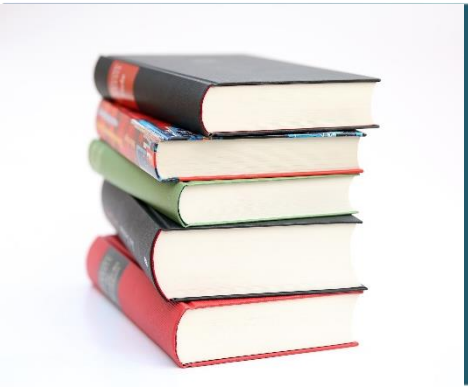
Dynamické smerovanie

SN (ccna3) – Chapter 5, CCNA, v6

Katedra informačných sietí

Fakulta riadenia a informatiky, ŽU

KIS FRI UNIZA – Vytvorené v rámci projektu KEGA 011STU - 4/2017.



Čo nás dnes čaká…

- Opakovanie
  - Čo je to smerovanie
    - IP adresy, maska a smerovacia tabuľka
  - Statické smerovanie
- Dynamické smerovanie:
  - Charakteristiky dynamických smerovacích protokolov
    - Oblasť nasadenia, algoritmus, metrika, správanie (Classfull/classless, sumarizácia)
  - Princíp distance-vector (DV) protokolov
  - Princíp link-state (LS) protokolov

Čo je smerovanie v IP sieťach?

- **Smerovanie**
  - Je proces zisťovania a výberu ďalšej cesty pre paket smerom k cieľu na základe cieľovej IP adresy v hlavičke smerovaného paketu a lokálnych znalosti smerovača o cieľových sieťach

Čo je sieťová IP adresa?

- IP adresa = logická adresa sieťového rozhrania
  - V IPv4 má každé sieťové rozhranie samostatnú adresu
    - Zariadenie má toľko adries, koľkými rozhraniami komunikuje
  - V IPv6 jednu a viac (globálnu, lokálnu, multicast)
- IP adresa je rôzne dlhá
  - IPv4 adresa: 4B, zapísané ako štyri oktety oddelené bodkou
  - IPv6 adresa: 16B, zapísane ako osem hextetov oddelených dvojbodkou
- Každá sieťová adresa (IPv4 aj IPv6) má dve časti:
  - **Identifikátor siete** (predčíslie, prefix, network part, net ID)
  - **Identifikátor počítača v danej sieti** (číslo, host part, host ID)
    - Prirodzená analógia s inými hierarchicky štruktúrovanými číslami, napr. PSČ alebo telefónnymi číslami
- Smerovanie v ľubovoľnom L3 protokole sa zaoberá identifikátormi sietí (**predčísliami**)
  - Pre smerovanie nie je číslo konkrétneho počítača zaujímavé:
    - ak sme dopravili paket na okraj cieľovej siete, o zvyšok sa postará L2 (susedné stanice)

Ako zistiť predčíslie siete (identifikátor siete) z IP adresy?

- Viaceré spôsoby, ako z IPv4 adresy zistiť predčíslie:
  - Prvý prístup: prvý oktet je predčíslie, zvyšok je číslo počítača
  - Druhý prístup: triedy IP adries (A, B, C, D, E)
  - Tretí prístup: zavedenie sieťovej masky (CIDR, VLSM) lebo veľkosť predčíslia siete v moderných IP sieťach je premenlivá
    - Platný aj pre IPv6

- Keďže veľkosti predčíslí sú premenlivé, zaviedol sa pojem „*adresa siete*“, ktorá má vždy rovnakú dĺžku
  - IPv4=4B or IPv6=16B
  - **Adresa siete =** Predčíslie siete doplnené nulami na veľkosť IP adresy
    - Adresa siete: numericky najnižšie číslo s daným predčíslím
- Ako zistiť z IP adresy premenlivú IP adresu siete?
  - Zavedenie IP (Sub)Sieťovej masky, 32 bit pre IPv4, 128bit pre IPv6
    - Ak je n-ty bit v maske nastavený na
      - 1: n-ty bit v IP adrese patrí do predčíslia
      - 0: n-ty bit v IP adrese patrí do čísla stanice
  - A binárnej AND operácie masky s IP adresou

Príklad

- **Príklad 1:** 158.193.138.40 AND255.255.255.0

158	193	138	40
10011110	11000001	10001010	00101000
11111111	11111111	11111111	00000000

- **Príklad 2:** 158.193.138.40 AND 255.255.255.224 = 158.193.138.32
  - Hranice medzi predčíslím siete a číslom počítača nemusia byť na hraniciach bajtov
  - Výsledné IP čísla sietí *nemusia* po prepočte do desiatkovej sústavy končiť 0

10011110	11000001	10001010	00101000
11111111	11111111	11111111	11100000
10011110	11000001	10001010	00100000

Lokálne znalosti smerovača

- Zoznamy cieľových sietí => tie ktoré smerovač pozná, si uchováva v **smerovacej tabuľke**
  - Vo forme smerovacích informácií (položiek)
    - Cieľová sieť a jej maska
    - AD a metrika
    - IP adresa ďalšieho smerovača (next hop) na ceste
    - Ďalšie informácie o položke
  - Smerovacia tabuľka je interne (nie vo výpise show ip route) usporiadaná podľa stĺpca „Maska siete“ *zostupne* od záznamov s najväčšími maskami po najmenšie
    - T.j. od najkonkrétnejších položiek k všeobecným
      - Default route je najvšeobecnejší záznam
    - Dôvod usporiadania? Zrýchlenia prehľadávania pri smerovaní

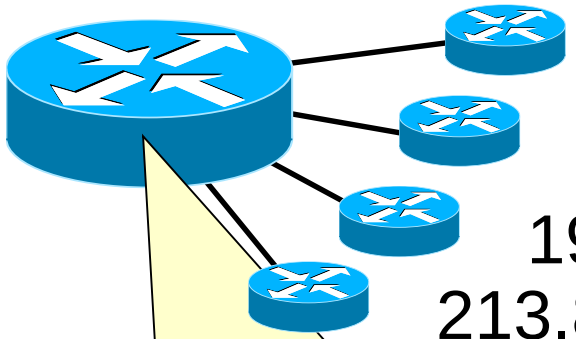
```
show ip route
 <output omitted>
 Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 4 subnets
R       172.16.1.0 [120/1] via 172.16.2.1, 00:00:00, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

Čo sa deje pri smerovaní?

- Smerovanie
  - Je proces zisťovania a výberu ďalšej cesty pre paket smerom k cieľu na základe cieľovej IP adresy v hlavičke smerovaného paketu a lokálnych znalosti smerovača o cieľových sieťach
- Pri smerovaní (výbere cesty) paketu smerovač
  - Vyberie z paketu cieľovú IP adresu
  - Riadok po riadku prechádza smerovacou tabuľkou, realizuje binárne AND medzi cieľovou IP adresou a maskou z riadka tabuľky a výsledok porovnáva s adresou siete v tomto riadku
  - Pri prvej zhode odošle paket príslušnému susednému smerovaču
    - Tzv. longest prefix match
- Treba mať na pamäti, že pri výbere cesty:
  - Smerovač sa rozhoduje sám pre seba
  - Rozhodovanie sa opakuje na každom smerovači nezávisle
  - Rozhodnutie o ceste v jednom smere nič nehovorí o ceste nazad

Činnosť IP smerovačov – príklad



62.30.100.200

120.11.40.3

193.87.55.4

213.81.21.2

Cieľ paketu: 213.81.187.59

213.81.187.59 & 255.255.255.248 =
213.81.187.56 ☹

213.81.187.59 & 255.255.255.240 =
213.81.187.32 ☹

213.81.187.59 & 255.255.0.0 =
213.81.0.0 ☹

213.81.187.59 & 0.0.0.0 =
0.0.0.0 ➔ NH 213.81.21.2

Maska	Cieľová sieť	Next hop
255.255.255.248	87.197.31.40	62.30.100.200
255.255.255.240	193.87.160.0	120.11.40.3
255.255.0.0	158.193.0.0	193.87.55.4
0.0.0.0	0.0.0.0	213.81.21.2

Budovanie smerovacej tabuľky

- Smerovač je zodpovedný za to, aby poznal cieľové siete a ďalší smerovač na ceste do nich
  - Smerovač defaultne vie len o priamo pripojených sieťach
- Ak má smerovač doručovať pakety do sietí, ktoré nie sú priamo pripojené, musia byť ich adresy do smerovacej tabuľky pridané istým procesom
  - O vzdialených sieťach sa musí „nejako“ dozvedieť „z vonku“

- Tieto informácie môže smerovač získať
  - **Staticky**
    - Budovaná a udržovaná manuálnym pridávaním statických smerovacích ciest administrátorom siete
  - **Dynamicky**
    - Budovaná a aktualizovaná použitím dynamických smerovacích protokolo

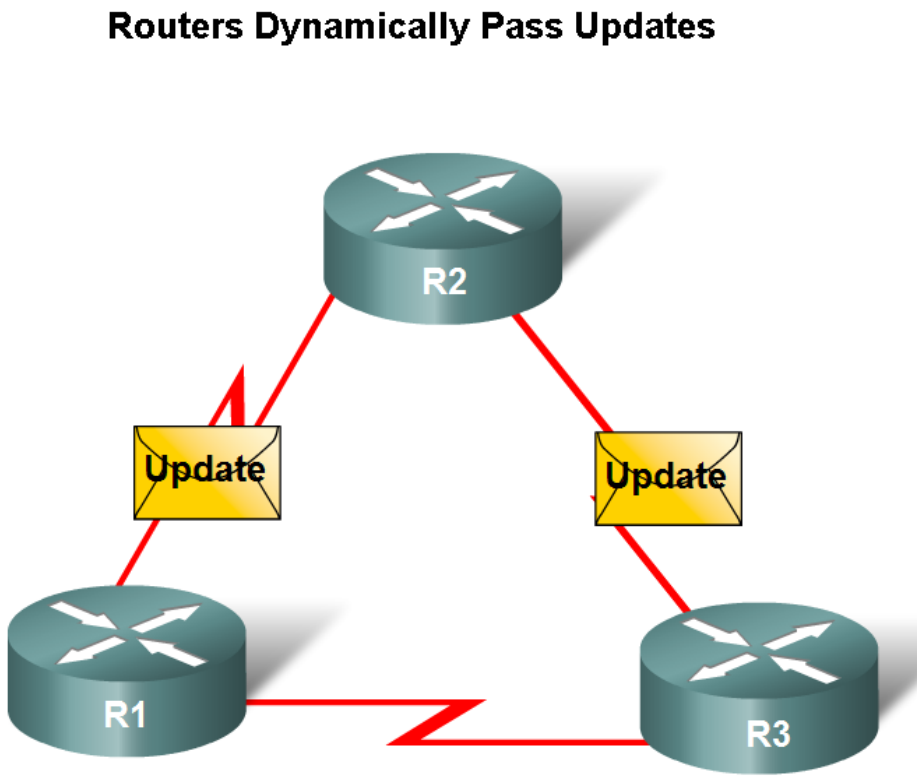
Statické smerovanie

Výhody	Nevýhody
Jednoduchá implementácia v malej sieti.	Je ich nutné vkladať ručne na každý smerovač Za ich správnosť a aktuálnosť zodpovedá administrátor.
Bezpečné. Smerovače si neposielajú žiadne správy ako pri dynamickom smerovaní.	Iba pre jednoduché topológie, alebo ako default static route. Ak topológia narastie, zväčší sa aj zložitosť konfigurácie
Cesta do cieľa je stále rovnaká.	Neprispôsobujú sa aktuálnemu stavu siete. Pri zmene ak je potrebné presmerovať prevádzku, treba manuálne prekonfigurovať.
Nespôsobujú však dodatočnú záťaž pre smerovače nakoľko nevyžaduje žiadne extra zdroje (CPU, RAM)	

+ -

Dynamické smerovacie protokoly

- Dynamické smerovacie protokoly sú mechanizmy pre automatizované napĺňanie obsahu smerovacej tabuľky
  - Po úvodnej konfigurácii pracujú samočinne
  - Pri objavovaní vzdialených sietí smerovače vzájomne spolupracujú
  - Ku každej objavenej vzdialenej sieti vedia určiť najlepšiu (najkratšiu) cestu do nej
  - Zabezpečujú, že smerovacie tabuľky všetkých smerovačov vždy obsahujú aktuálne informácie
  - Automaticky sa prispôsobujú všetkým zmenám v sieti ak súčasná najkratšia cesta prestane byť použiteľná
  - Predstavujú dodatočnú činnosť, ktorú smerovače musia vykonávať, a teda aj dodatočnú spotrebu ich systémových prostriedkov

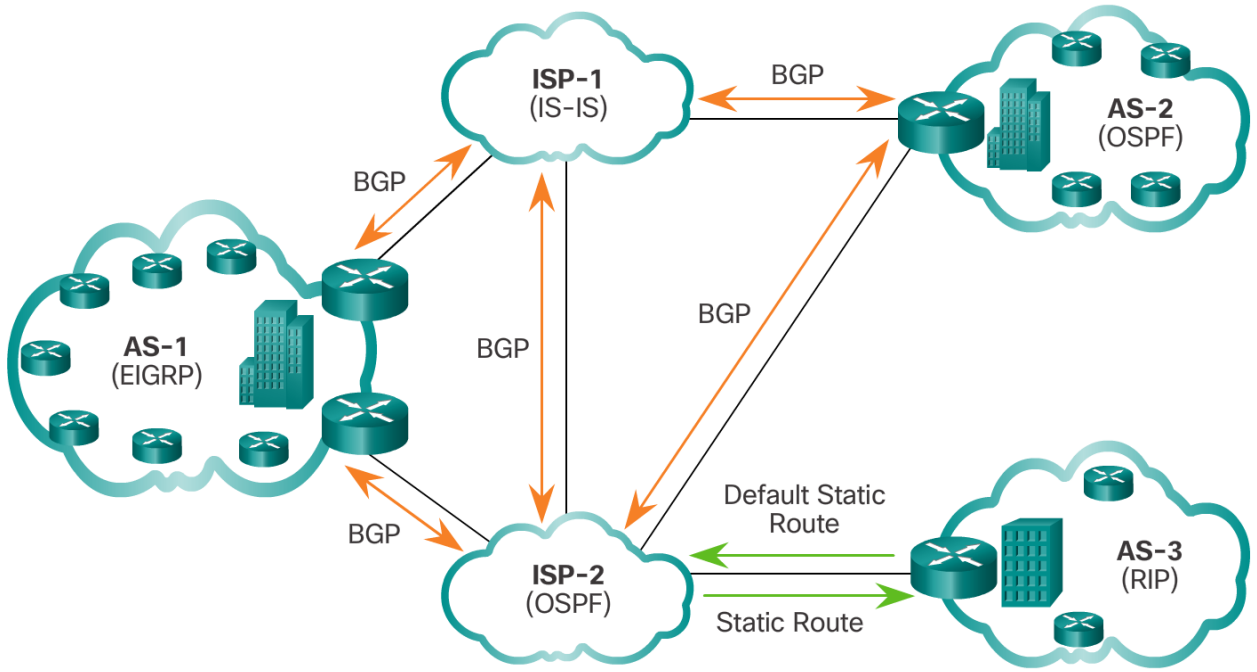


Charateristiky dynamických smerovacích protokolov

- Existuje viacero dynamických smerovacích protokolov
- Každý z nich má svoje charakteristické vlastnosti:
  - Oblasť či účel nasadenia
    - Smerovanie v sieti jedného vlastníka (IGP), smerovanie medzi sieťami rôznych vlastníkov (EGP)
  - Princíp činnosti (Typ algoritmu)
    - Distance-vector, Link-state, Path-vector
  - Správanie
    - Metrika (Ohodnotenie cesty)
      - Počet hopov, výhodnosť na základe rýchlosti, spoľahlivosť, oneskorenie, záťaž...
    - Práca s adresami a maskami
      - Classful a classless, sumarizácia
  - Škálovateľnosť
    - Správy, posielanie aktualizácií, rýchlosť reakcie na zmeny a konvergencia, počet ciest, nároky na CPU a pamäť, apod..

Oblasť nasadenia - IGP verzus EGP

- Autonómny systém (AS) je skupina sietí a smerovačov, ktorá používajú spoločnú smerovaciu politiku a patria pod spoločnú administratívnu doménu
- **Oblasť nasadenia**
  - **Interior gateway protocol (IGP)**
    - Smerovací protokol pracujúci vo vnútri Autonomous System (AS).
      - Napr. RIP, OSPF, a EIGRP
  - **Exterior gateway protocol (EGP)**
    - Smerovací protokol pracujúci medzi rôznymi AS
    - BGP je tzv. interdomain routing protocol (IDRP) a je aj EGP



Smerovacie protokoly podľa typu algoritmu

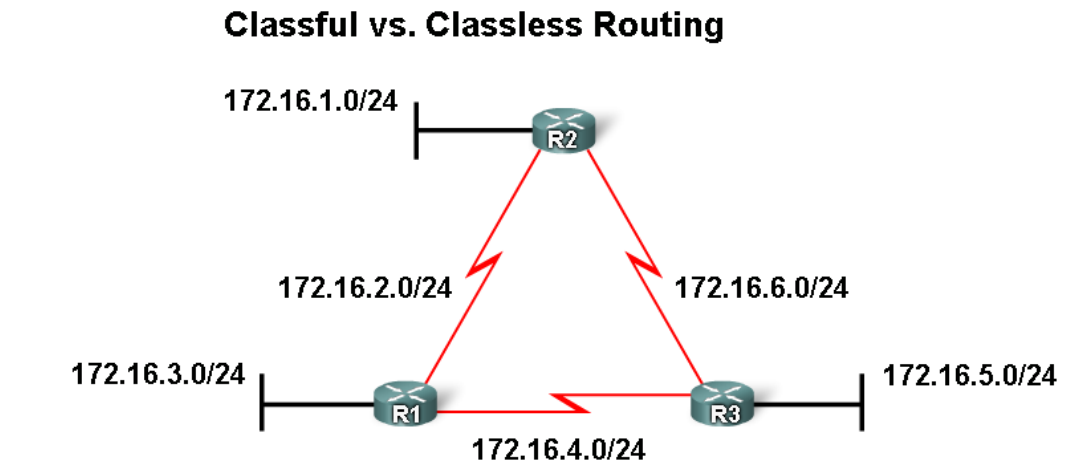
- Princípy smerovacích algoritmov:
  - Distance-Vector (RIPv1/RIPv2/RIPng, EIGRP)
    - Smerovače si vymieňajú zoznam cieľových sietí a svojich najlepších vzdialeností do nich
    - Správy: vektory (t.j. polia) vzdialeností
  - Link-State (OSPF, IS-IS)
    - Smerovače si vymieňajú informácie pre vytvorenie grafovej reprezentácie siete
    - Správy: popisy prepojov
  - Path-Vector (BGP)
    - Smerovače si vymieňajú zoznam cieľových sietí a popis cesty od seba do cieľovej siete (napr. zoznam tranzitných AS)
    - Správy: vektory (t.j. polia) atribútov

Metriky v smerovacích protokoloch

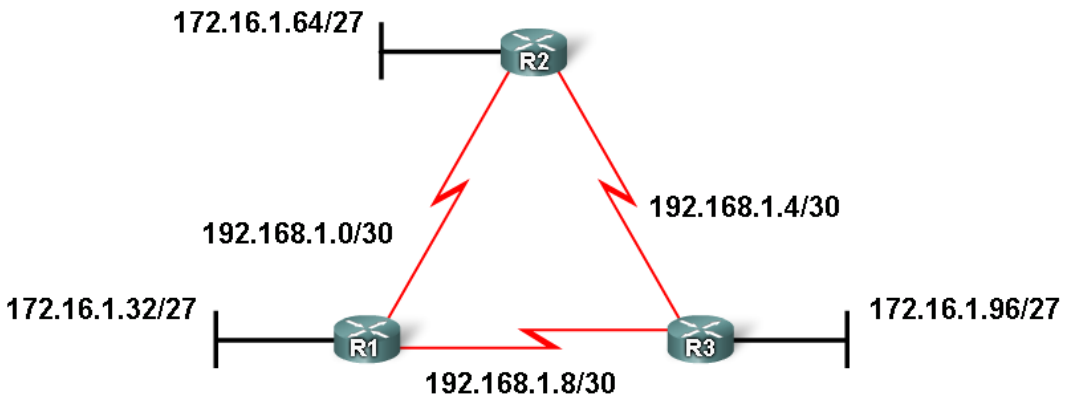
- „Metrika“ predstavuje ohodnotenie cesty do cieľovej siete
  - Ak existuje do cieľovej siete viacero ciest, smerovací protokol vyberie cestu s najnižšou metrikou
- Rôzne smerovacie protokoly používajú rôzne metriky (ohodnotenia cesty)
  - Rýchlosť, Oneskorenie, Spoľahlivosť, Aktuálna záťaž, Počet smerovačov (hopov)
- Smerovacie protokoly z pohľadu použitej metriky:
  - Protokoly pracujúce s jedným typom metriky
    - RIP/RIPv2/RIPng: hops
    - OSPFv2/v3: rýchlosť
  - Protokoly pracujúce s kompozitnou metrikou
    - Kombinácia viacerých hodnôt
    - EIGRP: rýchlosť + oneskorenie, voliteľne aj záťaž a spoľahlivosť

Classfull a classless smerovacie protokoly

- Classfull smerovacie protokoly
  - Starší predchodcovia súčasných protokolov, už nie veľmi využívané
    - RIPv1, IGRP
  - Vo svojich správach neprenášajú informáciu o maske siete, len ich adresy
    - Predpokladajú, že ak je sieť podsieťovaná, každá podsieť má rovnakú masku
- Classless smerovacie protokoly
  - Všetky moderné smerovacie protokoly
    - OSPFv2/v3, IS-IS, EIGRP, RIPv2/RIPng
  - Vo svojich správach prenášajú **adresy** i **masky** sietí
    - Podpora VLSM/CIDR

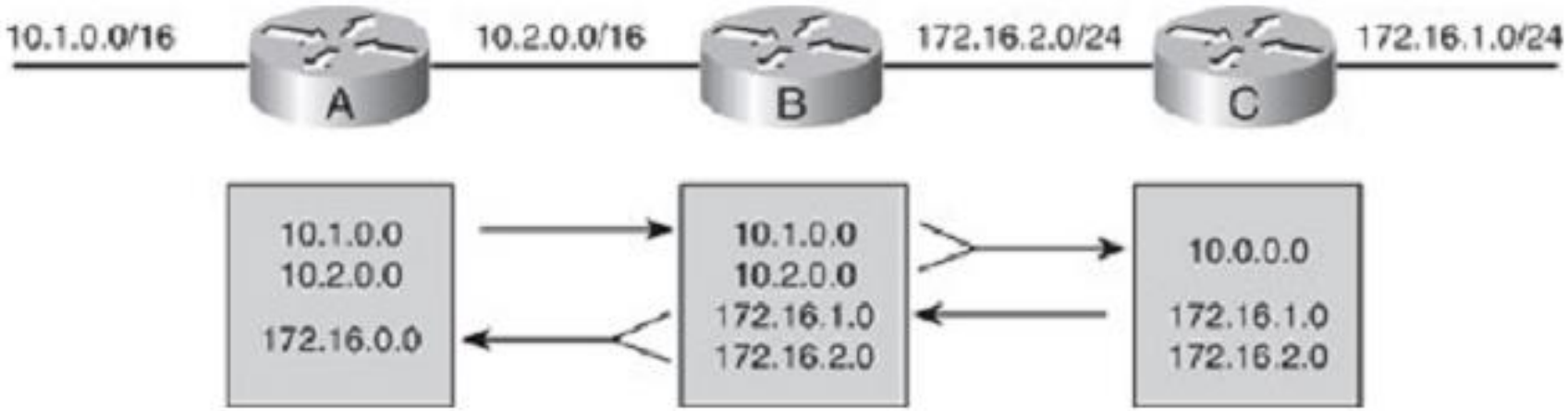


Classful: Subnet mask is the same throughout the topology



Classless: Subnet mask can vary in the topology

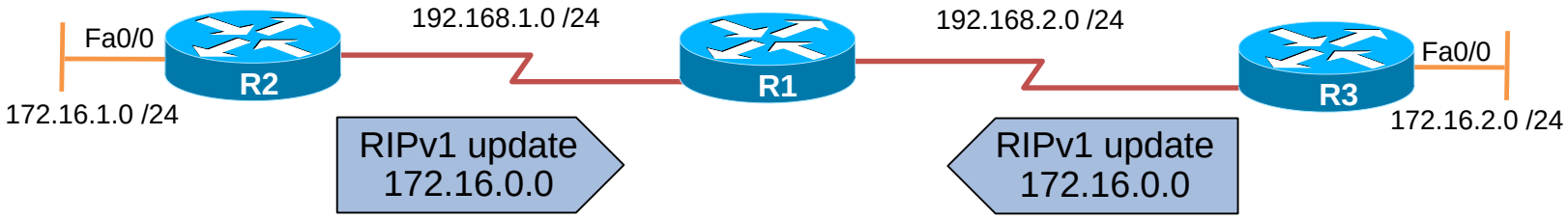
Sumarizácia ciest



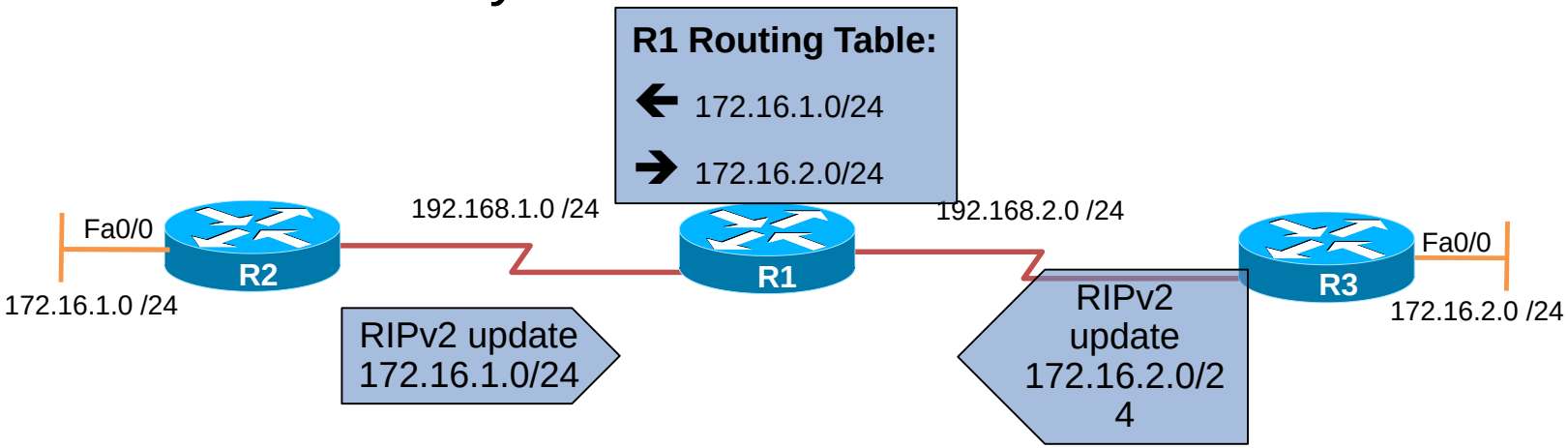
- Technika na zmenšovanie veľkosti smerovacích tabuliek
  - Potreba vhodného adresového dizajnu
- Classfull smerovacie protokoly
  - Automaticky sumarizujú na hranici siete na adresnú triedu (Major network)
  - Auto sumarizácia sa nedá vypnúť
- Classless smerovacie protokoly
  - Tiež vedia automaticky alebo manuálne sumarizovať
  - Autosumarizácia sa však dá *vypnúť* (`no auto-summary`)
- Vieme ako sa tvorí sumárny záznam?

Classfull vs. classless autosumarizácia

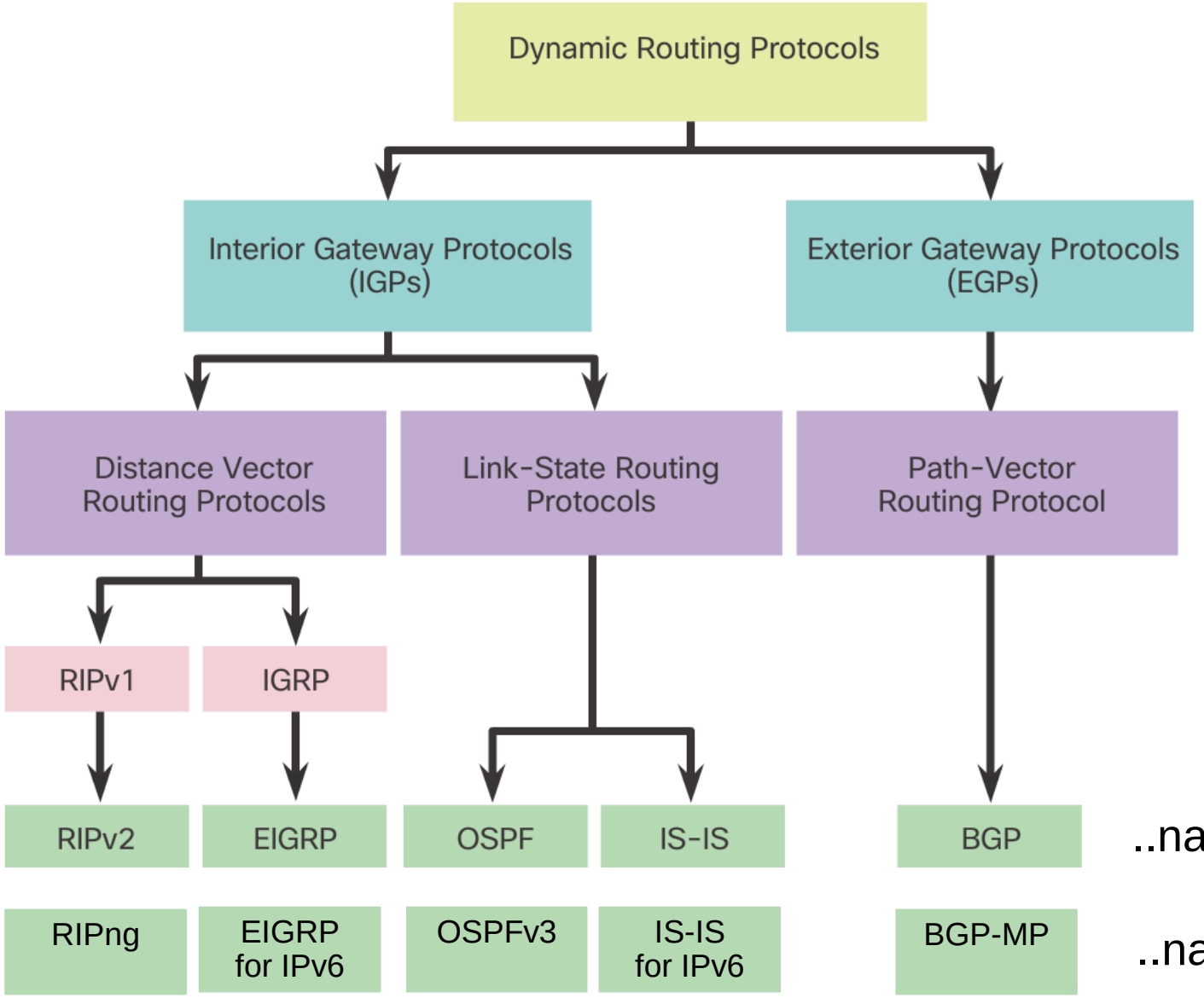
- Problém pri nespojitých adresových priestoroch
- Classfull alebo autosumary **ON**



- Classless s autosumary **OFF**



Kategorizácia smerovacích protokolov



..nad IPv4

..nad IPv6

Administratívne vzdialenosti

- Na jednom smerovači môže bežať viac smerovacích protokolov
- Každý hlási svoju cestu ako najlepšiu
- Vzhľadom na nekompatibility metrík, smerovač do R.T. musí umiestniť len jednu
- Výber: dôveryhodnosť „informátora“, t.j. zdroja smerovacej informácie
  - Ináč nazývané aj ako **Administratívna vzdialenosť**
  - Čím nižšia AD, tým vyššia dôveryhodnosť zdroja

Typ informácie	Administratívna vzdialenosť
Priamo pripojená sieť	0
Staticky vložená informácia	1
EIGRP sumárna sieť	5
BGP sieť z iného AS	20
EIGRP interná sieť	90
OSPF	110
IS-IS	115
RIP	120
On-Demand Routing (ODR)	160
EIGRP externá sieť	170
BGP sieť z toho istého AS	200
DHCP	254
Absolútne nedôveryhodný zdroj	255

Charakteristiky smerovacích protokolov

Characteristics	RIPv1	RIPv2	EIGRP	IS-IS	OSPF	BGP
Distance vector	✓	✓	✓			✓
Link-state				✓	✓	
Classless		✓	✓	✓	✓	✓
VLSM support		✓	✓	✓	✓	✓
Automatic route summarization	✓	✓ (can be disabled using `no auto-summary`)	✓ (can be disabled using `no auto-summary`)			✓
Manual route summarization		✓	✓	✓	✓	✓
Hierarchical topology required				✓	✓	
Size of network	Small	Small	Large	Large	Large	Very large
Metric	Hops	Hops	Composite metric	Metric	Cost	Path attributes
Convergence time	Slow	Slow	Very fast	Fast	Fast	Slow

Smerovacie protokoly typu distance vector

Distance-Vector protokoly

- Smerovač pri DV protokoloch vychádza z predpokladu
  - Pozná vlastné priamo pripojené siete
  - Pozná „cenu“ svojich rozhraní do pripojených sietí,
    - a teda aj vzdialenosť k susedným smerovačom v týchto sieťach
  - A túto informáciu zdieľa so svojimi susedmi (periodicky ako RIP, on demand ako v EIGRP)
    - Sused = smerovač, na ktorom musí bežať ten istý DV protokol
  - A následne sa tým vlastne smerovač od susedov **učí** nové siete
  - Pri detegovanej zmene ju smerovač hneď ohlási svojim susedom
- Susedia si tak pri DV protokoloch časom navzájom posielajú zoznamy sietí, ktoré poznajú (svoju smerovaciu tabuľku)
  - Zoznam sietí a vzdialeností od nich je pole štruktúr (vektor) s položkami
    - <Sieť, Vzdialenosť>
  - Pre toto posielanie **vektorov vzdialeností** smerovača sa tieto protokoly volajú DISTANCE VECTOR

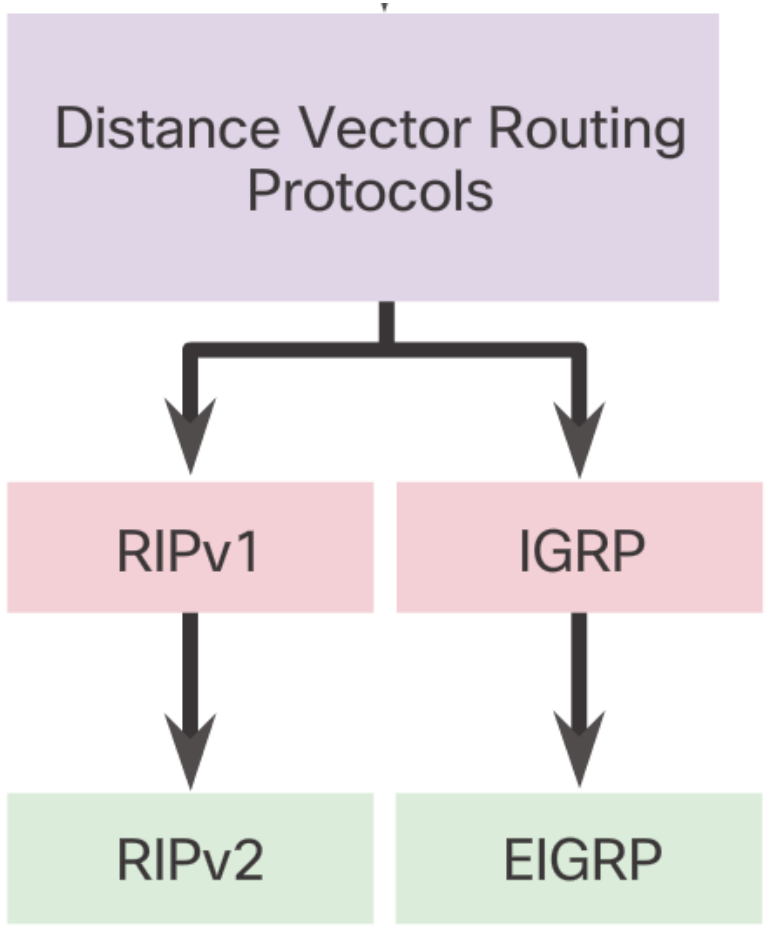
Distance-Vector protokoly

- Na samotné určenie najkratšej cesty do cieľa stačí smerovaču s DV protokolom poznať:
  - Adresu cieľovej siete a jej masku
  - Vzdialenosť jednotlivých bezprostredných susedov od tejto siete ako sa nahlásili
  - Vzdialenosť medzi smerovačom a jeho bezprostrednými susedmi
  - Najkratšia cesta je následne ponúknutá do smerovacej tabuľky (R.T.)

- Na riadenie činnosti protokolu a výberu ciest sa používajú rôzne algoritmy
  - RIPv1/v2/RIPng: Bellman-Ford
  - EIGRP: Difúzny algoritmus DUAL (vyvinul J.J. Garcia-Luna-Aceve)

Charakteristiky Distance-Vector protokolov

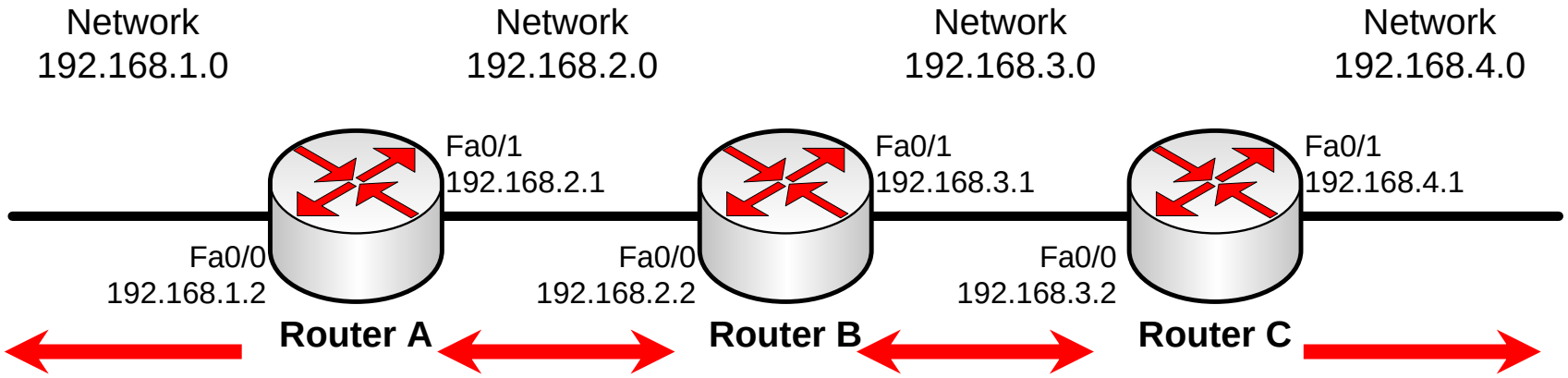
- Updates
  - Smerovacie informácie sú posielané ***periodicky*** aj keď sa ***nič nedeje*** (slúži aj ako keep-alive)
    - Celá rodina RIP + IGRP
    - Spotrebúvajú šírku pásma (bandwidth) liniek a zdroje smerovačov (CPU)
  - EIGRP posiela celú R.T. len pri úvodnej synchronizácii a potom len keď sa niečo zmení
    - Na keep-alive používa Hello mechanizmus
  - V starších protokoloch posielané ako broadcast (255.255.255.255)
    - RIPv1, IGRP
  - Novšie protokoly posielajú ako multicast
    - RIPv2, RIPng, EIGRP



Distance-Vector protokoly – neznalosť topológie

- Zo smerovacej informácie od suseda DV protokoly nepoznajú celú topológiu siete
  - t.j. DV smerovač pozná svoje bezprostredné okolie
    - pozná seba, vlastné priamo pripojené siete, bezprostredne susedné smerovače a siete „dakde za susedmi“
  - viem čo mi povedal sused
    - princíp JPP (jedna pani povedala), alebo JRP (jeden ....)
  - ale nemám presnú predstavu, čo vlastne za týmto susedom ďalej je
    - okrem zoznamu nahlásených sietí a ich metrík

RIPv1/v2 princíp činnosti



Routing table		
Network	**Metric**	**Next hop**
192.168.1.0	0	-
192.168.2.0	0	-
192.168.3.0	1	Fa0/1
192.168.4.0	2	Fa0/1

Routing table		
Network	**Metric**	**Next hop**
192.168.2.0	0	-
192.168.3.0	0	-
192.168.1.0	1	Fa0/0
192.168.4.0	1	Fa0/1

Routing table		
Network	**Metric**	**Next hop**
192.168.3.0	0	-
192.168.4.0	0	-
192.168.2.0	1	Fa0/0
192.168.1.0	2	Fa0/0

```
Router(config)#router rip
Router(config-router)# version 2
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
```

Zhodnotenie DV protokolov

Výhoda

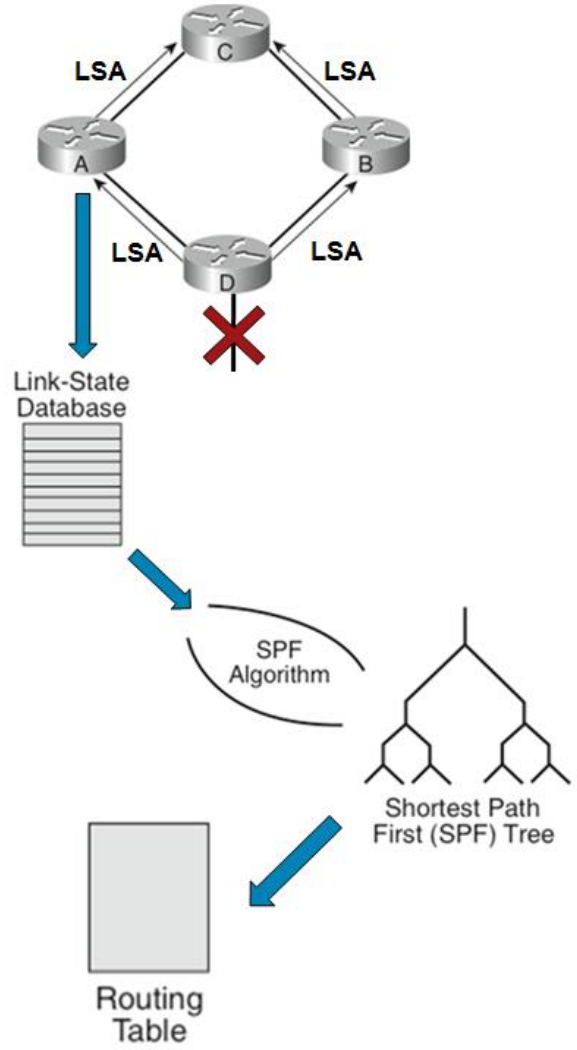
- Jednoduché v činnosti, konfigurácii ako aj v porozumení
- Nenáročný na zdroje

Nevýhoda

- Pracujú na princípe „povery“
- Pomalšia konvergencia z dôvodu záplavového šírenia aktualizácie
- Neznalosť topológie
- Náchylnosť na vznik prechodných smerovacích slučiek
  - Riešenia ochrán proti vzniku slučiek
    - Časovače/Timery
      - Update, hold down, invalid after, flush after
    - Definovanie maxima pre vzdialené siete
      - Siete za maximom sú nekonečne vzdialené a smerovač s nimi nepracuje, neohlasuje ich
    - Split horizon s poisson reverse

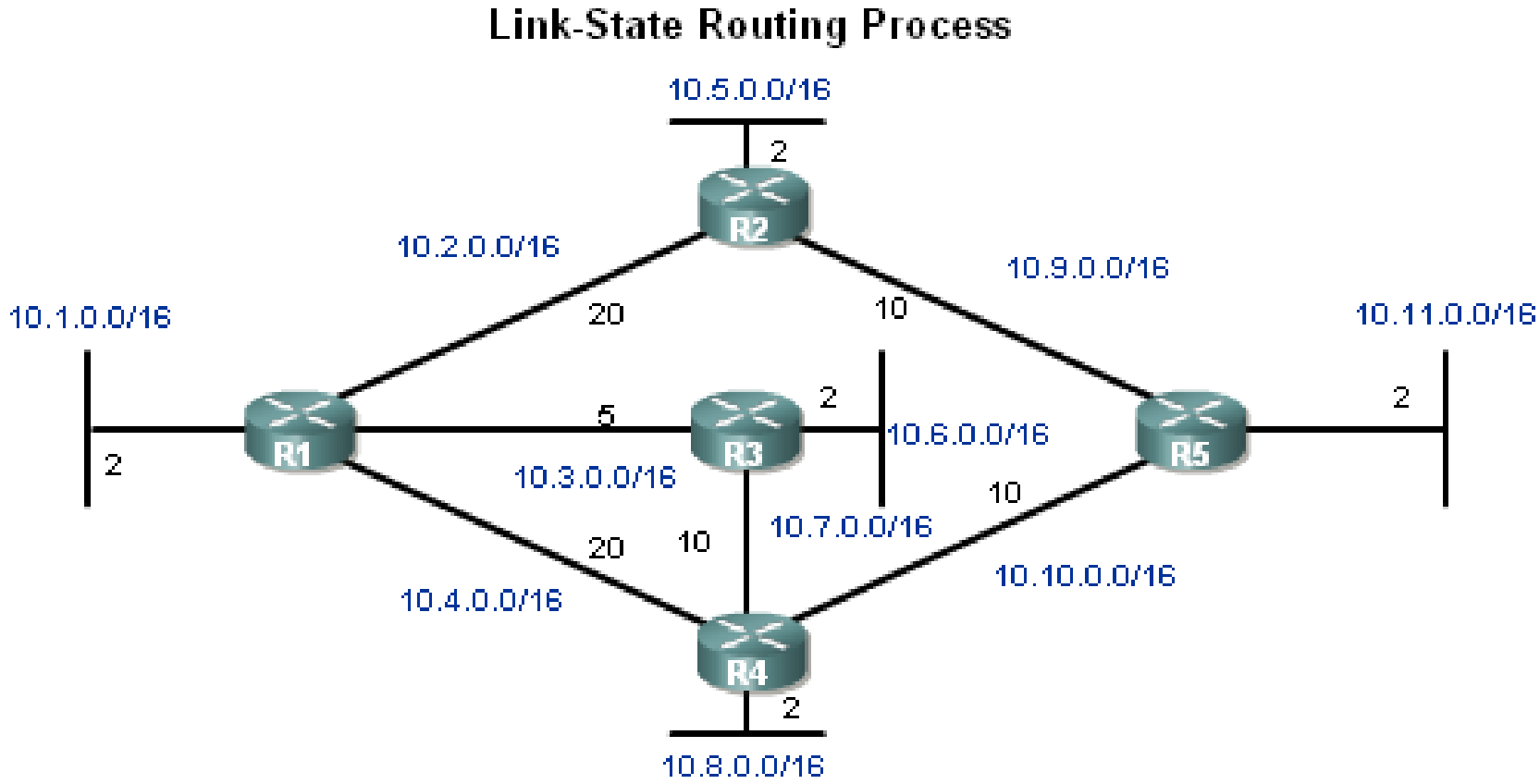
Link-State protokoly

- LS protokoly k svojej činnosti využívajú teóriu grafov – hľadanie najkratšej cesty v grafe
  - Siete rozdeľujú na oblasti (areas)
  - Každý smerovač detailne pozná topológiu siete v oblasti a má jej grafovú reprezentáciu v topologickej databáze
    - Poznám seba, svoje linky a svojich susedov
    - ako aj všetky ďalšie smerovače, ich linky a ich susedov
    - T.j. vypísaním pracovnej databázy LS protokolu na ľubovoľnom smerovači sme schopní nakresliť diagram celej siete
  - Nad týmto grafom siete každý smerovač nezávisle určí strom najkratších ciest od seba do všetkých cieľových sietí
- Pre svoju činnosť sú LS pamäťovo i výpočtovo zložitejšie než DV
  - Viac pracovných tabuliek, viac výpočtov
- V stave kľudu je však na zdroje smerovačov a siete šetrnejší
  - No changes, no updates



Vzorová topológia

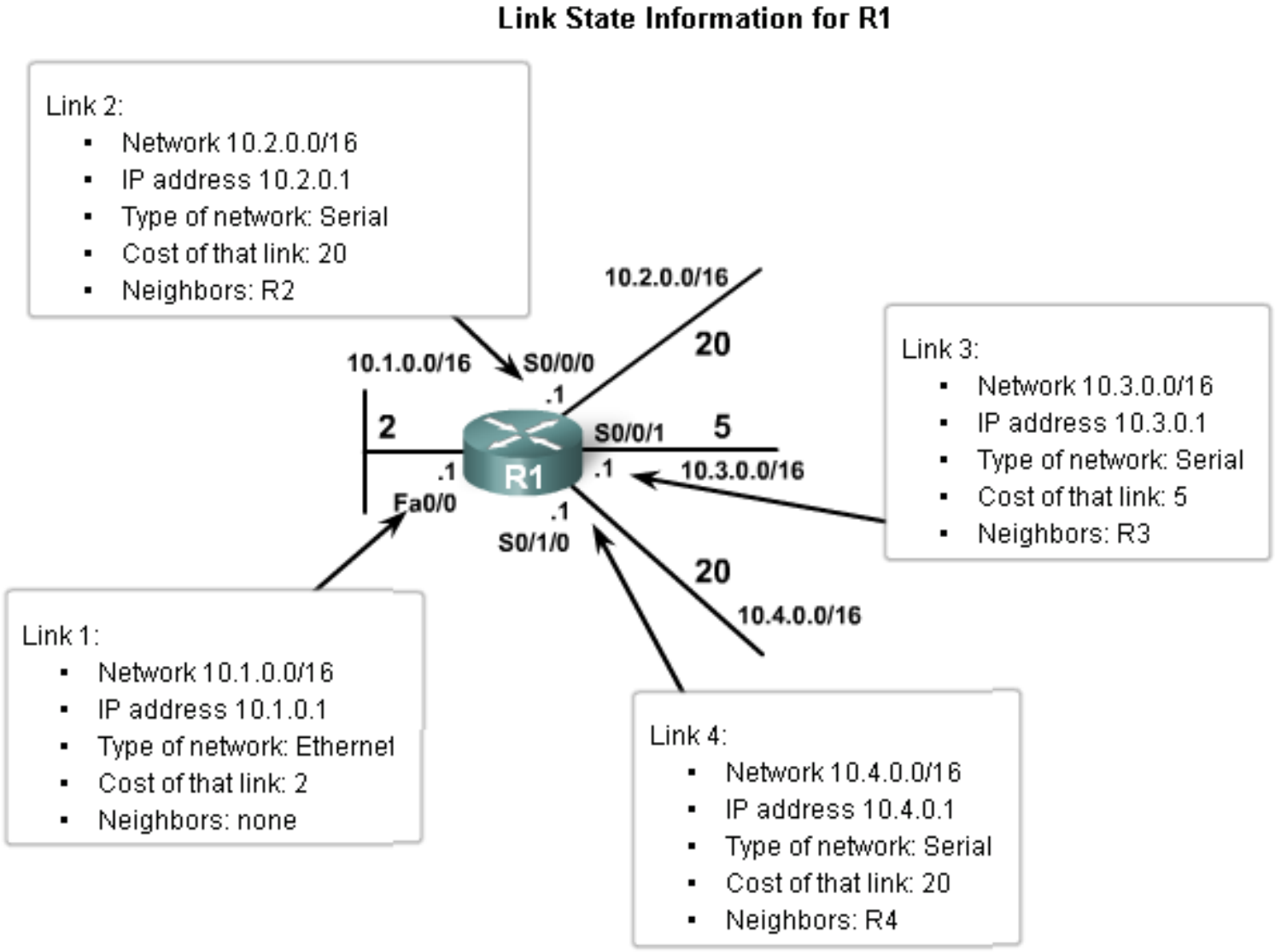
- Na hľadanie najkratších ciest sa využíva tzv. Dijkstrov algoritmus



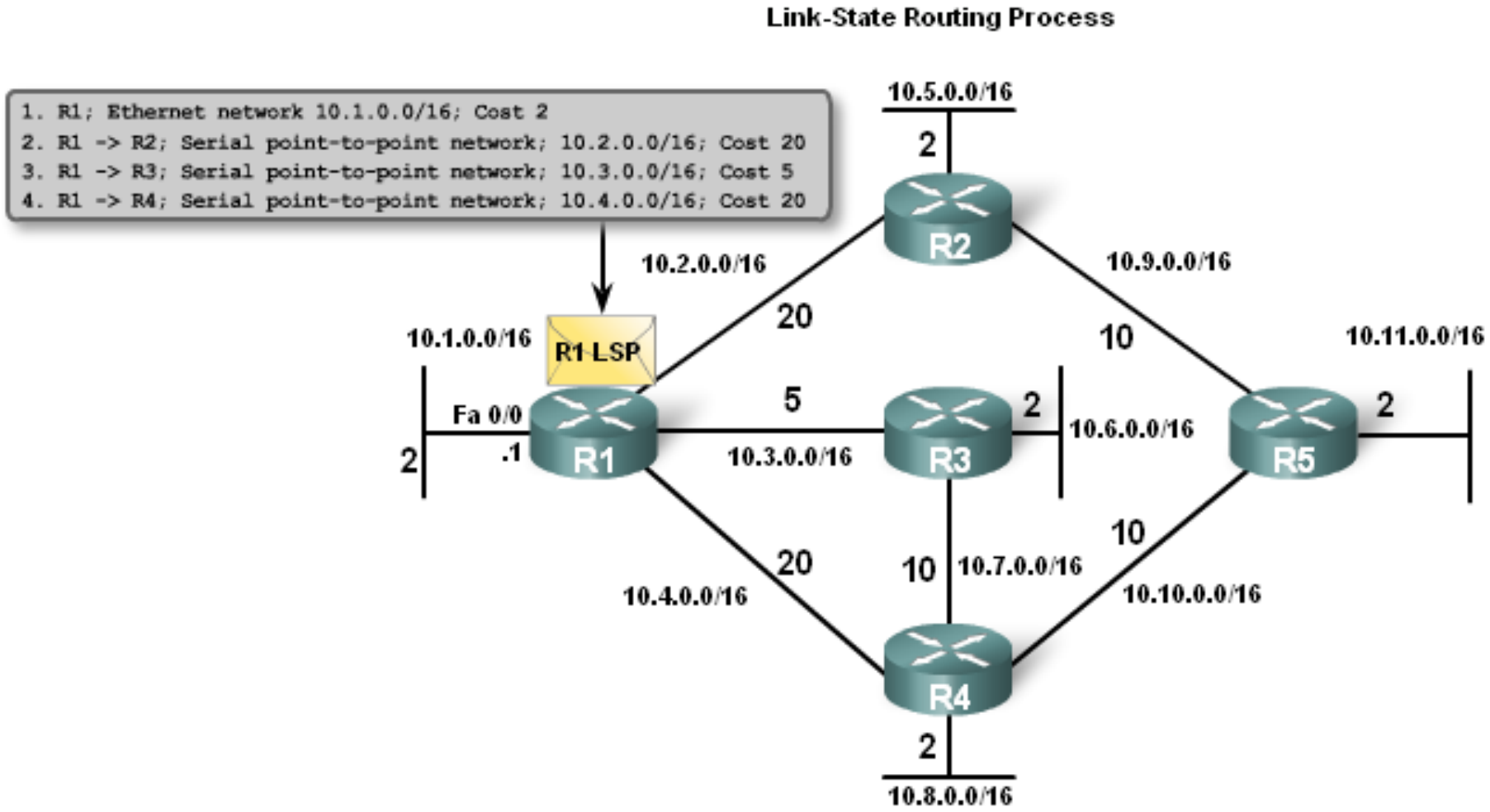
Činnosť link-state protokolov

- Každý smerovač identifikuje a uloží si objekty, s ktorými je bezprostredne spojený
  - Seba a svoje priamo pripojené siete
  - Svojich susedov na priamo pripojených linkách
- Následne všetkým svojim susedom smerovač odošle správu, tzv. Link State Packet alebo Link State Advertisement (LSP/LSA),
  - v ktorej presne popíše svoje lokálne prepojenia s okolitými objektmi
- Iné smerovače si túto správu uložia do lokálnej DB a preposielajú ju ďalej v rámci oblasti
  - ale nesmú ju pri preposielaní zmeniť
- Po istom čase každý smerovač má vo svojej DB a pozná všetky ostatné smerovače a objekty v sieti a ich presné vzájomné zapojenie
- Nad touto topologickou mapou siete (tzv. orientovaným grafom) smerovač využije niektorý z algoritmov, ktorý vytvára strom najkratších ciest
  - Tzv. SPT – Shortest Path Tree
- Výsledne najkratšie cesty ponúkne R.T.
  - Tá na základe AD protokolu to môže prijať alebo odmietnuť

Link-state popis okolia smerovača

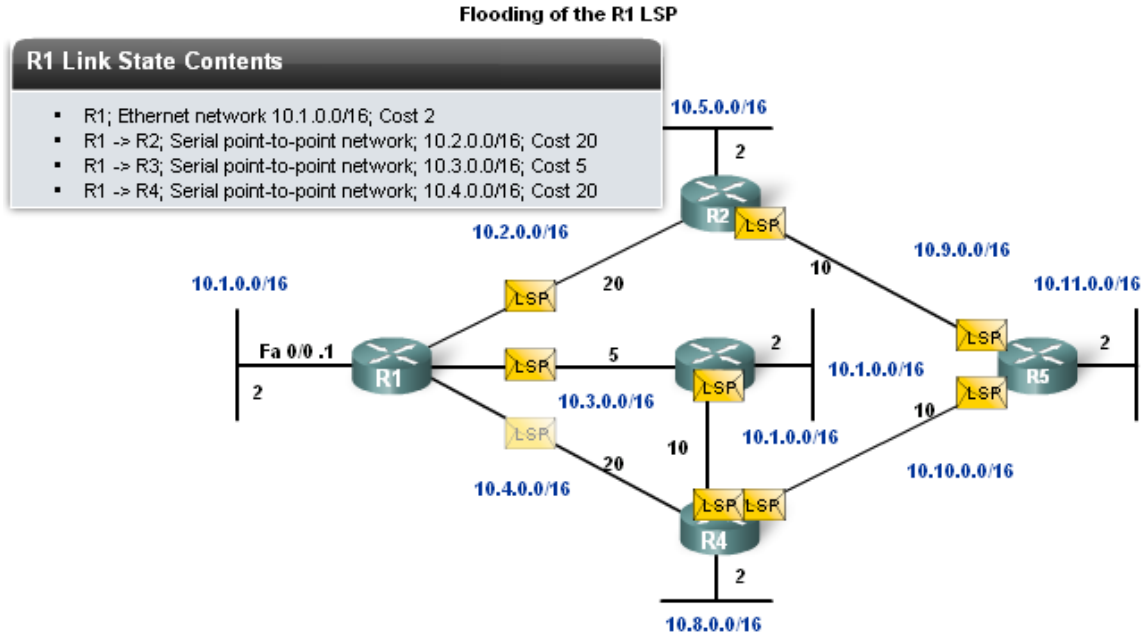


Link-state paket z R1



Rozosielanie LSP paketov

- LSP paket generuje každý smerovač sám za seba
  - Vždy pri zmene topológie, ktorá sa smerovača týka
  - Periodicky rádovo v desiatkach minút
- LSP sa rozosielajú medzi všetkými smerovačmi
  - Každý smerovač si prijaté LSP zapamätá a pošle svojim susedom
  - Po krátkom čase každý smerovač pozná LSP všetkých smerovačov v sieti



Link-state databáza na smerovači R1

R1s Link-State Database

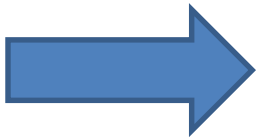
LSPs from R2:
- Connected to neighbor R1 on network 10.2.0.0/16, cost of 20
- Connected to neighbor R5 on network 10.9.0.0/16, cost of 10
- Has a network 10.5.0.0/16, cost of 2

LSPs from R3:
- Connected to neighbor R1 on network 10.3.0.0/16, cost of 5
- Connected to neighbor R4 on network 10.7.0.0/16, cost of 10
- Has a network 10.6.0.0/16, cost of 2

LSPs from R4:
- Connected to neighbor R1 on network 10.4.0.0/16, cost of 20
- Connected to neighbor R3 on network 10.7.0.0/16, cost of 10
- Connected to neighbor R5 on network 10.10.0.0/16, cost of 10
- Has a network 10.8.0.0/16, cost of 2

LSPs from R5:
- Connected to neighbor R2 on network 10.9.0.0/16, cost of 10
- Connected to neighbor R4 on network 10.10.0.0/16, cost of 10
- Has a network 10.11.0.0/16, cost of 2

R1 Link-states:
- Connected to neighbor R2 on network 10.2.0.0/16, cost of 20
- Connected to neighbor R3 on network 10.3.0.0/16, cost of 5
- Connected to neighbor R4 on network 10.4.0.0/16, cost of 20
- Has a network 10.1.0.0/16, cost of 2



- Výpočtom strom vzdialeností s cestami do cieľových sietí
- Naj cesty ponúknuté R.T.
- Na základe AD akcept or nie

Zhodnotenie LS protokolov

Výhody

- Znalosť celej topológie
- Rýchla konvergencia pri zmenách
  - šírením nie celej R.T., ale len týkajúcej sa topo informácie
- Nižšia pravdepodobnosť vzniku smerovacích slučiek než pri distance-vector smerovacích protokoloch
- Optimalizácia R.T. použitím konceptu oblastí

Nevýhody

- Vyššia spotreba pamäte a výpočtového výkonu CPU k behu LS protokolu
- Vyššia spotreba CPU a siete pri inicializácii smerovačov a topol. zmenách
- Nemožnosť sumarizovať alebo filtrovať oznamované siete na ľubovoľnom mieste siete, iba na tzv. hraniciach oblastí
- Zložitejšie mechanizmy a nutnosť kompetentného nasadenia

Poznámky k DV a LS

- DV protokoly sú jednoduchšie
  - Spotrebúvajú menej systémových prostriedkov smerovačov
  - Princíp činnosti je jednoduchý
  - Zvládnu ich (ako-tak ☺) aj menej skúsení administrátori sietí
  - Reagujú vo všeobecnosti pomalšie, sú vhodné pre menšie siete
- LS protokoly sú komplexnejšie
  - Sú náročnejšie na pamäť a CPU než DV protokoly
  - Princíp činnosti je zložitejší než pri DV protokoloch
  - Na ich dobré zvládnutie treba kvalifikovaného administrátora
  - Siete majú v LS protokoloch vždy hierarchický dizajn – musia mať vyčlenenú chrbticovú oblasť, ktorá prepája ďalšie časti siete
  - Reagujú vo všeobecnosti rýchlejšie, sú vhodné pre veľké siete

MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť!

Ohodnoť našu CNA na google:

- https://goo.gl/maps/BAnFvQKYCBpffcEX7