



# Optimalizácia smerovania, redistribúcia



ROUTE modul 4

# Problematika výkonnosti a optimálnosti smerovania

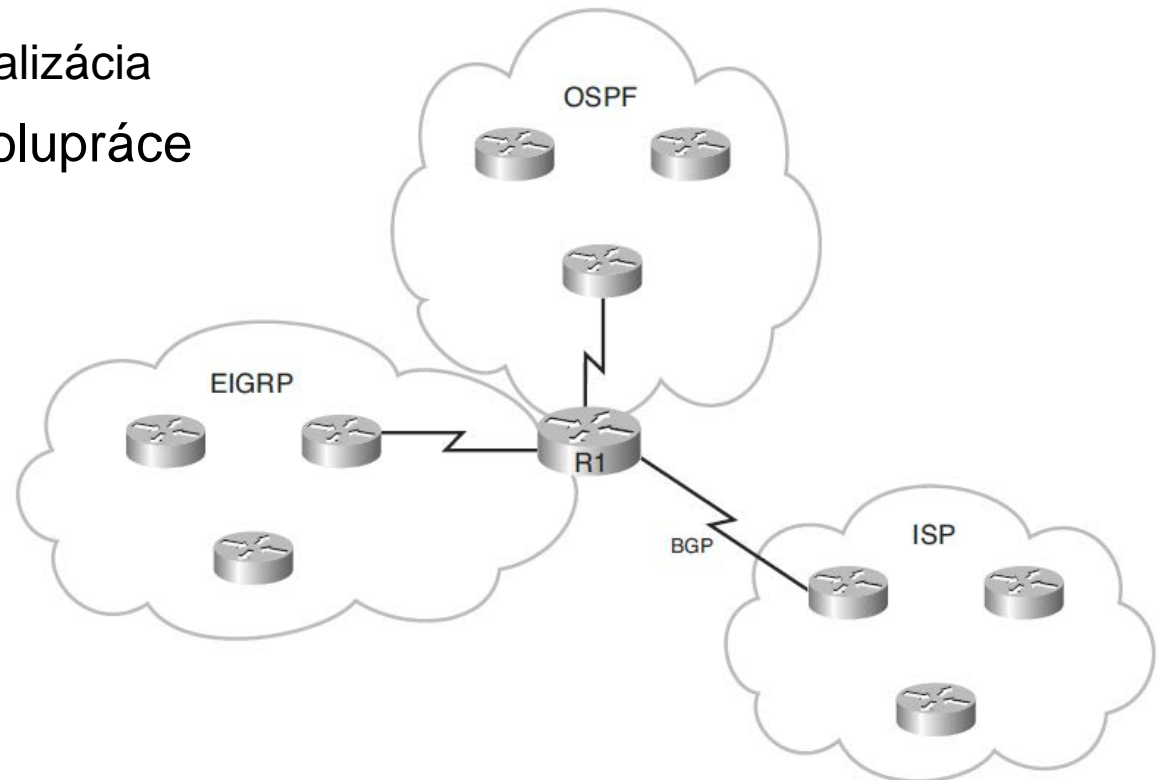


# Od jednoduchých ku komplexným sieťam

- Jednoduchým sieťam zvyčajne stačia jednoduché smerovacie protokoly
  - Ich funkcionálnosť je dostatočná
  - Zvyčajne stačí jeden smerovací protokol.
- Použitie jedného protokolu pre celú IP sieť je vysoko žiaduce
  - Avšak nie vždy jednoducho dosiahnuteľné z viacerých dôvodov
    - Dočasný stav pri migrácii smerovacích protokolov
    - Niektoré protokoly podporujú špecifické funkcie
      - Neexistuje univerzálny „všeobjímajúci“ smerovací protokol
    - Spojenie sietí pod rôznou administratívnou správou
      - Napríklad zákaznícke lokality a sieť ISP
    - „Politické“ dôvody
      - Iné než technické dôvody, prečo musí v sieti pracovať niekoľko smerovacích protokolov
    - Nekompatibilita zariadení
      - Rôzni výrobcovia – rôzne protokoly – rôzne problémy
  - Veľké siete preto prevádzkujú viaceré protokoly

# Používanie viacerých smerovacích protokolov

- Problém s viacerými smerovacími protokolmi v jednej sieti
  - Rôzne smerovacie protokoly neboli navrhnuté zo schopnosťou spolupracovať navzájom
    - Každý protokol používa iný typ informácií a reaguje iným spôsobom
  - Beh viacerých smerov. protokolov na jednom zariadení vyžaduje viac zdrojov
    - Výkonnosť a optimalizácia
  - Otázka vhodnej spolupráce



# Problematika výkonnosti a optimálnosti smerovania vo veľkých sieťach

- Nadmernosť smerovacích update-ov
  - Kolísanie záťaže CPU (až dosiahnutie špičky) závisí od:
    - Veľkosti smerovacích updatov
    - Frekvencie updatov
    - L3 dizajnu siete
- Od počtu smerovacích protokolov použitých v AS závisí
  - Množstvo a intenzita updates
  - Spolupráca
  - Prítomnosť a vhodnosť/nehodnosť nasadenia smerovacích máp a filtrov

# Riešenie smerovania v komplexných sieťach

- Pri riešení dizajnu komplexných sietí je treba brať do úvahy
  - Plánovanie nasadenia vhodných smer. protokolov
  - Obmedzenia počtu nasadených smerovacích protokolov
    - Ideál jeden
  - Vhodné riešenie spolupráce smerovacích protokolov
  - Optimalizácia komunikácie a prevádzky medzi nasadenými protokolmi
- Riešenia spolupráce a optimalizácie zahŕňajú
  - Použitie pasívnych rozhraní
    - Zabránenie zasielania updates cez dané rozhranie
  - Vhodne plánovaná a nasadená sumarizácia
  - Redistribúcia ciest medzi rôznymi smerovacími protokolmi
  - Filtrovanie smerovacích updatov
    - Kontrola čo bude rozširované a spracovávané
    - Zahŕňa
      - Access control lists (ACLs)
      - Route maps
      - Distribute lists
      - Prefix lists
      - Filter lists

# Redistribúcia medzi smerovacími protokolmi



# Spolupráca smerovacích protokolov: Redistribúcia

- V istých situáciách je potrebné smerovacie informácie preniesť z jedného protokolu do druhého (jednosmerne), prípadne prenášať ich navzájom (obojsmerne)
- Tento prenos smerovacej informácie sa v Cisco poňatí nazýva **redistribúcia**
- Pre pripomenutie
  - Každý smerovací protokol má vlastné nezávislé pracovné databázy a z týchto databáz napĺňa smerovaciu tabuľku
  - Daným smerovacím protokolom sa prenáša len obsah príslušných databáz
    - EIGRP si distribuuje svoje siete, RIP svoje, OSPF svoje, IS-IS svoje



# Redistribúcia

- Na smerovači teda môže bežať niekoľko smerovacích protokolov (routing domains)
  - ale informácie si navzájom bez dodatočnej konfigurácie navzájom nevymenia
- Jediné spoločné miesto, v ktorom sa „stretnú“ informácie zo všetkých smerovacích protokolov, je **smerovacia tabuľka**
- Redistribúcia je vlastne prevzatie smerov **cudzieho** smerovacieho protokolu, ktoré sú *zaznamenané* v smerovacej tabuľke
  - Istá sieť musí byť **najprv v smerovacej tabuľke**, až potom ju možno redistribuovať
  - Smerovacia tabuľka smerovača, ktorý robí redistribúciu, sa nezmení
    - Redistribúcia vykonávaná v outbound smere
  - Neprenáša sa topologický detail, len info o existencii siete
- Smerovač, ktorý vykonáva redistribúciu sa nazýva „*boundary router*“

# Problémy pri redistribúcii

- Pri redistribúcii treba brať do úvahy riešenie nasledujúcich problémov:
  - **Routing feedback (loops)**
    - Ak redistribúciu vykonáva viacero smerovačov, redistribuované cesty prijaté jedným z nich (z jedného AS) môžu byť poslané naspäť druhým z nich (do daného pôvodného AS)
  - **Incompatible routing information**
    - Každý protokol používa na určenie najlepšej cesty inú metriku
    - Použitie redistribuovanej cesty nemusí byť preto z pohľadu smerovania optimálne
  - **Inconsistent convergence times**
    - Rozdielne protokoly konvergujú rozdielne rýchlo (resp. pomaly)

# Výber najlepšej cesty

▪ Ak má smerovač na výber pre danú sieť viaceré cesty poskytnuté od rôznych smerovacích protokolov rozhoduje sa podľa:

- **Administratívna vzdialenosť (Administrative distance)**

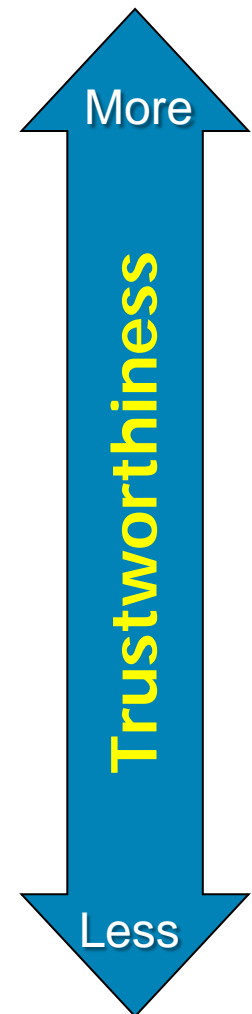
- Určuje dôveryhodnosť zdroja smerovacej informácie
  - Ktorému smerovaciemu protokolu viac dôverujem

- **Smerovacia metrika (Routing metric)**

- Hodnota reprezentujúca ohodnotenie cesty medzi daným lokálnym smerovačom a cieľovou sieťou

# Administratívne vzdialenosti v Cisco IOS

Routing Protocol	Default Administrative Distance Value
Connected interface	0
Static route out an interface	1
Static route to a next-hop address	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIPv1 and RIP v2	120
Exterior Gateway Protocol (EGP)	140
On-Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown	255



# Redistribúcia

- Pretože každý smerovací protokol funguje inak a inak si počíta svoju metriku, nedá sa metrika len tak prevziať
- Riešenie:
  - Pri redistribúcii sa na okrajovom smerovači stanoví počiatočná metrika v cieľovom protokole (tzv. **seed metric**), s ktorou sa smery z iného protokolu redistribuujú
  - Táto metrika sa potom zvyšuje v danom smerovacom protokole obvyklým spôsobom
- Link-state protokoly dosadzujú istú implicitnú počiatočnú metriku, distance-vector protokoly dosadzujú **nekonečno**
  - Je zásadne vhodné stanoviť metriku pre redistribúciu **vždy**, nespoliehať sa na automaticky dosadené hodnoty

# Štandardné počítačové metriky

Protokol	Štandardná počítačová metrika
RIP	Nekonečno
IGRP/EIGRP	Nekonečno
OSPF	20 pre všetky smerovacie protokoly okrem BGP, 1 pre BGP
IS-IS	0
BGP	BGP metrika sa nastaví na metriku príslušného IGP protokolu

# Definovanie „Seed Metric“

- Nastavenie „seed“ metriky mimo default hodnôt sa môže konfiguračne modifikovať dvomi spôsobmi
  - Príkaz **default-metric** nastaví metriku pre všetky redistribuované cesty
    - Bez ohľadu na to z akého zdroja/protokolu
  - Príkaz **redistribute** môže obsahovať definíciu metriky pre daný protokol z ktorého sa redistribuuje
    - Môžem nastaviť iné metriky per protokol
    - Príkaz „prebíja“ default-metric

# OSPF Seed Metric – Príklad 1

```
R3(config)# router rip
R3(config-router)# network 172.18.0.0
R3(config-router)# network 172.19.0.0
R3(config-router)# router ospf 1
R3(config-router)# network 192.168.2.0 0.0.0.255 area 0
R3(config-router)# redistribute rip subnets metric 30
R3(config-router)#
```

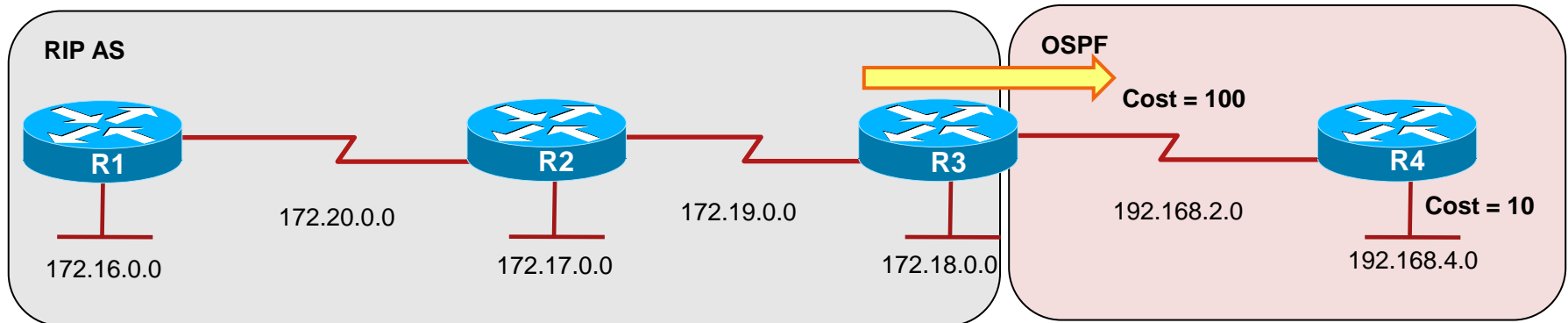


Table R1

```
C 172.16.0.0
C 172.20.0.0
R [120/1] 172.17.0.0
R [120/1] 172.19.0.0
R [120/2] 172.18.0.0
```

Table R2

```
C 172.17.0.0
C 172.19.0.0
C 172.20.0.0
R [120/1] 172.16.0.0
R [120/1] 172.18.0.0
```

Table R3

```
C 172.18.0.0
C 172.19.0.0
R [120/1] 172.17.0.0
R [120/1] 172.20.0.0
R [120/2] 172.16.0.0
C 192.168.2.0
O [110/110] 192.168.4.0
```

Table R4

```
C 192.168.1.0
C 192.168.2.0
O E2 [110/30] 172.16.0.0
O E2 [110/30] 172.17.0.0
O E2 [110/30] 172.18.0.0
O E2 [110/30] 172.19.0.0
O E2 [110/30] 172.20.0.0
```



# OSPF Seed Metric - Príklad 2

```

R3(config)# router rip
R3(config-router)# network 172.18.0.0
R3(config-router)# network 172.19.0.0
R3(config-router)# router ospf 1
R3(config-router)# network 192.168.2.0 0.0.0.255 area 0
R3(config-router)# default-metric 30
R3(config-router)# redistribute rip subnets
    
```

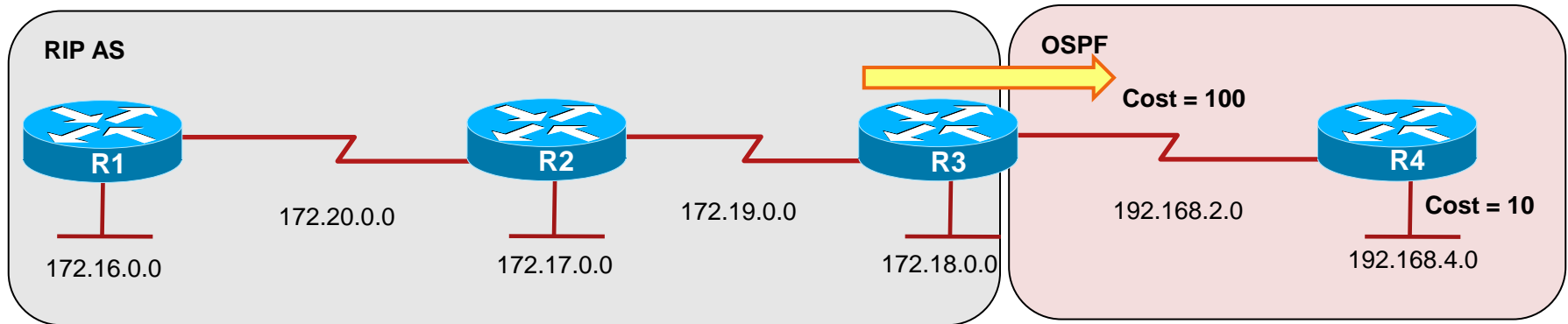


Table R1

```

C 172.16.0.0
C 172.20.0.0
R [120/1] 172.17.0.0
R [120/1] 172.19.0.0
R [120/2] 172.18.0.0
    
```

Table R2

```

C 172.17.0.0
C 172.19.0.0
C 172.20.0.0
R [120/1] 172.16.0.0
R [120/1] 172.18.0.0
    
```

Table R3

```

C 172.18.0.0
C 172.19.0.0
R [120/1] 172.17.0.0
R [120/1] 172.20.0.0
R [120/2] 172.16.0.0
C 192.168.2.0
O [110/110] 192.168.1.0
    
```

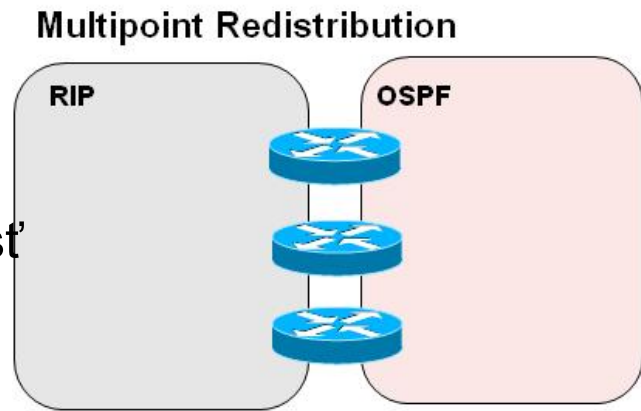
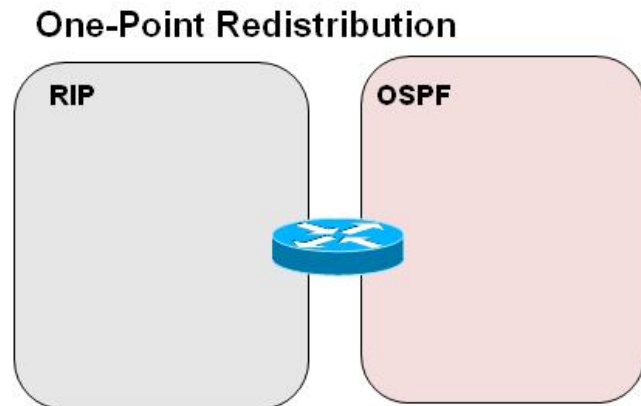
Table R4

```

C 192.168.1.0
C 192.168.2.0
O E2 [110/30] 172.16.0.0
O E2 [110/30] 172.17.0.0
O E2 [110/30] 172.18.0.0
O E2 [110/30] 172.19.0.0
O E2 [110/30] 172.20.0.0
    
```

# Redistribúcia

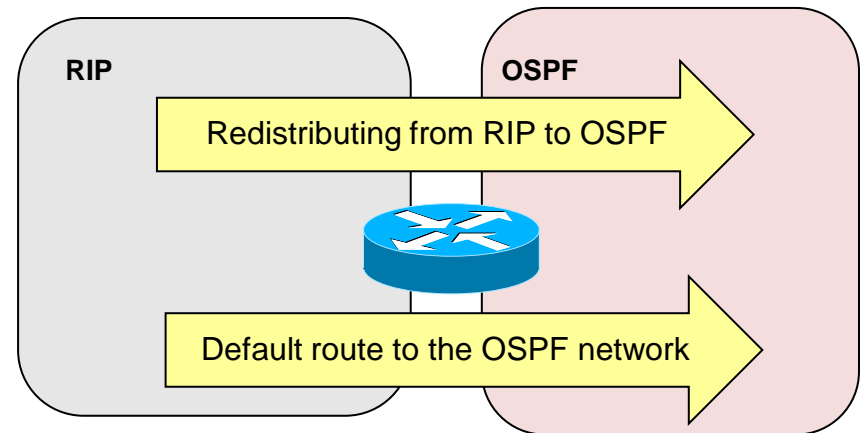
- Redistribuovať možno z ľubovoľného smerovacieho protokolu
  - Presnejšie – redistribuovať možno z čohokoľvek, čo naplní smerovaciu tabuľku, čiže aj statické smery, priamo pripojené siete, ...
- Redistribuovať sa dá do všetkých bežných smerovacích protokolov
  - Nedá sa redistribuovať do ODR
- Redistribúcia sa deje na jednom resp. viacerých smerovačoch, na ktorých beží súčasne viacero smerovacích protokolov
  - Buď len na jednom smerovači (*one-point*) alebo na viacerých (*multipoint*)
  - Iba z jedného protokolu do druhého (*one-way*) alebo obojsmerne (*two-way*)
  - Pri one-point redistribúcii nehrozia smerovacie slučky, pri multipoint je potrebná veľká opatrnosť



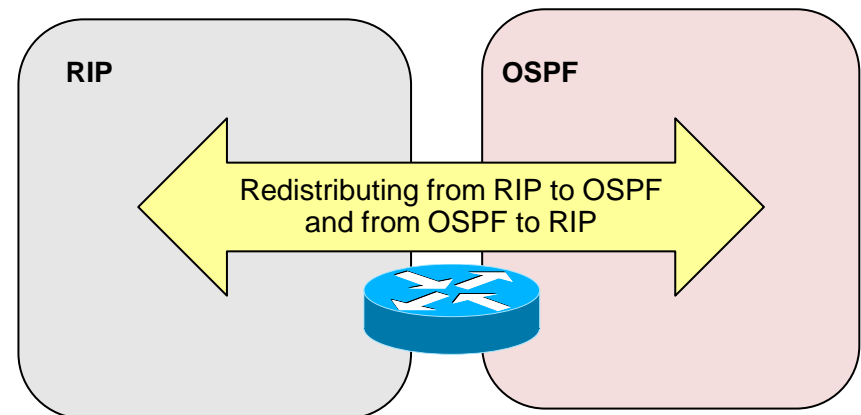
# One-Point Redistribution

- Redistribúcia typu „One-point“ môže byť buď:
  - **One-point One-way**
    - Redistribúcia z jedného smerovacieho protokolu do druhého
    - Typicky ako doplnok používa defaultnú cestu alebo statické cesty
  - **One-point Two-way**
    - Redistribúcia ciest medzi dvomi protokolmi v oboch smeroch

## One-Point One-Way Redistribution

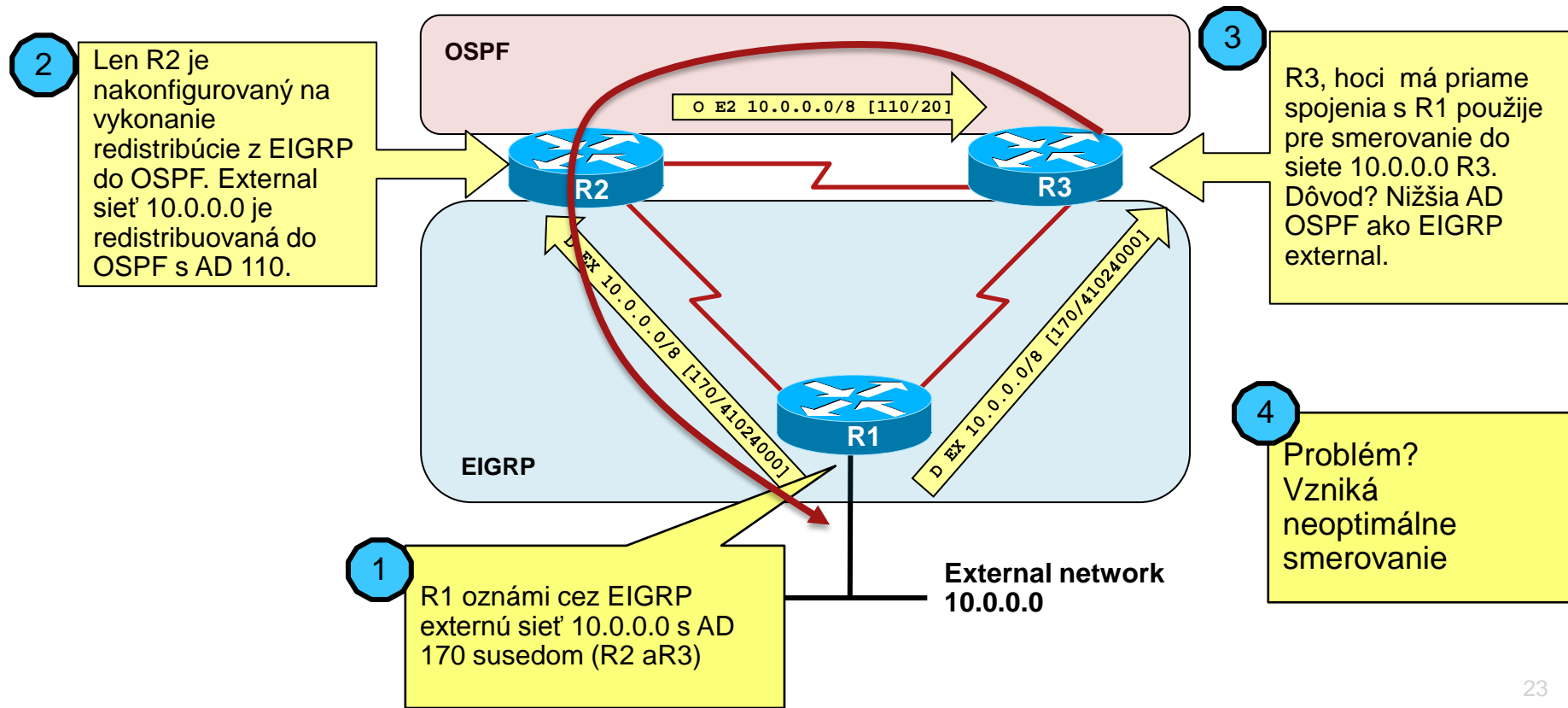


## One-Point Two-Way Redistribution



# Problém pri One-Point One-Way redistribúcií

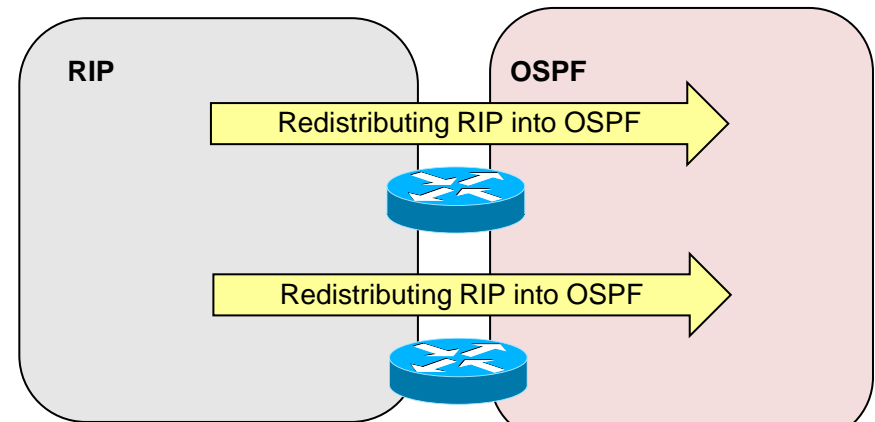
- One-point one-way alebo two-way redistribúcia zvyčajne nevedie k vzniku smerovacích slučiek
  - Ale môže vzniknúť neoptimálne smerovanie
    - Napr. v prípade, že sú dva boundary smerovače ale len jeden robí „one-point one-way“ redistribúciu



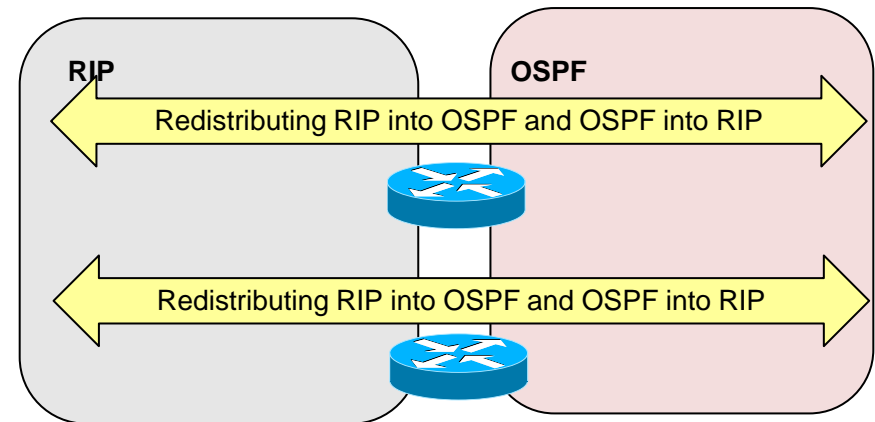
# Redistribúcia typu Multipoint

- Redistribúcia vykonávané na dvoch alebo viac smerovačoch
- Riešená ako:
  - Multipoint one-way redistribution
  - Multipoint two-way redistribution
- Obe riešenia sú problematické z pohľadu vzniku smerovacích slučiek
  - Špeciálne two-way

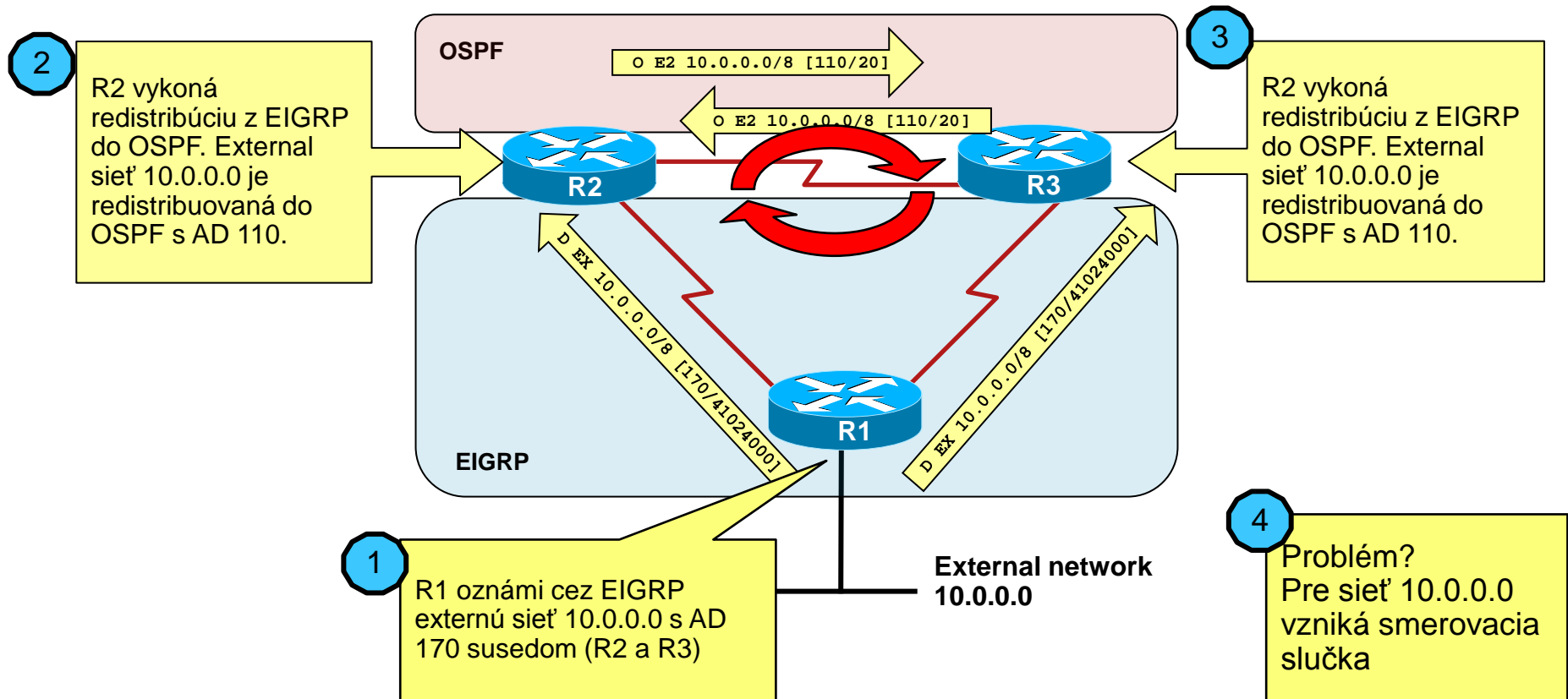
## Multipoint One-Way Redistribution



## Multipoint Two-Way Redistribution

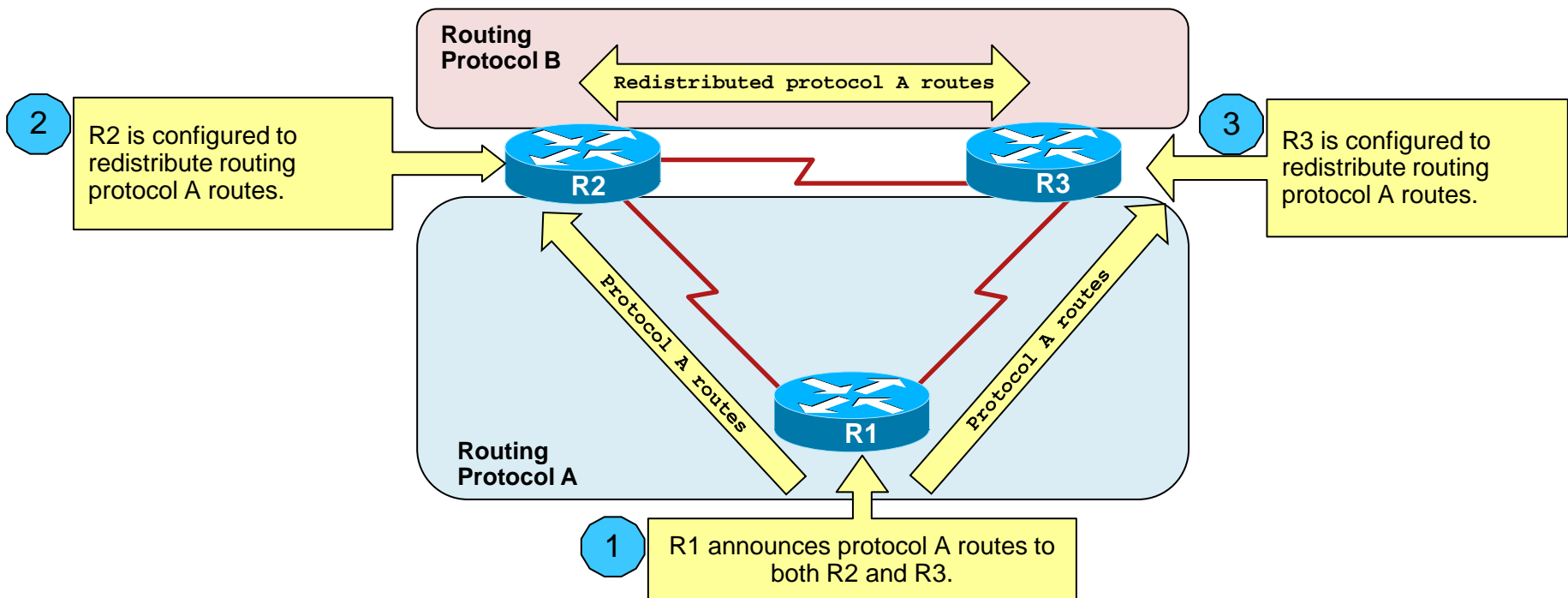


# Problém pri multipoint one-way redistribúcií

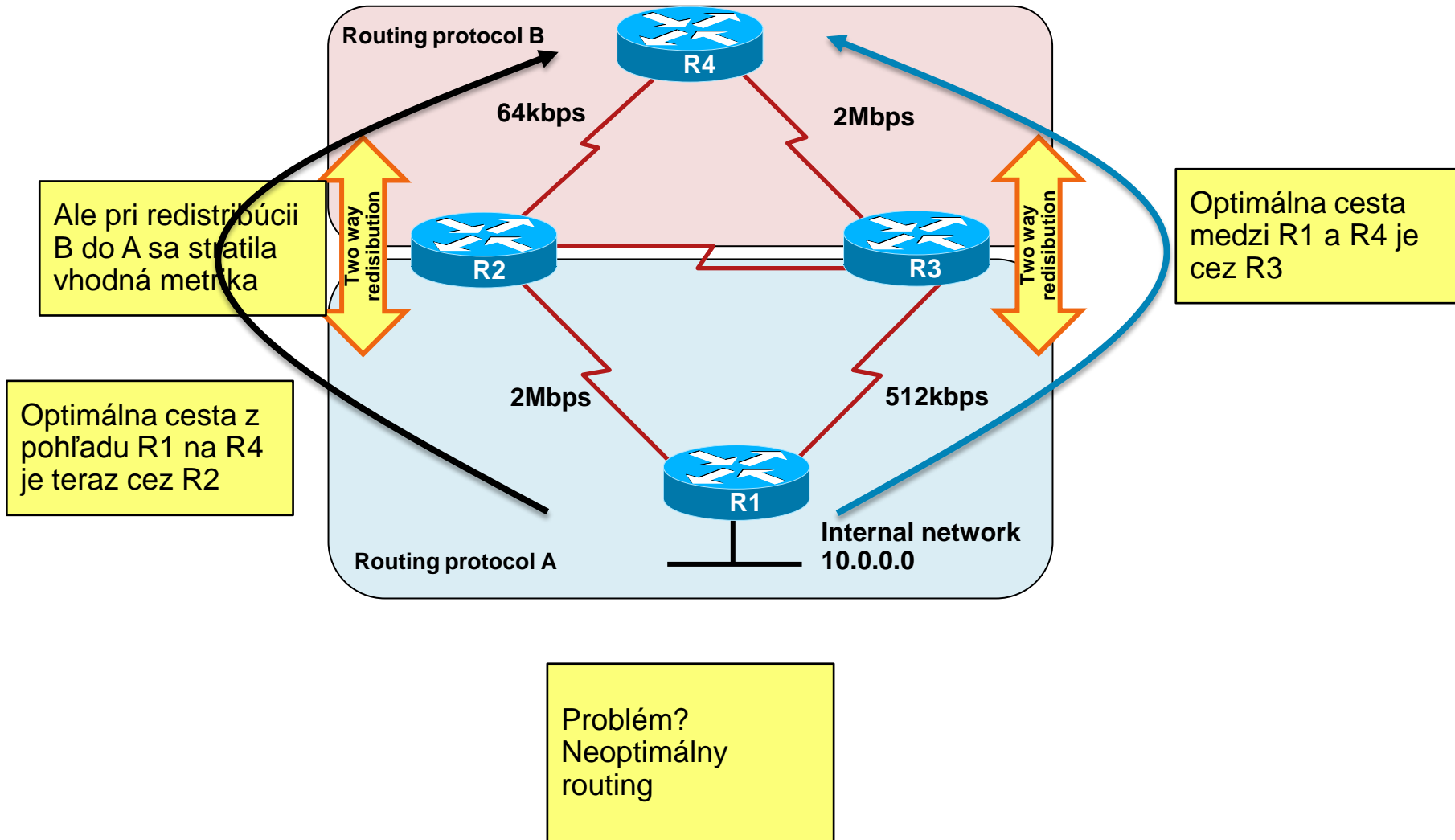


# Multipoint one-way redistribúcia - odporúčania

- Multipoint one-way redistribúcia pracuje bezproblémovo jedine ak:
  - Prijímajúci smerovací protokol je buď EIGRP, BGP alebo OSPF
    - Pretože podporujú odlišné AD pre interné a externé smerovacie cesty
  - Administratívna vzdialenosť externých ciest protokolu B je vyššia ako AD ciest protokolu A,
    - Takže R2 a R3 použijú vhodné cesty



# Problém pri multipoint two-way redistribúcií





# Multipoint two-way redistribúcia - odporúčania

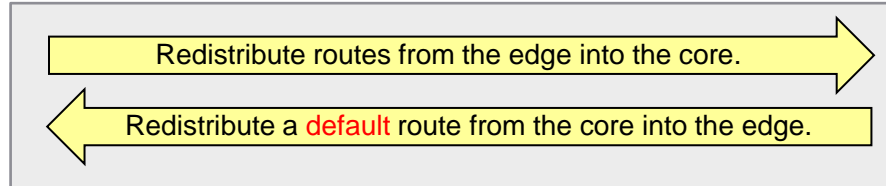
- Pri redistribúcii A do B vkladaj len ich interné cesty
- Na redistribučných smerovačoch značkuj (taguj) cesty a následne v opačnom smere ich filtruj
- Pri redistribúcii z A do B propaguj korektne metriky
- Používaj default routes na vyhnutie sa two-way redistribúcii

# Core and Edge Routing Protocols - pojmy

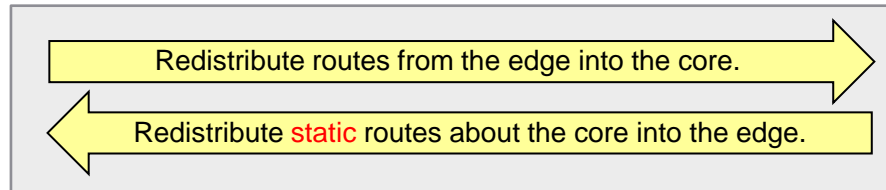
- Na rozlíšenie úloh pri redistribúcii sa zavádzajú dva nové pomocné pojmy:
  - Core routing protocol
  - Edge routing protocol
- V sieťach, kde bežia viaceré IGP smerovacie protokoly
  - Core routing protokol
    - Je pokročilejší sm. protokol, v úlohe hlavného protokolu v sieti (napr. EIGRP, OSPF)
  - Edge routing protokol
    - Je smerovací protokol jednoduchšieho typu (napr. RIP)
- Pri migrácii zo starého IGP protokolu na nový IGP protokol
  - Core routing protokol je nový/zavádzaný smerovací protokol
  - Edge routing protokol je starý smerovací protokol

# Redistribučné techniky - sumár

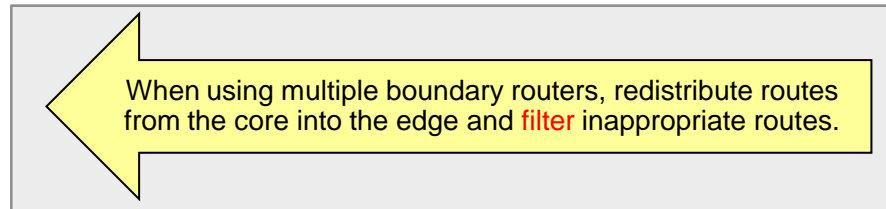
## Technique #1



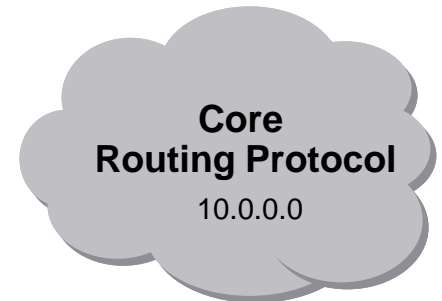
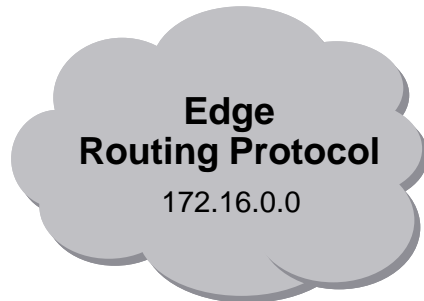
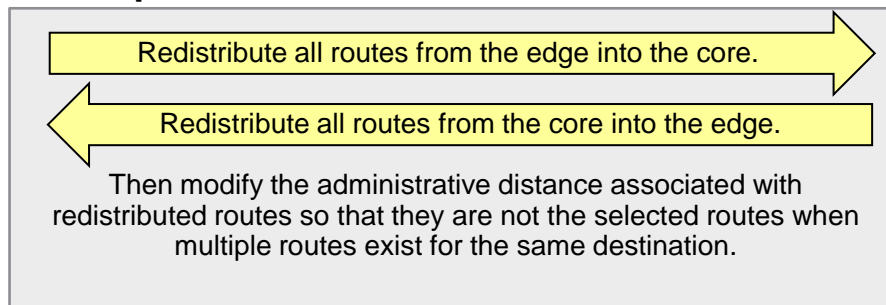
## Technique #2



## Technique #3



## Technique #4



# Redistribúcia - odporúčania

- **Poznaj svoju sieť!!!**
  - Pre optimálne rozhodnutie
- Vyhni sa prekrytiu (overlap) smerovacích protokolov
  - Nepoužívaj v tej istej sieti viaceré protokoly
  - Jasne definuj hranice medzi sieťami s inými sm. protokolmi
- Vyhni sa slučkám
  - Ak sa dá distribuuj cesty len jedným smerom a len na jednom okrajovom smerovači
    - Ale pozor, vzniká centrálny bod chyby
- Ak musí byť redistribúcia riešená na viacerých smerovačoch a v oboch smeroch
  - je potrebné redistribúciu vyladiť voči slučkám a neoptimálnemu smerovaniu.
- Nastav metriku pre cesty z redistribúovaného protokolu na vyššiu ako je najvyššia používaná v danej doméne (AS)



# Implementácia redistribúcie



# Redistribúcia – základné info o konfigurácii

- Uvedomenie si, ktorý smerovací protokol je cieľový a ktorý je zdrojový, je kľúčové pre správnu konfiguráciu
  - Cieľový proces je príjemcom, preberateľom smerovacej informácie
  - Zdrojový proces je autorom, dodávateľom preberanej smerovacej informácie
- Na Cisco smerovačoch sa redistribúcia konfiguruje vždy ako súčasť **cieľového** protokolu
  - Cieľový protokol si vyberá, odkiaľ preberie smerovacie info
- Príkaz **redistribute** hovorí o **zdrojovom** smerovacom protokole, z ktorého sa budú preberať smerovacie informácie
  - Konkrétna aplikácia sa líši podľa smerovacieho protokolu
- Nemožno vykonávať redistribúciu medzi rozdielnymi protokolovými zásobníkmi
  - Napr. IPv4 routes do IPv6

# Konfigurácia redisitribúcie - kroky

1. Urči okrajový smerovač (-če), ktorý vykoná redistribúciu
2. Urči, ktorý smerovací protokol bude core protokol (cieľ)
3. Urči, ktorý smerovací protokol bude edge protokol (zdroj)
  - Urči, či sa budú pri redistribúcii distribuovať všetky cesty z edge do core
  - Pokiaľ sa dá redukuje počet ciest (sumarizácia)
4. Vyber metódu na vloženie ciest z edge do core
5. Zváž aké cesty a ako sa budú vkladať z core smerovacieho protokolu do edge smerovacieho protokolu

# Redistribúcia do RIP

```
Router(config-router)# redistribute protocol  
[process-id] [match route-type]  
[metric metric-value] [route-map map-tag]
```

```
RtrA(config)# router rip  
RtrA(config-router)# redistribute ospf ?  
  
<1-65535> Process ID  
RtrA(config-router)# redistribute ospf 1 ?  
  
match      Redistribution of OSPF routes  
metric     Metric for redistributed routes  
route-map  Route map reference  
...  
<cr>
```

- **Poznámka:** Štandardná počítačová metrika je **nekonečno!**



# Parametre príkazu `redistribute` pre RIP

Parameter	Popis
<code>protocol</code>	Zdrojový protokol, z ktorého sa preberú smerovacie informácie
<code>process-id</code>	Identifikátor čísla procesu (OSPF) alebo autonómneho systému (EIGRP, BGP)
<code>match route-type</code>	(Nepovinné) Test na typ OSPF ciest (interné, externé, NSSA-externé, typ 1, typ 2). Nepoužiteľné pri iných zdrojových smerovacích protokoloch.
<code>metric metric-value</code>	(Nepovinné) Definuje počiatočnú metriku. Pokiaľ nie je parameter uvedený, preberie sa hodnota z príkazu <code>default-metric</code> v konfigurácii RIP. Ak ani tento príkaz nie je prítomný, dosadí sa nekonečná metrika a smery sa neredistribuujú. Metrikou v protokole RIP je počet hopov.
<code>route-map map-tag</code>	(Nepovinné) Identifikátor route-map, ktorá sa použije na filtrovanie a úpravu importovaných smerov.

# Redistribúcia do RIP – príklad

```
R1(config)# router rip  
R1(config-router)# redistribute ospf 1 metric 3  
R1(config-router)#
```

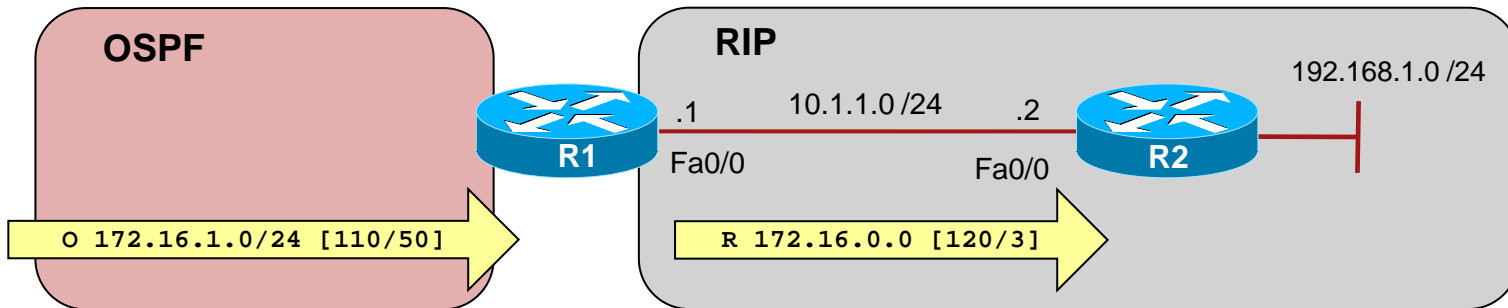


Table R1

```
C 10.1.1.0  
R 192.168.1.0 [120/1]  
O 172.16.1.0 [110/50]
```

Table R2

```
C 10.1.1.0  
C 192.168.1.0  
R 172.16.0.0 [120/3]
```

# Redistribúcia do OSPF

```
Router(config-router)# redistribute protocol  
[process-id] [metric metric-value] [metric-type  
type-value] [route-map map-tag] [subnets] [tag  
tag-value]
```

- Štandardná počiatočná metrika je 20 (ak z BGP, potom 1)
- Redistribuované smery sa vždy prenášajú ako externé smery (LSA5 resp. LSA7), štandardne typ **metriky External 2 (E2 or N2)**
- Podsieť sa štandardne neredistribuuje (preberú sa iba classful siete a supernety)
  - Daná Classful sieť musí byť v Smerov. tabuľke
  - Default route nemožno do OSPF redistribuovať
  - Redistribúcia podsiet'ovaných rozsahov sa povolí parametrom **subnets**

# Parametre příkazu redistribute pre OSPF

Parameter	Description
<i>protocol</i>	The source protocol from which routes are redistributed.
<i>process-id</i>	For EIGRP or BGP, this value is an AS number. This parameter is not required for RIP or IS-IS.
<i>metric-value</i>	(Optional) A parameter that specifies the OSPF seed metric used for the redistributed route. The default metric is a cost of 20 (except for BGP routes, which have a default metric of 1).
<i>metric-type</i>	Redistribute route as type one or type two
<i>map-tag</i>	(Optional) Specifies the identifier of a configured route map to be interrogated to filter the importation of routes from the source routing protocol to the current OSPF routing protocol.
<b>subnets</b>	(Optional) OSPF parameter that specifies that subnetted routes should be redistributed. Otherwise, only classful routes are redistributed.
<i>tag-value</i>	(Optional) A 32-bit decimal value attached to each external route to be used by ASBRs.

# Redistribúcia do OSPF – príklad

```
R1(config)# router ospf 1  
R1(config-router)# redistribute eigrp 100 subnets metric-type 1  
R1(config-router)#
```

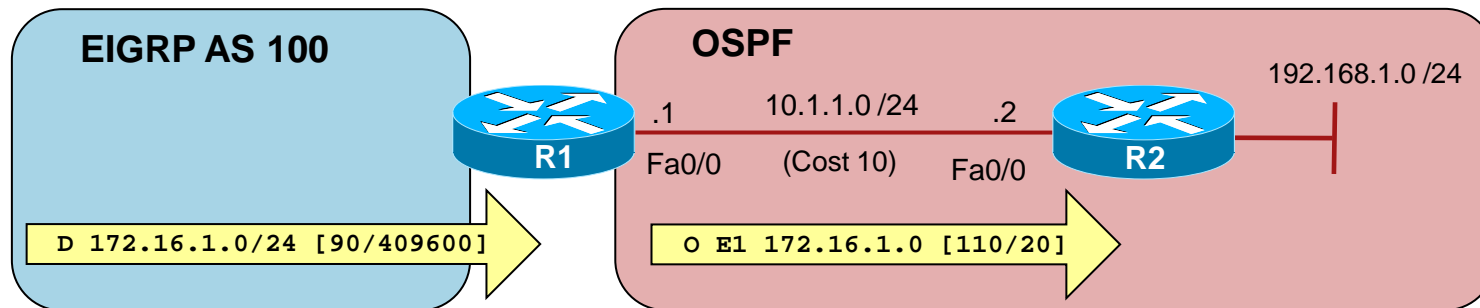


Table R1

```
C 10.1.1.0  
O 192.168.1.0 [110/20]  
D 172.16.1.0 [90/409600]
```

Table R2

```
C 10.1.1.0  
C 192.168.1.0  
O E1 172.16.1.0 [110/30]
```

# Redistribúcia do EIGRP

```
Router(config-router)# redistribute protocol  
  [process-id] [match route-type] [metric metric-  
  value] [route-map map-tag]
```

Parameter	Description
<i>protocol</i>	The source protocol from which routes are redistributed.
<i>process-id</i>	For OSPF, this value is an OSPF process ID. For BGP, this value is an AS number. This parameter is not required for RIP or IS-IS.
<i>route-type</i>	(Optional) A parameter used when redistributing OSPF routes into another routing protocol. { <b>internal</b>   <b>external 1</b>   <b>external 2</b> }
<i>metric-value</i>	Required if the <b>default-metric</b> command is not configured otherwise it is optional . A parameter that specifies the EIGRP seed metric, in the order of bandwidth, delay, reliability, load, and maximum transmission unit (MTU), for the redistributed route. If this value is not specified when redistributing from another protocol and no default metric has been configured, then no routes will not be redistributed.
<i>map-tag</i>	(Optional) Specifies the identifier of a configured route map to be interrogated to filter the importation of routes from the source routing protocol to the current EIGRP routing protocol.

- Štandardná počiatočná metrika je nekonečno

# Redistribúcia do EIGRP – príklad

```
R1(config)# router eigrp 100
R1(config-router)# redistribute ospf 1 metric 10000 100 255 1 1500
R1(config-router)#
```

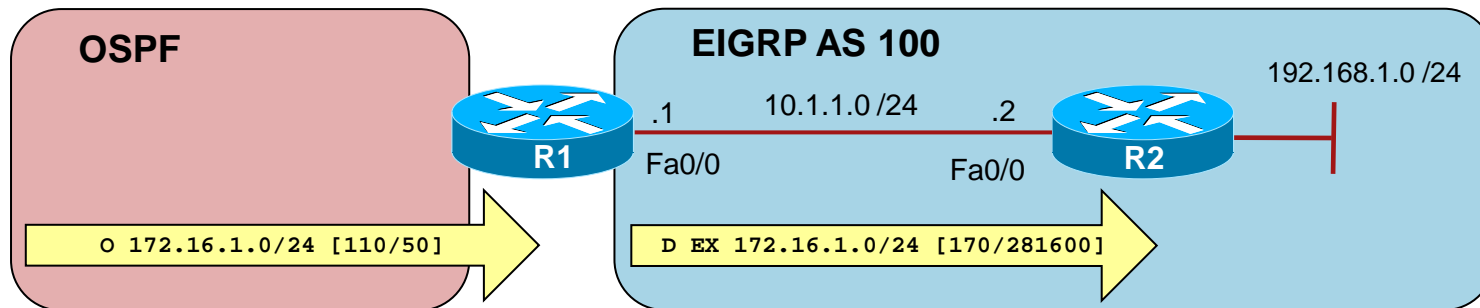


Table R1

```
C 10.1.1.0
O 192.168.1.0 [90/307200]
O 172.16.1.0 [110/50]
```

Table R2

```
C 10.1.1.0
C 192.168.1.0
D EX 172.16.1.0 [170/307200]
```

- **B**andwidth v kilobitoch za sekundu = 10000
- **D**elay v desiatkach mikrosekúnd = 100
- **R**eliability = 255 (maximum)
- **L**oad = 1 (minimum)
- **M**TU = 1500 bajtov

# Nastavenie default metriky pre EIGRP

```
Router(config-router)#
```

```
default-metric BANDWIDTH DELAY RELIABILITY LOADING MTU
```

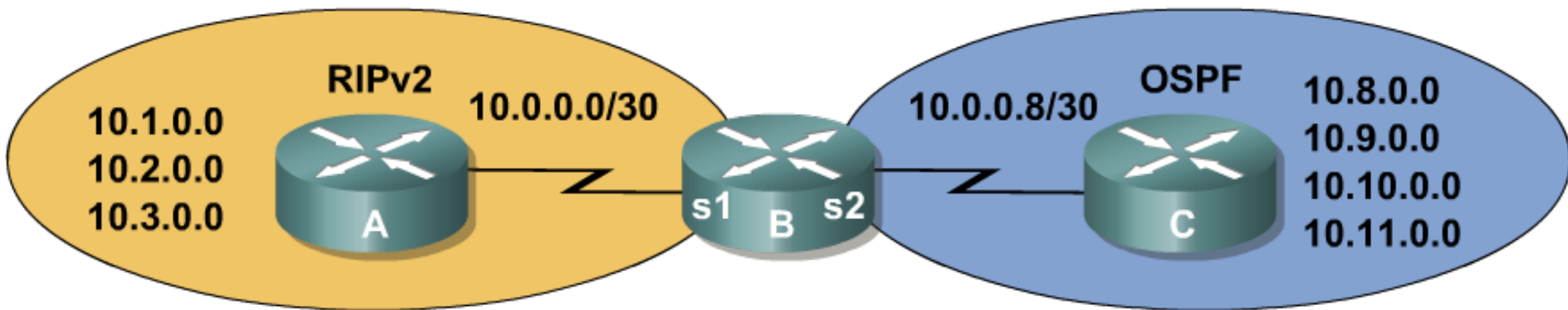
Parameter	Description
<i>bandwidth</i>	The route's minimum bandwidth in kilobits per second (kbps). It can be 0 or any positive integer.
<i>delay</i>	Route delay in tens of microseconds. It can be 0 or any positive integer that is a multiple of 39.1 nanoseconds.
<i>reliability</i>	The likelihood of successful packet transmission, expressed as a number from 0 to 255, where 255 means that the route is 100 percent reliable, and 0 means unreliable.
<i>loading</i>	The route's effective loading, expressed as a number from 1 to 255, where 255 means that the route is 100 percent loaded.
<i>mtu</i>	Maximum transmission unit. The maximum packet size in bytes along the route; an integer greater than or equal to 1.



# Príklad na redistribúciu



# Pred redistribúciou

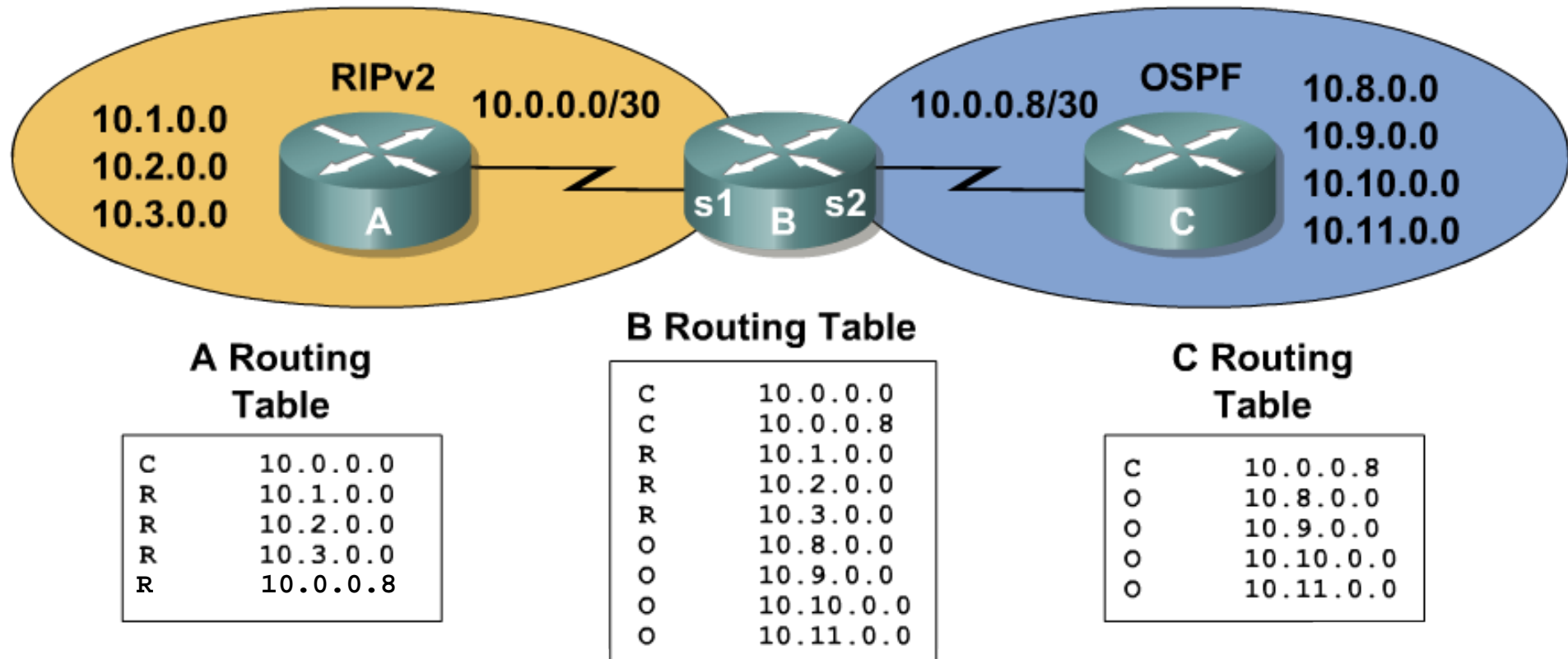


## Router B Configuration

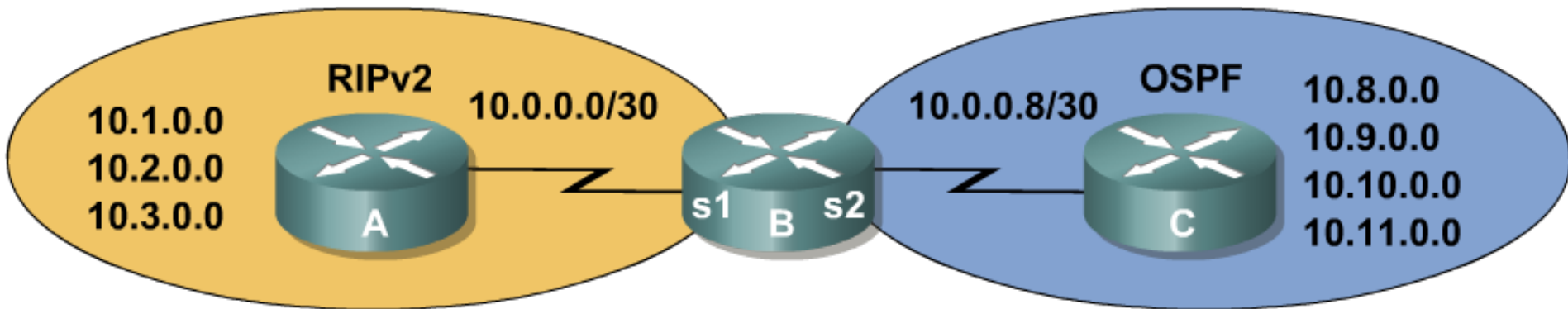
```
router ospf 1
  network 10.0.0.8 0.0.0.3 area 0

router rip
  network 10.0.0.0
  version 2
  passive-interface s2
```

# Pred redistribúciou



# Redistribúcia na smerovači B

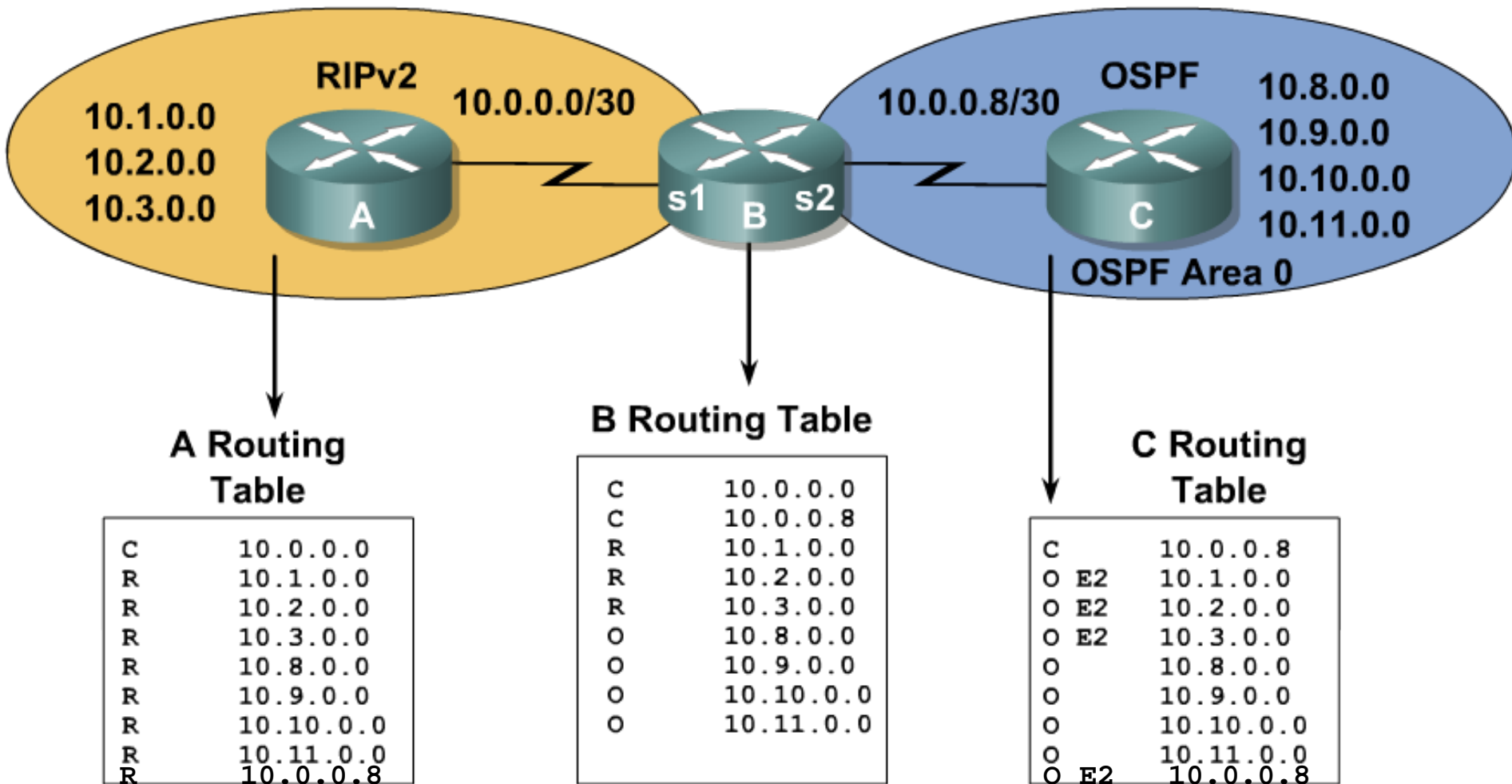


## Router B Configuration

```
router ospf 1
  network 10.0.0.8 0.0.0.3 area 0
  redistribute rip subnets metric 300

router rip
  network 10.0.0.0
  version 2
  passive-interface s2
  redistribute ospf 1 metric 5
```

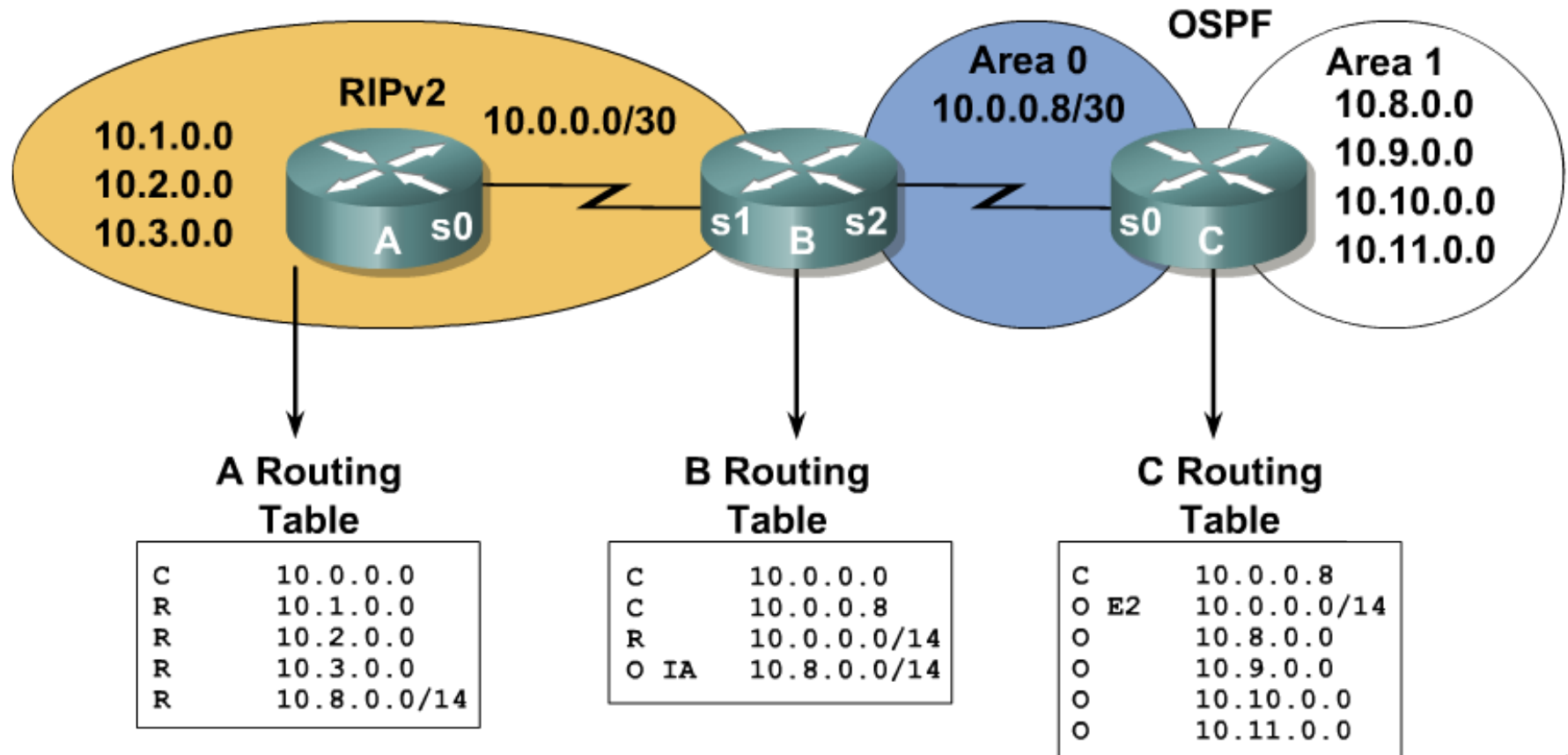
# Po nakonfigurovaní redistribúcie



# Konfigurácia sumarizácie, výsledné smerovacie tabuľky

```
RouterA(config) #interface s0
RouterA(config-if) #ip summary-address rip 10.0.0.0 255.252.0.0
```

```
RouterC(config) #router ospf 1
RouterC(config-router) #area 1 range 10.8.0.0 255.252.0.0
```

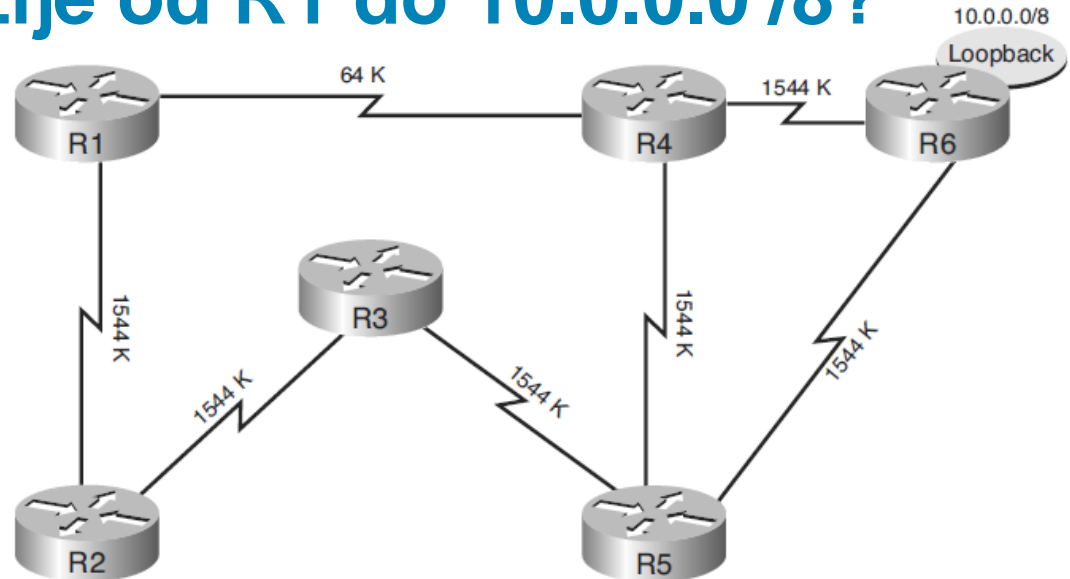




# Výber ciest



# Ktorá cesta sa použije od R1 do 10.0.0.0 /8?

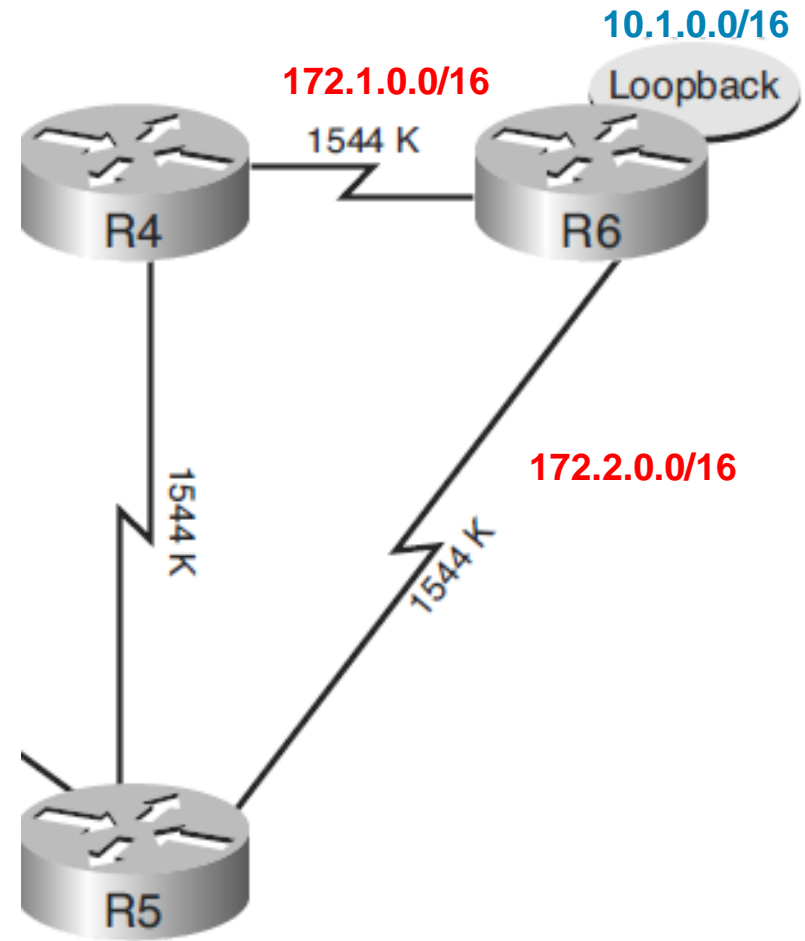


- Máme tri protokoly v sieti, RIP, OSPF, a EIGRP
- Akú cestu použije R1 pre dosiahnutie danej siete daným protokolom?
  - RIP?
    - Cesta: R1 ⇒ R4 ⇒ R6
    - Metrika? Hop count, 3hopy
  - OSPF?
    - Cesta: R1 ⇒ R2 ⇒ R3 ⇒ R5 ⇒ R6
    - Metrika: = (100 Mbps / 1.544 Mbps) + (100 Mbps / 1.544 Mbps) + (100 Mbps / 1.544 Mbps) + (100Mbps / 1.544 Mbps)= 256
  - EIGRP?
    - Cesta: R1 ⇒ R2 ⇒ R3 ⇒ R5 ⇒ R6
    - Metrika: ((107 / 1544) \* 256) + (400 \* 256) = 1,760,431
- Čo bude v smerovacej tabuľke a prečo? **EIGRP, lebo AD=90**



# Ktorá cesta sa použije od R1 do 10.1.0.0/16?

- Tá istá topológia, tri protokoly v sieti, RIP, OSPF, a EIGRP
- Ale na R6 je sieť 10.1.0.0/16
  - Prepojená cez iné „major“ network subsiete
- Čo bude v smerovacej tabuľke R1 a prečo?
  - 10.0.0.0/8
    - Lebo EIGRP aj RIP robia automatickú sumarizáciu
    - V tabuľke bude cesta od EIGRP kvôli AD
  - 10.1.0.0/16 cez OSPF
    - Lebo OSPF nerobí automatickú sumarizáciu



# Ktorá cesta?

- Smerovač má tri smerovacie procesy a prijme cez každý z nich nasledujúce info :
  - EIGRP (internal): 192.168.32.0/26
  - RIP: 192.168.32.0/24
  - OSPF: 192.168.32.0/19
- Ktorá z ciest bude v smerovacej tabuľke?
- **Každá z nich!**
  - EIGRP má najnižší AD, ale ten sa používa len pri cestách s rovnakým prefixom
  - Tu každá cesta má iný prefix, je chápaná ako samostatný cieľ
  - Každá bude v smerovacej tabuľke.

# Modifikácia administratívnej vzdialenosti

- Pri určitých situáciách je potrebné modifikovať AD
  - Redistribúcia, kde sa môže stratiť dôležitá informácia
  - Kde má smerovač informácie od viacerých zdrojov a verí smerovaciemu protokolu s horšou smerovacou info ale s lepšou AD
    - Príklad one point one way redistrib.
- Modifikáciou smerovaču zmeníme rozhodovanie o preferencii pri voľbe cesty
  - Riešime skôr konzistenciu rozhodovania ako optimálnosť smerovania
- Konfigurácia príkazom **distance** *administrative-distance*.
  - Pre OSPF navyše : **distance ospf**
  - Pre EIGRP navyše: **distance eigrp**

# Modifikácia administratívnej vzdialenosti

- Zmena defaultnej AD

```
Router(config-router)#
```

```
distance administrative-distance [address wildcard-mask [ip-  
standard-list] [ip-extended-list]]
```

Parameter	Description
<i>administrative-distance</i>	Sets the administrative distance, an integer from 1 to 255.
<i>address</i>	(Optional) Specifies the IP address; this allows filtering of networks according to the IP address of the router supplying the routing information. For OSPF it is the Router ID.
<i>wildcard-mask</i>	(Optional) Specifies the wildcard mask used to interpret the IP address.
<i>ip-standard-list</i> <i>ip-extended-list</i>	(Optional) The number or name of a standard or extended access list to be applied to the incoming routing updates. Allows setup AD for advertised routes specified by the ACL.

# Modifikácia AD pre OSPF

- Zmena defaultnej AD pre OSPF podľa oblasti.

```
Router(config-router)#
```

```
distance ospf {[intra-area dist1] [inter-area dist2] [external  
dist3]
```

Parameter	Description
<i>dist1</i>	(Optional) Specifies the administrative distance for all OSPF routes within an area. Acceptable values are from 1 to 255 while the default is 110.
<i>dist2</i>	(Optional) Specifies the administrative distance for all OSPF routes from one area to another area. Acceptable values are from 1 to 255 while the default is 110.
<i>dist3</i>	(Optional) Specifies the administrative distance for all routes from other routing domains, learned by redistribution. Acceptable values are from 1 to 255 while the default is 110.

# Modifikácia AD pre EIGRP

- Zmena defaultnej AD pre EIGRP

```
Router(config-router)#
```

```
distance eigrp internal-distance external-distance
```

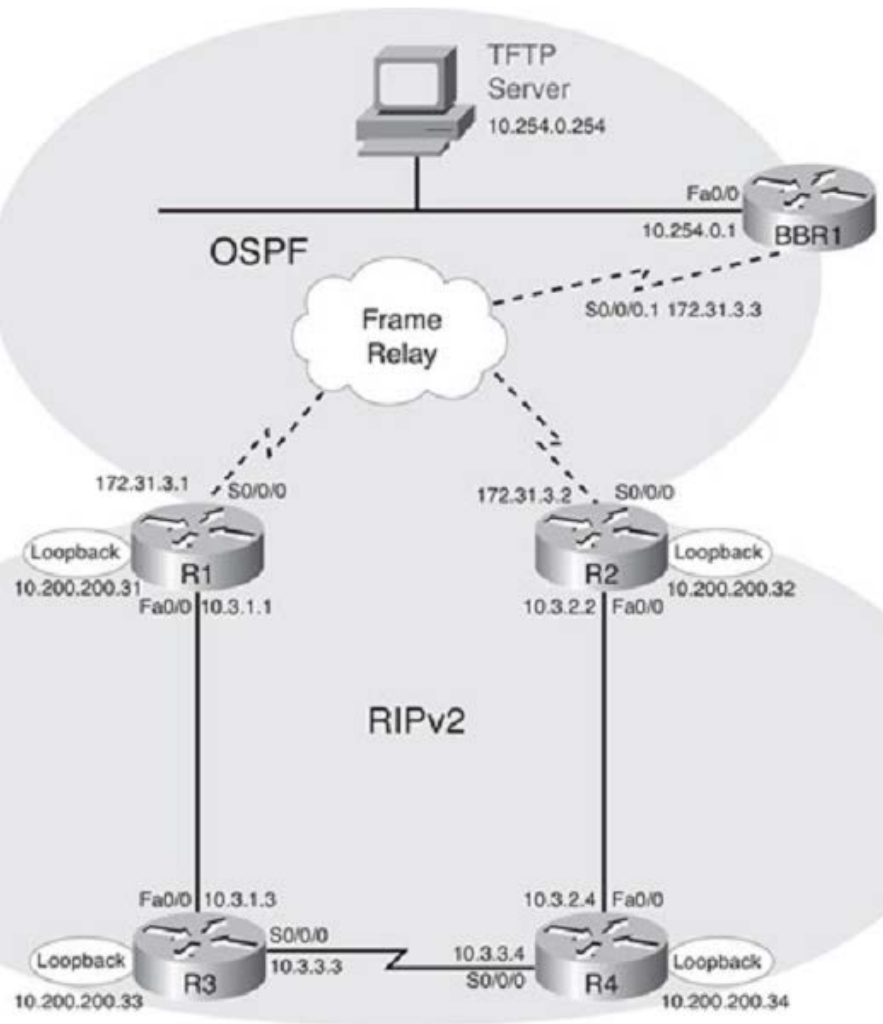
Parameter	Description
<i>internal-distance</i>	Specifies the administrative distance for EIGRP internal routes. The distance can be a value from 1 to 255 while the default is 90.
<i>external-distance</i>	Specifies the administrative distance for EIGRP external routes. The distance can be a value from 1 to 255 while the default is 170.

# Príklad

```
router eigrp 100
  network 192.168.7.0
  network 172.16.0.0
! Nastavi AD 80 pre interne siete a 130 pre externe
distance eigrp 80 130
! Nastavi AD 90 pre siete naucene od smerovacov zo siete ...
distance 90 192.168.7.0 0.0.0.255
! Nastavi AD 120 pre cesty naucene od smerovaca s IP
distance 120 172.16.1.3 0.0.0.0
```

```
router ospf 10
  network 192.168.7.0 0.0.0.255 area 0
  network 172.16.0.0 0.0.255.255 area 0
! Nastavi AD pre externe siete na 100, inter area na 100 a
! intra area tiez na 100
distance ospf external 100 inter-area 100 intra-area 100
! Pri OSPF nastavi AD na 90 pre siete naucene od smerovacov
! s RID (nie IP) 10.0.0.0 0.0.0.255
distance 90 10.0.0.0 0.0.0.255
! ...
distance 110 10.11.0.0 0.0.0.255
! ...
distance 130 10.11.12.0 0.0.0.255
```

# Príklad – kde je problém?



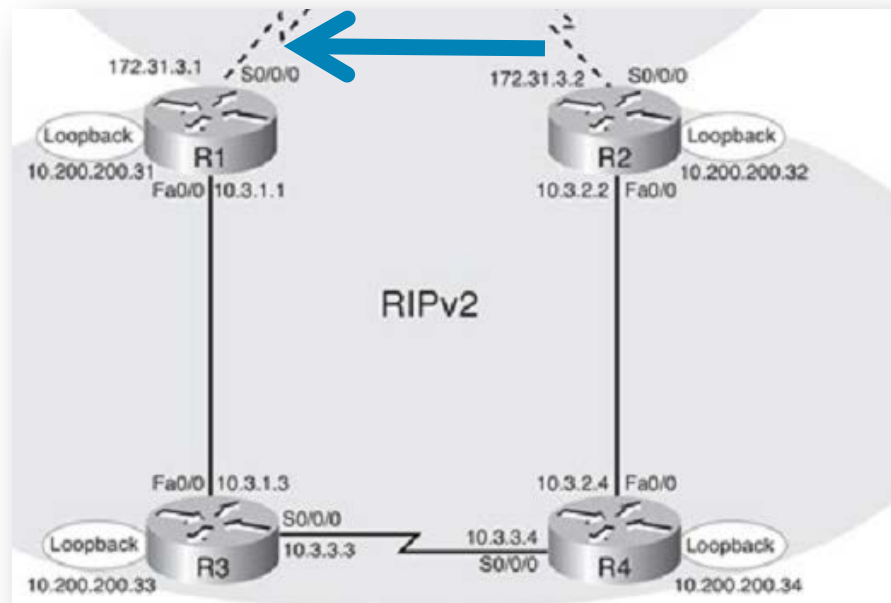
**Aká bude cesta z R2 do loop siete na R4?**

```
hostname R1
!  
router ospf 1  
redistribute rip metric 10000 metric-type  
1 subnets  
network 172.31.0.0 0.0.255.255 area 0  
!  
router rip  
version 2  
redistribute ospf 1 metric 5  
network 10.0.0.0  
no auto-summary
```

```
hostname R2  
!  
router ospf  
redistribute rip metric 10000 metric-type  
1 subnets  
network 172.31.0.0 0.0.255.255 area 0  
!  
router rip  
version 2  
redistribute ospf 1 metric 5  
network 10.0.0.0  
no auto-summary 1
```



# Neoptimálne smerovanie



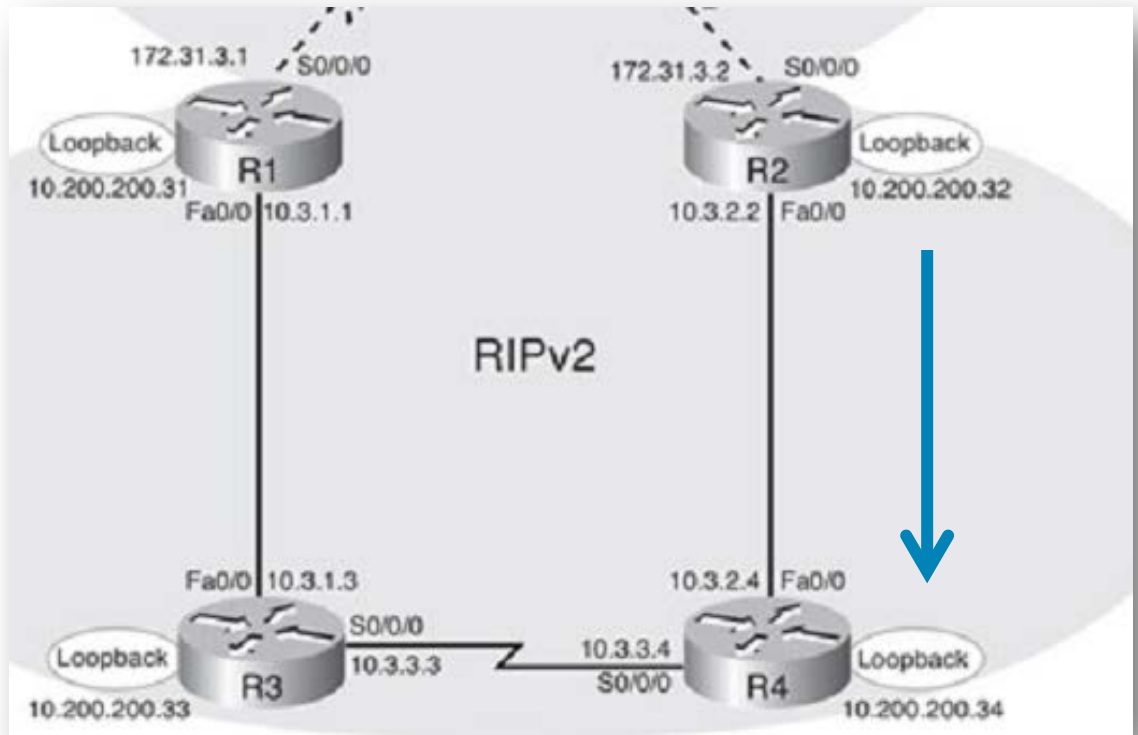
```
R2# show ip route
<output omitted>
Gateway of last resort is not set
  172.31.0.0/24 is subnetted, 1 subnet
C       172.31.3.0/24 is directly connected, Serial0/0/0
C       10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O E1    10.3.1.0/24 [110/10781] via 172.31.3.1, 00:09:47, Serial0/0/0
O E1    10.3.3.0/24 [110/10781] via 172.31.3.1, 00:04:51, Serial0/0/0
C       10.3.2.0/24 is directly connected, FastEthernet0/0
O E1    10.200.200.31/32 [110/10781] via 172.31.3.1, 00:09:48, Serial0/0/0
O E1    10.200.200.34/32 [110/10781] via 172.31.3.1, 00:04:52, Serial0/0/0
C       10.200.200.32/32 is directly connected, Loopback0
O E1    10.200.200.33/32 [110/10781] via 172.31.3.1, 00:04:52, Serial0/0/0
O E2    10.254.0.0/24 [110/50] via 172.31.3.3, 00:09:48, Serial0/0/0
R2#
```

# Príklad – riešenie

```
hostname R1
!
router ospf 1
redistribute rip metric 10000 metric-type
 1 subnets
network 172.31.0.0 0.0.255.255 area 0
distance 125 0.0.0.0 255.255.255.255 64
!
router rip
version 2
redistribute ospf 1 metric 5
network 10.0.0.0
no auto-summary
!
access-list 64 permit 10.3.1.0
access-list 64 permit 10.3.3.0
access-list 64 permit 10.3.2.0
access-list 64 permit 10.200.200.31
access-list 64 permit 10.200.200.32
access-list 64 permit 10.200.200.33
access-list 64 permit 10.200.200.34
```

```
hostname R2
!
router ospf 1
redistribute rip metric 10000 metric-type
 1 subnets
network 172.31.0.0 0.0.255.255 area 0
distance 125 0.0.0.0 255.255.255.255 64
!
router rip
version 2
redistribute ospf 1 metric 5
network 10.0.0.0
no auto-summary
!
access-list 64 permit 10.3.1.0
access-list 64 permit 10.3.3.0
access-list 64 permit 10.3.2.0
access-list 64 permit 10.200.200.31
access-list 64 permit 10.200.200.32
access-list 64 permit 10.200.200.33
access-list 64 permit 10.200.200.34
```

# Po úprave



```
R2#show ip route
<output omitted>
172.31.0.0/24 is subnetted, 1 subnet
C       172.31.3.0/24 is directly connected, Serial0/0/0
      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
R       10.3.1.0/24 [120/2] via 10.3.2.4, 00:00:03, FastEthernet0/0
R       10.3.3.0/24 [120/1] via 10.3.2.4, 00:00:03, FastEthernet0/0
C       10.3.2.0/24 is directly connected, FastEthernet0/0
R       10.200.200.31/32 [120/3] via 10.3.2.4, 00:00:04, FastEthernet0/0
R       10.200.200.34/32 [120/1] via 10.3.2.4, 00:00:04, FastEthernet0/0
C       10.200.200.32/32 is directly connected, Loopback0
R       10.200.200.33/32 [120/2] via 10.3.2.4, 00:00:04, FastEthernet0/0
O E2    10.254.0.0/24 [110/50] via 172.31.3.3, 00:00:04, Serial0/0/0
```



## Riadenie obsahu smerovacích aktualizácií



# Riadenie obsahu smerovacích aktualizácií

- Cisco smerovače majú mnohé prostriedky, ktorými dokážu riadiť obsah a rozposielanie smerovacích informácií
  - Ani jeden nie je univerzálne nasaditeľný do každej situácie, skôr nasadené v kombinácii
- **Pasívne rozhrania**
  - Týmito rozhraniami sa neodosielajú nijaké smerovacie informácie
  - Alebo sa nenadväzujú ADJ vzťahy
- **Route-map**
  - Filtrujú a upravujú obsah smerovacích informácií, ktoré do daného smerovacieho protokolu redistribuujeme
  - Niektoré smerovacie protokoly dovoľujú využiť route-map aj v distribučných zoznamoch alebo v príkaze neighbor
- **Distribučné zoznamy**
  - Filtrujú obsah smerovacích informácií, ktoré v rámci daného smerovacieho protokolu posielame alebo prijímame
- **Prefix-lists**
  - Špeciálne prístupové zoznamy dizajnované na využitie pre filtrovanie updates

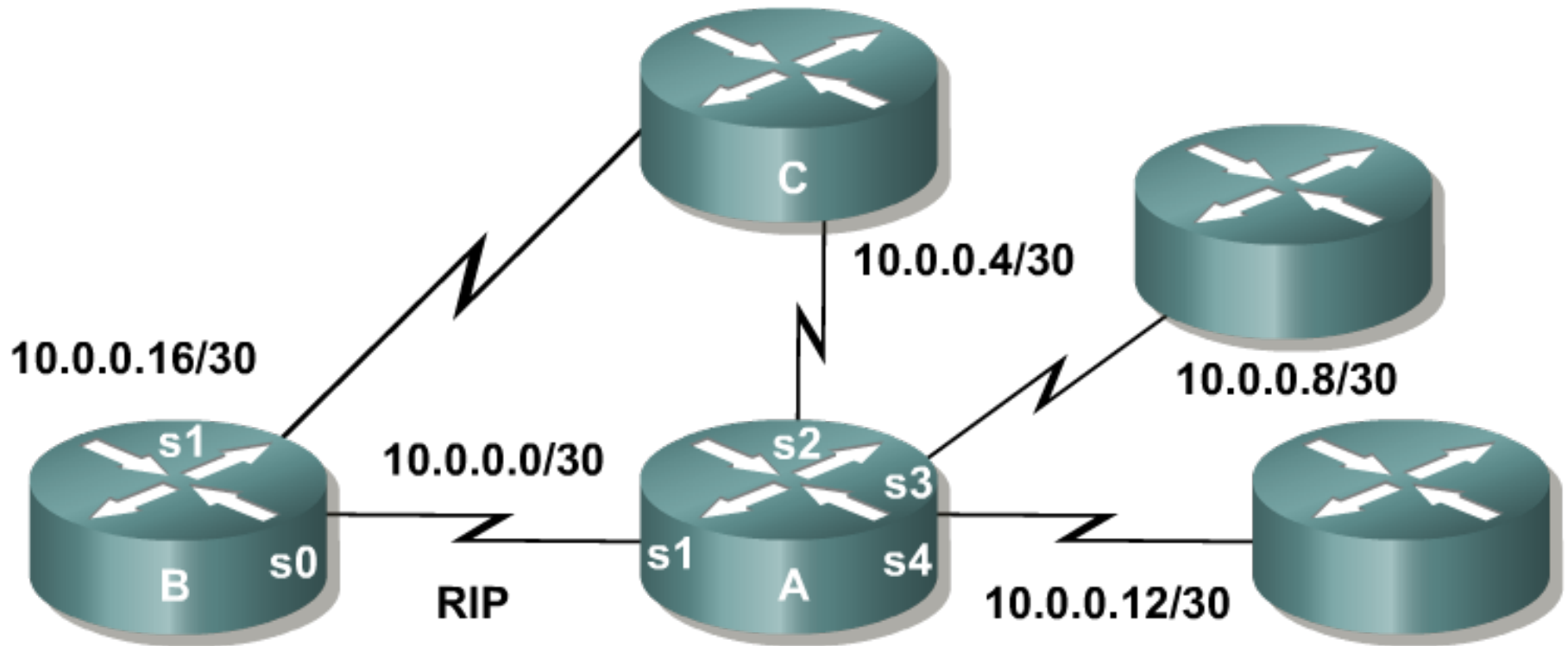
# Príkaz `passive-interface`

- Pasívne rozhrania v zásade neodosielaajú pakety smerovacieho protokolu, čiže na danom rozhraní efektívne odfiltrujú úplne všetky siete odosielané daným protokolom
  - V protokole RIP však pasívne rozhranie akceptuje prijaté RIP pakety. Pokiaľ je to neželané, treba ich odfiltrovať pomocou ACL
  - V protokoloch používajúcich Hello pakety (EIGRP, OSPF, IS-IS) pasívne rozhranie neposiela ani neprijíma pakety príslušného smerovacieho protokolu
  - V IS-IS definovanie pasívneho rozhrania navyše spôsobí, že sa bude sieť z neho oznamovať, a to bez toho, aby na rozhraní bol príkaz `ip router isis`
    - Podobne sa chová aj EIGRP pre IPv6 vo väčšine IOSov

# Príkaz `passive-interface`

- Pasívne rozhrania možno vymenovať v konfigurácii daného smerovacieho protokolu:
  - Buď vymenovaním konkrétnych rozhraní príkazom `passive-interface IFACE`
  - Alebo konštruktom `passive-interface default` a následným „aktivovaním“ konkrétnych rozhraní príkazom `no passive-interface IFACE`

# Príkaz passive-interface



## Router B Configuration

```
router rip
network 10.0.0.0
passive-interface s1
```

## Router A Configuration

```
router rip
network 10.0.0.0
passive-interface default
no passive-interface s1
```



# Route Map

- Route map je sofistikovaná konštrukcia, ktorá dovoľuje vytvárať pravidlá v tvare if-then-else
- Základná idea:
  - Route-map sa skladá z jedného alebo viacerých blokov tvaru Test, Zmena, Akcia
    - Skontrolovať, či sú splnené predpísané predpoklady – test ([match](#))
    - Ak áno, vykonať požadovanú akciu ([permit/deny](#))
    - a prípadne realizovať v obsahu paketu alebo v jeho putovaní nejaké zmeny ([set](#))
- Spracovanie je podobné ako v ACL
  - Postupuje sa jednotlivými blokmi zhora nadol
    - Bloky sú číslované (umožňujú post editáciu)
  - Pri prvej zhode sa vykoná akcia spolu so zmenami a vyhodnocovanie končí
  - Na konci každej route-map je implicitné „match any (test) / deny (akcia)“
- Route-map ako celok má meno, každý jeho blok musí mať to isté meno

# Definovanie Route Mapy

Router(config)#

```
route-map map-tag [permit | deny] [sequence-number]
```

Parameter	Description
<i>map-tag</i>	Name of the route map.
<i>permit</i>   <i>deny</i>	(Optional) A parameter that specifies the action to be taken if the route map match conditions are met; the meaning of permit or deny is dependent on how the route map is used.
<i>sequence-number</i>	(Optional) A sequence number that indicates the position that a new route map statement will have in the list of route map statements already configured with the same name.

- Každý **route map** blok je číslovaný sekvenčným číslom
  - Preto môže byť neskôr editovaný
- Default správanie pre **route-map** príkaz je **permit**, so sekvenčným číslom 10.

# Tvar a činnosť route-map konštruktu


- Route-map pozostáva z blokov, každý blok má
  - nepovinnú časť pre test (**match**),
  - nepovinnú časť pre zmeny (**set**) a
  - povinnú časť pre akciu (**permit/deny**)
- Bloky sa vyhodnocujú zhora nadol, konkrétne ich časti pre test
- Blok, v ktorom sa nájde prvá zhoda, uplatní svoje zmeny a akciu.
  - Tým vyhodnocovanie konkrétnej route-map končí
- Poradové čísla sa využívajú pri vsúvaní alebo odstraňovaní konkrétneho bloku z konkrétnej pozície

```
route-map my_bgp permit 10
    { match statements }
    { match statements }
    { set statements }
    { set statements }
route-map my_bgp deny 20
    ::          ::      ::
    ::          ::      ::
route-map my_bgp permit 30
    ::          ::      ::
    ::          ::      ::
```

# Tvar a činnosť route-map konštruktu

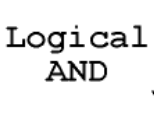
- Route map bez žiadnej test podmienky sa považuje za spĺňajúci podmienku (matched)
- Príkaz *match* môže obsahovať viacero argumentov v jednom riadku
  - Medzi nimi platí logické OR – stačí zhoda v jednom argumente

```
route-map my_bgp permit 10
match ip address  x  y  z
```



Logical OR

```
route-map my_bgp deny 20
match ...a
match ...b
match ...c
```



Logical AND

014G\_330

- Ak blok obsahuje viaceré match príkazy, musia byť splnené všetky
  - platí logické AND
- Ak testovaná sieť resp. paket vyhoveli všetkým riadkom match v bloku, akcia permit alebo deny v záhlaví bloku určí definitívny osud

# Príkazy na tvorbu route-map

```
router(config)#
```

```
route-map map-tag [permit | deny] [sequence-number]
```

- Vytvorí blok route-map a definuje akciu

```
router(config-route-map)#
```

```
match {conditions}
```

- V bloku route-map definuje test

```
router(config-route-map)#
```

```
set {actions}
```

- V bloku route-map definuje zmenu

```
router(config-router)#
```

```
redistribute protocol [process id] route-map map-tag
```

- Príklad použitia definovanej route-map v redistribúcii

# Príkazy match

- Príkaz/-y `match` tvoria testovaciu časť bloku `route-map`
- Akcia v záhlaví tohto bloku sa vykoná na všetkých paketoch resp. sieťach, ktoré testom vyhoveľi

```
router(config-route-map)#
```

```
match {condition}
```

```
options :
```

```
ip address ip-access-list
```

```
ip route-source ip-access-list
```

```
ip next-hop ip-access-list
```

```
interface type number
```

```
metric metric-value
```

```
route-type [external | internal | level-1 | level-2 | local]
```

```
...
```

# Príkazy match

Príkaz	Popis
<code>match community</code>	Testuje BGP atribút Community
<code>match interface</code>	Testuje, či next hop pre danú cieľovú sieť leží v sieti za uvedeným rozhraním
<code>match ip address</code>	Testuje tvar cieľovej siete a jej masku voči definovanému ACL alebo prefix listu
<code>match ip next-hop</code>	Testuje next-hop cieľovej siete voči definovanému ACL
<code>match ip route-source</code>	Testuje autora danej smerovacej informácie voči definovanému ACL
<code>match length</code>	Testuje L3 dĺžku paketu
<code>match metric</code>	Testuje metriku cieľovej siete
<code>match route-type</code>	Testuje typ cieľovej siete
<code>match tag</code>	Testuje návěstie (značku, tag) cieľovej siete

# Príkazy set

- Príkaz **set** ovplyvňuje obsah smerovacej informácie (napr. metriku) alebo postup paketu

```
router(config-route-map)#
```

```
set {action}
  options :
  ▪ metric metric-value
  ▪ metric-type [type-1 | type-2 | internal | external]
  ▪ level [level-1 | level-2 | level-1-2 | stub-area | backbone]
  ▪ ip next-hop next-hop-address
```



# Príkazy set

Príkaz	Popis
<code>set as-path</code>	Modifikuje AS cestu v BGP
<code>set automatic-tag</code>	Automaticky určí hodnotu značky v cieľovej sieti
<code>set community</code>	Nastaví hodnotu BGP atribútu Community
<code>set default interface</code>	Interfejs, ktorým preposlať pakety, pre ktoré nie je v smerovacej tabuľke explicitná cieľová sieť
<code>set interface</code>	Interfejs, ktorým preposlať pakety
<code>set ip default next-hop</code>	Brána, na ktorú preposlať pakety, pre ktoré nie je v smerovacej tabuľke explicitná cieľová sieť
<code>set ip next-hop</code>	Brána, na ktorú preposlať pakety
<code>set level</code>	Definuje, kam importovať externé smery v IS-IS alebo OSPF
<code>set local-preference</code>	Nastaví hodnotu BGP atribútu local preference
<code>set metric</code>	Nastaví metriku cieľovej siete
<code>set metric-type</code>	Nastaví typ metriky cieľovej siete
<code>set tag</code>	Nastaví značku cieľovej siete
<code>set weight</code>	Nastaví hodnotu BGP atribútu weight

# Použitie konštrukcie route-map

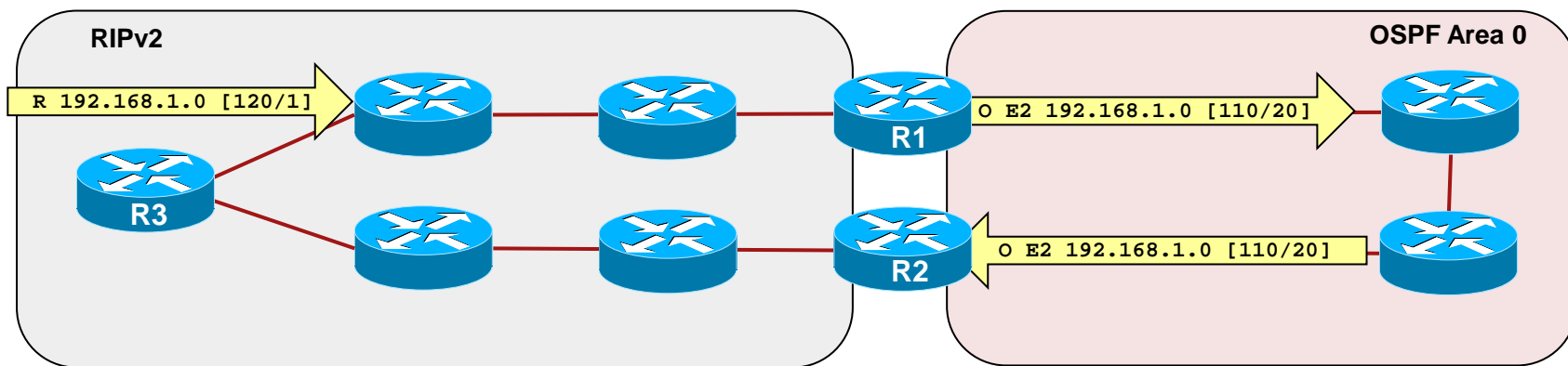
- Route-map má široké využitie vo viacerých aplikáciách, preto je jej špecifikácia pomerne rozsiahla a univerzálna
  - Riadenie redistribúcie alebo filtrovanie obsahu rozosielaných smerovacích informácií
    - Rozširuje možnosť filtrovania, ako ju poznáme z distribučných zoznamov, o schopnosť čiastočných úprav obsahu
  - Policy-based routing (PBR)
    - Schopnosť smerovať tok paketov nielen na základe príjemcu, ale i dodatočných kritérií
  - BGP politiky
    - Route-map je jeden z kľúčových prostriedkov efektívneho využívania protokolu BGP

# Použitie route-map v redistribúcii

- Cieľové siete vyhovujúce ACL 23 alebo 29 sa redistribuujú ako OSPF E1 smery s metrikou 500
- Cieľové siete vyhovujúce ACL 37 sa neredistribuujú
- Všetky ostatné smery sa importujú ako E2 s metrikou 5000
- Poznámka: Siete sa (ne)redistribuujú nie na základe permit/deny v ACL ale permit/deny v route-map bloku

```
R1(config)# access-list 23 permit 10.1.0.0 0.0.255.255
R1(config)# access-list 29 permit 172.16.1.0 0.0.0.255
R1(config)# access-list 37 permit 10.0.0.0 0.255.255.255
R1(config)#
R1(config)# route-map REDIS-RIP permit 10
R1(config-route-map)# match ip address 23 29
R1(config-route-map)# set metric 500
R1(config-route-map)# set metric-type type-1
R1(config-route-map)#
R1(config-route-map)# route-map REDIS-RIP deny 20
R1(config-route-map)# match ip address 37
R1(config-route-map)#
R1(config-route-map)# route-map REDIS-RIP permit 30
R1(config-route-map)# set metric 5000
R1(config-route-map)# set metric-type type-2
R1(config-route-map)#
R1(config-route-map)# exit
R1(config)# router ospf 10
R1(config-router)# redistribute rip route-map REDIS-RIP subnets
R1(config-router)#
```

# Route Feedback s Route mapou



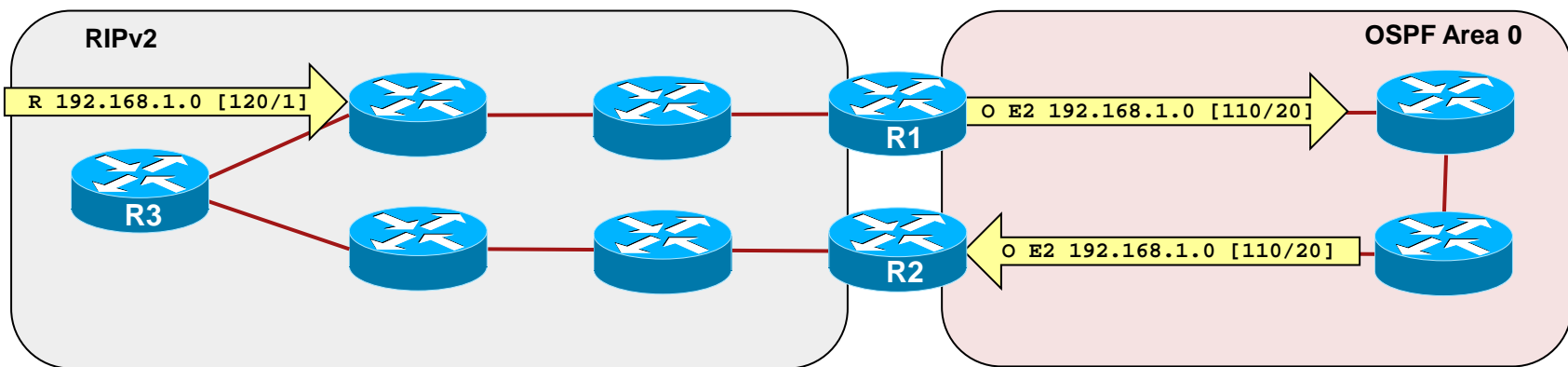
## Route feedback

- Potencionálna situácia, kedy je redistribuovaná cesta z edge do core následne redistribuovaná späť iným smerovačom z core do edge protokolu
  - Napr. pri multipoint two way redistribúcii
- Dôsledky v neoptimálnom smerovaní alebo vzniku smerovacích slučiek

## Príklad

- R3 cez RIPv2 preposiela info o sieti 192.168.1.0
- R1 redistribuuje sieť 192.168.1.0 do OSPF
- OSPF propaguje cestu cez OSPF v rámci danej smerovacej domény
  - OSPF sieť potencionálne posunie info o sieti na R2
- R2 redistribuuje sieť 192.168.1.0 z OSPF späť do pôvodnej RIPv2 siete, čím vytvorí slučku

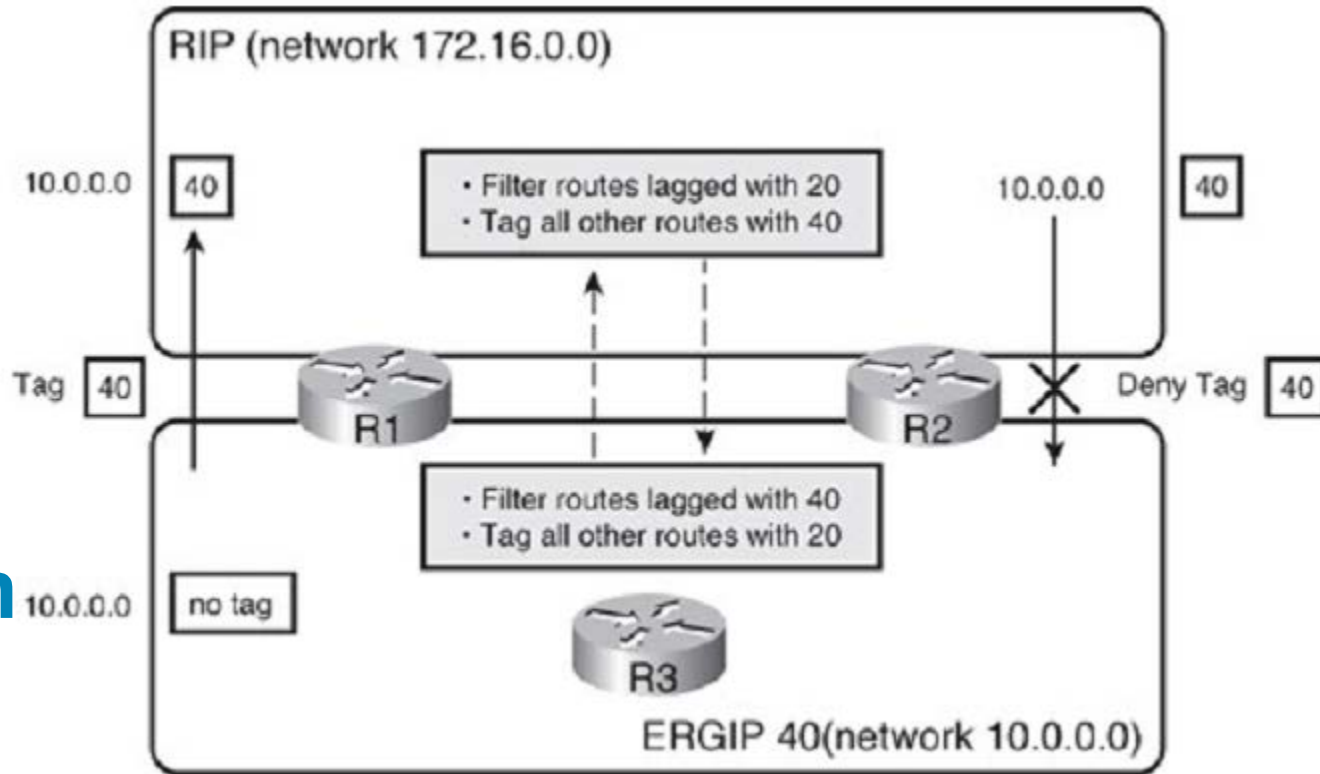
# Riešenie Route Feedback s Route Mapou a redistribúciou



```
R1(config)# access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)# route-map OSPF-into-RIP deny 10
R1(config-route-map)# match ip address 1
R1(config-route-map)# route-map OSPF-into-RIP permit 20
R1(config-route-map)# router rip
R1(config-router)# redistribute ospf 10 metric 5 route-map OSPF-into-RIP
R1(config-router)# router ospf 10
R1(config-router)# redistribute rip subnets
R1(config-router)#
```

- V bloku 10, ľubovoľná sieť ktorá sa zhoduje s ACL 1 je zakázaná a nebude redistribuovaná späť do RIP
- V bloku 20, všetky ostatné siete majú povolenie byť redistribuované z OSPF do RIPv2 s metrikou 5


# Riešenie Route Feedback s route mapou a značkováním



- Značkovanie je technika umožňujúca si označiť dané cesty
  - A neskôr na základe značky vykonať akcie
  - Musí byť podporovaná smerovacím protokolom
- Príklad
  - Cesty redistribuované z EIGRP do RIP sú označované tagom 40
    - Cesty otagované značkou 40 teda nesmú byť spätne redistribuované do EIGRP
  - Cesty redistribuované z RIP do EIGRP sú označované tagom 20
    - Cesty otagované značkou 20 teda nesmú byť spätne redistribuované do RIP

# Nasadenie Route mapy na označkovanie redistribuovaných smerov

```
router eigrp 100
  redistribute rip metric 10000 100 255 1 1500 route-map intoeigrp
<output omitted>
!
router rip
  redistribute eigrp 100 metric 3 route-map intorip
<output omitted>
!
route-map intoeigrp deny 10
  match tag 40
!
route-map intoeigrp permit 20
  set tag 20
!
route-map intorip deny 10
  match tag 20
!
route-map intorip permit 20
  set tag 40
!
```



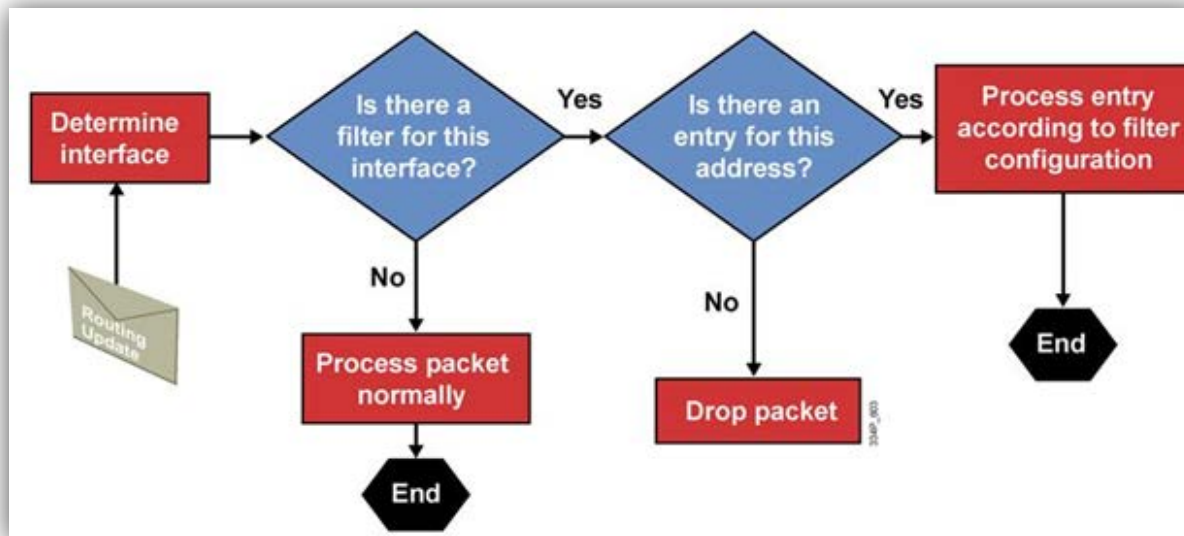
# Použitie ACL v route-map

- Pri redistribúcii s využitím route-map sa veľmi často využívajú ACL na výber resp. odfiltrovanie sietí
  - Sieť je pre tento účel chápaná ako dvojica [IP adresa, Maska]
- Do ACL v route-map táto dvojica vstupuje ako fiktívny odosielateľ a príjemca paketu
  - IP adresa siete je „odosielateľ“ (source condition)
  - Maska siete je „adresát“ (destination condition)
- Podľa typu ACL sa kontrolujú redistribuované siete
  - Štandardné ACL kontroluje iba IP adresu siete, nie masku
  - Rozšírené ACL kontroluje aj IP adresu siete, aj jej masku
- Celý tento zmätok s ACL naznačuje, že pre filtrovanie sietí je najlepšie používať prefix-list ... 😊
  - Ukážeme za chvíľu



# Distribučné zoznamy

- Distribučný zoznam (distribution list)
  - Umožňuje z prenášaných/prijímaných informácií v rámci jedného smerovacieho protokolu odfiltrovať neželané siete
    - Na vstupnom rozhraní
    - Na výstupnom rozhraní
    - Pri redistribúcii
  - Distribučný zoznam je príkaz, ktorý sa odvoláva na ACL alebo tzv. prefix list, ktorým sú oznamované/prijímané siete filtrované
  - Nie je to samostatný zoznam pravidiel, iba spôsob využitia ACL alebo iných nástrojov pre filtrovanie **obsahu správ** smerovacích protokolov



# Distribučné zoznamy - správanie

- Medzi IGP sa chovanie distribučných zoznamov líši:
  - Distance-vector protokoly (RIP, EIGRP)
    - Pomocou distribučných zoznamov dokážu odfiltrovať ľubovoľnú sieť prijatú alebo odoslanú v smerovacej správe (pakete)
  - OSPF
    - v smere **in** filtruje len cesty, ktoré sa dostanú **do smerovacej tabuľky**, ale zmena v LSDB nenastane;
      - Nesmie filtrovať topo LSA
    - v smere **out** filtruje iba externé smery, ak je daný router v úlohe ASBR
      - LSA5/7
  - Protokol IS-IS nepodporuje distribučné zoznamy

# Konfigurácia distribučných zoznamov pre filtrovanie vo vstupnom smere (IN)

```
Router(config-router)#
```

```
distribute-list {access-list-number | name} [route-  
map map-tag] in [interface-type interface-number]
```

## ■ Parametre:

- *access-list-number* | *name*: identifikácia ACL
- **route-map** *map-tag*: identifikácia tzv. route-map
- **in**: smer, v ktorom sa má filtrovanie diať
- *interface-type* *interface-number*: rozhranie, na ktorom sa filtrovanie informácií má diať
- Zoznam so špecifikovaným rozhraním má prednosť pred zoznamom bez udaného rozhrania, lebo sa považuje za adresnejší

# Konfigurácia distribučných zoznamov pre filtrovanie vo výstupnom smere (OUT)

```
Router(config-router)#
```

```
distribute-list {access-list-number | name} out  
[interface-type interface-number | routing-process  
[routing-process parameter]]
```

## ■ Parametre:

- *access-list-number* / *name*: identifikácia ACL
- *out*: smer, v ktorom sa má filtrovanie diať
- *interface-type interface-number*: rozhranie, na ktorom sa filtrovanie informácií má diať
- *routing-process*: (voliteľné) Špecifikuje meno smerovacieho procesu, or *static* or *connected*, ktorý sa redistribuuje a z ktorého sa budú filtrovať updates
- *routing-process parameter*: (voliteľné) Špecifikuje parameter smerovacieho procesu, ako napr. AS

# Distribučné zoznamy a ACL

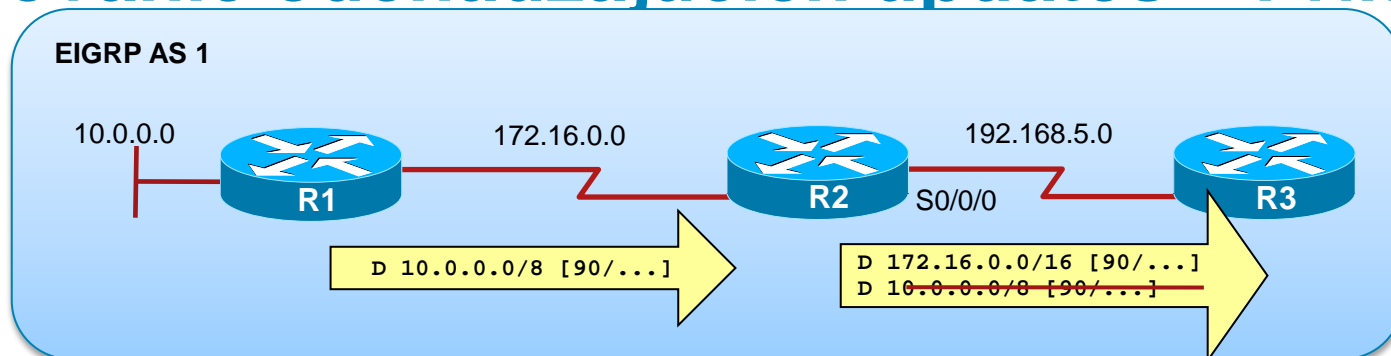
- Podľa typu ACL sa rôzne kontrolujú položky v smerovacom pakete
  - Štandardné ACL kontroluje iba IP adresu siete
  - Rozšírené ACL kontroluje next hop (zdrojová časť v ACL) a IP adresu siete (cieľová časť v ACL)
    - Ak si nie sme istí, použime pravidlo **permit ip any any log**
- Význam akcií:
  - Permit: povolí odoslanie resp. prijatie danej siete
  - Deny: zakáže odoslanie resp. prijatie danej siete
- Príklad: odstrániť všetky siete tvaru 10.X.Y.Z a sieť 192.168.1.0

```
access-list 1 deny 10.0.0.0 0.255.255.255
access-list 1 deny 192.168.1.0 0.0.0.0
access-list 1 permit any
```

- Príklad: od next-hop 1.2.3.4 prevziať iba siete tvaru 172.16.X.X

```
access-list 100 permit ip host 1.2.3.4 172.16.0.0 0.0.255.255
```

# Filtrovanie odchádzajúcich updates – Príklad 1



## ▪ Cieľ

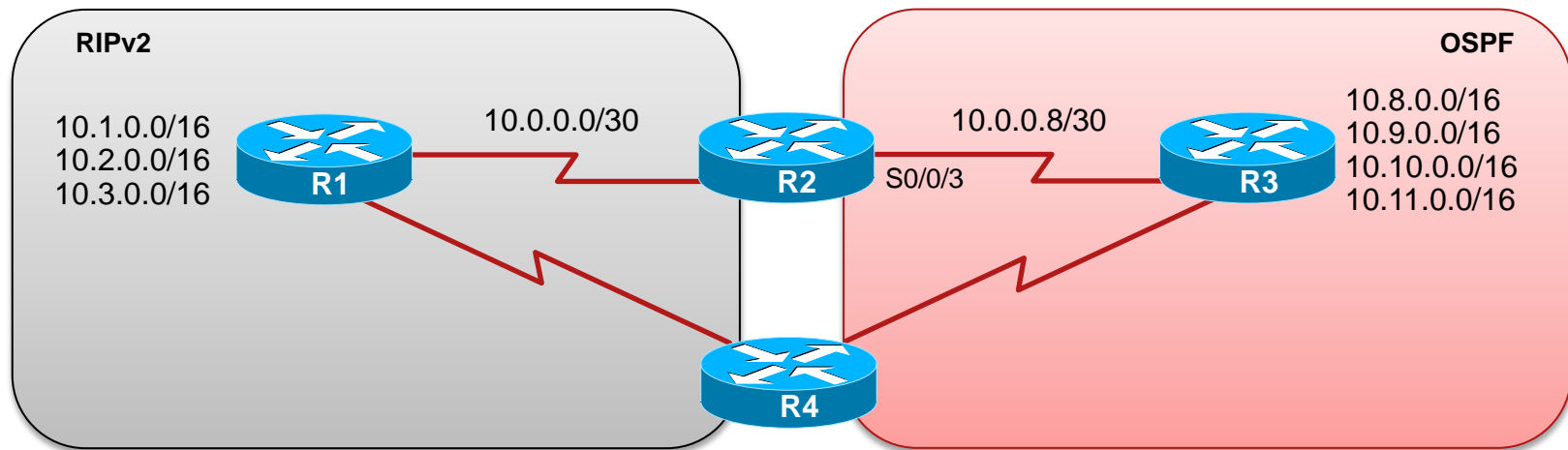
- Odfiltruj sieť 10.0.0.0, ktorá bude pre zariadenia v sieti 192.168.5.0 neviditeľná
- Zasielanie info o ostatných sieťach povol'

```
R2(config)# access-list 7 permit 172.16.0.0 0.0.255.255
R2(config)#
R2(config)# router eigrp 1
R2(config-router)# network 172.16.0.0
R2(config-router)# network 192.168.5.0
R2(config-router)# distribute-list 7 out Serial0/0/0
```

## alebo

```
R2(config)# access-list 7 deny 10.0.0.0 0.255.255.255
R2(config)# access-list 7 permit any
R2(config)#
R2(config)# router eigrp 1
R2(config-router)# network 172.16.0.0
R2(config-router)# network 192.168.5.0
R2(config-router)# distribute-list 7 out Serial0/0/0
```

# Riešenie Route Feedback distribučným zoznamom



```
R2(config)# access-list 2 deny 10.8.0.0 0.3.255.255
R2(config)# access-list 2 permit any
R2(config)# access-list 3 permit 10.8.0.0 0.3.255.255
R2(config)# router ospf 1
R2(config-router)# network 10.0.0.8 0.0.0.3 area 0
R2(config-router)# redistribute rip subnets
R2(config-router)# distribute-list 2 out rip
R2(config-router)# router rip
R2(config-router)# network 10.0.0.0
R2(config-router)# version 2
R2(config-router)# passive-interface Serial0/0/3
R2(config-router)# redistribute ospf 1 metric 5
R2(config-router)# distribute-list 3 out ospf 1
R2(config-router)#
```

# Distribučné zoznamy a prefix listy

- Použitie **distribučných zoznamov** s ACL má určité nevýhody
  - Použitie ACL na filtrovanie obsahu smerovacích info je síce použiteľné
    - ale trochu ťažkopádne
  - ACL sú vyhodnocované sekvenčne pre každý IP prefix smerovacieho updatu
  - DL schovávajú sieťové informácie, čo je niekedy považované za problematické
    - Pri redundantných cestách nasadenie DL môže viesť k utajeniu backup routy
- **Prefix listy**
  - Umožňujú to isté filtrovanie ako ACL,
    - avšak zápis je efektívnejší
  - Vykonávanie je výkonnejšie ako ACL
  - Sú podporované inkrementovateľné modifikácie
  - Ponúka príjemnejšie používateľské prostredie



# Filtrovacie pravidlá pre Prefix List

- Prázdny prefix list povoľuje **všetky** prefixy (permit any)
- Ak prefix list je povolený (**permit**), cesta **je** použitá;
- Ak je prefix list zakázaný (**deny**), cesta **nie je** použitá
- Prefix list je číslovaný zoznam vyhlásení
- Vyhlásenie PL je číslo (prefix) siete(-tí), rozsah ich masiek s definovanou akciou **permit** alebo **deny**
- Smerovač prehľadáva PL od najnižšieho sekvenčného čísla až kým nenastane zhoda
- Na konci prefix listu je implicitné deny

# Konfigurácia Prefix Listu

Router(config)#

```
ip prefix-list {list-name | list-number} [seq seq-value] {deny  
| permit} network/length [ge ge-value] [le le-value]
```

Parameter	Description
<i>list-name</i>	The name of the prefix list that will be created (it is case sensitive).
<i>list-number</i>	The number of the prefix list that will be created.
<b>seq</b> <i>seq-value</i>	A 32-bit sequence number of the <b>prefix-list</b> statement. Default sequence numbers are in increments of 5 (5, 10, 15, and so on).
<b>deny</b> / <b>permit</b>	The action taken when a match is found.
<i>network</i> / <i>length</i>	The prefix to be matched and the length of the prefix. The network is a 32-bit address; the length is a decimal number.
<b>ge</b> <i>ge-value</i>	(Optional) The range of the prefix length to be matched. The range is assumed to be from <i>ge-value</i> to 32 if only the <b>ge</b> attribute is specified.
<b>le</b> <i>le-value</i>	(Optional) The range of the prefix length to be matched. The range is assumed to be from length to <i>le-value</i> if only the <b>le</b> attribute is specified.

ge value <= le value <= 32

# Overenie a diagnostika Prefix Listov

Command	Description
<code>show ip prefix-list [detail   summary]</code>	Displays information on all prefix lists. Specifying the <b>detail</b> keyword includes the description and the hit count in the display.
<code>show ip prefix-list [detail   summary] prefix-list-name</code>	Displays a table showing the entries in a specific prefix list.
<code>show ip prefix-list prefix-list-name [network/length]</code>	Displays the policy associated with a specific <i>network/length</i> in a prefix list.
<code>show ip prefix-list prefix-list-name [seq sequence-number]</code>	Displays the prefix list entry with a given sequence number.
<code>show ip prefix-list prefix-list-name [network/length] longer</code>	Displays all entries of a prefix list that are more specific than the given network and length.
<code>show ip prefix-list prefix-list-name [network/length] first-match</code>	Displays the entry of a prefix list that matches the network and length of the given prefix.
<code>clear ip prefix-list prefix-list-name [network/length]</code>	Resets the hit count shown on prefix list entries.

# Prefix listy

- Povedané inak, riadku

```
ip prefix-list PL permit 192.0.2.0/26  
ge 28 le 31
```

bude vyhovovať každá sieť A.B.C.D/M, pre ktorú platia obe tieto podmienky:

1. Prienik a zhoda na prvých 26bitoch
    - $A.B.C.D \& 255.255.255.192 = 192.0.2.0$
  2. Dĺžka masky medzi 28 až 31 bitmi
    - $255.255.255.240 \leq M \leq 255.255.255.254$
- Ak **ge** ani **le** nie je zadané, potom maska siete musí byť **zhodná**

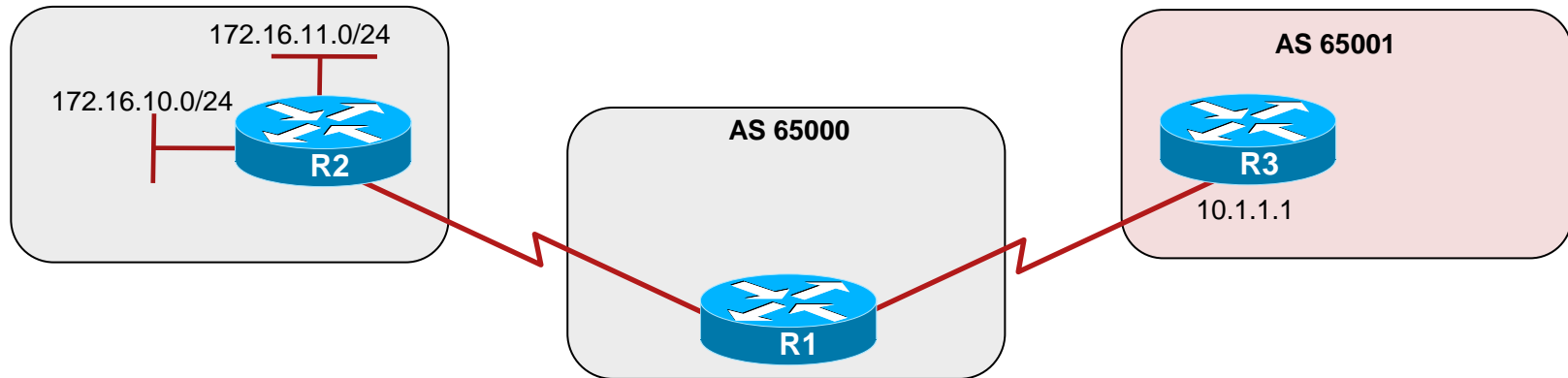
# Prefix listy - príklady

- Máme PL1:
  - `ip prefix-list MyList permit 192.168.0.0/16`
- Máme PL2:
  - `ip prefix-list List2 permit 192.168.0.0/16 le 20`
- Máme PL3:
  - `ip prefix-list List3 permit 192.168.0.0/16 ge 18`
- A siete:
  - 192.168.0.0/16, 192.168.0.0/20, 192.168.2.0/24?
- Ktorá zo sietí sa zhoduje s PL1?
  - Odpoveď: len 192.168.0.0/16
- Ktorá zo sietí sa zhoduje s PL2?
  - Odpoveď: 192.168.0.0/16 a 192.168.0.0/20
- Ktorá zo sietí sa zhoduje s PL3?
  - Odpoveď: 192.168.0.0/20 a 192.168.2.0/24

## Prefix listy – příklady (2.)

- **ip prefix-list NextList1 0.0.0.0/0**
  - Vyhovuje len sieť s maskou /0, t.j. default route
- **ip prefix-list NextList2 0.0.0.0/0 ge 32**
  - Vyhovuje ľubovoľná sieť s maskou /32
- **ip prefix-list NextList3 0.0.0.0/0 le 32**
  - Vyhovuje ľubovoľná sieť s maskou medzi 0/ až po /32
  - T.j. všetky cesty
- **ip prefix-list NextList4 0.0.0.0/1 le 24**
  - Vyhovuje ľubovoľná sieť s maskou od /1 do /24

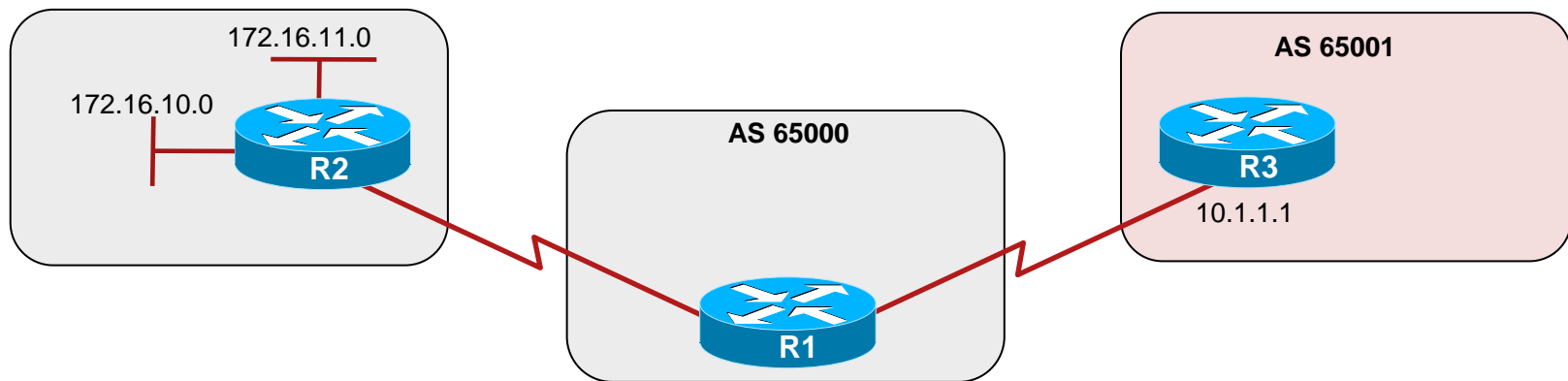
# Prefix-list Scenario #1



```
R1(config)# ip prefix-list TEN-ONLY permit 172.16.10.0/8 le 24
R1(config)# router bgp 65000
R1(config-router)# aggregate-address 172.16.0.0 255.255.0.0
R1(config-router)# neighbor 10.1.1.1 remote-as 65001
R1(config-router)# neighbor 10.1.1.1 prefix-list TEN-ONLY out
R1(config-router)# exit
R1(config)# do show running-config | include ip prefix-list
ip prefix-list TEN-ONLY seq 5 permit 172.0.0.0/8 le 24
R1(config)#
```

- PL `ip prefix-list TEN-ONLY permit 172.0.0.0/8 le 24`
  - Prvých 8 bitov je významových pre zhodu
- Sused R3 sa naučí info o sieťach 172.16.0.0/16 (summary), 172.16.10.0/24 a 172.16.11.0/24.
  - Lebo tieto siete odpovedajú na prvých 8 bitoch 172.0.0.0 a majú dĺžku prefixu medzi 8 a 24

# Prefix-list Scenario #2

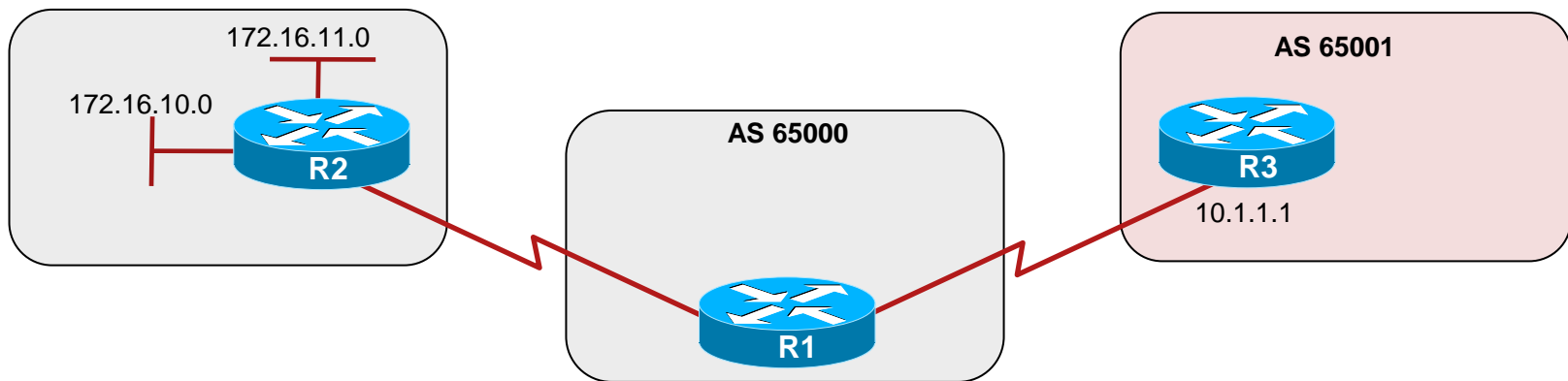


```
R1(config)# ip prefix-list TEN-ONLY permit 172.16.10.0/8 le 16
R1(config)# router bgp 65000
R1(config-router)# aggregate-address 172.16.0.0 255.255.0.0
R1(config-router)# neighbor 10.1.1.1 remote-as 65001
R1(config-router)# neighbor 10.1.1.1 prefix-list TEN-ONLY out
R1(config-router)# exit
R1(config)#
```

- Sused R3 sa naučí len o sieti 172.16.0.0/16
  - Toto je cesta, ktorá sa na prvých 8 bitoch zhoduje s 172.16.10.0 a má prefix medzi 8 až 16 bitmi



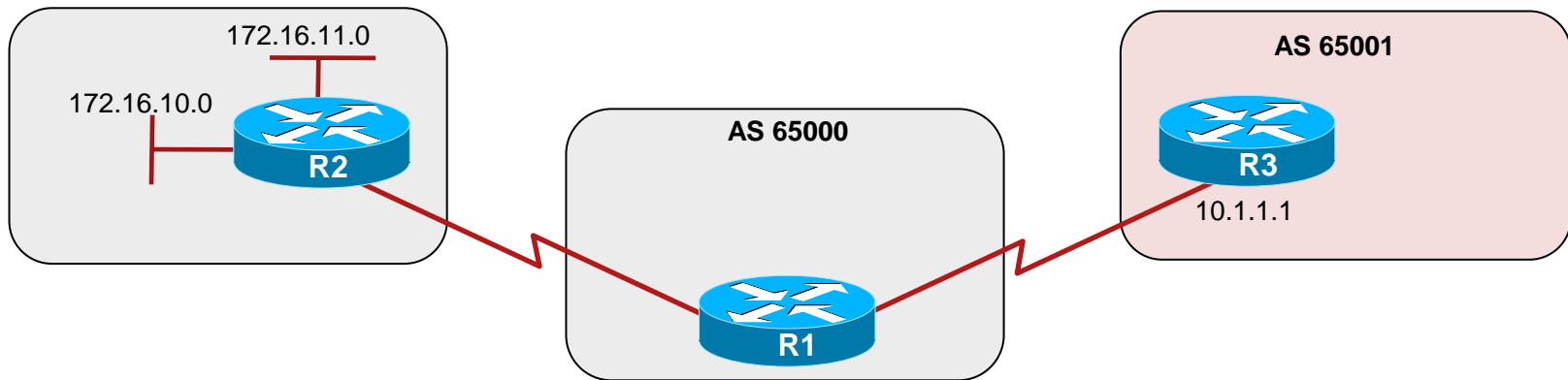
# Prefix-list Scenario #3



```
R1(config)# ip prefix-list TEN-ONLY permit 172.16.10.0/8 ge 17
R1(config)# router bgp 65000
R1(config-router)# aggregate-address 172.16.0.0 255.255.0.0
R1(config-router)# neighbor 10.1.1.1 remote-as 65001
R1(config-router)# neighbor 10.1.1.1 prefix-list TEN-ONLY out
R1(config-router)# exit
R1(config)#
```

- Sused R3 sa naučí len o sieťach 172.16.10.0/24 a 172.16.11.0/24
  - R1 ignoruje parameter /8 a príkaz berie akoby bol zadaný s parametrom ge 17 le 32.

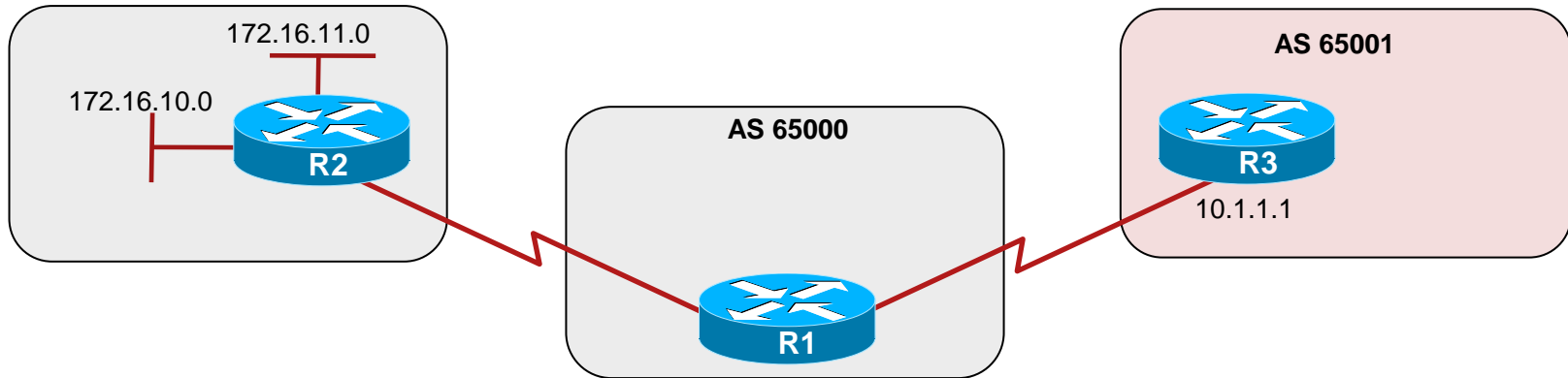
# Prefix-list Scenario #4



```
R1(config)# ip prefix-list TEN-ONLY permit 172.16.10.0/8 ge 16 le 24
R1(config)# router bgp 65000
R1(config-router)# aggregate-address 172.16.0.0 255.255.0.0
R1(config-router)# neighbor 10.1.1.1 remote-as 65001
R1(config-router)# neighbor 10.1.1.1 prefix-list TEN-ONLY out
R1(config-router)# exit
R1(config)#
```

- Sused R3 sa naučí o sieťach 172.16.0.0/16, 172.16.10.0/24 a 172.16.11.0/24
  - R1 ignoruje parameter /8 s príkaz berie akoby bol zadaný s parametrom `ge 16 le 24`.

# Prefix-list Scenario #5



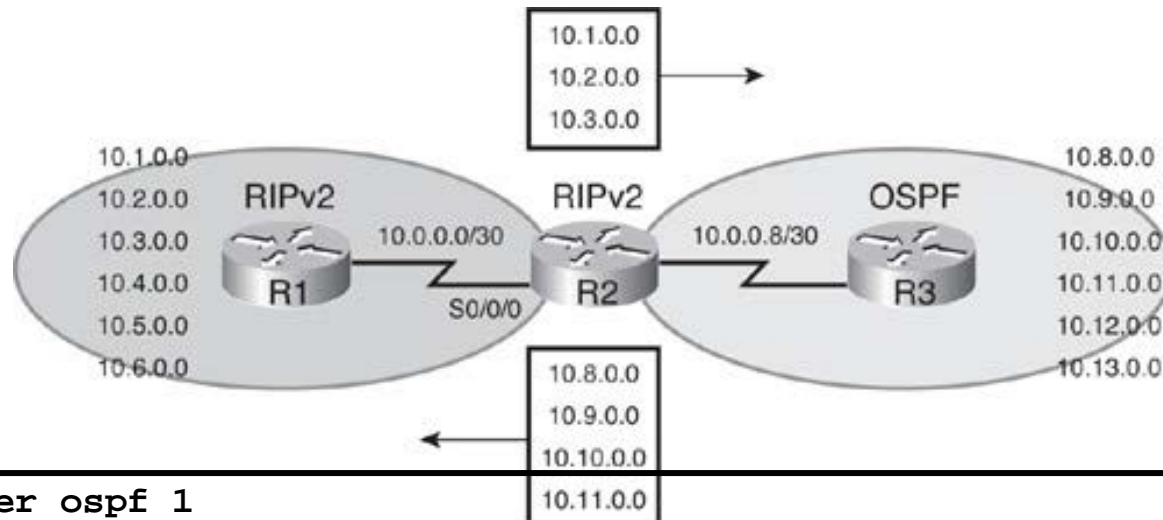
```
R1(config)# ip prefix-list TEN-ONLY permit 172.16.10.0/8 ge 17 le 24
R1(config)# router bgp 65000
R1(config-router)# aggregate-address 172.16.0.0 255.255.0.0
R1(config-router)# neighbor 10.1.1.1 remote-as 65001
R1(config-router)# neighbor 10.1.1.1 prefix-list TEN-ONLY out
R1(config-router)# exit
R1(config)#
```

- Sused R3 sa naučí len o sieťach 172.16.10.0/24 a 172.16.11.0/24
  - R1 ignoruje parameter /8 s príkaz berie akoby bol zadaný s parametrom ge 17 le 24.

# Distribučné listy a prefix listy resp. ACL

- Prefix listy sú spracovávané efektívnejšie než ACL, preto by sa mali prednostne používať na implementovanie filtrovania obsahu smerovacích paketov
- Prefix listy sú určené len na použitie v súvislosti s riadením obsahu posielanej alebo prijímanej smerovacej informácie
  - Nie sú použiteľné ako náhrada ACL v iných aplikáciách, kde sa doposiaľ ACL používa
- Treba pamätať na to, že aj ACL, aj prefix listy končia implicitným pravidlom „deny any“
  - Každá sieť, ktorá nie je povolená, bude odfiltrovaná
- Pre najlepšiu výkonnosť najčastejšie používané vyhlásenia by mali byť nasadené ako prvé
  - S najnižším sekvenčným číslom

# Prefix list s route mapou



```
router ospf 1
  network 10.0.0.8 0.0.0.0 area 0
  redistribute rip route-map intoOSPF subnets
router rip
  network 10.0.0.0
  version 2
  passive-interface s0/0/0
  redistribute ospf 1 route-map intoRIP metric 5
!
route-map intoOSPF permit 10
  match ip address prefix-list PFX1
!
route-map intoRIP permit 10
  match ip address prefix-list PFX2
!
ip prefix-list PFX1 permit 10.0.0.0/14
ip prefix-list PFX2 permit 10.8.0.0/14
```

