (area)
- informace o připojených sítích jednotlivých směrovačů v rámci OSPF směrovací domény se rozesílají všem směrovačům v dané oblasti (area), nejen pouze sousedům, jak je tomu u RIP protokolu
- všechny směrovače uchovávají a aktualizují topologickou tabulku, která musí být za neměnného stavu sítě identická lidově řečené, každý směrovač "vidí" stejnou topologii propojení směrovačů v rámci dané oblasti, topologická tabulka obsahuje informace o všech směrovačích v rámci dané OSPF oblasti a jejich vzájemné propojení
- OSPF používá jednoduchou nekompozitní metriku vyjádřenou parametrem tzv. ceny (cost) propojení mezi směrovači, velikost ceny (cost) je nepřímo úměrná přenosová rychlosti propojovacího datového okruhu mezi směrovači
- cena jedné uvažované cesty v IP sítě je u OSPF dána součtem všech cen dílčích segmentů cesty, které ji tvoří
- každý směrovač na základě topologické tabulky (lidově říká, co je s čím propojeno a jak) vypočítá nejkratší cestu mezi sebou a každým zbývajícím směrovačem v rámci dané oblasti
- k výpočtu nejkratší cesty používá OSPF **Dijkstra algoritmus**, který funguje za předpokladu, že všechna propojení mezi směrovači mají přiřazenou hodnotu metriky větší než nula což je splněno, cena nemůže být menší než nula
- na základě výpočtu všech nejkratších cest modifikuje OSPF algoritmus směrovací tabulku směrovače
- směrovače v rámci OSPF si mezi sebou neustále vyměňuji krátké zprávy (hello), které slouží pro detekci funkčního
 či nefunkčního stavu spojení mezi směrovači tyto zprávy se většinou vysílají s periodou 10 s



Směrovací protokol OSPF(2)

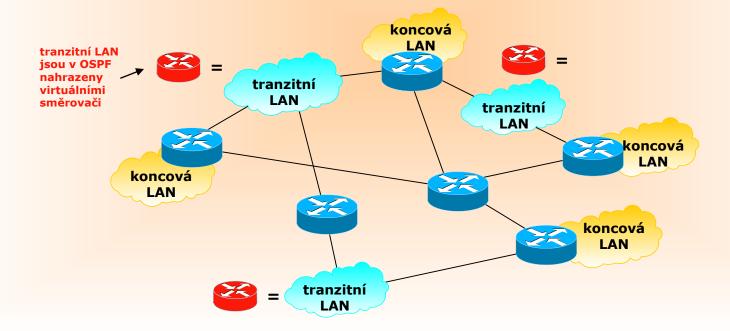
- směrovací doménu OSPF lze pro rozsáhlé sítě rozdělit do menších OSPF oblastí
- zvláštní postavení má u OSPF oblast č.0, která tvoří pomyslnou páteřní síť
- všechny ostatní oblasti musí být napojené k oblasti č.0 (jsou však určité výjimky)
- rozhraní mezi oblastmi je skryté uvnitř směrovače, který se nazývá hraniční směrovač oblasti ABR (Area Border Router)
- spojení mezi doménou OSPF a jinými vnějšími doménami zprostředkovává hraniční směrovač OSPF domény ASBR (Autonomous System Border Router)





Směrovací protokol OSPF(3)

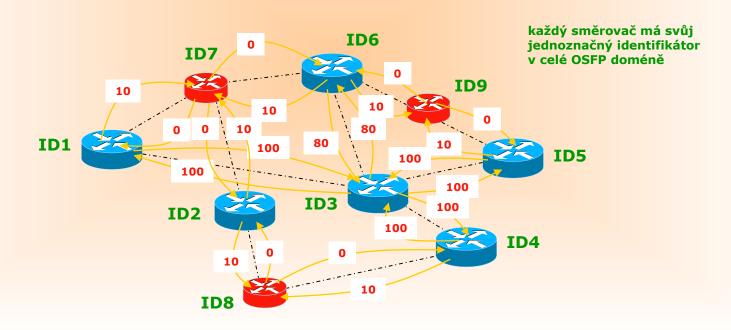
- OSPF protokol chápe IP sítě buď jako koncové nebo tranzitní
- koncová síť je vždy jen zdrojem nebo příjemcem IP paketů, pakety nikdy touto sítí neprochází "napříč"
- tranzitní síť je sítí, ve které mohou být pakety nejen generované nebo v ní končit, ale také jí mohou procházet
- funkční dvoubodové propojení směrovačů chápe OSPF protokol jako tranzitní síť
- dvoubodové připojení koncové stanice k směrovači chápe OSPF jako koncovou síť
- z hlediska nalezení nejkratší cesty Dijkstra algoritmem se berou v úvahu jen tranzitní sítě a směrovače celá
 topologie sítě se překreslí do grafu, v němž směrovače a tranzitní LAN sítě tvoří uzly, hrany grafu jsou tvořeny
 buď dvoubodovými spoji nebo spoji k tranzitním LAN sítím





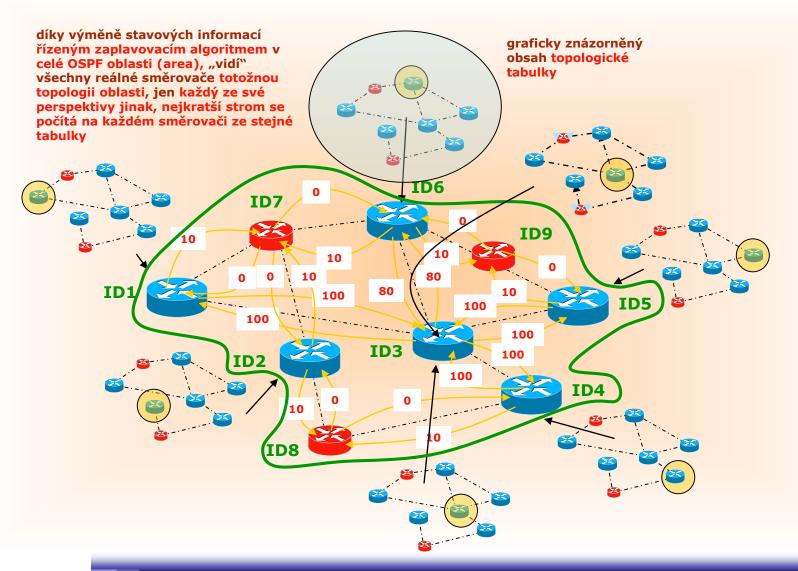
Směrovací protokol OSPF(4)

- celá fyzická síť se transformuje na orientovaný ohodnocený graf
- hodnota každé hrany grafu je dána metrikou "cost", která je u OSPF nepřímo úměrná přenosové rychlosti datového okruhu a typicky se vypočítá COST=108/B, kde B je přenosová rychlost datového okruhu v bit/s, např. pro 10 Mbit/s LAN je COST=10, pro rychlost >=1Git/s je nutné COST volit ručně
- každá tranzitní LAN síť je nahrazena v grafu pomyslným virtuálním směrovačem (červená značka), který je v grafu připojen hranami k ostatním uzlům nesymetricky (hrana orientovaná ve směru od virtuálního směrovače má vždy COST=0) důvodem je, aby se COST pro tranzitní LAN uvažoval při výpočtu jen jednou, např. pokud je součástí vybrané cesty spojení mezi ID1 a ID6 (dílčí segment), vede sice v grafu přes virtuální směrovač ID7, ale ve skutečnosti jsou pakety posílané přímo mezi těmito směrovači pokud by byl hraně grafu vedoucí od virtuálního směrovače přiřazen COST (také 10), byl by celkový COST dvojnásobný, což ve skutečnosti ale není

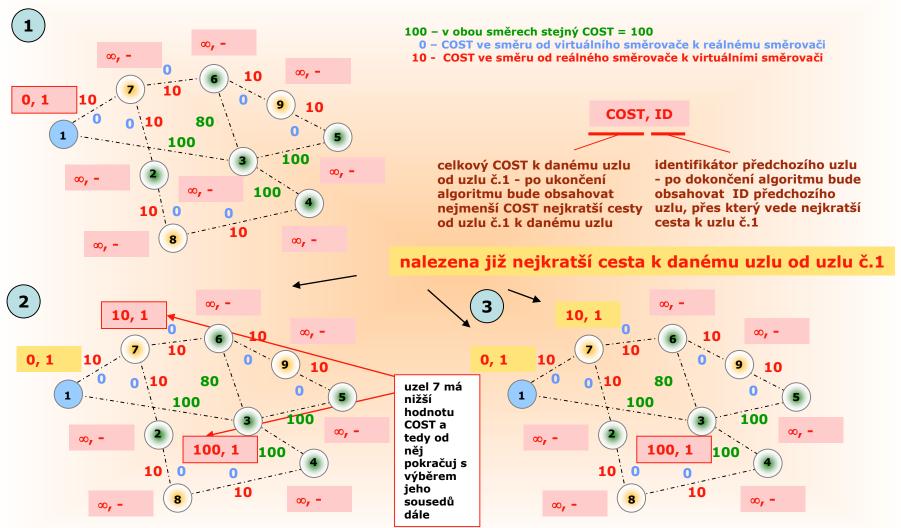




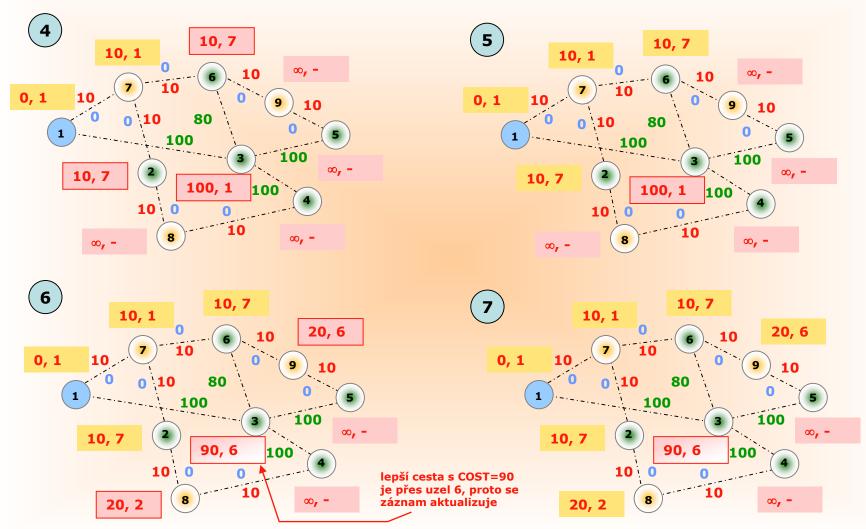
Směrovací protokol OSPF(5)



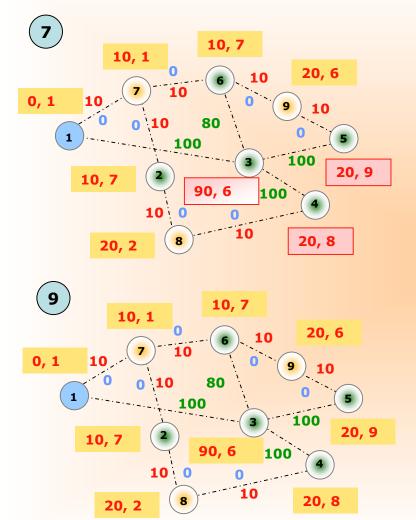


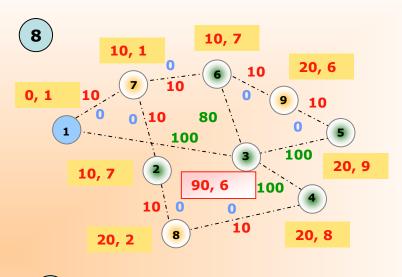


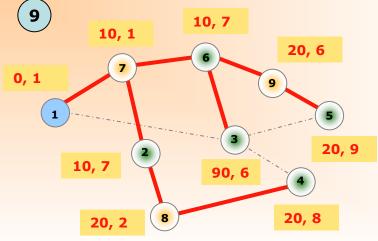




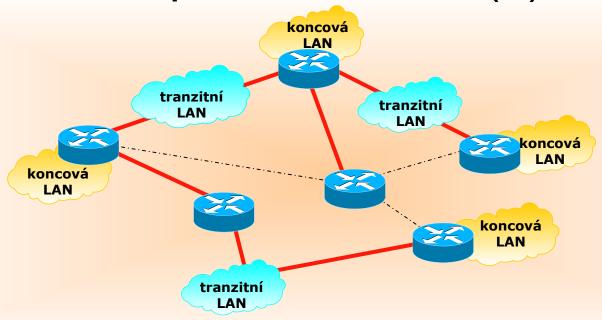












- vzhledem k tomu, že směrovače s ID 7,8,9 (viz předchozí) jsou jen virtuální, musí spojení pře tranzitní LAN procházet přímo mezi reálnými směrovači
- smysl zavedení konceptu virtuálních směrovačů v OSPF je snížit celkový počet tranzitních sousedních vztahů v topologické tabulce při spojení N směrovačů v rámci tranzitní LAN sítě, by bylo nutné v topologické tabulce udržovat N*(N-1) +1 záznamů, při zavedení konceptu virtuálního směrovače stačí v topologické tabulce uchovávat jen N+1 záznamů, dále se také sníží počet generovaných "hello" paketů mezi OSPF směrovači v rámci tranzitní LAN sítě
- virtuální směrovač se u OSPF nazývá <u>vyvoleným směrovačem DR (Designated Router)</u> a jeho roli zastává jeden z reálných směrovačů připojených do tranzitní LAN sítě volí se automaticky
- vzhledem k tomu, že role DR je velice důležitá pro to, aby OSPF oblast mohla chápat LAN síť jako tranzit, funguje ještě v
 rámci LAN náhradní vyvolený směrovač <u>BDR (Backup Designated Router)</u>, který přebírá roli DR v případě jeho výpadku
- DR posílá do celé oblasti (area) informaci o IP rozhraních a ID číslech všech k němu připojených reálných směrovačů



OSPF – řízená distribuce LSA

- každý směrovač v IP síti generuje stavový záznam připojení LSA (Link State Advertisement), který udává seznam všech připojených sítí různých typů
- pokud je připojení k dané síti (LAN, ale i dvoubodový spoj) aktivní a funkční, vygeneruje směrovač konkrétní typ LSA a ten <u>řízeným systémem pošle</u> všem směrovačům v dané oblasti (area)
- typ LSA závisí, kromě jiného, na tom, jestli je daná síť tranzitní nebo jen koncová (Stub network)
- řízené doručování LSA záznamů všem směrovačům se realizuje postupným zasíláním LSA všem OSFP sousedům, které správný příjem musí potvrdit odesílateli a poté stejným způsobem LSA posílají dále svým dalším sousedům, atd. než se daná informace rozešle po celé oblasti > nový stav sítě se velice rychle rozšíří
- pokud směrovač zjistí poruchu konektivity k dané síti, musí okamžitě vymazat z celé OSPF oblasti odpovídající LSA
- každý LSA záznam disponuje sekvenčním číslem, které umožňuje směrovači rozpoznat, který z případným dvou přijatých LSA je aktuálnější
- každé správně přijaté LSA od souseda se uloží do topologické tabulky
 OSPF, z níž se poté Dijkstra algoritmem přepočítá nejkratší strom v síti



OSPF - shrnutí funkce

směrovač zjistí seznam všech připojených a aktivních IP sítí

na těchto sítích zjistí, zda jsou přes ně dostupné OSPF sousedé - pokud je přes danou síť dostupný OSPF soused, bude tato síť ve svém LSA označena jako tranzitní - pokud ne, bude síť označena jako koncová (Stub)

směrovač vytvoří odpovídající LSA (obsahem jsou připojené sítě) a pošle jej do celé oblasti všem směrovačům - tuto LSA taktéž uloží do své topologické tabulky

přijímá LSA od ostatních směrovačů -pokud jsou neporušené a aktuální, uloží je také do své topologické tabulky při změně obsahu topologické tabulky aktivuje směrovač s jistým zpožděním Dijkstra algoritmus, který přepočítá nejkratší cesty v síti ke každému zbývajícímu směrovači v oblasti a potažmo i k odpovídajícím sítím

podle výsledku Dijkstra algoritmu se aktualizují záznamy ve směrovací tabulce směrovače

