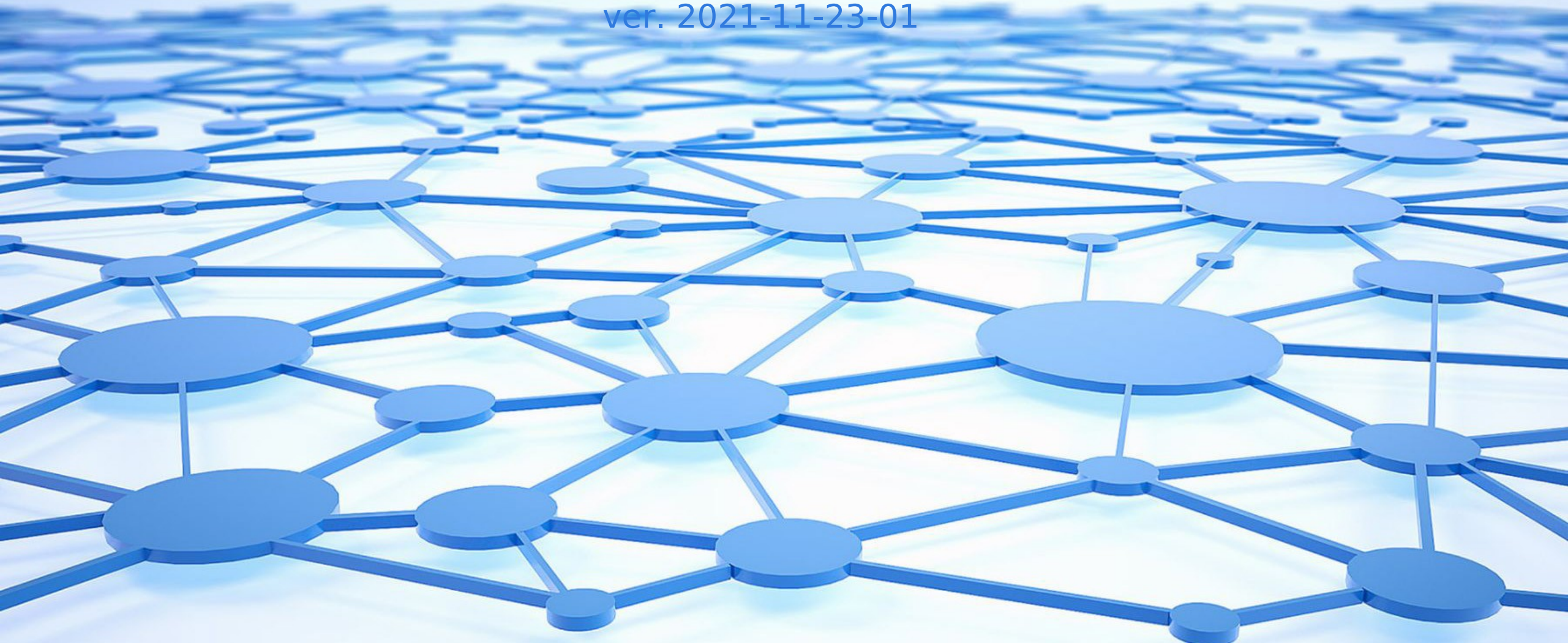


Úvod do počítačových sítí

Přednáška 8
(2021/2022)
ver. 2021-11-23-01



L3 – Síťová vrstva

- Základním funkce
 - Hledání cesty – směrování – routing
 - Zjistit kam se mají data poslat
 - Předávání dat – forwarding
 - Když už vím kam data patří, tak je předám zvoleným směrem
- Rozšiřující / nepovinné funkce
 - Předcházení zahlcení
 - Snaha upravit provoz / směrování tak, aby se zahlcení předešlo
 - Protože pokud už k němu dojde, nejde dělat nic jiného než data zahazovat, což vede k nutnosti znovu poslání a tím znovu zatížení sítě
 - Řízení toku
 - Snaha předejít tomu, aby se zahltil příjemce – tedy síť je ok, ale nestíhá příjemce
 - Výsledné chování může být velice podobné jako zahlcení sítě, ale má jinou příčinu a i řešení
 - Pokud je zahlcena síť, můžeme za určitých okolností posílat data jinudy/rozložit tok mezi více zařízení, ale pokud je zahlcen klient můžeme jen zpomalit vysílání
- QOS – Quality of Service
 - Zajištění minimálně požadovaných zdrojů pro vybrané služby
 - Například pro hlas / multimédia – nepotřebují moc, ale potřebují pravidelně

Spojení a stabilita

- V rámci L3 předpokládáme síť s přepínáním paketů, které používají přenos dat metodou Store&Forward a můžeme realizovat jako službu/spojení:
 - Spojovanou
 - Pak přenášený blok dat označuje jako Paket
 - Obecněji je ale jako paket nazýván jakýkoliv blok dat naformátovaný jako paket
 - Před přenosem je jednorázově nalezena cesta a jako adresa je pak přenášen jen identifikátor cesty
 - Obdobně jako přepojování okruhů, ale cesta není vyhrazena, jedná se o virtuální okruh
 - Jednotlivé prvky – routery – si pamatují výsledek předešlého hledání
 - Například u ATM
 - Nespojovanou
 - Pak se přenášený blok označuje jako Datagram
 - Přenáší se celá adresa příjemce
 - K rozhodování o směrování dochází na každém uzlu / routeru
 - Například IP
- Přenos můžeme dělit i z pohledu spolehlivosti
 - Spolehlivý
 - Potvrzovaný – víme, že data došla
 - Typicky pro spojované protokoly
 - Nespolehlivý
 - Nepotvrzovaný – data odešleme, ale nemáme zajištěno, zda data dojdou a zda se o tom dozvíme
 - Pro spojované i nespojované protokoly
- Z výše uvedeného by to vypadlo, že nad IP(nespojovaná služba) nejde realizovat spolehlivý přenos – to není zcela pravda, protože TCP spolehlivý je a je zároveň i spojovaný – ALE řeší se až na L4

Směrovací tabulka

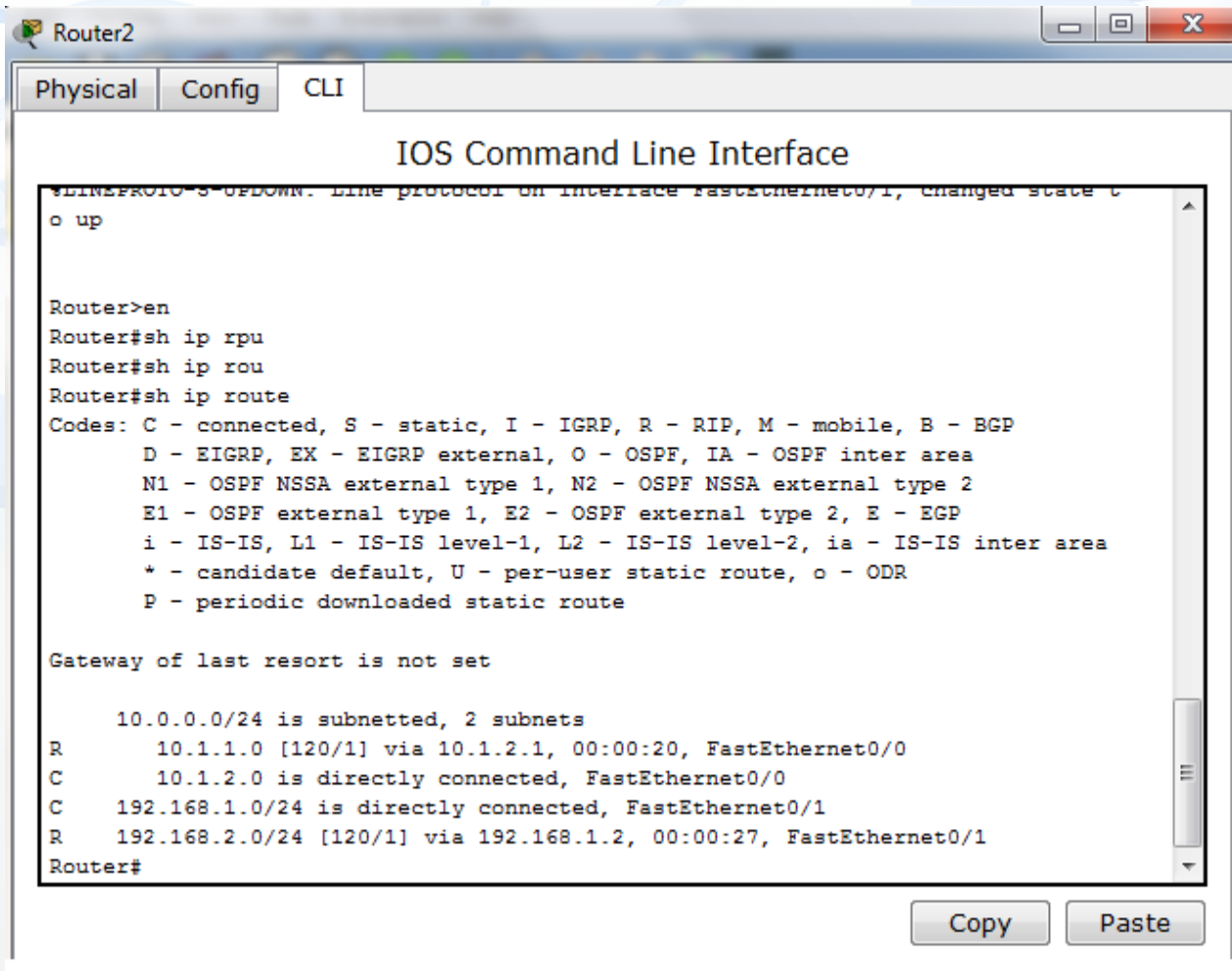
- Informace i **možnostech** směrování se ukládají do směrovací tabulky
- V tabulce jsou uloženy VŠECHNY dostupné cesty
- Logicky v tabulce nemohou být cesty ke všem strojům v síti
 - Jeden problém je že tabulka by byla obrovská
 - Druhý problém, že všechny cesty neznáme
- Náhradou cest o kterých nevím je výchozí cesta
 - Default gateway – pokud nevím kam, použiji toto pravidlo
- Cíle ve směrovací tabulce mohou být násobné
 - Tedy k jednomu cíli vede více cest
- Typy záznamů ve směrovací tabulce
 - Static – ručně zadané cesty
 - Mají nejvyšší váhu – administrátor „ví co dělá“
 - Directly connect – cesty vzniklé z lokálně připojených sítí
 - Druhá nejvyšší váha – jsem součástí dané sítě, takže mohu této informaci věřit
 - Dynamic – cesty vložené dynamickými směrovacími protokoly
 - Tyto cesty mohou být vložena přímo nebo zprostředkovaně pomocí redistribuce

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
    is directly connected, Serial0/0/1
    172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C   172.16.1.0/24 is directly connected, GigabitEthernet0/0
L   172.16.1.1/32 is directly connected, GigabitEthernet0/0
R   172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
R   172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R   172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R   192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03, Serial0/0/0
    209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C   209.165.200.224/30 is directly connected, Serial0/0/0
L   209.165.200.225/32 is directly connected, Serial0/0/0
R   209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
C   209.165.200.232/30 is directly connected, Serial0/0/1
L   209.165.200.233/32 is directly connected, Serial0/0/1
R1#
```


Forwardovací tabulka

- Ve směrovací tabulce toho může být hodně
- Informace v ní mohou násobně
 - Tedy více cest jednomu cíli, ale my už potřebujeme data někam předat a je nutné říci kam
- K samotnému předání se pak použije forwardovací tabulka
- Jedná se podmnožinu informací ze směrovací tabulky
 - Pro každý cíl je jen jedna cesta
 - Je snaha počet řádek co nejvíce snížit
 - Například pomocí agregace
- Čím méně řádků v tabulce, tím rychlejší odbavení



```
Router2
Physical Config CLI
IOS Command Line Interface
Router>en
Router#sh ip rpu
Router#sh ip rou
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 2 subnets
R       10.1.1.0 [120/1] via 10.1.2.1, 00:00:20, FastEthernet0/0
C       10.1.2.0 is directly connected, FastEthernet0/0
C      192.168.1.0/24 is directly connected, FastEthernet0/1
R      192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:27, FastEthernet0/1
Router#
```

zdroj: <https://community.cisco.com/t5/routing/unable-to-understand-this-routing-table-created-by-rip/td-p/1842945>

Forwardovací tabulka: Agregace

- Kromě default gateway může počet řádek při směrování snížit agregace
- Cíl je z více řádků udělat jeden, který pokryje všechny původní řádky

- Logickým požadavkem je, že odchozí port/IP musí být stejné

- Agregace může probíhat dvojím způsobem

- Ručně – spojím vybrané sítě do jedné větší - viz obrázek

- Automaticky – směrovač sám agreguje jednotlivé cesty

- Zde může nastat problém, že agregace může probíhat na úrovni tříd adres a nemusí být tedy žádoucí

- Např. 10.0.0.0/24 a 10.1.0.0/24 se agregují na 10.0.0.0/8

- Jedná se o třídu adres A, kde defaultní maska je /8

- Automatická agregace lze na směrovačích vypnout

Route Summarization

FIGURES

1

2

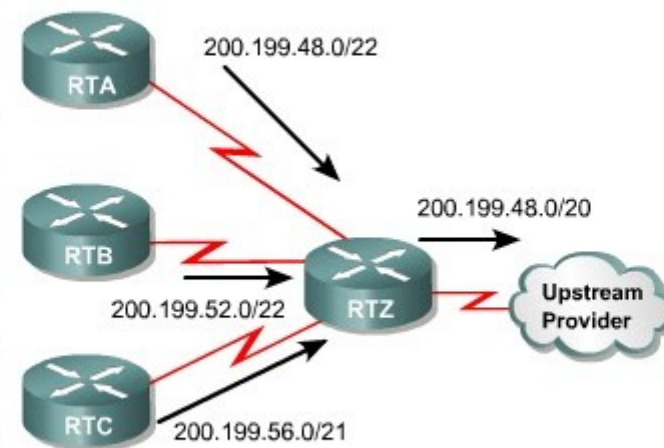
3

4

200.199.48.0/24
200.199.49.0/24
200.199.50.0/24
200.199.51.0/24

200.199.52.0/24
200.199.53.0/24
200.199.54.0/24
200.199.55.0/24

200.199.56.0/24
200.199.57.0/24
200.199.63.0/24



Route summarization reduces the routing table size by aggregating routes to multiple networks into one supernet.

Forwardovací tabulka: Administrative distance

- Pokud máme ve směrovací tabulce více cest se stejným cílem potřebujeme na základě „něčeho“ rozhodnout, kterou použít
- Toto rozhodnutí se dělá na základě „Administrative distance“
 - Jedná se o celé kladné číslo
 - Tato hodnota určuje váhu / důvěryhodnost dané informace
- Do forwardovací tabulky se ukládají informace s nejnižší dostupnou hodnotou AD pro danou cestu
- Důvěryhodnost protokolů je ve výchozím stavu dané, ale lze v případě potřeby i měnit
- Jednotlivé protokoly mohou mít různou důvěryhodnost dle místa použití
 - Interní EIGRP – 20
 - Externí EIGRP – 170
 - Jinak řečeno se každý protokol nehodí na všechna použití

```
Router_A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/24 is subnetted, 1 subnets
D       10.0.0.0 [90/30720] via 192.168.0.2, 00:00:09, FastEthernet0/0
C       192.168.0.0/24 is directly connected, FastEthernet0/0
Router_A#
```

zdroj: <https://study-ccna.com/administrative-distance-metric/>

Routing Technique	Preference
Connected Interface	0
Static Route	1
EIGRP Summary Route	5
EBGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
ISIS	115
RIP	120
EGP	140
ODR	160
External EIGRP	170
Internal BGP	200
Unknown	255

zdroj: <http://packetsanalyzed.blogspot.com/2013/04/hp-administrative-distance.html>

Základní principy v směrování

- Směrování na základě cílové adresy / Destination base routing
 - Nejběžnější varianta směrování
 - Rozhodujícím kritériem je „cílová adresa“
 - Obsah ani zdroj data není relevantní pro rozhodování
 - Rozhodnutí nemusí (ale může) být vázáno na konkrétní adresu, ale spíše na síť do které adresa patří
 - Tedy se jedná o zobecnění ve snaze snížit počet záznamu ve směrovací / forwardovací tabulce
 - Dnes patrně nejrozšířenější metoda
- Směrování dle cesty s nejnižší „cenou“ / Least cost routing
 - Síť beme jako orientovaný ohodnocený graf, ve kterém hledáme nejlevnější cestu
 - Orientovaný – každá cesta nemusí být obou směrná
 - Ohodnocený – každá cesta má nějakou cenu (latence, zatížení, konstanty – např realně cena přenosu)
 - Klasická grafová úloha řešitelná například pomocí Dijkstrova algoritmu
- Směrování se řeší samostaně v každém uzlu – routeru / Hop by hop
 - Každý jeden uzel rozhoduje o dalším kroku – kam data předá
 - Rozhodování je samostatné, ale může vycházet ze společně získaných/sdílených informací
- Směrování je nezávislé na obsahu
 - Obsah dat / služba vyšších vrstev která jsou přenášena nemají na směrování vliv
 - Neplatí v případě QOS
- Směrování je bezstavovost
 - Nezáleží na obsahu / cíly předchozího paketu při rozhodování o aktuálním

Další možné principy v směrování

- Tyto principy nejsou obecně používány, ale mohou se v některých specifických situacích hodit
- Směrování podle zdrojové adresy / Source base routing
 - Je opakem k destination base routing
 - Může se destination base routingem kombinovat – napřed zkusím source base routing a když se pravidlo nenajde, použiji destination base routing
 - Je třeba doplnit rozhodovací pravidla – v Linuxu ip rules – který pomohou rozhodnout dle čeho se směruje
- Směrování na základě obsahu / Content switching
 - Může se někdy hodit moci směrovat podle informací od vyšších vrstev - například L4
- Směrování se zohledněním historie / Flows
 - Pokud nějaká data patří k sobě – například stream multimédií, může být výhodné je posílat stejnou cestou

Kategorizace směrování

- Dle reakce na změny
 - Neadaptivní
 - Adaptivní
- Dle metody řízení
 - Centralizované
 - Isolované
 - Distribuované
 - Hierarchické

Kategorizace směrování: Dle reakce na změnu: Neadaptivní

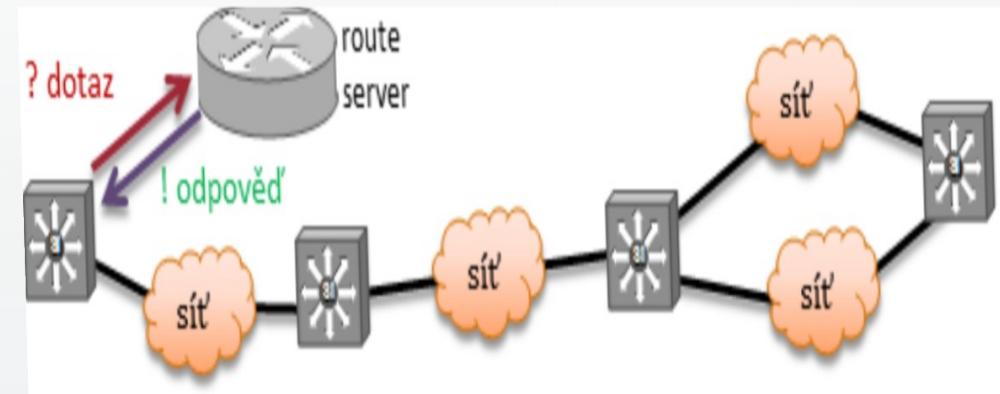
- Většinou se jedná o statické nastavení
- Nereaguje na změny v prostředí
 - Pokud je změna třeba – například při výpadku směrovače – musí někdo přijít a udělat změnu ručně
- Výhodou je vysoká míra predikovatelnosti
 - Bez ohledu nato co se děje, víte kudy vám data tečou
 - Což s ohledem na fakt, že jednotlivé spoje mohou mít různou cenu za přenos může být výhodné
 - Bezpečné řešení
 - Změny neprobíhají na základě stavu sítě, tedy nejde se směrováním manipulovat
 - Nemá žádnou přidanou režii z hlediska přenosu

Kategorizace směrování: Dle reakce na změnu: Adaptivní

- Řeší nedostatky neadaptivního směrování
 - Tento požadavek vznikl „časem“ - u prvních sítí s nízkým využitím a malým počtem uzlů nebyl nutný
- Adaptivní směrování se cyklicky snaží zjišťovat stav sítě a tyto informace pak promítnout do směrování
 - Reaguje na výpadek či přidání datové cesty
 - Může reagovat i na zhoršení parametrů existující přenosové cesty
 - Ke zhoršení může dojít vlivem vnějších vlivů – například interference nebo počasí, ale i vliv zatížení spoje – saturace linky
- Nevýhodou je nenulová režie adaptivních protokolů
 - Informace nutné k nastavení směrování se přenáší jako další data
 - Snižuje využití kapacity přenosového kanálu
 - Režie je tím větší čím více uzlů a změn je v síti
 - Vzniká bezpečnostní riziko spojené s možností manipulovat s dynamickými směrovacími protokoly
 - V podstatě se jedná o snahu odklonit provoz jinam než kam správně patří z důvodů:
 - Možnosti zachytávání a případně modifikace dat – Man in the Middle
 - Znepřístupnění služby / sítě – Denial of Service

Kategorizace směrování: Dle metod rozhodování: Centralizované

- Nejjednodušší cesta z pohledu implementace
- Máme jednu stanici, která řídí obsah směrovacích tabulek jednotlivých uzlů / směrovačů
 - Označuje se jako **route server**
- Ostatní stanice pouze realizují forwarding provozu na základě směrovacích informací od route serveru
 - Označované např jako **edge device**
- Výhodou je komplexní pohled na síť
 - Všechny informace jsou na jednom místě
 - Všechny informace se předávají v síti jen na jednu stanici
 - Je velice snadné, jako u všech centralizovaných řešení, měnit algoritmy
- Tak jako u všech centralizovaných řešení je problém výpadek route serveru
 - Single point of failure

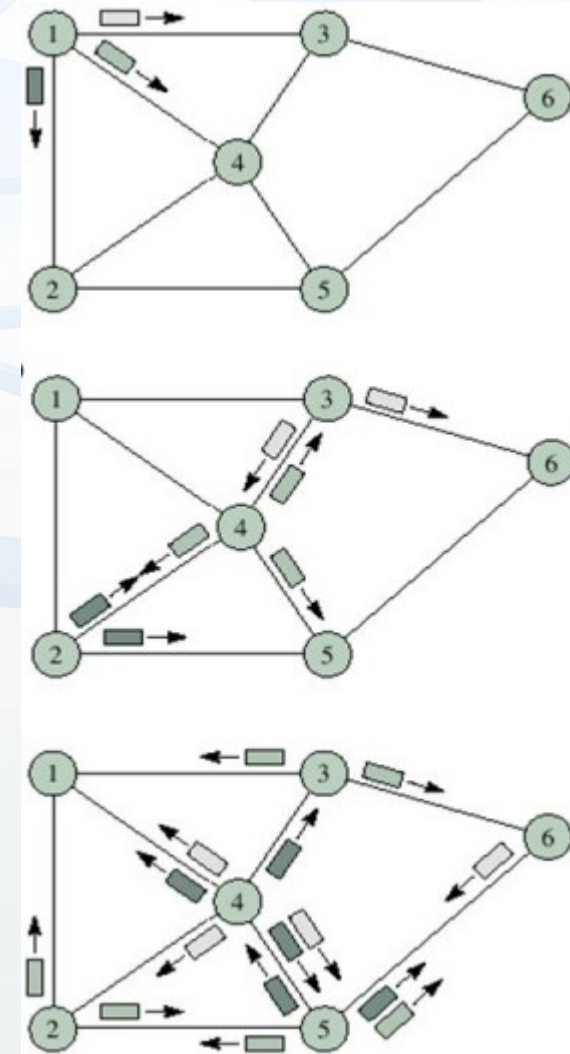


Kategorizace směrování: Dle metod rozhodování: Isolované

- Každý uzel funguje autonomně a s ostatními nespolupracuje a ani není nikým řízen
- Data ostatním posílá a přijímá je, ale jen jako data, nikoliv jako řídicí informace
- Existuje více metod izolovaného směrování
 - Záplavové směrování
 - „Horká brambora“
 - Náhodné směrování
 - Zpětné učení
 - Source routing
 - Policy base routing
- Nejsou tak masivně využívány samostatně, ale mají svůj význam ve speciálních případech – slouží jako řešení krizových či počátečních situací
 - Krizová – zařízení přestává stačit rozhodovat o směrování
 - Mohu použít náhodné směrování či metodu horké brambory
 - Počáteční – potřebuji nějakou informaci zjistit, ale zatím nemám jak
 - Použiji například záplavové směrování, protože pokud cesta existuje – najde ji

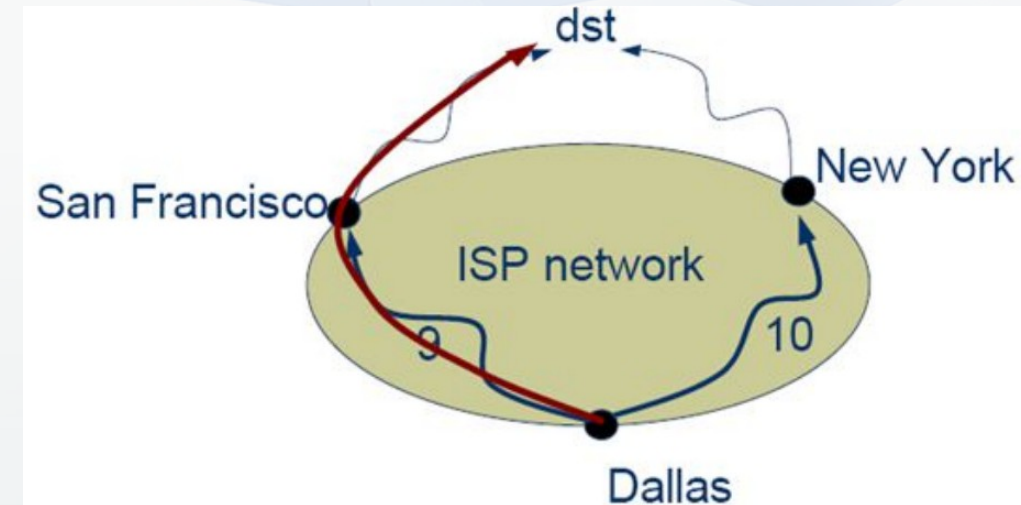
Kategorizace směrování: Dle metod rozhodování: Isolované: Záplavové směrování

- Někdy označované jako Flooding
- Podobně jako u broadcastu pro switch jsou data rozslána na všechny porty, krom toho ze kterého dorazila
 - Nepotřebuje žádnou směrovací tabulku
- Logickým důsledkem je fakt, že pokud nějaká cesta existuje, je nalezena a data doručena
- Nevýhod je ale více:
 - Pokud jsou v síti smyčky vniká problém násobných paketů
 - Stejně jako pro switch – broadcastová bouře
 - Násobné pakety je třeba nalézt a odstranit z provozu
 - Celá síť je násobně zatížena – nehodí se na běžný intenzivní provoz
- Může být použit jako nástroj pro hledání a sestavení virtuální cesty
- Může být použit tam, kde bez ohledu na režii potřebujeme mít jistotu, že data nakonec dojdou



Kategorizace směrování: Dle metod rozhodování: Isolované: „Horká brambora“

- Metoda „horké brambory“ - Hot Potato
- Cílem je přicházející data co nejrychleji odbavit bez ohledu na vše ostatní
- Data se neodesílají podle směrovací tabulky, ale dle toho kterým portem mohou nejrychleji odejít
 - Což lze zjistit na základě délky výstupního bufferu jednotlivých portů
 - Což samozřejmě nemusí nutně být ten ideální nebo správný port
- Může mít dvojí reálné využití
 - Jako doplněk jiného „klasického“ směrování, kdy se na toto přepne v případě potíží
 - Na routeru se v bufferech hromadí data a router přestává stíhat, přepne na tuto metodu a v co nejkratším čase fronty vyprázdní nebo alespoň výrazně sníží jejich délku.
A to i za cenu toho, že některá data nemusí nutně dojít k cíli a už vůbec ne ideální cestu => přehodím ten problém „tu horkou bramboru“ na někoho dalšího
 - Pro vyvažování zátěže násobných linek
 - Pokud mám dvě či více cesty z bodu A do bodu B, mohu jejich provoz pomocí této metody optimalizovat/vyvažovat
 - Protože jak se řeklo, aktuální paket odejde cestou s nejkratším bufferem

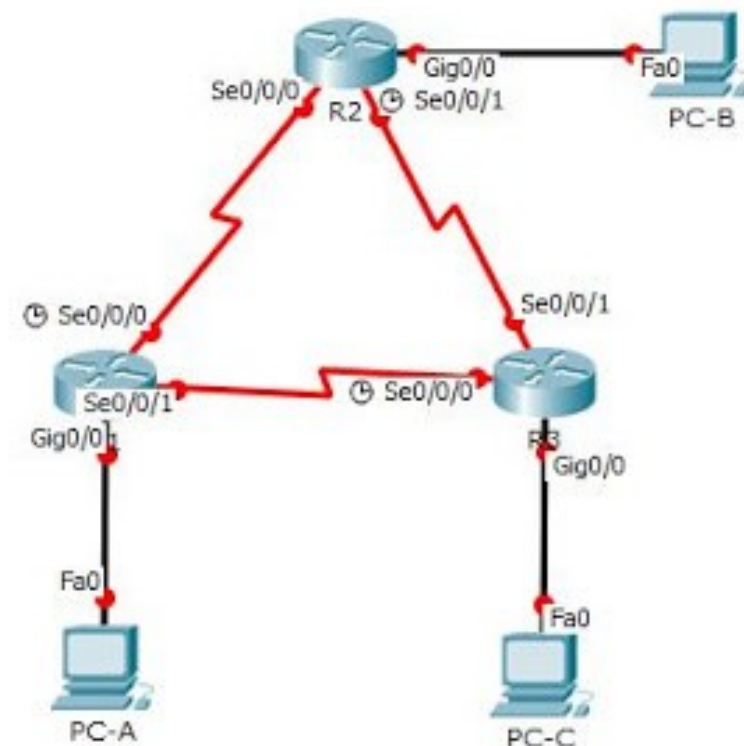


Kategorizace směrování: Dle metod rozhodování: Isolované: Náhodné směrování

- Náhodné směrování - Random walk
- Jak už název napovídá jedná se o náhodné směrování
- Směr / port není volen na základě nějakého kritéria, ale náhodně
 - Například na rozdíl od „horké brambory“, kde sice také není směrovací tabulka, ale nějaký princip ano
- Používá se v situacích kdy na rozhodování není čas / zdroje / důvod
 - Například při zahlcení směrovače toto zařízení typicky data zahazuje, s použitím náhodného směrování se počítá s dvojnásobným možným benefitem
 - Jednak i náhodně mohou trefit tu správnou cestu – šance není velká – podle počtu portů – ale je nějaká
 - I pokud netrefím správný směr, je pořád možné, že další směrovač na tom bude lépe a bude vědět kam data poslat
 - Takže sice o jeden či více kroků cestu prodloužím, ale zabráním ztrátě dat, timeoutu a znovu poslání
- Reálně se používá například v senzorických nebo bezdrátových sítích

Kategorizace směrování: Dle metod rozhodování: Isolované: Zpětné učení

- Zpětné učení - Backward learning
- Používá směrovací tabulku, kterou si postupně plní
 - Na počátku je prázdná – nepotřebuje počáteční informace
 - Pokud přijde paket od A pro B, poznačí si do směrovací tabulky cestu k A
 - Data mají jít k B, ale neví se kudy, takže není na výběr a data pošleme na všechny ostatní porty daného routeru
 - Použije se záplavové směrování jako „berlička“ k nalezení cesty, protože pokud existuje, záplavové směrování ji najde
 - Pokud data dorazí až do B a ten pošle odpověď – kam ví, protože to se naučil na základě příchozích dat – naučí se z odpovědi první router i cestu k B
- Výhodou je, že nepotřebuji žádnou výchozí konfiguraci
- Nevýhoda je dlouhá doba a režie na učení
 - Ta je o to horší, čím více se síť mění v čase
 - S počtem komunikujících stanic narůstá i délka tabulek, což také není žádoucí
- V reálu se nepoužívá na L3, ale používá se tento princip na L2 v Ethernetu
 - Pro mosty/přepínače kde data chodí jen ne konkrétní porty, na rozdíl od hubu

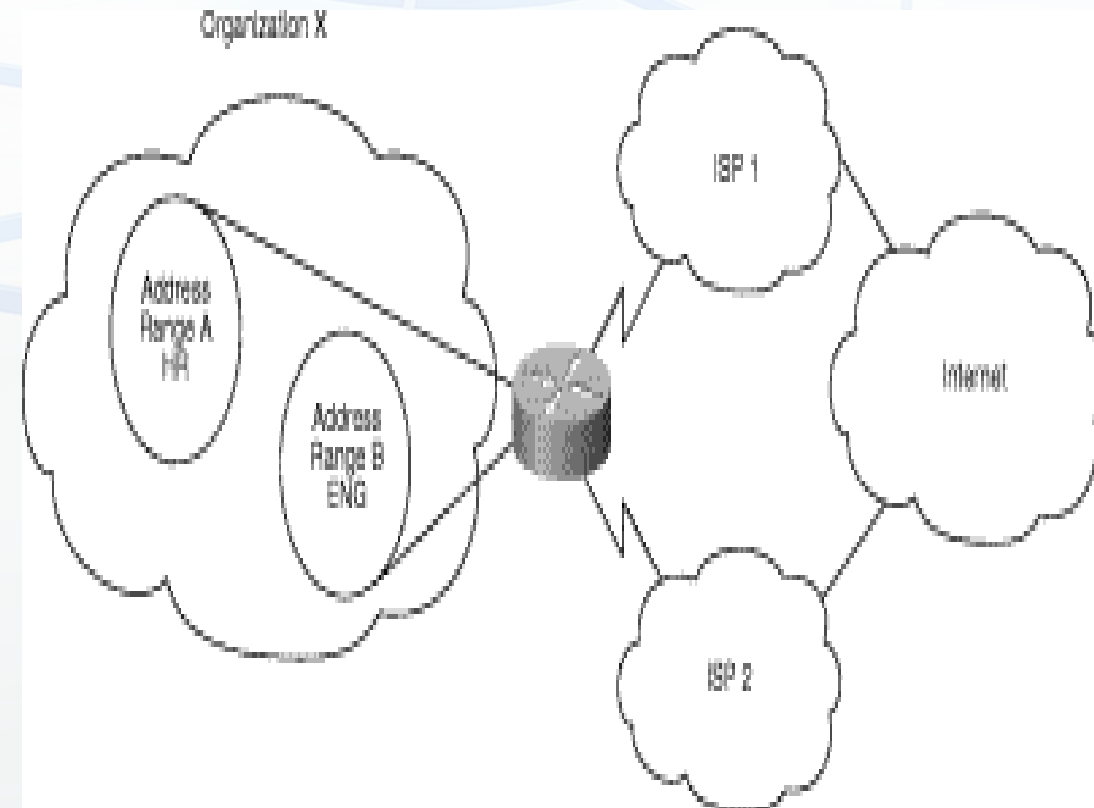


Kategorizace směrování: Dle metod rozhodování: Isolované: Source routing

- Směrování od zdroje – Source routing
- Kudy data půjdou určuje odesílatel tím, že tyté informace vloží do hlavičky paketu
 - Tedy ne jen adresa cíle, ale rovnou celá cesta
- Kudy mohou data jít odesílatel nejprve zjistí pomocí záplavového směrování
 - Drobné modifikace je v tom, že záplavově směrovaný paket do sebe uchovává informaci o uzlech kterými prošel
 - Až dojde k cíli použije tuto sekvenci k návratu a zároveň tím zjistil cestu
- V praxi se opět na L3 nepoužívá
 - Je nutná podpora na směrovačích
 - Má vysokou režii
- Používá se ale na L2 v rámci Token Ringu
- **POZOR – neplést se Source base routingem**

Kategorizace směrování: Dle metod rozhodování: Isoloované: Policy base routing

- Směrování podle pravidel – Policy base routing
- Varianta směrování dle „dalších pravidel“
 - Zdrojová adresa
 - Port / protokol
 - Metadata jako je typ paketu, jeho velikost atd.
- Běžně se nepoužívá kvůli vyšší režii, ale má své využití v krajních situacích
 - Například při použití více směrovacích tabulek v jednom stroji na základě adresy zdroje
- Typicky PBR má vyšší prioritu než běžné směrovací tabulky
- Příklad:
 - firma X má nařízeno, že provoz z rozsahu IP adres A, je směrováno přes ISP 1 a provoz z rozsahu IP adres B je směrováno přes ISP 2
 - Tohle běžným routingem řešit nejde, protože by se vždy použila výchozí brána => potřebujeme PBR kde podle pravidla testujícího zdrojovou adresu může použít jinou směrovací tabulku s jinou výchozí bránou



zdroj:

<http://www.cs.vsb.cz/grygarek/SPS/projekty0405/RouteOptimization/dokumentace/ar01s02.html>

Kategorizace směrování: Dle metod rozhodování: Distribuované

- Distribuované směrování není založené na samostatném směrování každého jednoho uzlu ani na jedné centrální autoritě, ale využívá společného algoritmu a předávání informací
- Jednotlivé uzly se vzájemně informují o dostupných sítích, o jejich parametrech atd. a na základě toho si každý uzel sestaví svoji směrovací tabulku
- Tyto algoritmy počítají se změnami v síti a informace průběžně nebo na základě změny aktualizují
 - Jedná se o adaptivní řešení
- Distribuované směrovací algoritmy dělí na :
 - Interní - IGP (Interior gateway protokol)
 - Distance vector protokoly
 - Link state
 - Externí - EGP (Exterior gateway protokol)
 - „Path vector“
- **POZOR: Dynamické směrovací protokoly provoz Nesměrují/Nepřenášejí data, ale jen plní směrovací tabulky, které se ke směrování následně používají**
- Z pohledu počítačové sítě se jedná o běžné aplikační protokoly

Kategorizace směrování: Dle metod rozhodování: Distribuované: Metrika

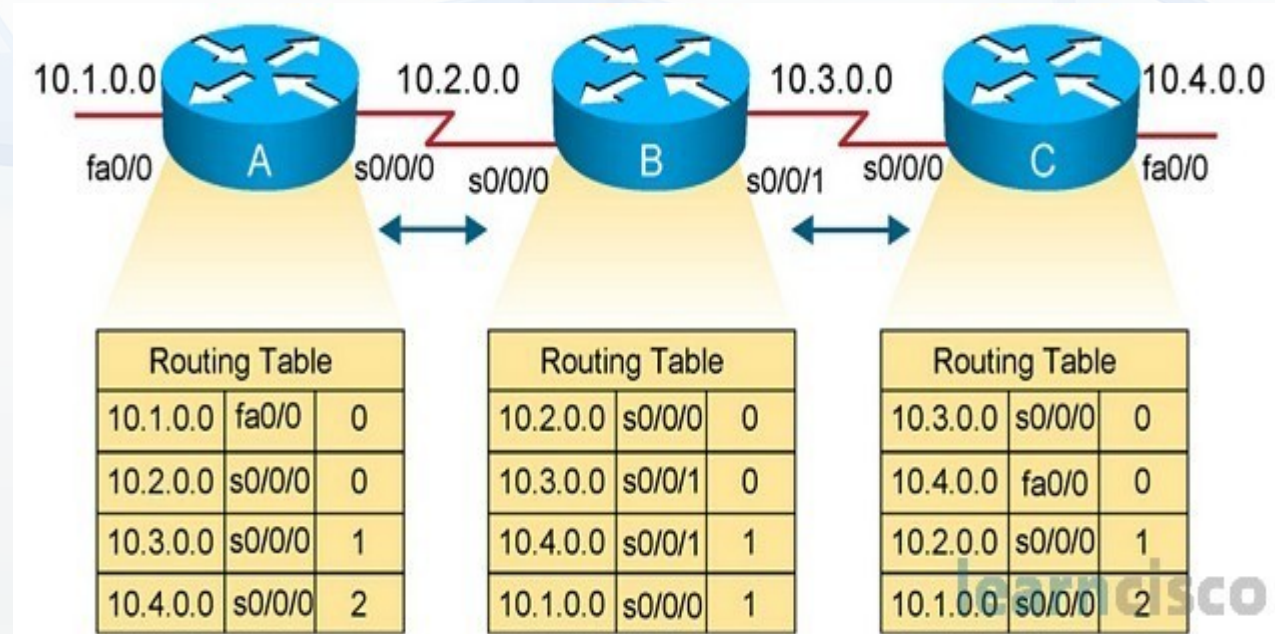
- Metrika je typicky číslo, které určuje „kvalitu“ dané cesty ve směrovací tabulce
- Pokladem pro metriku může být jedna nebo i více veličin
- Tři nejběžnější modely:
 - Distance vector – metrikou je délka vektoru vzdáleností
 - Tedy např. přes kolik dalších routerů musí paket projít aby došel k cíli
 - Link state – metrikou je cost/cena, která se typicky určuje na základě rychlosti linek, tedy šířky pásma
 - Path vector – obdobně jako u distance vector se hledá nejkratší cesta z pohledu skoků, ale ne po jednotlivých routerech, ale po jednotlivých autonomních oblastech
- Metrika se používá k rozhodnutí, kterou z násobných linek ve směrovací tabulce promítnout do forwardovací tabulky
- Podle konkrétního protokolu může hodnota metriky označovat i nedostupnou cestu
 - Pro Distance vector protokol RIP je to například 16
 - 16-ctý uzel se bere jako nekonečno – jako by tam už ani cesta nebyla

Kategorizace směrování: Dle metod rozhodování: Distribuované: IGP : Distance vector

- Distance vector protokoly – DVA nebo DVR
- Metrikou těchto protokolů je „vektor“ vzdáleností
 - Tedy např. počet mezilehlých směrovačů
- K vyhledávání používá Bellman-Fordův algoritmus
 - Hledání nejkratší cesty v ohodnoceném grafu
- Neberou v potaz reálné parametry linek, ale jen „vzdálenost“ v podobě počtu uzlů
 - Reálně tedy mohou data poslat kratší, ale mnohem pomalejší cestou
- Výhodou je snadné zjišťování „stavu sítě“, neboť se realizuje jen jako výměna informací mezi dvěma sousedy
 - Tedy mají je připojené nebo je dostaly od jiných sousedů
 - Není třeba linky proměřovat, tedy nebereme v potaz reálné parametry linek mezi uzly ani jejich zatížení
- Každý uzel má jen částečnou informaci o stavu celé sítě
- Problém nastává s timeouty u velkých sítí
 - Musí být zvolena hranice, kdy se další uzel za už považuje za nedostupný
 - Velikost sítí je tak reálně omezena dostupným počtem směrovačů v řadě
- DVA algoritmy pomalu konvergují
 - Informace o výpadku se šíří pomalu, protože v každém kroku se informace výpadku předá jen sousedům

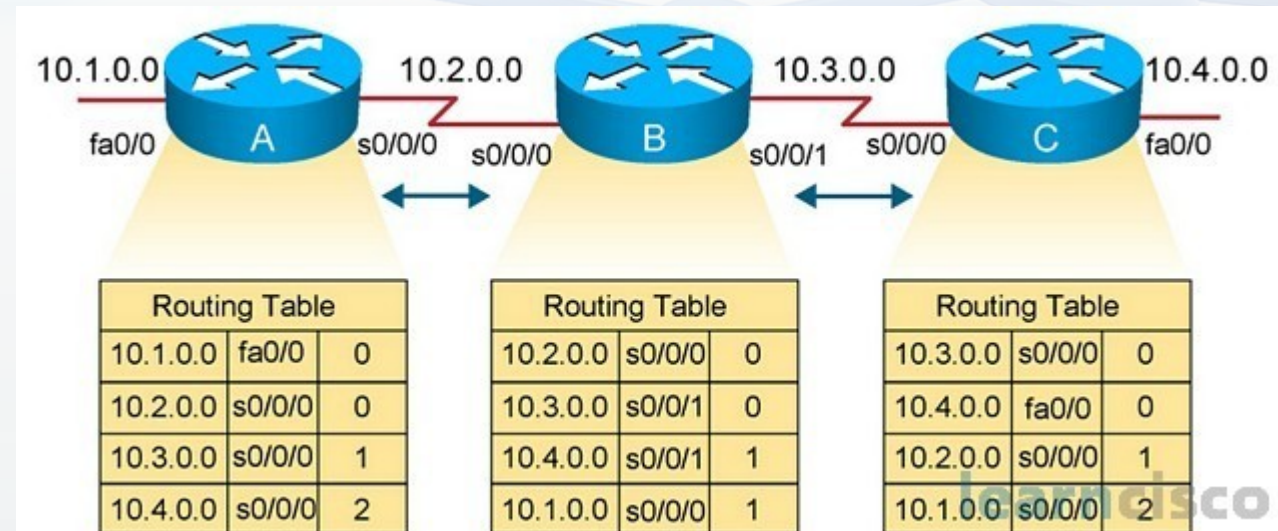
Kategorizace směrování: Dle metod rozhodování: Distribuované: IGP: Distance vector: Tvorba tabulky

- Postupná tvorba směrovací tabulky
 - V prvním kroku znám jen své připojení sítě, které inzeruji/posílám přímým sousedům
 - Pro A 10.1.0.0 a 10.2.0.0 s metrikou nula
 - Pro B 10.2.0.0 a 10.3.0.0 s metrikou nula
 - Pro C 10.3.0.0 a 10.4.0.0 s metrikou nula
 - V druhém kroku dostanu info od svých sousedů a ty doplním do své tabulky
 - Pro A
 - 10.1.0.0 a 10.2.0.0 s metrikou 0
 - 10.3.0.0 s metrikou 1 (od B)
 - Pro B
 - 10.2.0.0 a 10.3.0.0 s metrikou 0
 - 10.1.0.0 s metrikou 1 (od A)
 - 10.4.0.0 s metrikou 1 (od C)
 - Pro C
 - 10.3.0.0 a 10.4.0.0 s metrikou 0
 - 10.2.0.0 s metrikou 1 (od B)



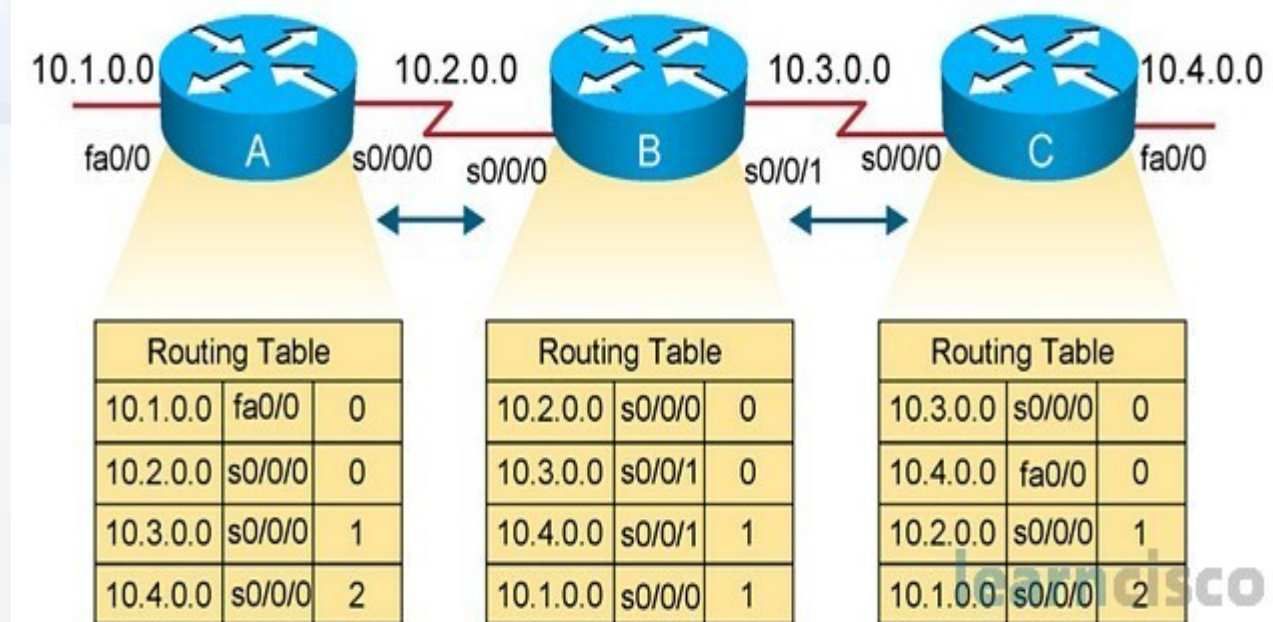
Kategorizace směrování: Dle metod rozhodování: Distribuované: IGP: Distance vector: Tvorba tabulky II.

- Postupná tvorba směrovací tabulky
 - V třetím kroku
 - Pro A
 - 10.1.0.0 a 10.2.0.0 s metrikou 0
 - 10.3.0.0 s metrikou 1 (od B)
 - 10.4.0.0 s metrikou 2 (od B, původně od C)
 - Pro B
 - 10.2.0.0 a 10.3.0.0 s metrikou 0
 - 10.1.0.0 s metrikou 1 (od A)
 - 10.4.0.0 s metrikou 1 (od C)
 - Pro C
 - 10.3.0.0 a 10.4.0.0 s metrikou 0
 - 10.2.0.0 s metrikou 1 (od B)
 - 10.1.0.0 s metrikou 2 (od B, původně od A)



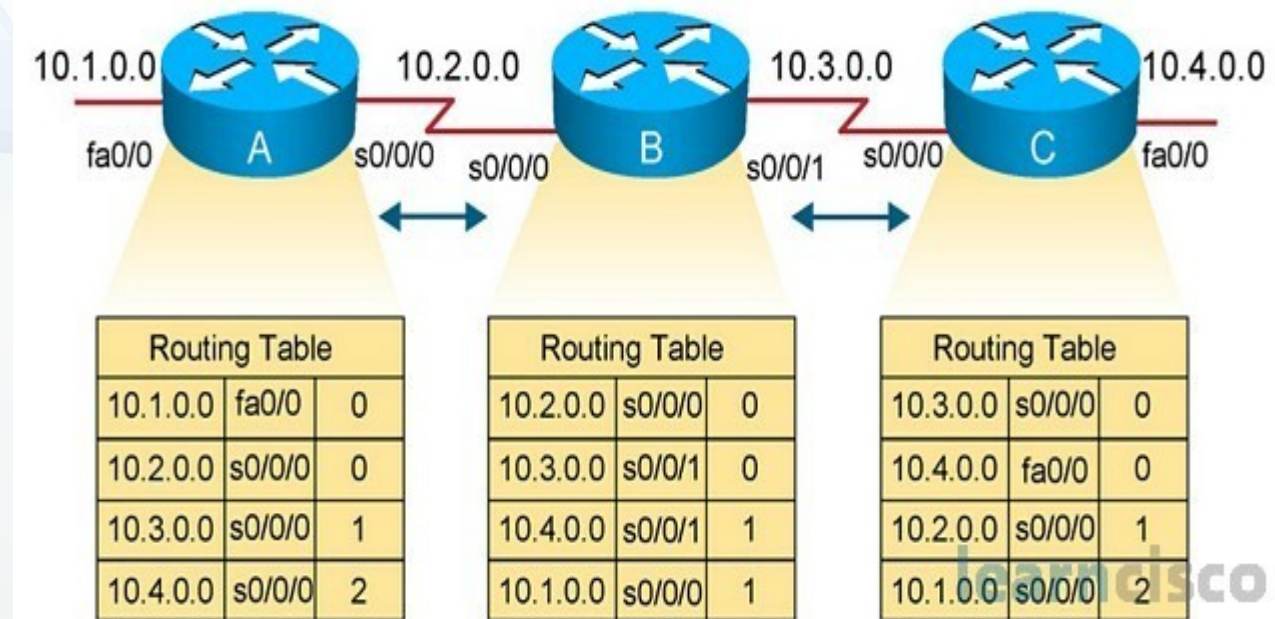
Kategorizace směrování: Dle metod rozhodování: Distribuované: IGP: Distance vector: Problém počítání do nekonečna

- Problém počítání do nekonečna – count of infinity
- Sousední routery si vyměňují informace včetně těch, které nejsou jejich lokální, ale naučily se je
- Problém nastává při výpadku, např. pro uzel A
 - Pokud je síť stabilní, má B dvě info k 10.1.0.0
 - Od A s cenou 1
 - Od C s cenou 2
 - Tu ale nepoužije, protože od A má lepší cenu
 - Pokud ale A vypadne, v B se použije cesta od C s hodnotou 2 a B si ji uloží s hodnotou 3 (2 od C + 1 cesta z B do C)
 - V dalším kroku C dostane info od B, že tuto síť umí s cenou 3 a upraví si svoji tabulku na 4 (3 od B + 1 na cestu z C do B)
 - A info zas pošle dále ...
 - Problémů je zde více
 - Tohle by nikdy neskončilo – můžeme vyřešit limitem – např 16 pro RIP
 - Celé šíření výpadku velice dlouho trvá



Kategorizace směrování: Dle metod rozhodování: Distribuované: IGP: Distance vector: Řešení problému počítání do nekonečna

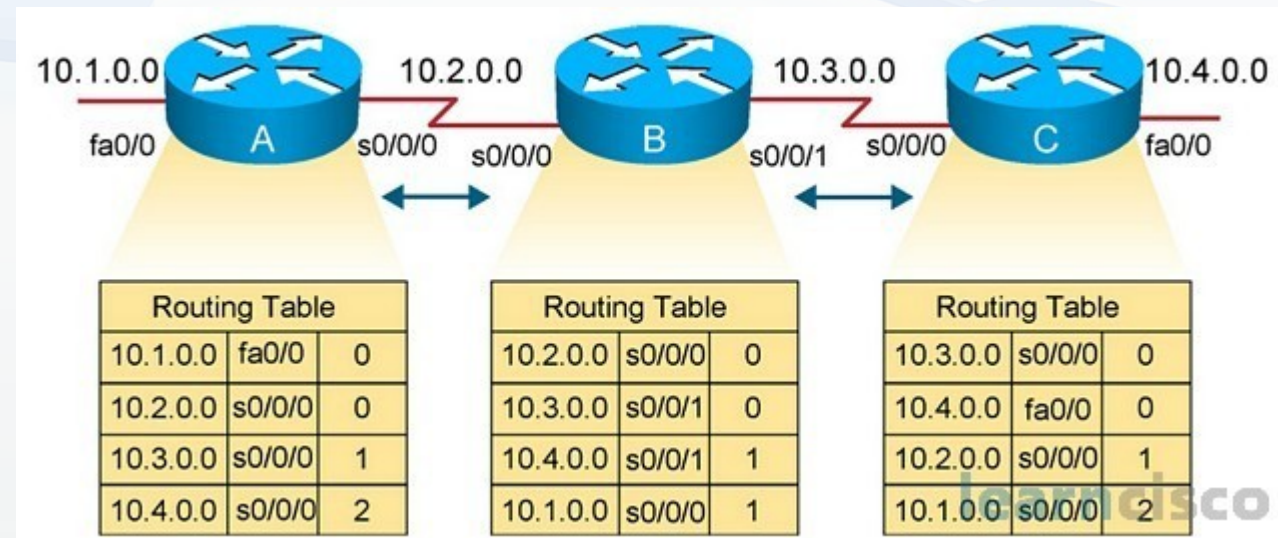
- Základní řešení se označuje jako „split horizon“ - rozštěpený horizont
 - Pokud se cestu do 10.1.0.0 dozví od B (jako uzel C), tak už ji zpět do B neinzeruji
 - Tedy pokud vypadne uzel A, cesta zmizí z B a v dalším kroku i z C
- Rozšířením „split horizon“ je „split horizon with poisoned reverse“
 - Rozštěpený horizont s otráveným zpětným kanálem
 - Já sice tu cestu zpět inzerovat budu, ale s hodnotou nekonečno
- Důsledkem obou metod je rychlejší šíření negativní informace – info o výpadku cesty
- Problém částečně zůstává, neboť nejde zabránit vzniku cyklů
 - Nevracím data zpět, ale pokračuji pořád dál jedním směrem
 - Možným řešením je neaktualizovat data ihned, ale počkat na info od dalších uzlů, ale to bude zpomalovat konvergenci
 - Řešením by byl triggered update – okamžitá informace o změně
 - Pokud jsem upravil svou tabulku IHNEED to info předám dále



zdroj: <https://www.learncisco.net/courses/icnd-1/ip-routing-technologies/enabling-rip.html>

Kategorizace směrování: Dle metod rozhodování: Distribuované: IGP: Distance vector: RIP

- Nejtypičtějším DVA protokolem je RIP
- Metrikou pro RIP je jen počet kroků k dosažení požadované sítě
 - Počet mezilehlých směrovačů
- Informaci o dostupných sítích rozesílá každý uzel každých 30s
 - Jedná se o vlastní směrovací tabulku složenou s lokálně připojených sítí a získaných informací
- Pokud nové info nepřijde od souseda déle než 180s, je prohlášen za mrtvého
- RIP pro komunikaci používá 520/UDP
 - Jako běžný aplikační protokol potřebuje přístup ve FW
- Používá „Split horizon with poisoned reverse“ a „Triggered update“
- Existují tři verze:
 - RIP 1
 - Původní verze, neřeší zabezpečení, pracuje jen s třídami adres
 - Podporuje 15 uzlů v řadě, 16-tý se rovná nekonečnu – nedostupný
 - Data posílá broadcastem
 - RIP 2
 - Rozšiřuje původní verzi o podporu CIDR – pracuje s maskami sítí
 - Data posílá multicastem
 - Zavádí autentizaci heslem
 - RIP ng (next generation)
 - Přináší podporu pro IPv6



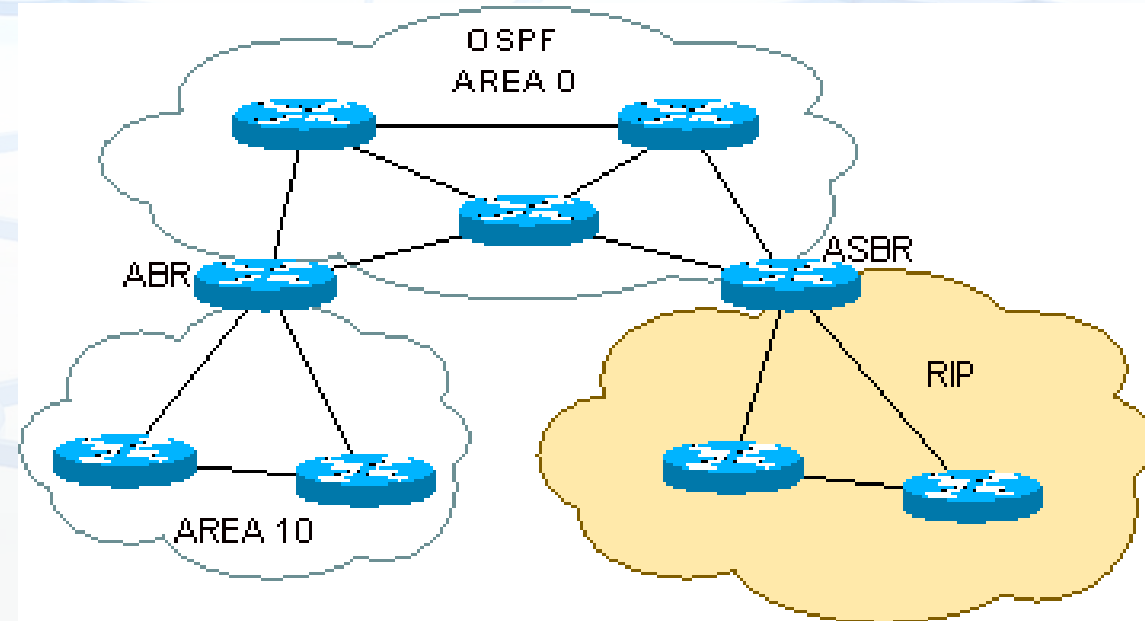
zdroj: <https://www.learncisco.net/courses/icnd-1/ip-routing-technologies/enabling-rip.html>

Kategorizace směrování: Dle metod rozhodování: Distribuované: IGP: Link state

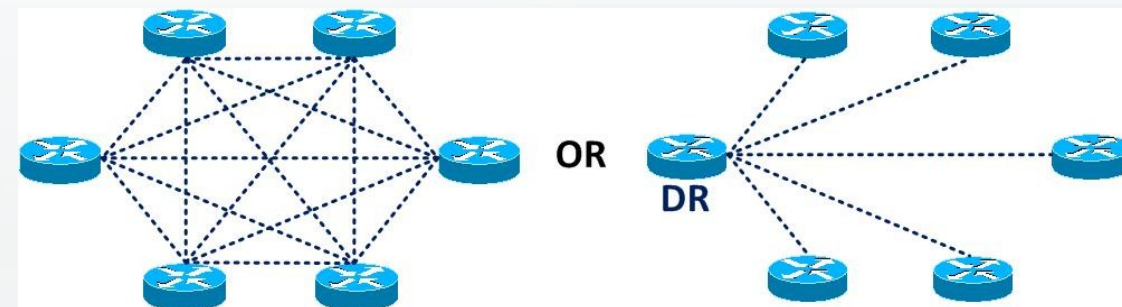
- Nedostatkem DVA je fakt, že nezohledňuje aktuální stav sítě ani její parametry
- Link state protokoly používají jako metriku cenu – cost, což je informace lince mezi uzly
 - Zda je linka 1Mbps, 10Mbps,
- Každý uzel cyklicky testuje dostupnost svých sousedů pomocí „Hello“ zpráv
 - Ví, že soused žije a ví jak „rychlá“ k němu vede linka
- Každý uzel šíří všem ostatním uzlům informace, které má
 - Zásadní rozdíl proti DVA – info už nepředávám jen sousedům, ale VŠEM
- Jednotlivé uzly si sami vypočítávají směrovací informace
 - Dostávám info od všech, takže vím o stavu celé sítě
 - Pokud jeden uzel udělá chybu ve výpočtu neovlivní to další uzly
 - Používá se Dijkstrův algoritmus
- Informace o stavu linek – Link State pakety - LSP
 - Informace se musejí rozesílat při změně, ale VŠEM uzlům
 - Novou informaci mají všechny uzly v prvním kroku, což výrazně urychluje konvergenci oproti DVA
 - Informace se může rozesílat i periodicky, ale spíše pro osvěžení informací a za delší dobu než u DVA
 - Například jen jednou za 30min
 - Uzel, který přijme LSP, jej pošle všem sousedům, kromě toho od koho info dostal
 - V rámci LSP je identifikace verze – pokud přijmu LSP se starší verzí zahodím jej
 - Přenos LSP je spolehlivý
 - Využívá potvrzení doručení, timeouty a případné opakování zaslání informace
- Ve výsledku má LSA menší režii než DVA v závislosti na počtu uzlů a proto se lépe hodí do rozsáhlejších sítí
- LSA rychleji konverguje a neobsahuje problém počítání do nekonečna

Kategorizace směrování: Dle metod rozhodování: Distribuované: IGP: Link state: OSPF

- Dnes nejběžnější představil LSA protokolů
- Používá Dijkstrův algoritmus
- Cyklicky posílá sousedům Hello pakety pro zjištění jejich stavu
 - A díky tomu může detekovat změny, kde info o změně pak posílá všem
 - Posílá se každých 10s a posílá se přes multicast
 - Pokud do 40s neobdržím Hello, prohlásím souseda za mrtvého
- Podporuje autentizaci a sumarizaci
- Pro velké sítě zavádí dělení na subsítě – area
 - Základní je Area0, ke které jsou připojeny další oblasti AreaX
 - Komunikaci mezi oblastmi zajišťují ABR směrovače
 - Mají přístup do obou sítí
 - Předávají JEN sumarizované informace z dané sítě, ne celou topologii
 - Existují ještě ASBR směrovače, které jsou pouze transportní
 - Umožňují importovat routy z jiných systémů jako je např RIP
- Pro broadcastové sítě zavádí tři stavy routerů
 - DR - Designed router - pověřený router
 - Je volen na základě konfigurační konstanty a MAC adresy
 - BDR - Backup Designed router - záložní pověřený router
 - DRO - ostatní routery, které se připojují k DR nebo BDR
 - Komunikace pak není každý s každým, čímž se šetří přenosy a zrychluje konvergence



zdroj: <http://www.cs.vsb.cz/grygarek/SPS/lect/OSPF/ospf.html>



zdroj: <https://jjrinehart.wordpress.com/2012/07/30/ospf-iv-there-is-no-i-in-team-more-about-drs/>

Kategorizace směrování: Dle metod rozhodování: Distribuované: IGP: Link state: OSPF: Cena linek

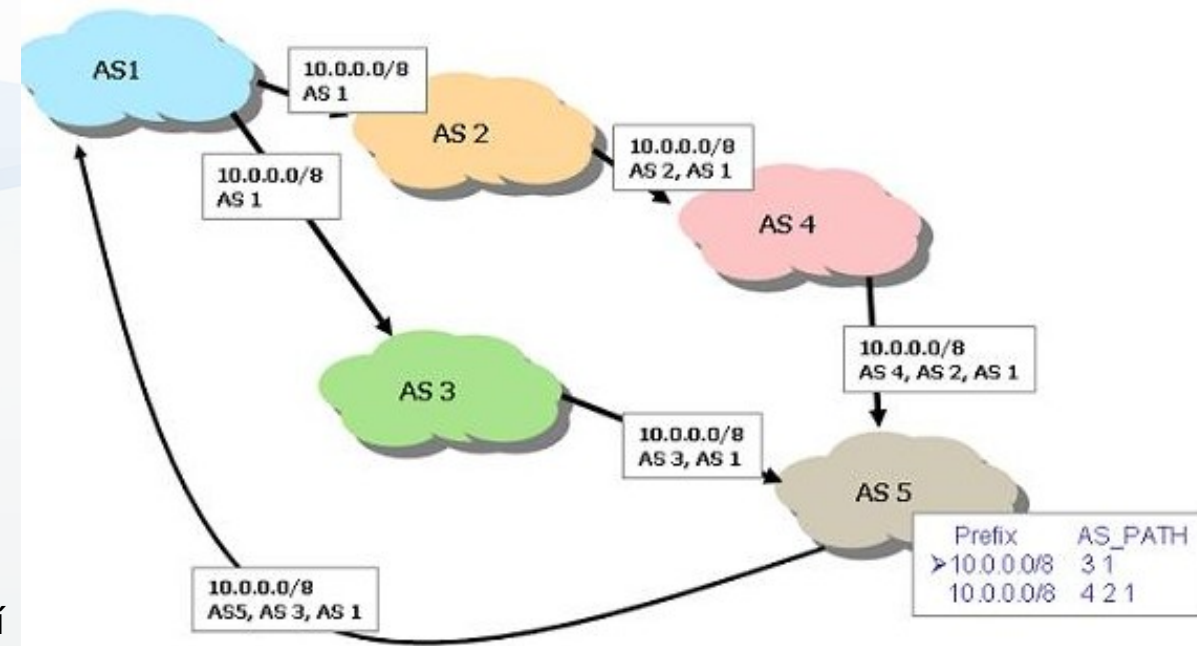
- Výchozí cena linky v OSPF je
 - $\text{Cena} = 100.000.000 / \text{bandwidth}$
 - Tedy reference k 100Mbps – vychází z historie, když se 100Mbps bral jako maximální možná hodnota
- Zde vzniká problém, protože od 100Mbps výše bude cena linek 1
 - Ale to neodpovídá, protože 100Mbps není stejný jako 10Gbps
- V routerech jsou dvě možnosti řešení
 - Upravit referenční hodnotu výpočtu
 - Pro cisco např `ospf auto-cost reference-bandwidth XXX`
 - Nastavit cenu linky ručně
 - Pokud se například jedná jen o jednu linku v systému
 - Např pro cisco `ip ospf cost XX`

Auto-Cost Reference-Bandwidth 1000

Interface Type	Cost Value
10 Gigabit Ethernet (10 Gbps)	1
Gigabit Ethernet (1 Gbps)	1
Fast Ethernet (100 Mbps)	10
Ethernet (10 Mbps)	100
Serial (1.544 Mbps)	647
Serial (128 Kbps)	7812
Serial (64 Kbps)	15625

Kategorizace směrování: Dle metod rozhodování: Distribuované: EGP: Path Vector

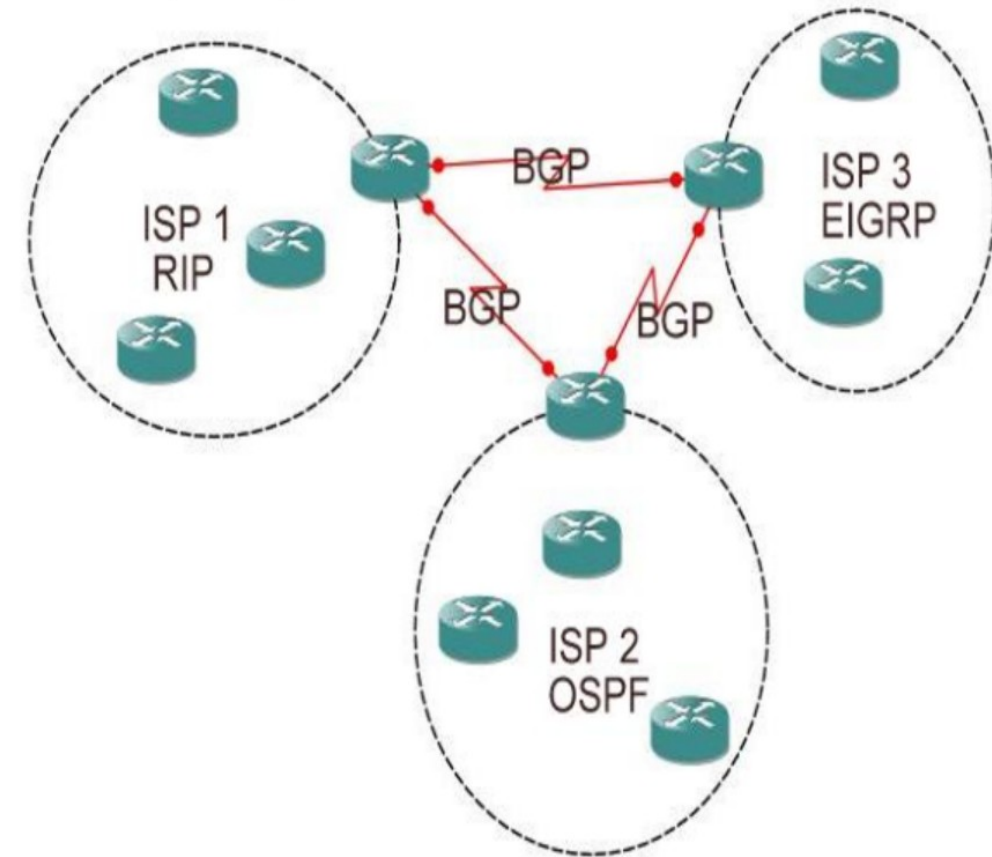
- Path vector se používá v externích dynamických směrovacích protokolech
- Kromě informace o cílové síti obsahuje
 - Router pomocí kterého je dostupný
 - Celou cestu k cílové síti
 - Cesta je definovaná jako seznam autonomních oblastí
- Někdy je zařazován mezi Distance vector protokoly
- Autonomní systém - AS
 - Samostatně spravovaná oblast s vlastním identifikátorem
 - Samostatná směrovací doména
 - Co se děje uvnitř se neprojevuje nahodile navenek, ale jen prostřednictvím hraničního uzlu, který předává informace
 - V každé AS (nebo také někdy area) může být použito jiné směrování
 - Směrování mezi AS zajišťují EGP protokoly – například BGP



zdroj: <https://bethepacketsite.wordpress.com/2016/04/20/dynamic-routing-path-vector/>

Kategorizace směrování: Dle metod rozhodování: Distribuované: EGP: Path Vector: BGP

- BGP – Border gateway protokol
- Nejpoužívanější představit EGP
- Používá Path-vector
- Podporuje autentizaci
- Komunikuje pomocí 179/TCP
- Na rozdíl od IGP protokolů BGP nehledá sousedy, ale má je zadané
 - Bavíme se o propojení AS/ISP, tedy typicky point-to-point spoje – hledání nemá smysl
- Používá hledání nejkratší cesty, kde nejkratší je ta, která prochází přes co nejméně AS
 - Ceny jednotlivých cest je také možné doplnit o statické části ceny – konstanty
 - To je pro EGP nesmírně důležité, protože se zde typicky řeší násobné spoje a s ohledem na jejich ceny je nutné mít možnost preference
- Při navázání spojení se sousedem jsou nejprve vyměněny všechny směrovací informace
- V dalším kroku už se posílají jen změny – šetříme přenos
- Cyklicky se kontroluje, zda všichni sousedi žijí
 - Typicky 1x za minutu



zdroj: <https://www.semanticscholar.org/paper/BIGP-a-new-single-protocol-that-can-work-as-an-igp-Gupta/20bd5da8b6a4dfa2ea862f096953e2ce2d9a373b>

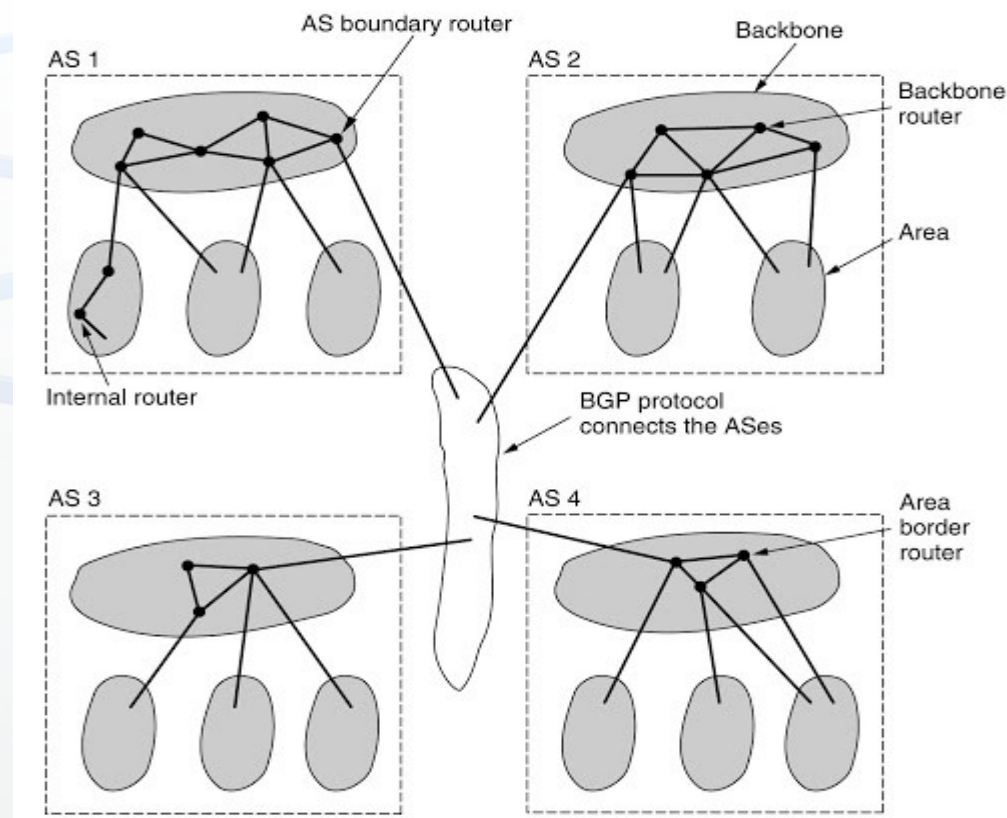
Kategorizace směrování: Dle metod rozhodování: Distribuované: EGP: Path Vector: BGP: Metrika

- Metrika u BGP není tak jednoduchá / jednoznačná jako u IGP protokolů, kde hledáme jen nejlepší cestu v rámci jednoho organizačního celku
- BGP směruje provoz mezi ISP / či přes ně a v tu chvíli hrají roli i další faktory:
 - Ceny linek / Ceny přenosů
 - Obchodní podmínky / vztahy jednotlivých ISP
- Parametrů je více – viz tabulka a mají různou váhu a dosah
 - Část parametrů zůstává jen v AS a k dalším ISP se nepřenáší
 - Část parametrů se exportuje jako preference i mimo AS
 - Weight – jen v routeru – lokální
 - Local_preference – v rámci AS
 - Med – exportované mezi AS

Priority	Attribute
1	Weight
2	Local Preference
3	Originate
4	AS path length
5	Origin code
6	MED
7	eBGP path over iBGP path
8	Shortest IGP path to BGP next hop
9	Oldest path
10	Router ID
11	Neighbor IP address

Kategorizace směrování: Dle metod rozhodování: Hierarchické směrování

- Hierarchické směrování se snaží řešit problematiku rozsáhlých sítí
 - V rozsáhlých sítích vzniká problém s rychlostí konvergence
 - Příliš dlouho trvá, než se nová informace dostane všude
 - Vzniká problém zatížení sítě obslužným provozem
 - Čím více routeru v jedné síti, tím více komunikace mezi nimi
- Řešením je rozdělit síť na více malých oblastí v a směrování řešit samostatně
 - Uvnitř dané oblasti
 - Nazývané směrovací doména / Area / Autonomní systém
 - Protokoly IGP
 - Externě mezi jednotlivými oblastmi
 - Protokoly EGP
- Historicky musely jednotlivé oblasti opravdu tvořit hierarchii
 - Počítalo se s páteřní oblastí na kterou se ostatní připojí – jako např v OSPF
 - Dnes už to není nutné a jednotlivé AS mohou být na stejné úrovni



zdroj: <https://lh3.googleusercontent.com/proxy/fWaDz-xR3WchuzrSYqH6xNaI49OxF15mYi7-sX6k98b2YFbAr3sdLjtQhQkG3XnkJK-NL4VljlentLgcnNwQM1Ae0y1WlVLMV50yopELdGlqLDvR8co>

Kategorizace směrování: Dle metod rozhodování: Hierarchické směrování: Peering

- Peering je vzájemné propojení jednotlivých ISP
 - Tedy propojení jednotlivých AS
- Peering je možné realizovat dvojím způsobem
 - Na přímo
 - Nejjednodušší cesta – dva ISP se dohodnou, udělají mezi sebou propoj a nastaví směrování kde si mezi sebou propagují informace o svých sítích
 - Problém je, že nemůžeme propojit na přímo všechny sítě
 - Pomocí peering centra
 - Více ISP se dohodne na spolupráce a společném „bodě“ kde bude docházet ke společnému propojení – peerigový uzel
 - Peeringové centrum je typicky hrazeno z členských poplatků
 - Je zde společný zájem na fungování
 - Fungování není levné protože zde tečou obrovská data
 - Jedná se citlivý bod z hlediska bezpečnosti
 - Cena za členství není malá a jednotliví partneři se mohou propojovat vzájemně na přímo
 - Ať už jako primární nebo jako záložní řešení
- Propojení je možné na více úrovních, u nás se typicky řeší čtyři možnosti
 - NIX – české peeringové centrum
 - SIX – propojení na slovenská peeringové centrum
 - Transit – zahraniční konektivita
 - Přímé propojení ISP
- Ceny za jednotlivé přenosy a stejně tak parametry linek v jednotlivých propojích jsou různé a je nutné je hlídat
 - Protože pokud například tečou dlouhodobě data k českému partnerovi pomocí zahraniční konektivity bude to velice drahé

