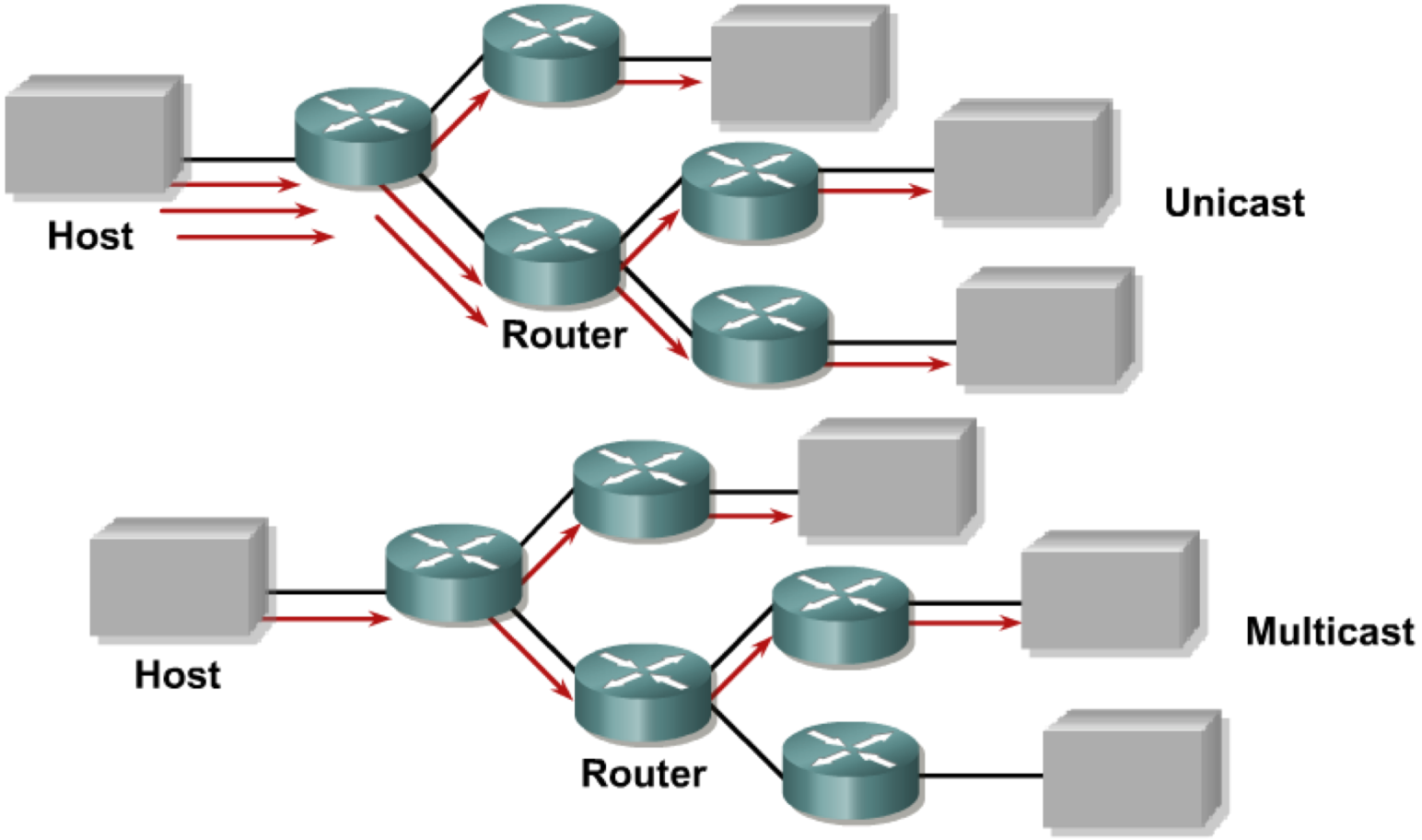
# IP Multicasting

## BSCI Module 7

# Načo multicast?

- Mnohé sieťové aplikácie požadujú príjem istého dátového toku mnohými príjemcami súčasne
  - Internetové analógy rozhlasu, televízie, konferenčných spojení
  - Music-on-hold v IP telefónii
  - Distribúcia informácií mnohým (potenciálne neznámym) príjemcom naraz (presný čas, konfiguračné parametre alebo celé obrazy pracovných staníc, smerovacie protokoly...)
- Multicasting: posielanie jedného rámca/paketu, ktorý je adresovaného viacerým vybraným príjemcom naraz
- Výhody multicastingu:
  - Lepšie využitie zdrojov siete (efektívnejšie využívanie prenosového pásma, menšia záťaž pre odosielateľa i pre sieťovú infraštruktúru)
  - Odosielateľ nemusí nevyhnutne poznať identitu každého príjemcu

# Unicast vs. Multicast



# Nevýhody multicastingu

- Multicast je zväčša založený na UDP
  - Best-effort delivery (možné straty paketov bez riešenia na transportnej vrstve)
  - Nerieši sa situácia zahltenia
  - Príjemcovia môžu dostávať duplikované pakety
  - Odoslané dáta nemusia prísť v pôvodnom poradí
  - Filtrovanie a zabezpečenie multicastov môže byť zložitejšie
  - Niektoré z týchto problémov sčasti riešia v súčasnosti iné protokoly, ktoré sú schopné zabezpečovať spoľahlivý multicasting (PGM)
- Smerovače musia podporovať smerovanie multicastov, aby bol multicasting použiteľný pre príjemcov v rôznych IP sieťach
- Prepínače by mali podporovať multicasting (pomocou CGMP/IGMP snoopingu), aby zabezpečovali efektívne doručovanie multicastov ich príjemcom

# Typy multicastových aplikácií

## Od jedného k mnohým (One-to-many)

- Jediná stanica odosielajúca dáta dvom alebo viacerým príjemcom

## Od mnohých k mnohým (Many-to-many)

- Ľubovoľný počet staníc vzájomne si posielajúcich multicastovo adresované dáta (všetky stanice sú členmi tej istej multicastovej skupiny)

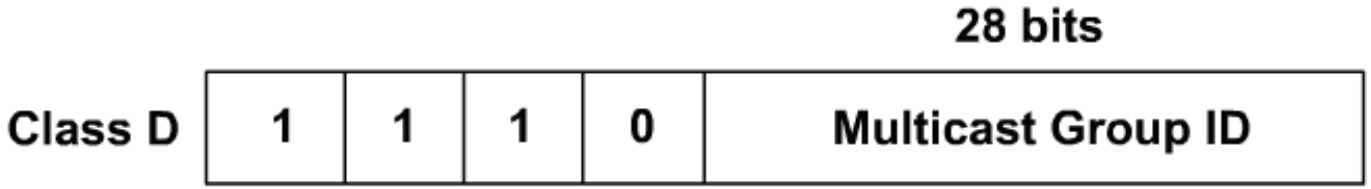
## Od mnohých k jednému (Many-to-one)

- Ľubovoľný počet príjemcov posielajúcich dáta späť odosielateľovi (cez unicast či multicast)

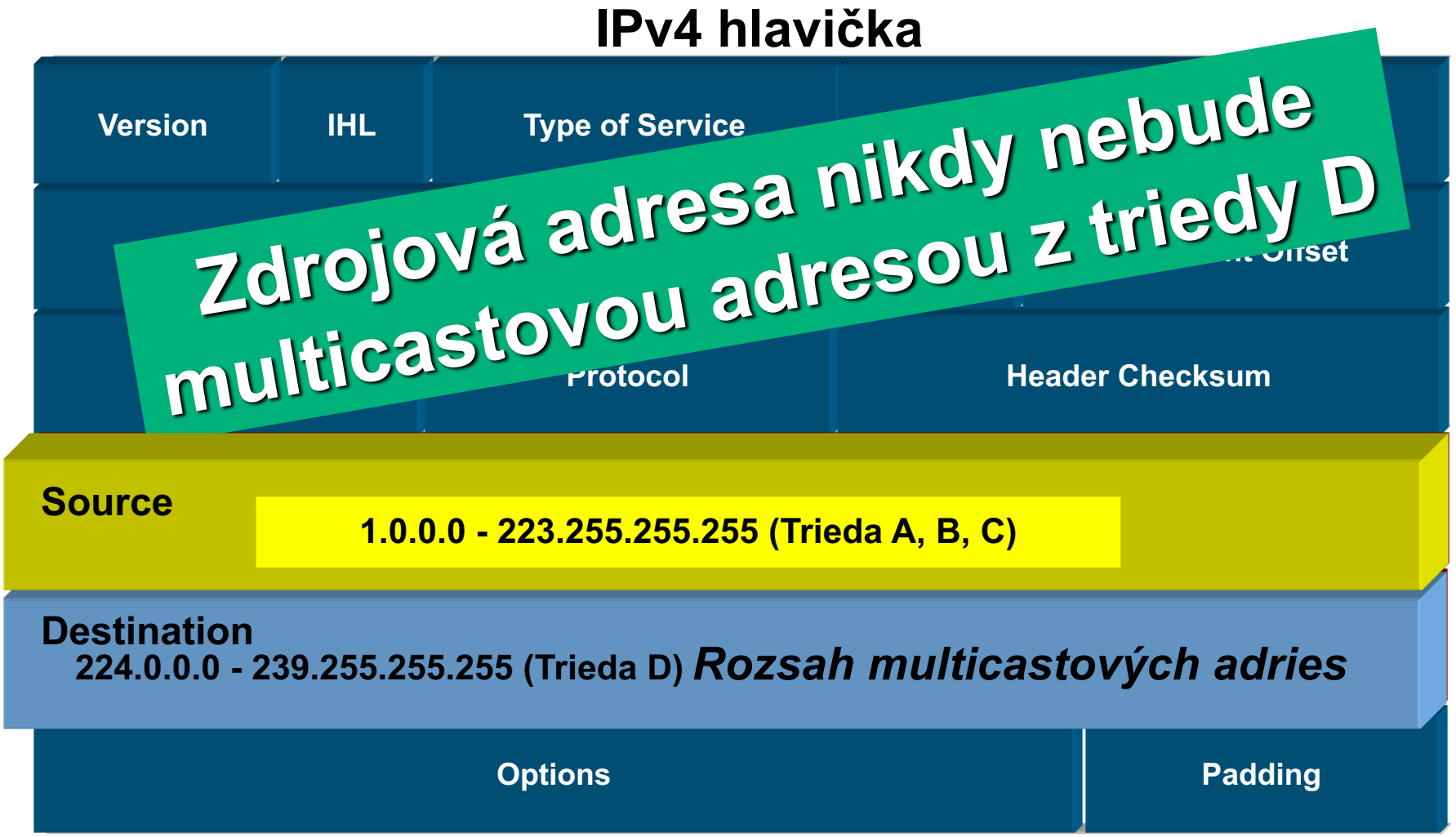
# Adresovanie multicastov

# Štruktúra multicastovej IP adresy

- Pre multicastové adresovanie sa využívajú IP adresy z triedy D
  - Horné 4 bity sú 1110 (definícia triedy D)
  - Zvyšných 28 bitov označuje číslo multicastovej skupiny
  - Skupina je tvorená členmi – stanicami, ktoré deklarovali záujem byť členom danej multicastovej skupiny
- Rozsah D adries je od 224.0.0.0 do 239.255.255.255



# IP adresovanie v multicastoch



# Rozdelenie multicastových IP adries

- Adresy typu local scope
  - 224.0.0.0 až 224.0.0.255
  - Pakety nemajú opustiť broadcastovú doménu, z ktorej pochádzajú (sú link-local)
  - Mnohé adresy z tohto rozsahu sú v súčasnosti vyhradené
- Adresy typu global scope
  - 224.0.1.0 až 238.255.255.255
- Adresy typu administratively scoped
  - 239.0.0.0 až 239.255.255.255
  - Tento rozsah je využitý pre použitie v privátnych doménach

# Adresy typu Local Scope

- Rezervovaný rozsah: 224.0.0.0 až 224.0.0.255
  - 224.0.0.1 (všetky multicast-capable systémy na segmente)
  - 224.0.0.2 (všetky smerovače na subnete)
  - 224.0.0.4 (všetky DVMRP smerovače)
  - 224.0.0.5, 224.0.0.6 (OSPF)
  - 224.0.0.9 (RIPv2)
  - 224.0.0.10 (EIGRP)
  - 224.0.0.13 (všetky PIMv2 smerovače)
  - 224.0.0.18 (VRRP)
  - 224.0.0.22 (IGMPv3)
  - 224.0.0.2,102 (HSRP)

# Adresy typu Global Scope a Administratively Scoped

- Global Scope: Adresy s prechodným významom, prideľované dynamicky:
  - Globálny rozsah: 224.0.1.0-238.255.255.255
  - 224.2.X.X sa zvyčajne používa v MBONE aplikáciách
  - Časť globálneho rozsahu sa v súčasnosti používa pre nové protokoly
- Administratively Scoped: Adresy s prechodným významom, prideľované dynamicky, povahovo privátne
  - Limited (local) scope: 239.0.0.0/8
    - Site-local scope: 239.255.0.0/16
    - Organization-local scope: 239.192.0.0 to 239.251.255.255

# Multicastové adresovanie na L2

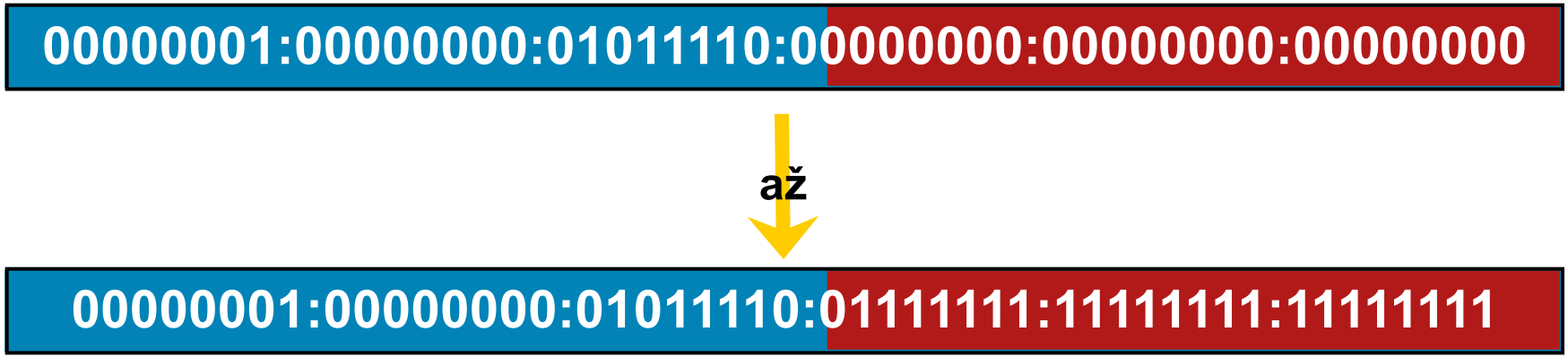
- Doposiaľ sme predpokladali, že MAC adresa v ethernetovom rámci označuje jedno konkrétne sieťové rozhranie
- V skutočnosti existujú MAC adresy, ktoré označujú nejakú skupinu počítačov (v broadcastovej doméne)
- MAC adresa: 6B, prvé 3B: OUI, druhé 3B: S/N
- Tvar prvého bajtu MAC adresy:

| **Bit** | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| **Význam** | n | n | n | n | n | n | U/L | I/G |

  - U/L: Universal (0), Local (1)
  - I/G: Individual (0), Global (1)

# Multicastové adresovanie na L2

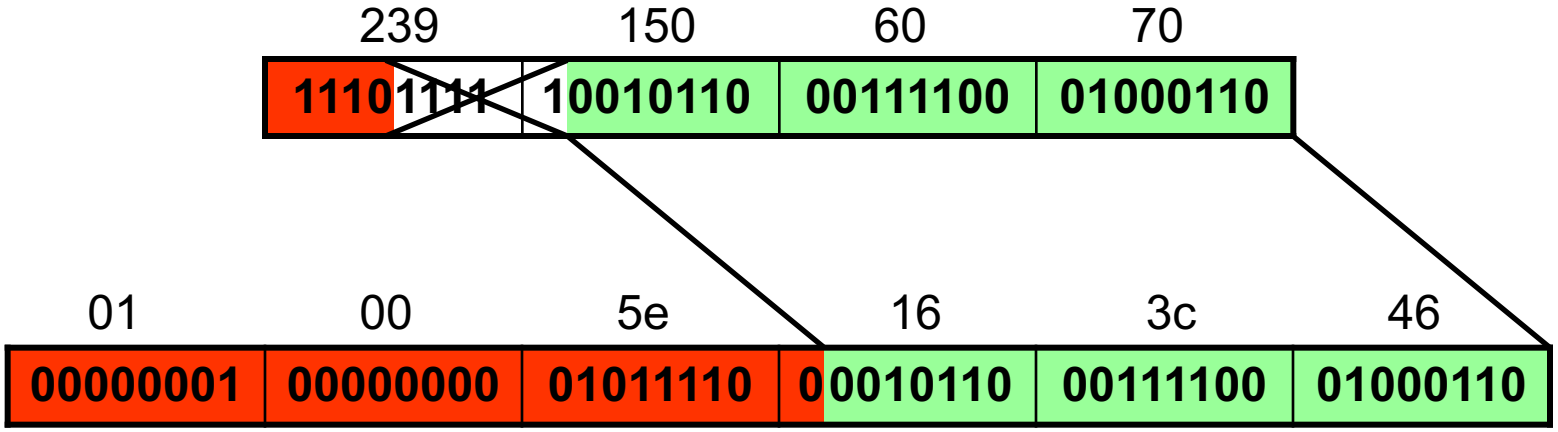
IANA vyčlenila pre multicastové MAC adresy rozsah MAC **01:00:5e:00:00:00 až 01:00:5e:7f:ff:ff**




- Prvých 25 bitov v každej MAC má fixnú hodnotu, ktorá sa musí dodržať
- Zostávajúcich 23 bitov v MAC slúži na popísanie multicastovej skupiny

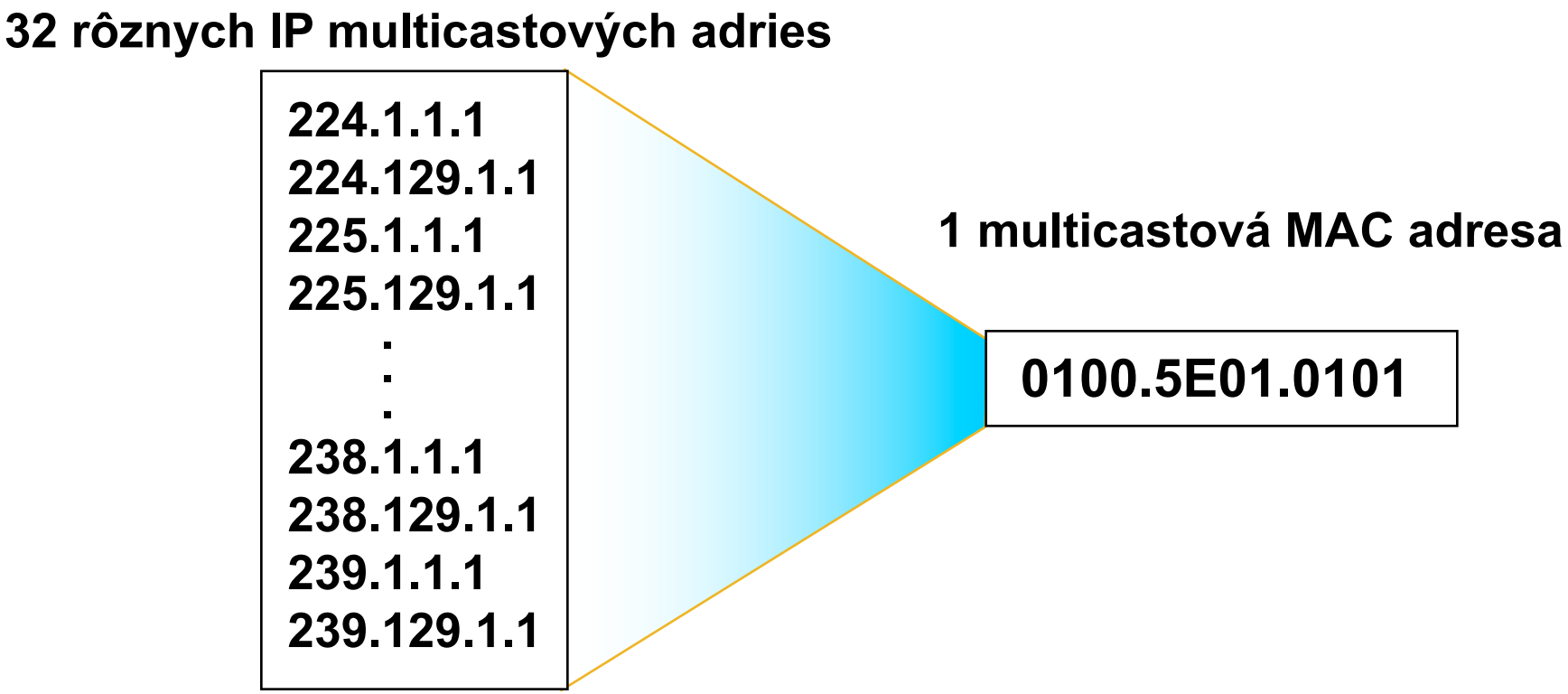
# Mapovanie multicastových IP adries na multicastové MAC adresy

- Bežné IP adresy sa mapujú na MAC adresy pomocou ARP, tento princíp však neplatí o adresách triedy D
- Namiesto neho sa pri multicastových adresách typu D používa iná, jednoduchá, avšak nie bijektívna operácia:



# Mapovanie multicastových IP adries na multicastové MAC adresy

**32 rôznych IP adries zodpovedá jednej MAC adrese**



# Prideľovanie/zisťovanie multicastových IP adries

- Zisťovanie
  - Načúvaním na známej multicastovej adrese
  - SAP (RFC 2974) (Cisco ho niekedy volá sdr)
  - Adresárové služby
  - Web, e-mail, ...
- Statické prideľovanie a zisťovanie
  - Existuje veľmi veľa pravidiel na vyhýbanie sa nevhodne navrhnutým adresám
  - Vhodný Cisco dokument: „Guidelines for Enterprise IP Multicast Address Allocation“ (cca 57 strán ☺)
- Prideľovanie podľa AS: 233.0.0.0 – 233.255.255.255
  - Tzv. GLOP adresovanie definované v RFC 3180
  - Prvý bajt IP čísla musí byť nastavený na hodnotu 233
  - Číslo AS sa zapíše dekadicky ako druhý a tretí oktet IP adresy
  - Posledný oktet zostáva na určenie multicastovej skupiny v rámci AS

# Protokol IGMP

# Internet Group Management Protocol (IGMP)

- Stanica sa stáva členom multicastovej skupiny tak, že svojej bráne (gateway – routeru) ohlási svoj záujem byť členom skupiny
  - Ak router dostane multicastový IP traffic adresovaný danej skupine, bude vedieť, že ho má preposlať aj do siete, kde sa nachádza táto stanica
  - Stanica si neprideľuje dodatočnú IP adresu. Inicializuje však podporu v sieťovej karte, aby akceptovala aj rámce adresované na príslušnú MAC adresu multicastovej skupiny
- Protokol na prihlásenie/odhlásenie sa stanice do multicastovej skupiny sa volá IGMP
  - IGMP je komunikácia medzi stanicou a jej bránou
- Existujú v súčasnosti 3 verzie:
  - IGMPv1 definované v RFC 1112
    - Podporujú všetky súčasné OS
  - IGMPv2 definované v RFC 2236
    - Podporujú všetky súčasné OS
  - IGMPv3 definované v RFC 3376
    - Podporované v posledných verziách Windows a Linux

# IGMPv1

- IGMPv1 má dve základné správy
  - Membership query
    - Periodicky generovaná smerovačmi (tzv. queriers), posielaná na IP adresu 224.0.0.1 (all-hosts)
    - Posiela sa zriedkavo, spravidla každú minútu
  - Membership report
    - Odosielaná stanicou na IP adresu skupiny, do ktorej si stanica želá byť prihlásená
    - Posiela sa 1 report pre každú skupinu, v ktorej je stanica členom
    - Report sa posiela buď ako odpoveď na query, alebo v momente, keď sa stanica prihlasuje do skupiny (bez vyžiadania)
    - Každá stanica pred odoslaním odpovede na výzvu náhodný čas (max 10 sekúnd) počká, či neodpovie nejaká iná stanica. Ak odpovie, netreba posielať ďalšiu odpoveď

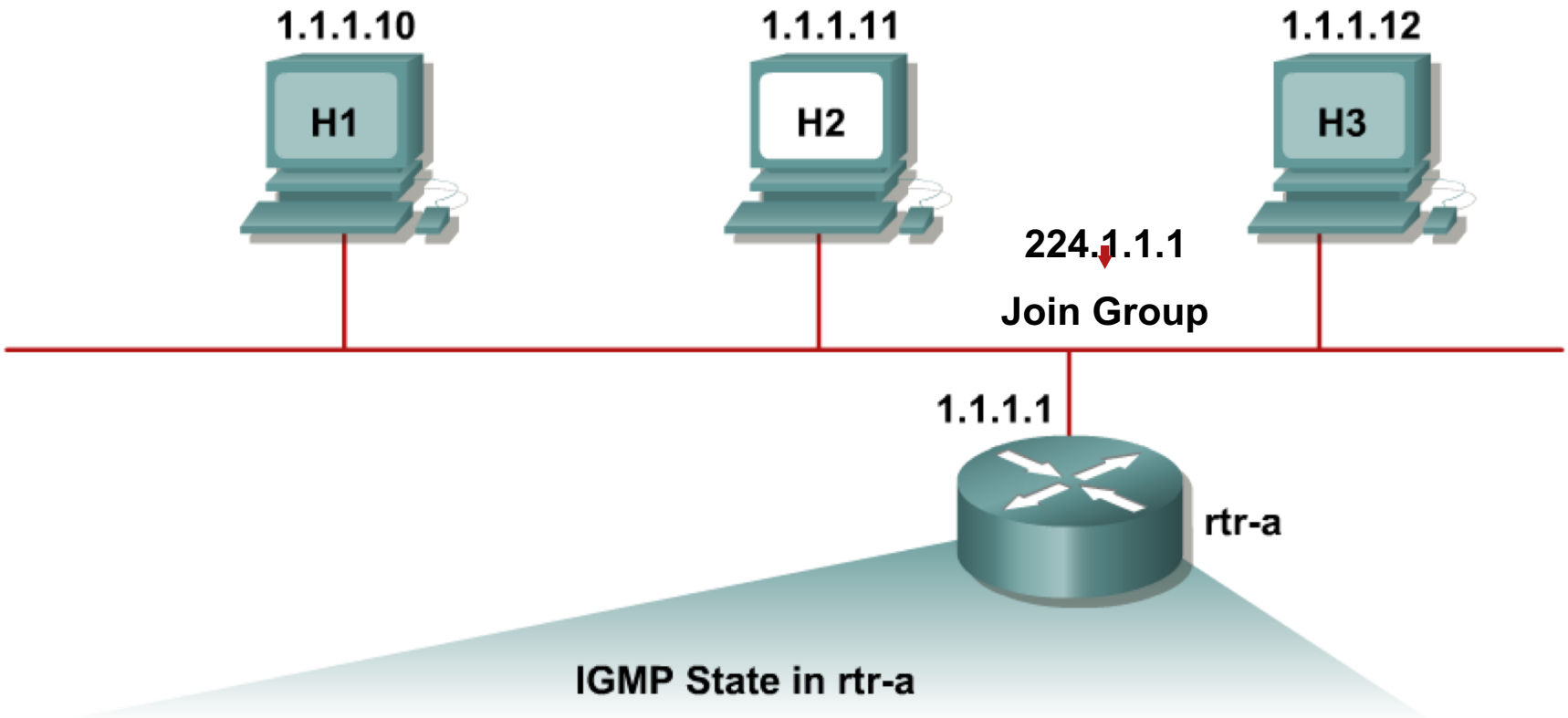
# IGMPv2

- Tri základné druhy správ
  - Membership query
    - Periodicky generované smerovačmi (queriers)
    - Môžu byť všeobecné (odosielané na IP 224.0.0.1) a špecifické (odosielané na IP skupiny)
  - Membership report
    - Odosielané stanicou na IP adresu skupiny, do ktorej si stanica želá byť prihlásená
  - Leave group
    - Stanica touto správou ohlasuje opustenie skupiny, posielaná na 224.0.0.2
    - Správu posiela tá stanica, ktorá odpovedala na poslednú Query na danú skupinu
- Query router (querier) vie vynútiť čas, dokedy očakáva odpoveď na Query (tzv. Query-Response čas)
- IGMPv2 štandardizuje spôsob voľby queriera spomedzi viacerých smerovačov na segmente (smerovač s **najnižšou** IP)

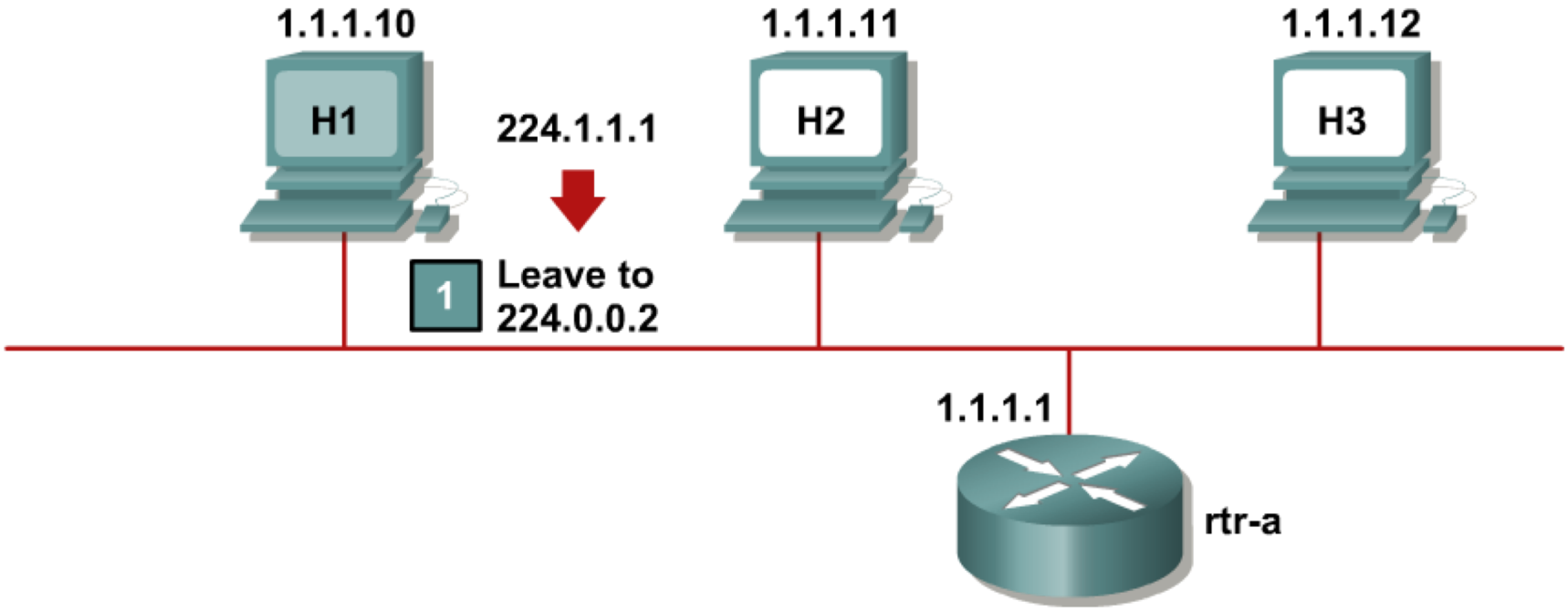
# IGMPv3

- Dva základné druhy správ:
  - Membership query
    - General query, posielané na 224.0.0.1
    - Group-specific query (*,G), posielané na skupinu
    - Group-and-source specific (S,G), posielané na skupinu
  - Membership report
    - Odosielané na adresu 224.0.0.22
- IGMPv3 má podstatne zložitejšiu internú sémantiku než jeho predchodcovia

# IGMPv2: Prihlásenie sa do skupiny



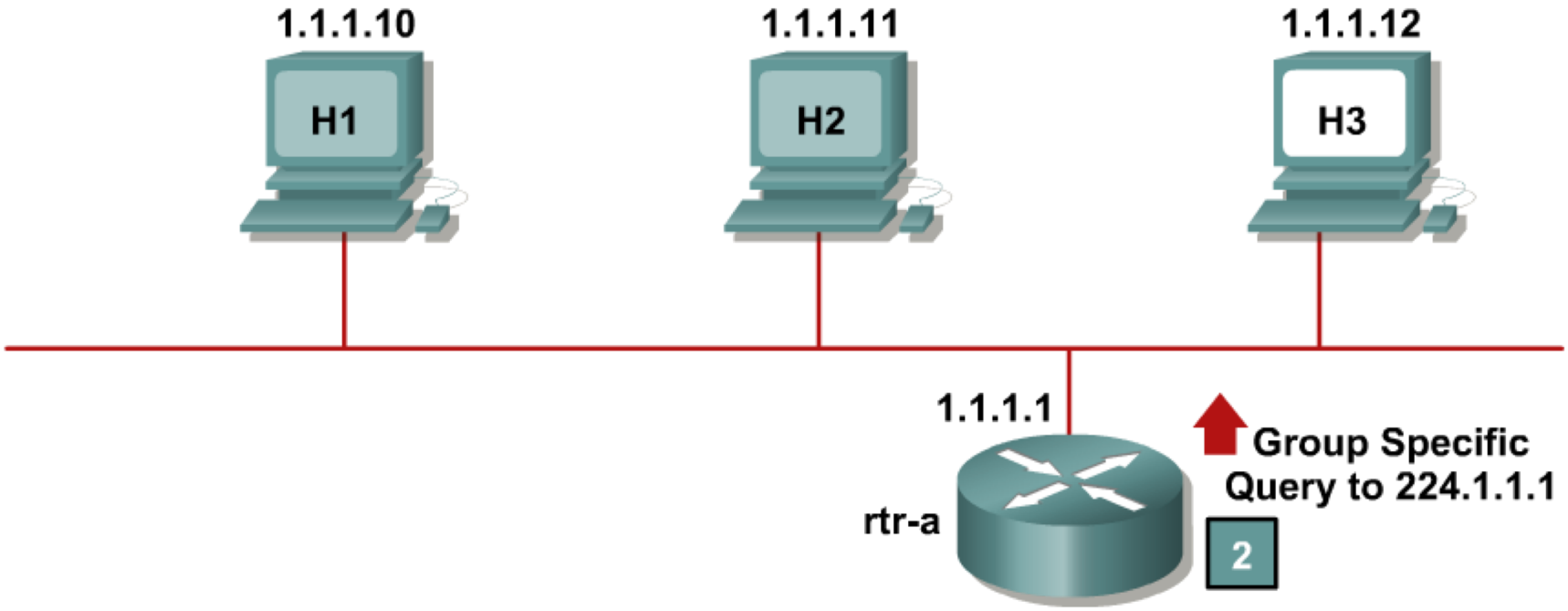
# IGMPv2: Opustenie skupiny




Stanice H2 a H3 sú členmi skupiny 224.1.1.1

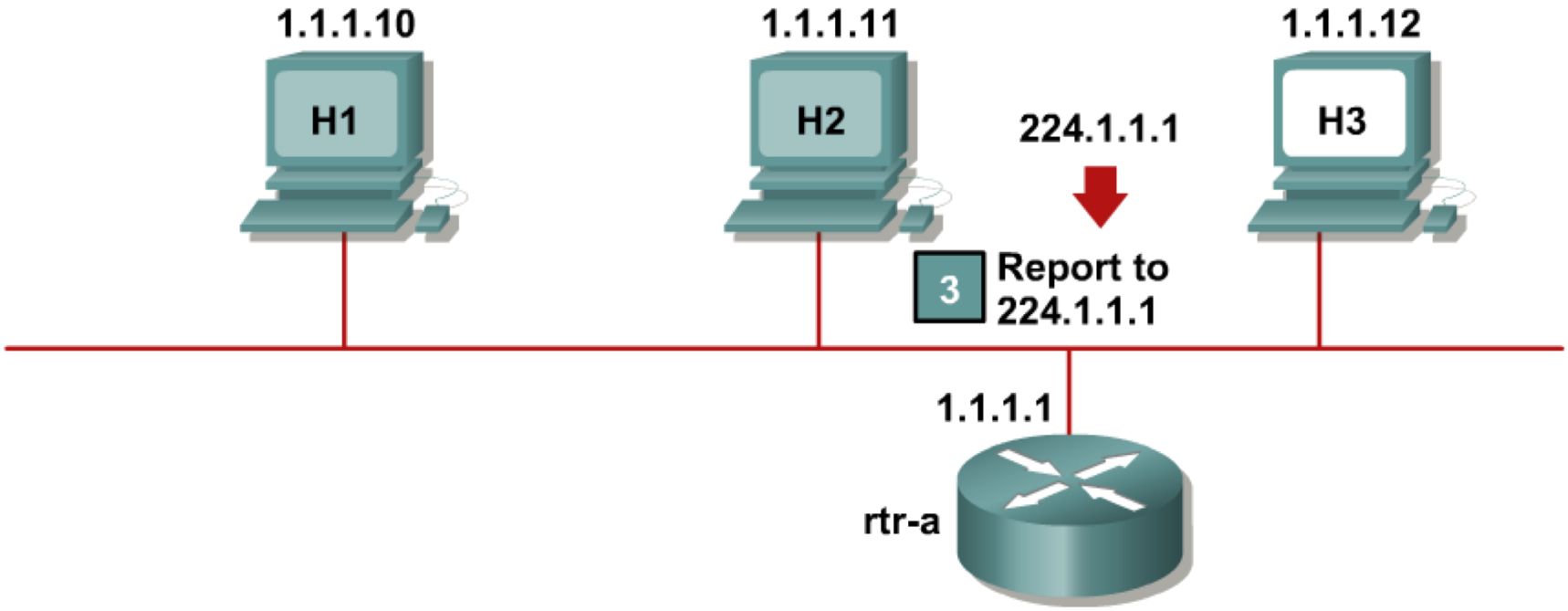
1. H2 pošle správu Leave group

# IGMPv2: Opustenie skupiny



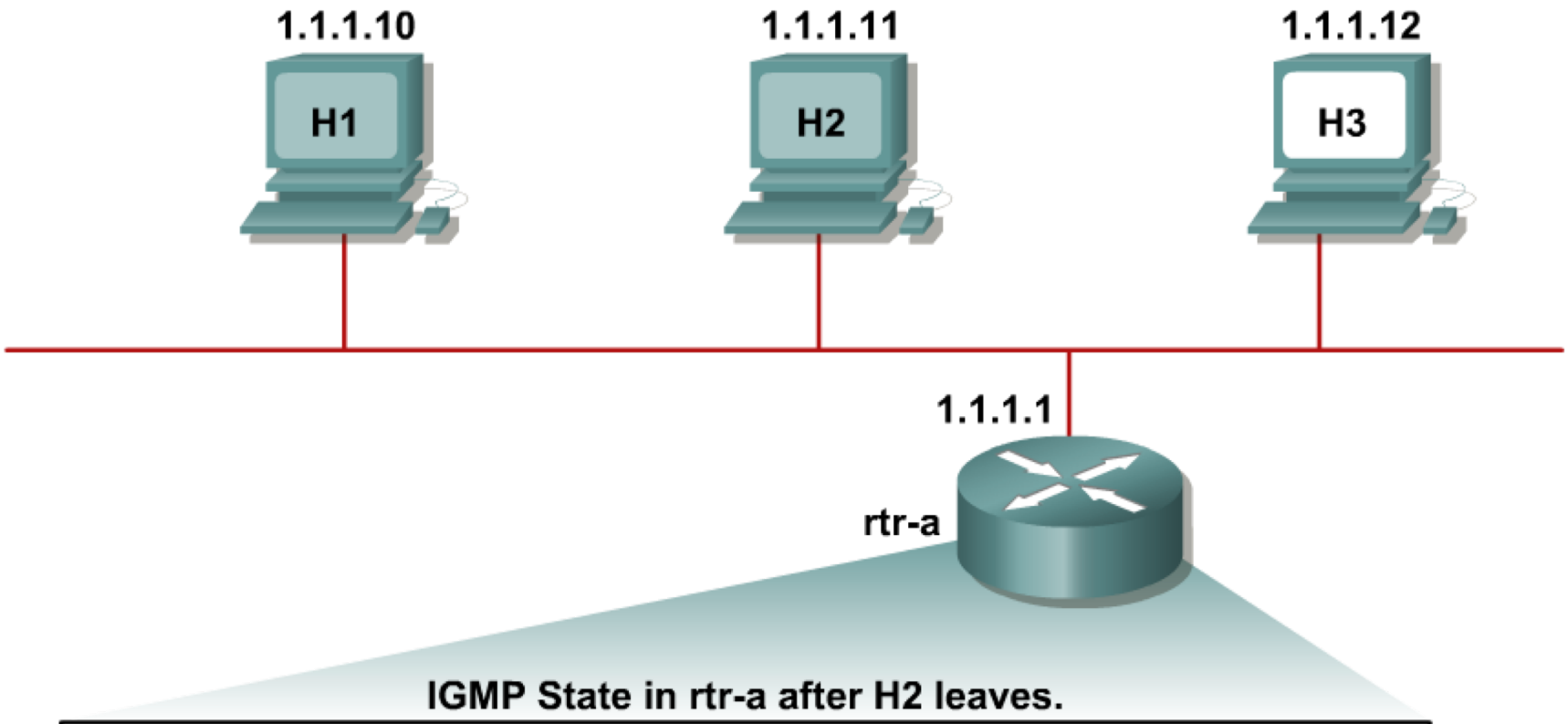

2. Router pošle group-specific query

# IGMPv2: Opustenie skupiny




3. Zostávajúci člen pošle report, takže router vie, že na segmente ešte sú príjemcovia

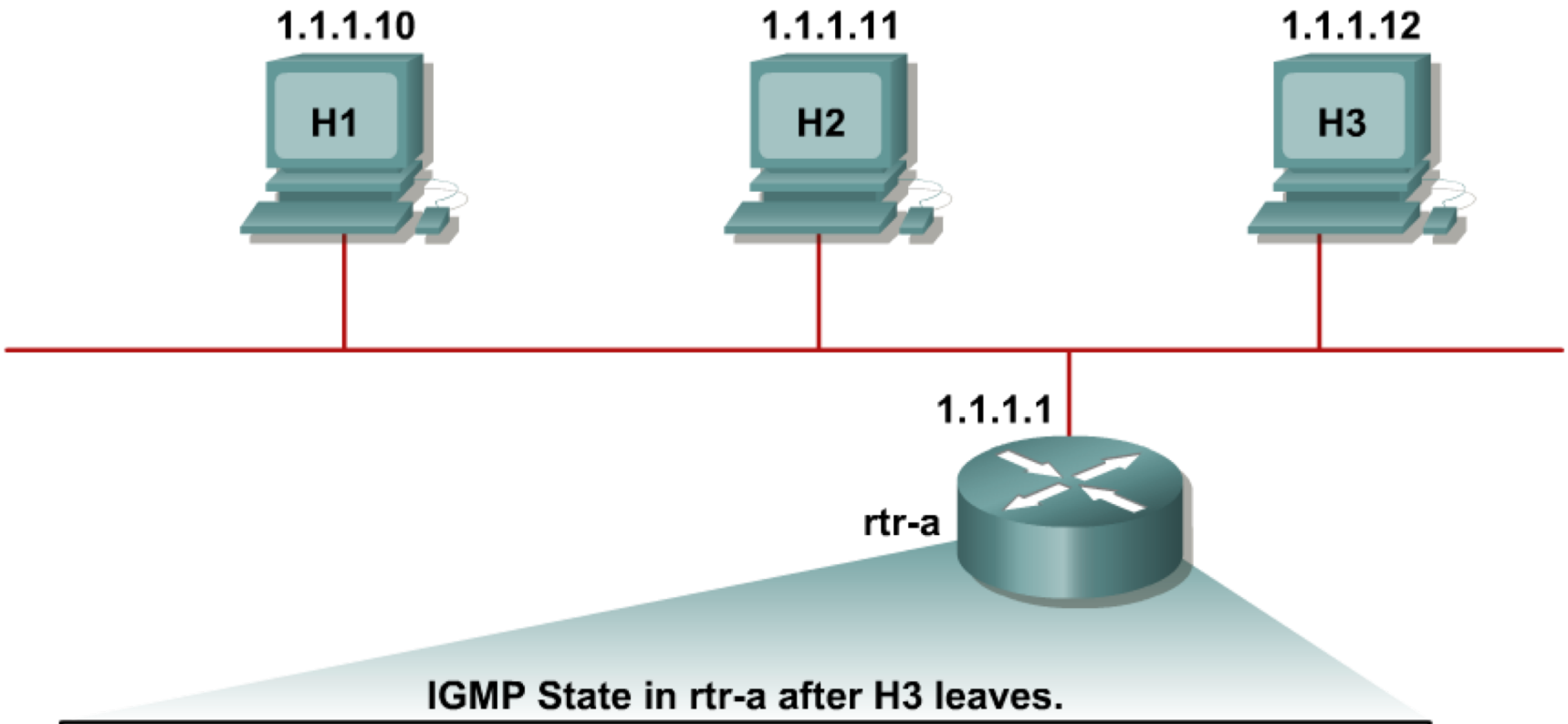
# IGMPv2: Opustenie skupiny




IGMP State in rtr-a after H2 leaves.

```
rtr-a>sh ip igmp group
IGMP Connected Group Membership
Group Address   Interface   Uptime   Expires    Last Reporter
224.1.1.1       Ethernet0   0d1h3m   00:01:47   1.1.1.12
```

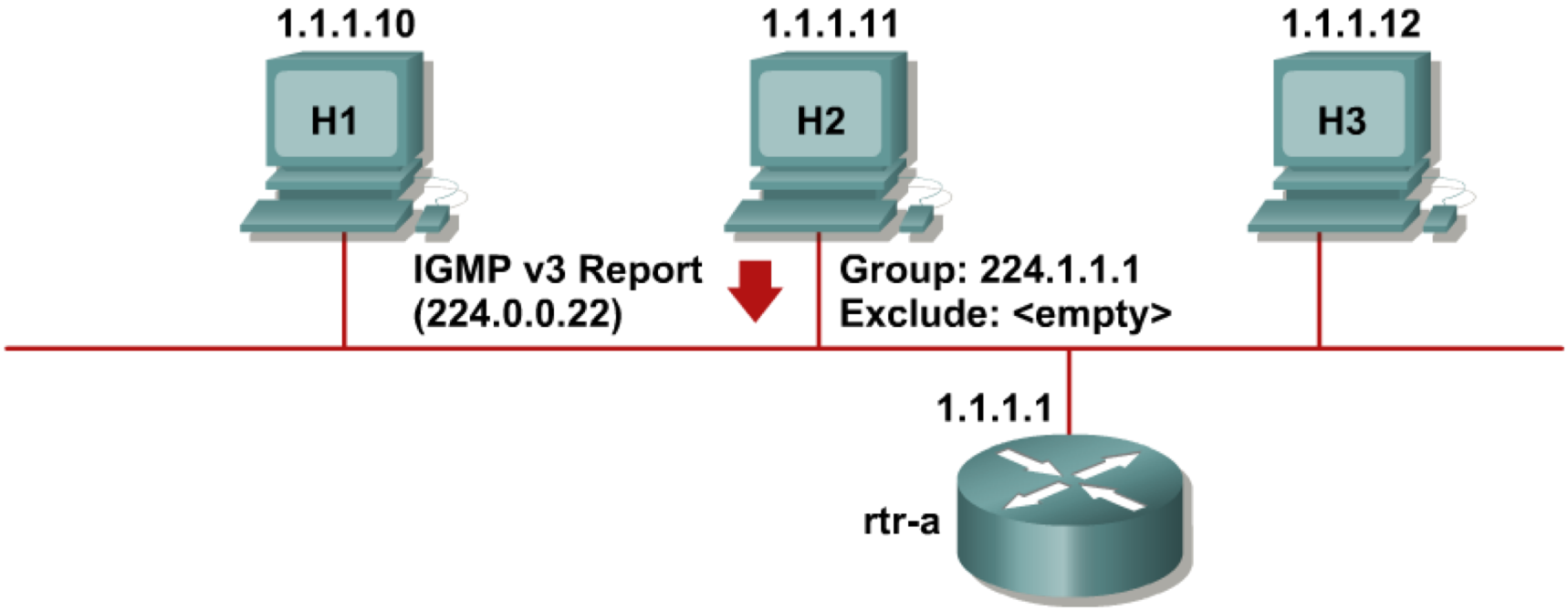
# IGMPv2: Opustenie skupiny




IGMP State in rtr-a after H3 leaves.

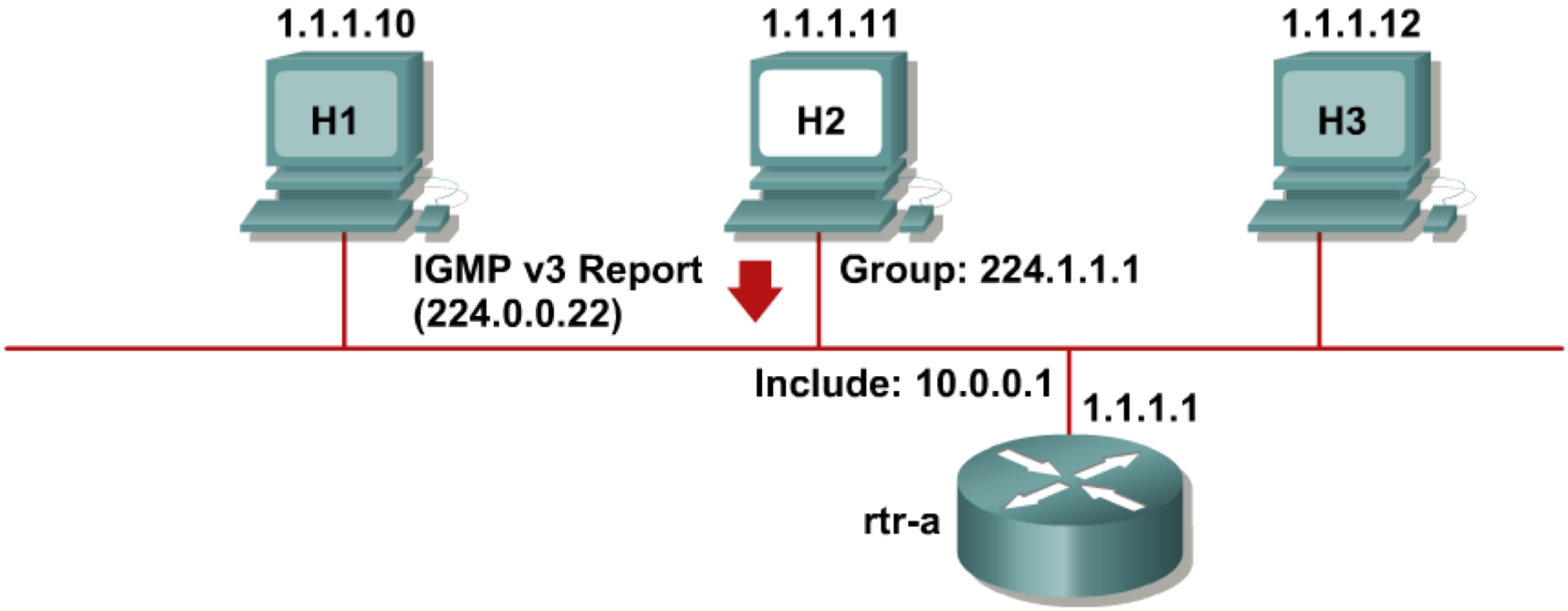
```
rtr-a>sh ip igmp group
IGMP Connected Group Membership
Group Address   Interface   Uptime   Expires    Last Reporter
```

# IGMPv3: Prihlásenie sa do skupiny



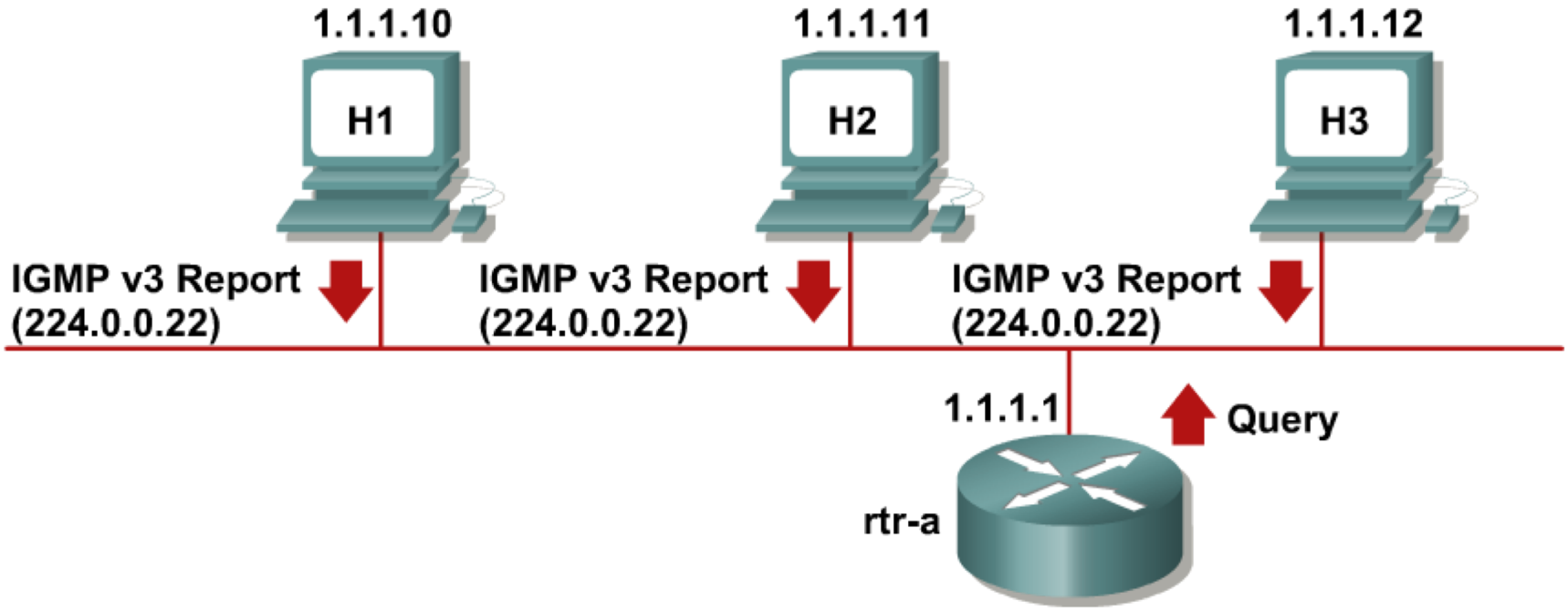

Nová stanica posiela IGMPv3 report na adresu 224.0.0.22 hneď, ako sa do skupiny prihlasuje.

# IGMPv3: Prihlásenie sa k špecifickému odosielateľovi v skupine




IGMPv3 report obsahuje zoznam žiadaných odosielateľov v zoznamoch typu INCLUDE alebo EXCLUDE.

# IGMPv3: Udržiavanie prehľadu o stave




Router posiela periodické queries:

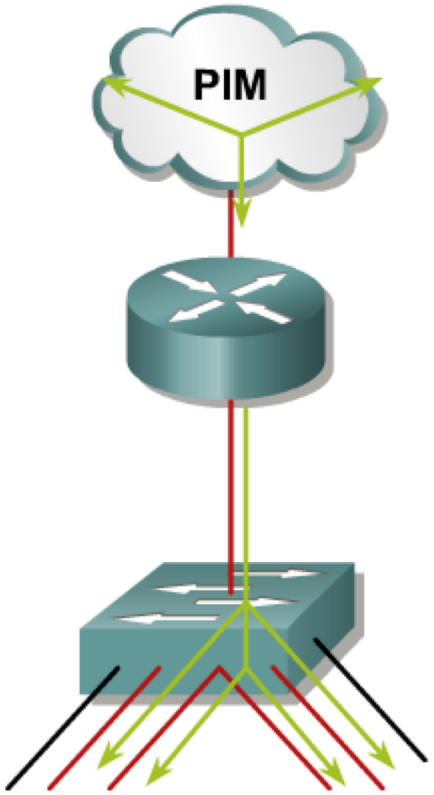
- Odpovedajú všetci IGMPv3 členovia
  - Report správy obsahujú viaceré položky o stave

# Efektívne doručovanie multicastov na Layer2

# Efektívne doručovanie multicastov na L2

Problém: Doručovanie multicastovo adresovaných rámcov na L2

- Bežné L2 switche spracúvajú multicasty rovnako ako rámce idúce na neznámeho príjemcu – floodujú ho von všetkými portami v danej VLAN
- Pokiaľ taký switch umožňuje manipulovať s obsahom CAM tabuľky, jedným z riešení je statická (ručná) manipulácia s ňou, tzn. zapísanie príslušných multicastových MAC adries k zodpovedajúcim rozhraniam, kde sú príjemcovia
- Inteligentnejšie switche majú pre tento účel dynamický mechanizmus



# Efektívne doručovanie multicastov na L2

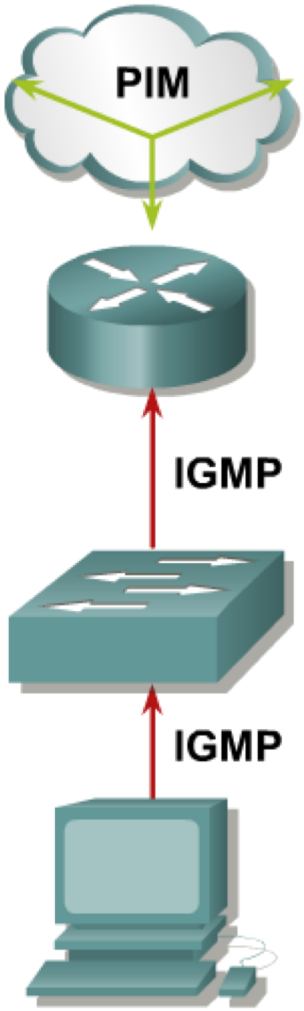
- Idea dynamického mechanizmu pre efektívne doručovanie multicastov na Layer2:
  - Switch si pre každú pripojenú stanicu zistí, či je stanica členom nejakej multicastovej skupiny
  - Prijatý multicastovo adresovaný traffic bude preposlaný iba tými rozhraniami, kde sa nachádzajú členovia danej skupiny
- Dva mechanizmy:
  - Cisco Group Management Protocol (CGMP): Jednoduchý, avšak proprietárny pomocný protokol, vyžaduje vzájomnú spoluprácu routera a switcha
  - IGMP snooping: Komplexný, avšak štandardizovaný spôsob, implementovaný priamo na switchoch

# CGMP

- CGMP protokol je pomocný signalizačný protokol medzi routerom a switchom
  - Nie je to náhrada ani analóg IGMP!
- CGMP pakety posiela router switchu na vyhradenej MAC adrese 0100.0cdd.dddd
- CGMP paket obsahuje:
  - Type: join alebo leave
  - MAC adresu IGMP klienta
  - Multicast MAC adresu skupiny
- Switch na základe CGMP informácie pridá alebo odoberie multicastovú MAC adresu na zvolenom porte

# IGMP Snooping

- Switche rozumejú protokolu IGMP v IP paketoch
- IGMP pakety sú spracovávané na CPU alebo špecializovanom ASICu (Application-Specific Integrated Circuit)
- Switch analyzuje obsah IGMP správ, aby vedel, na ktorom porte sú členovia ktorých skupín
- Dôsledok pre switche bez podpory Layer 3-aware Hardware/ASICs
  - Procesor musí analyzovať všetky L2 multicastové rámce
  - Znížená priepustnosť, zvýšená záťaž
- Dôsledok pre switche s podporou Layer 3-aware Hardware/ASICs
  - Priepustnosť je zachovaná, no switch je drahší



# IGMP Snooping

- IGMPv3 Report správy sa posielajú na osobitnú, avšak vždy tú istú IP adresu (224.0.0.22)
  - Zjednodušuje to analýzu – netreba analyzovať každý multicastovo adresovaný paket
  - Pri IGMPv3 by ani softvérová implementácia IGMP Snoopingu na low-end switchoch nemala spôsobovať významný nárast záťaže či pokles priepustnosti
- Na súčasných switchoch Catalyst je IGMP snooping automaticky aktívny
  - Výnimku z IGMP snoopingu tvoria MAC adresy zodpovedajúce rozsahu 224.0.0.x (01:00:5e:00:00:xx), ktoré sú floodované vždy
    - Pozor, k jednej MAC tohto tvaru existuje 32 rôznych IP

# Multicastové distribučné stromy

# Multicastové distribučné stromy

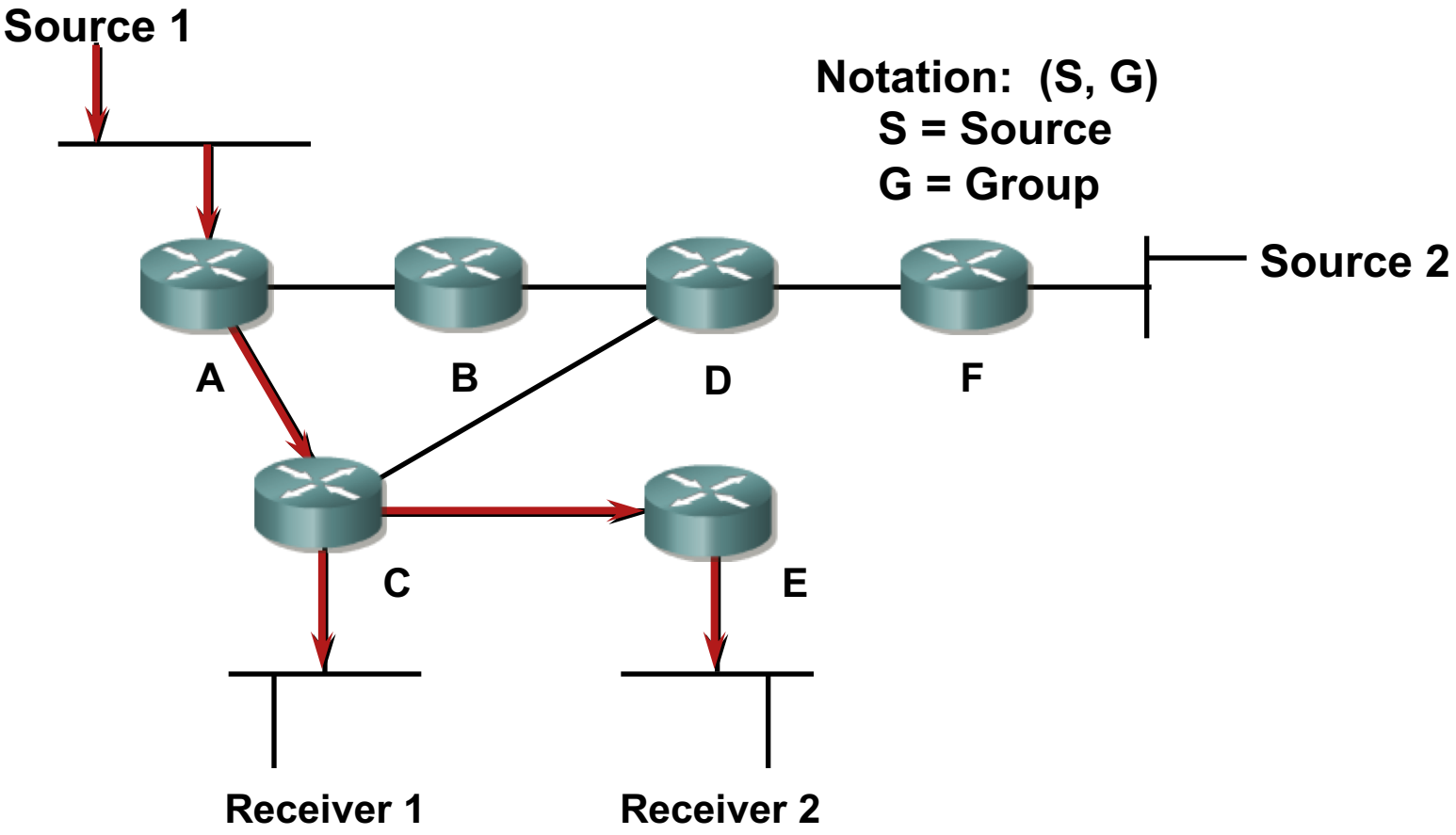
- Cesta, ktorou tečie multicastový tok dát od odosielateľa cez medziľahlé routery až po koncových príjemcov v jednej konkrétnej skupine, vytvára strom, ktorý sa nazýva multicastový distribučný strom
- Dva druhy stromov:
  - Zdrojové distribučné stromy čiže stromy najkratších vzdialeností (shortest path trees, SPTs)
    - Koreň týchto stromov je vždy v odosielateľovi
  - Zdieľané (Shared) distribučné stromy
    - Jeden strom je zdieľaný pre viacerých odosielateľov v tej istej skupine
    - Koreňom tohto stromu je jeden dohodnutý router, tzv. rendezvous point

# Multicastové distribučné stromy

- Charakteristiky stromov:
  - SPT stromy sú pamäťovo náročnejšie, avšak garantujú optimálne cesty od odosielateľa k všetkým príjemcom, čím minimalizujú oneskorenie
  - Shared stromy sú pamäťovo výhodnejšie, ale môžu viesť k toku dát suboptimálnymi cestami, a tak vniesť zbytočné oneskorenie

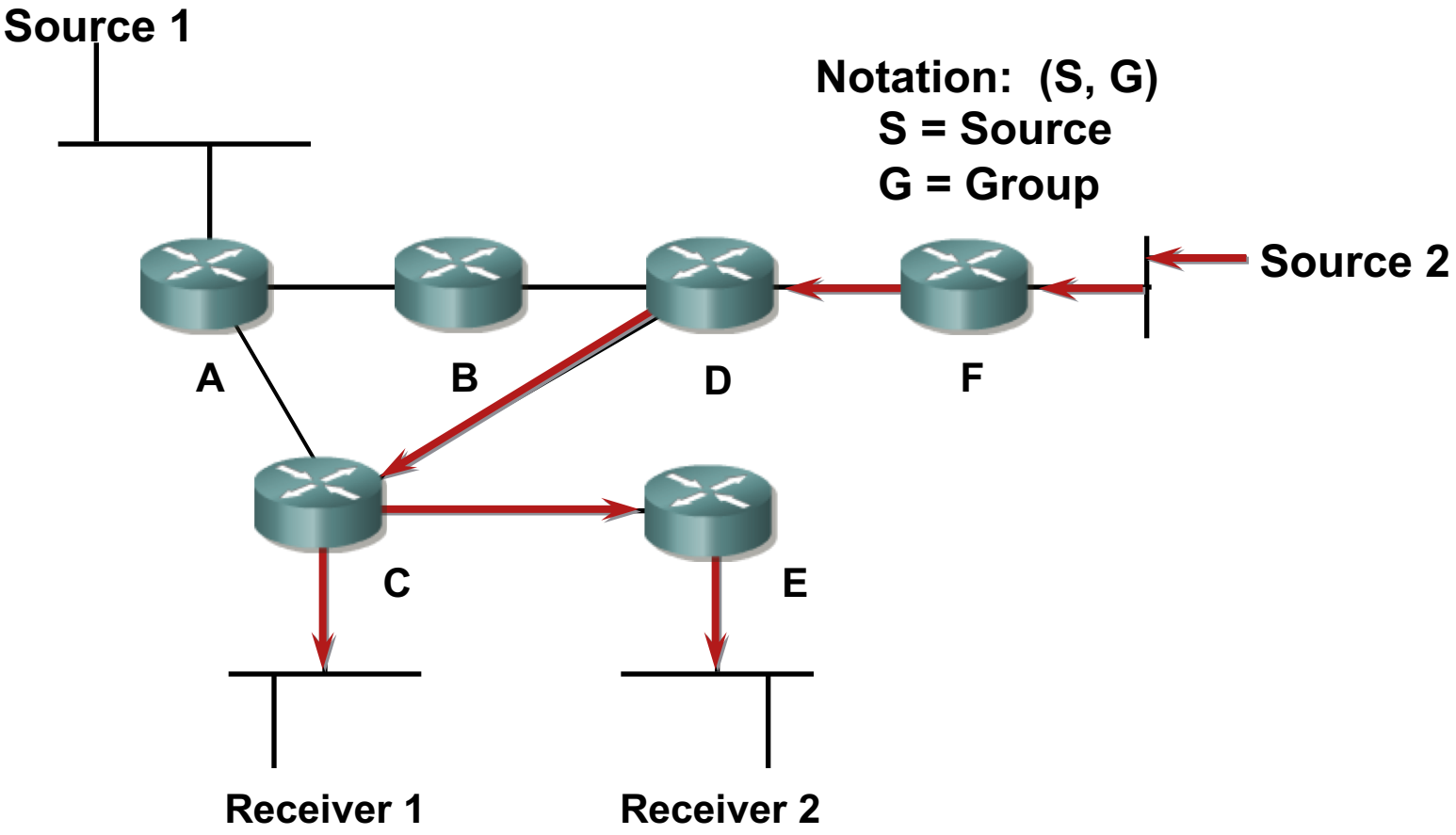
# Multicastové distribučné stromy

Shortest Path Tree (Source Distribution Tree)



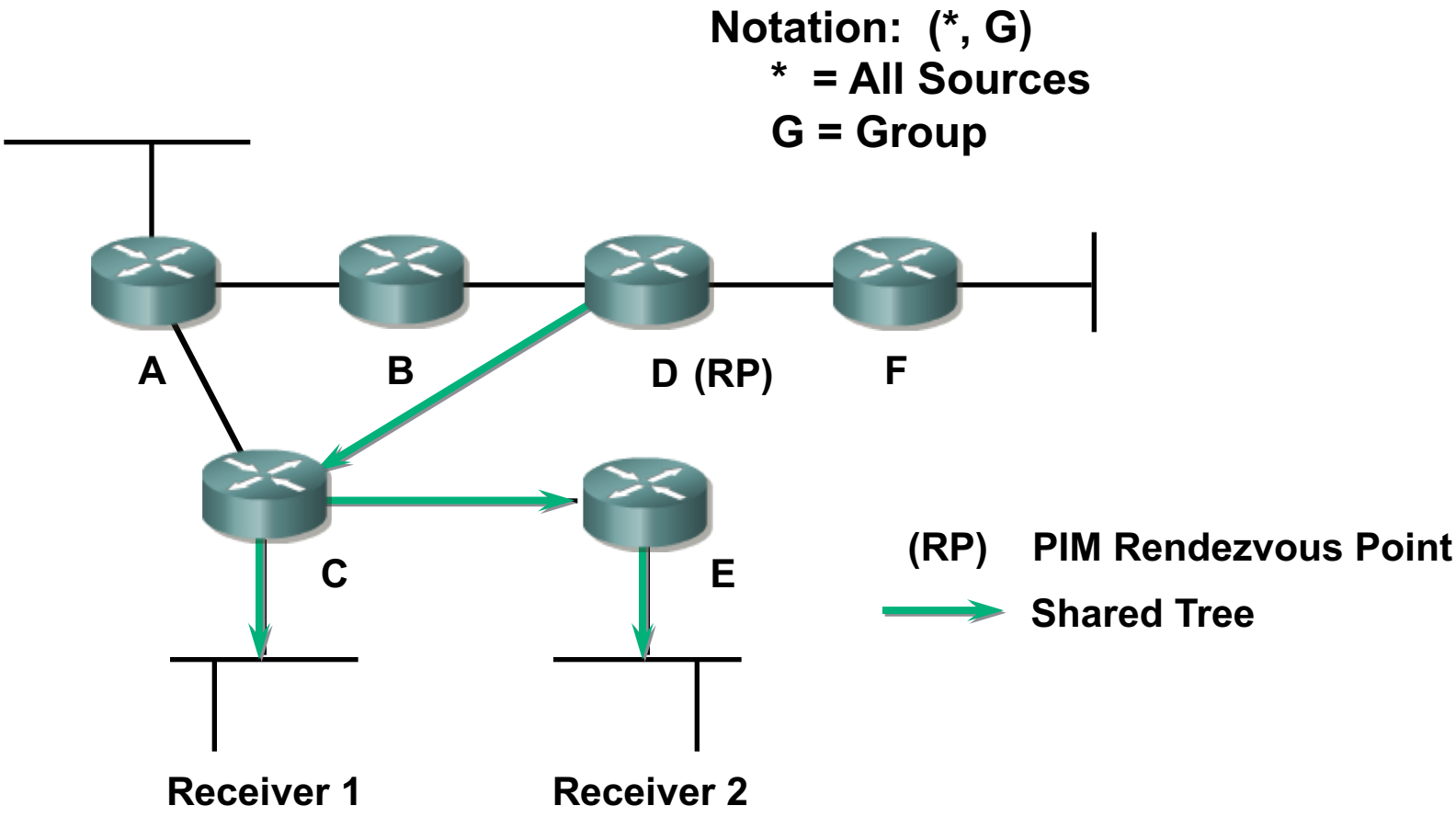
# Multicastové distribučné stromy

Shortest Path Tree (Source Distribution Tree)



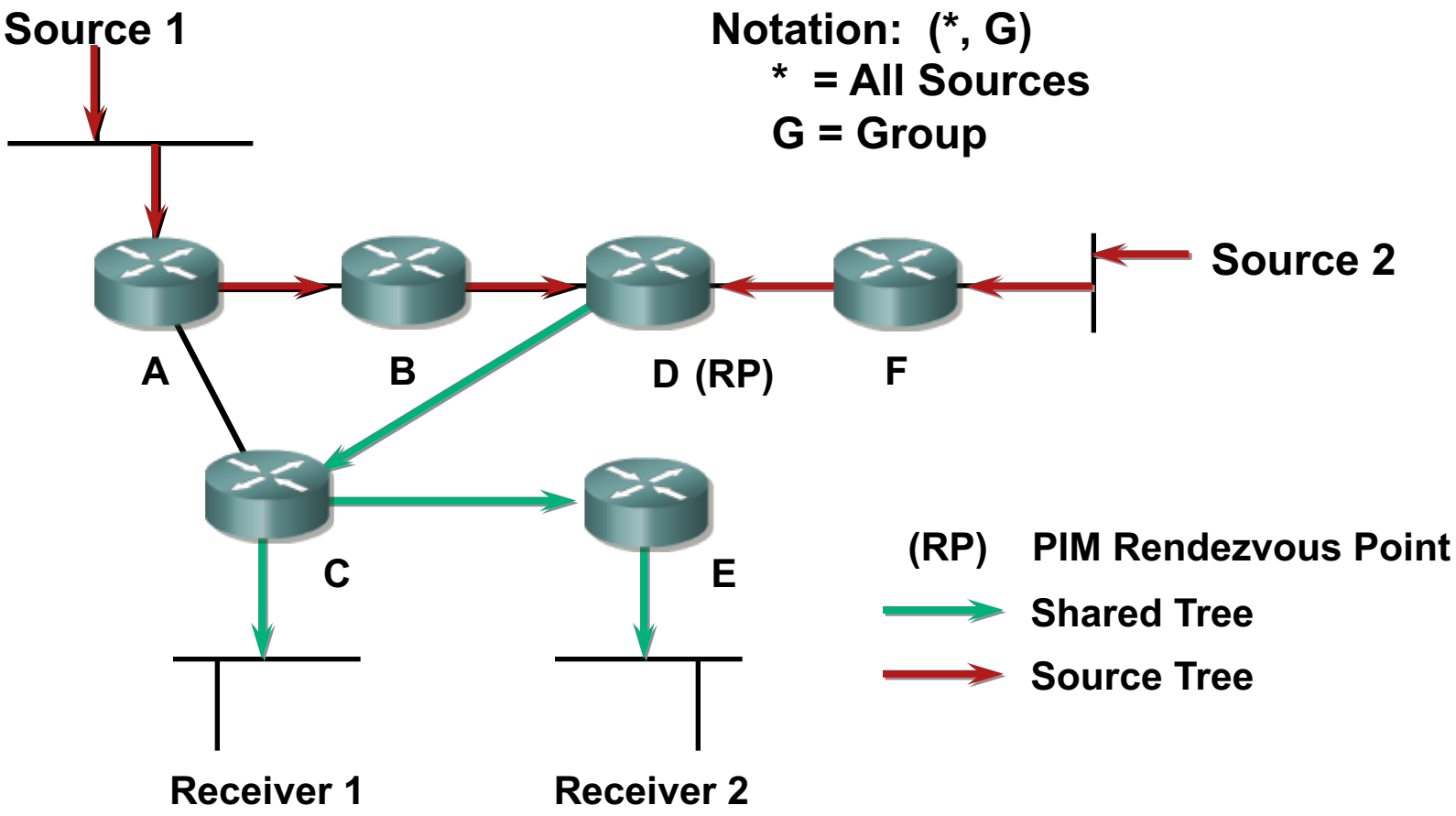
# Multicastové distribučné stromy

Shared Distribution Tree



# Multicastové distribučné stromy

## Shared Distribution Tree



# Identifikácia multicastových distribučných stromov

**Položky (S,G)**

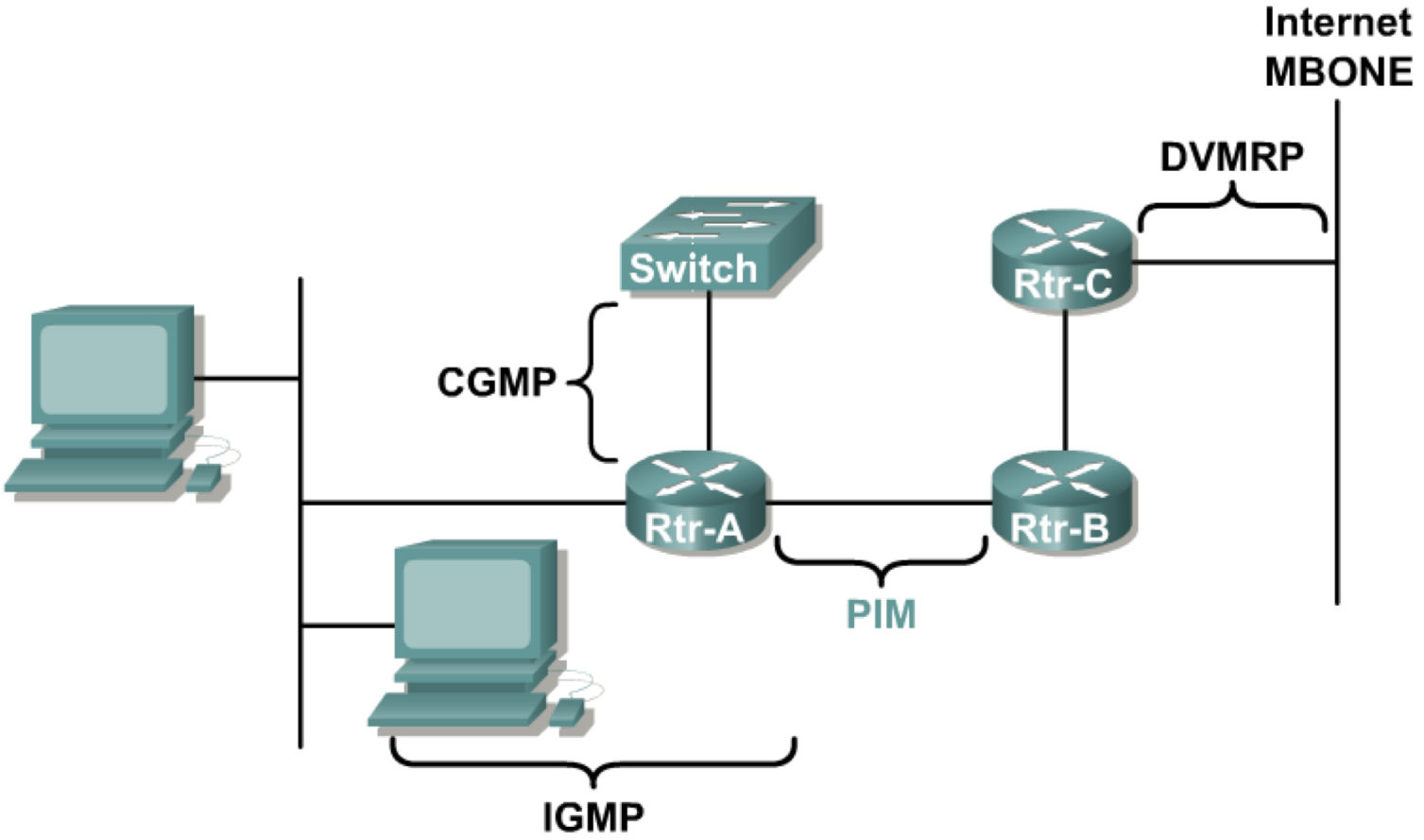
- Pre daný zdroj dát (S) posielajúci do danej skupiny (G)
- Tok dát tečie po najkratšej ceste od zdroja po každého člena skupiny

**Položky (*,G)**

- Pre ľubovoľný (*) zdroj dát posielajúci do danej skupiny (G)
- Tok dát tečie cez stretávacie miesto (RP) pre danú skupinu

# Smerovanie multicastov

# Protokoly súvisiace so smerovaním multicastov




Medzi smerovačmi sa používa protokol **PIM**, ktorý slúži na zistenie a dohodnutie, ktoré multicastové pakety sa kam majú preposlať

# Protocol-Independent Multicast (PIM)

- PIM protokol nie je skutočný smerovací protokol, ktorý by prenášal IP adresy a metriky, ale skôr má povahu signalizačného protokolu
  - PIM sa vkladá priamo do IP paketov, číslo protokolu 103
- PIM vychádza z modelu, kde členstvo v skupine iniciuje príjemca
- PIM vyžaduje, aby v sieti bol aktívny bežný smerovací protokol, avšak je od konkrétneho smerovacieho protokolu nezávislý
- PIM smerovače si vytvárajú smerovacie tabuľky na preposielanie multicastovo adresovaných datagramov
- PIM pracuje v dvoch rôznych režimoch:
  - Dense mode: multicastový traffic je preposielaný do celej siete. Ak smerovač dostáva traffic, pre ktorý nemá ďalšieho príjemcu, odhlási sa od prijímania daného toku (periodický flood-and-prune)
  - Sparse mode: multicastový traffic sa preposiela prostredníctvom distribučných stromov, ktoré sa zostavili na požiadanie pomocou explicitného prihlásenia sa príjemcov do danej skupiny

# Vytvorenie multicastového distribučného stromu v PIM

- Strom sa vytvára v PIM pomocou riadiacich správ Join/Prune
- Stromy typu Shortest Path:
  - Riadiace PIM správy sa posielajú na odosielateľa multicastového trafficu
- Stromy typu Shared:
  - Riadiace PIM správy sa posielajú na dohodnutý router, tzv. rendezvous point (RP)

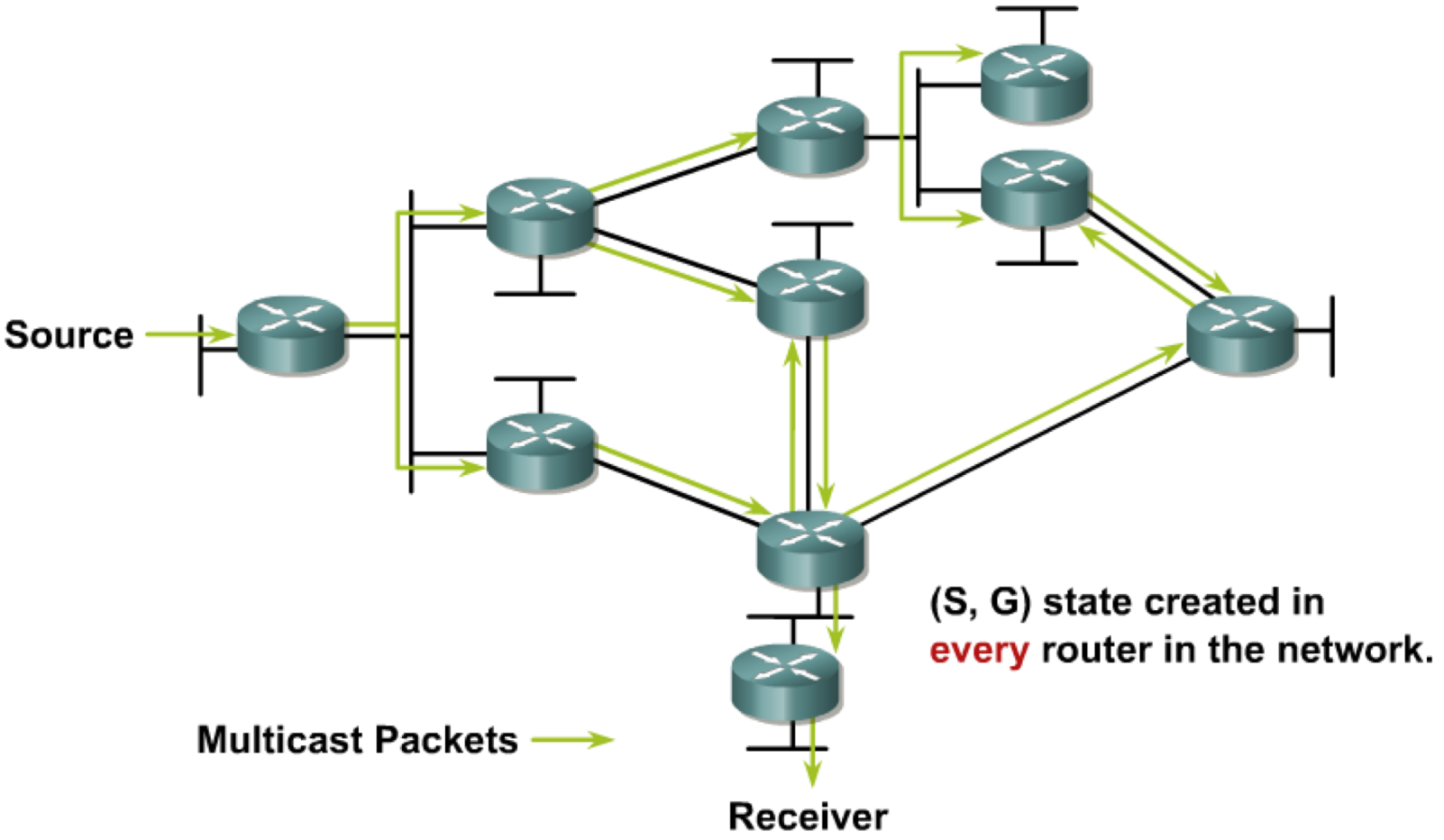
# Multicast Forwarding

- Multicastové smerovanie má opačnú povahu než smerovanie unicastov
  - **Unicastové** smerovanie sa zaujíma o to, **kam paket putuje**
  - **Multicastové** smerovanie sa zaujíma o to, **odkiaľ paket prichádza**
- Multicastové smerovanie používa tzv. Reverse Path Forwarding (**RPF**) na elimináciu **forwarding loops**
  - Pri prijatí paketu idúceho na multicastovú adresu nejakým rozhraním X sa v obyčajnej smerovacej tabuľke vyhľadá interfejs Y, ktorým sa dá najkratšou cestou dostať k odosielateľovi multicastového paketu (pri SPT) alebo k RP (pri shared tree)
  - Ak X == Y, paket sa prepošle ďalej, inak sa zahodí

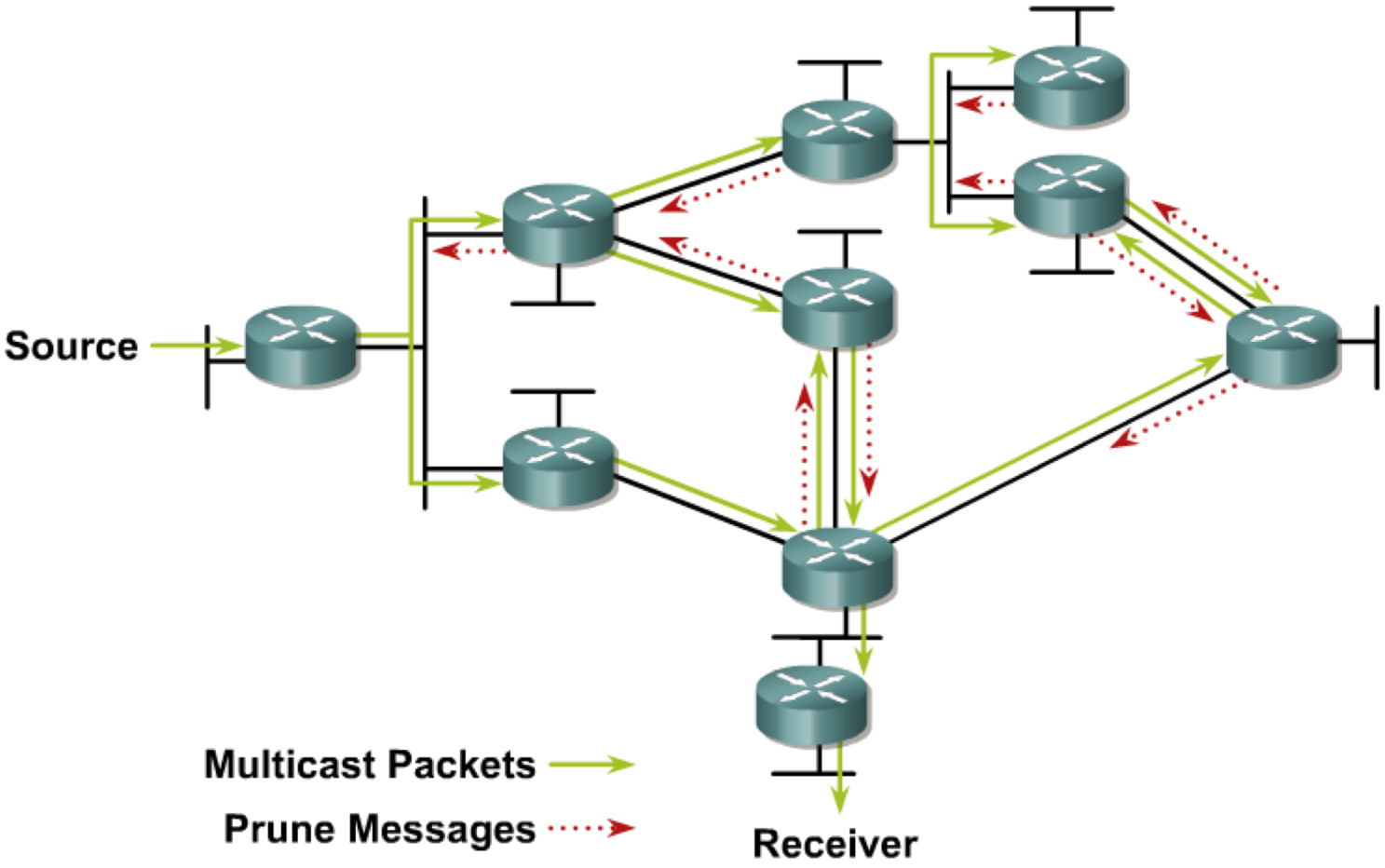
# PIM Dense Mode

# PIM-DM Flood and Prune

Počiatočný flooding

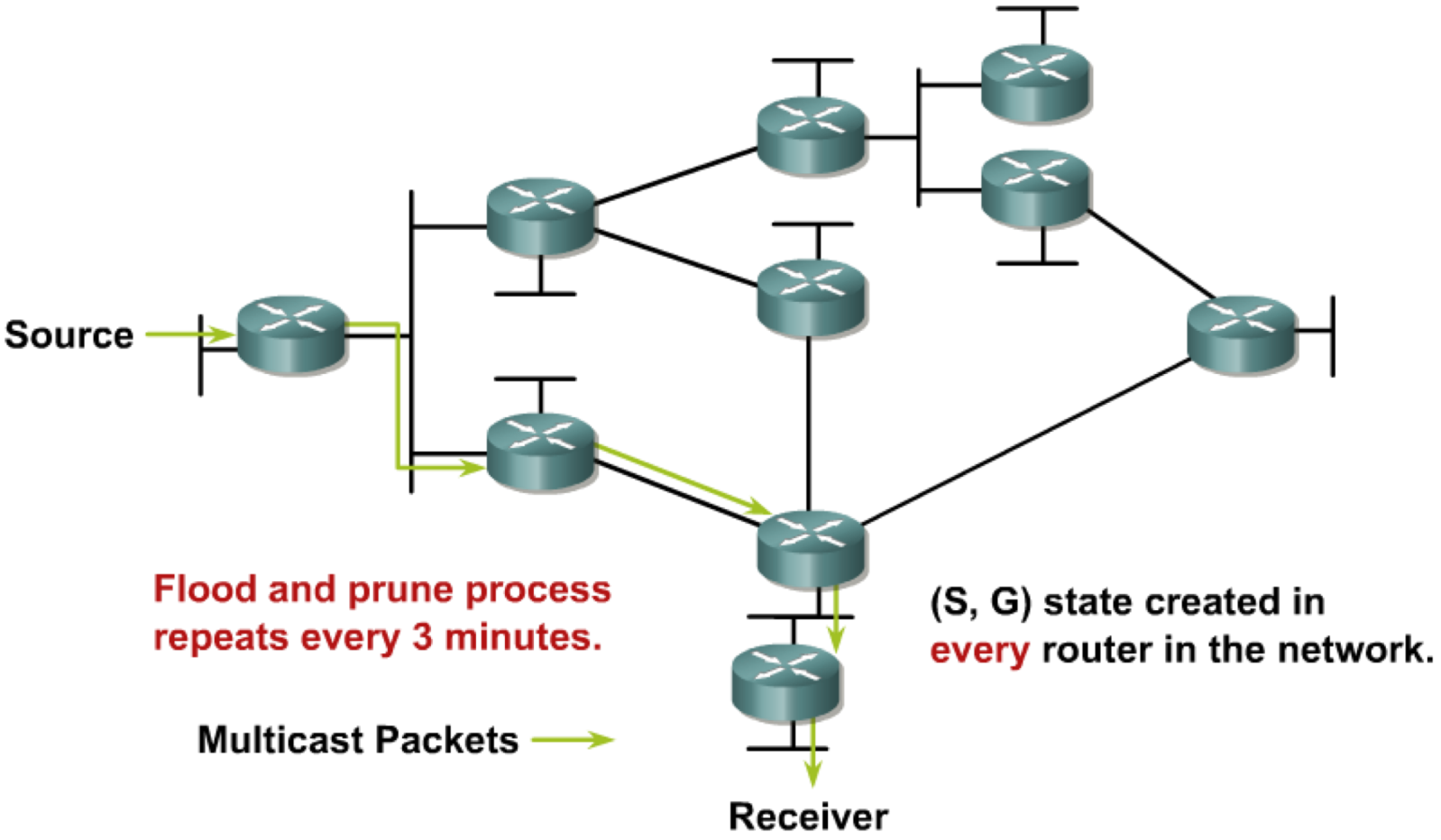


# PIM-DM Flood and Prune



# PIM-DM Flood and Prune

Výsledok po pruningu

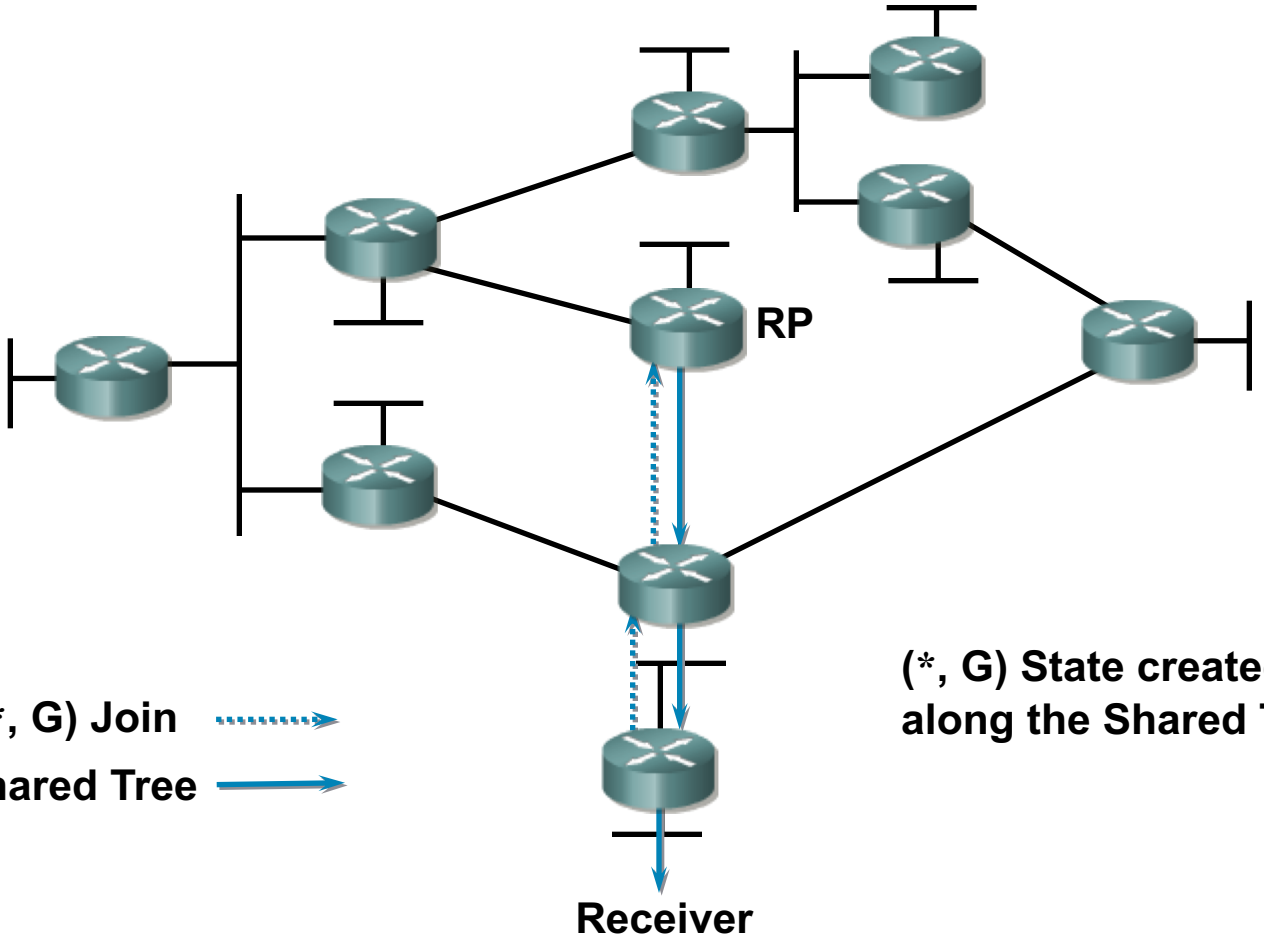


# PIM Sparse Mode

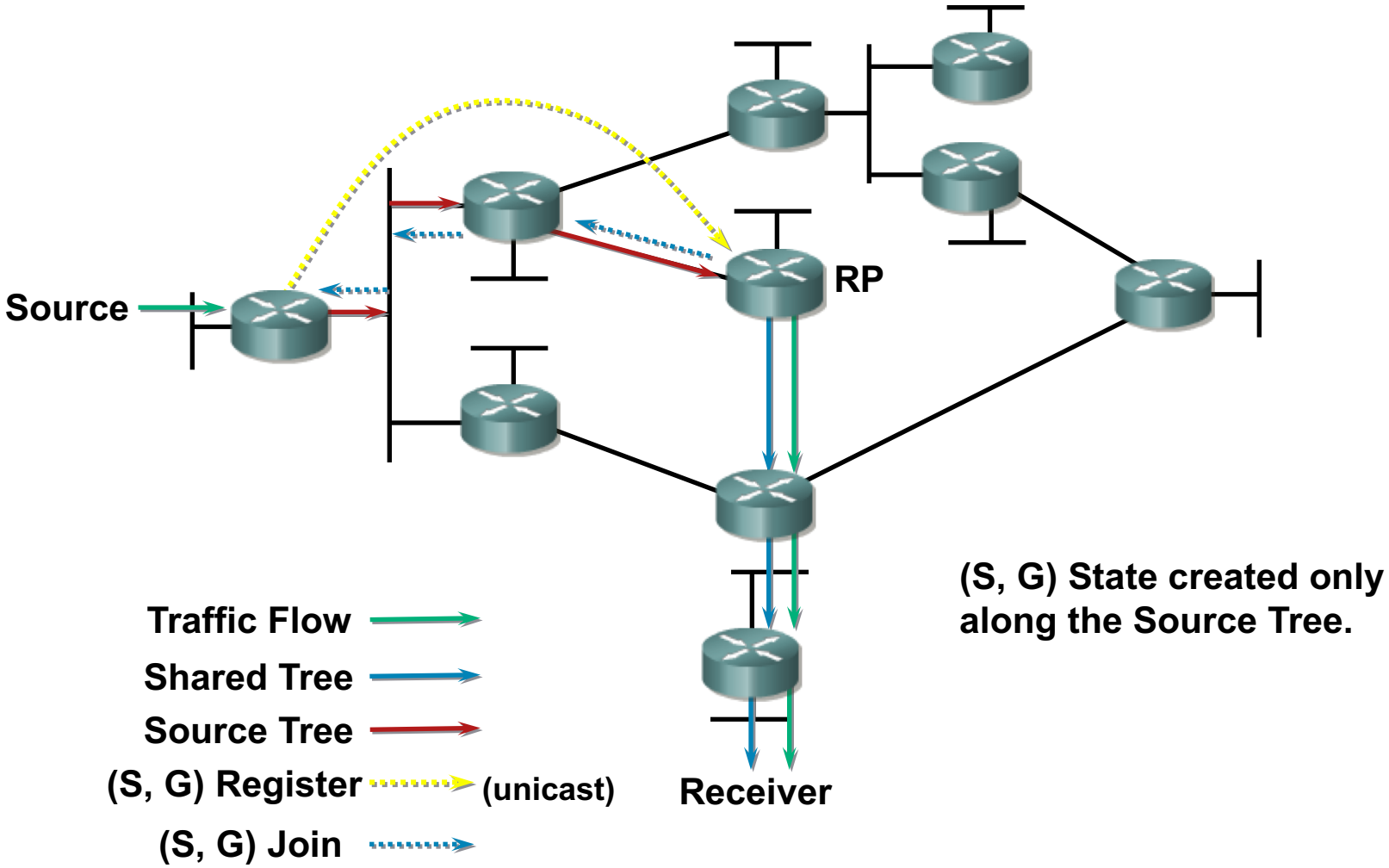
# PIM Sparse Mode

- PIM-SM podporuje aj **source**, aj **shared trees**
  - PIM-DM principálne vytvára iba shortest path trees
- PIM-SM vychádza z tzv. explicitného „pull modelu“
  - Príjemca musí o svoje členstvo explicitne požiadať, “pritiahnuť” si traffic k sebe
- PIM-SM používa tzv. rendezvous point (RP)
  - Odosielatelia a príjemcovia sa stretnú („dajú si rande“) na dohodnutom mieste – na routeri RP
  - Odosielateľov na RP nasmeruje ich príslušný first-hop router
  - Príjemcov zaradí do stromu (s koreňom v RP) ich vlastný designated router (analogický mechanizmus výberu DR ako pri OSPF – najprv najvyššia priorita, potom najvyššia IP)

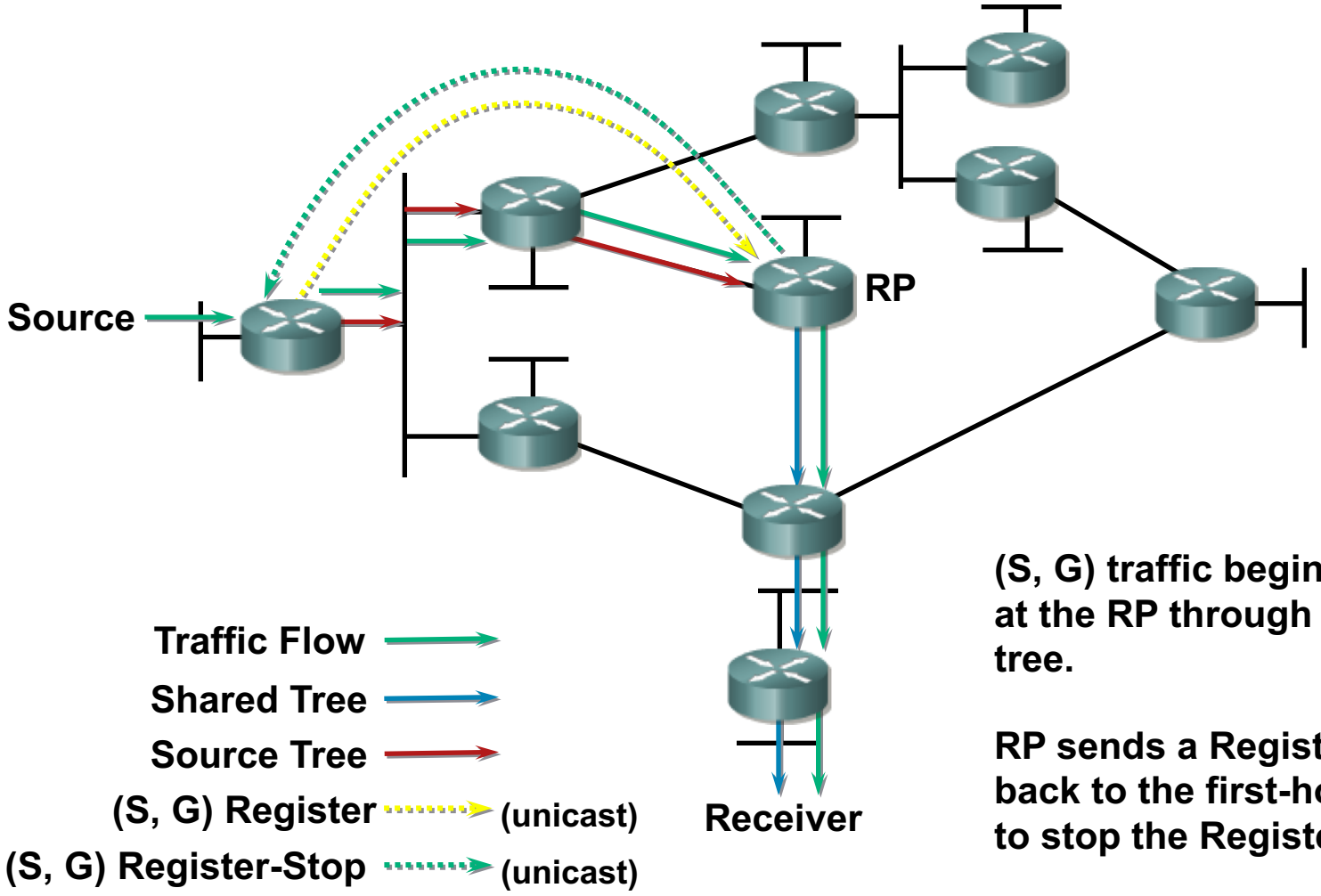
# PIM-SM Shared Tree Join



# PIM-SM Sender Registration



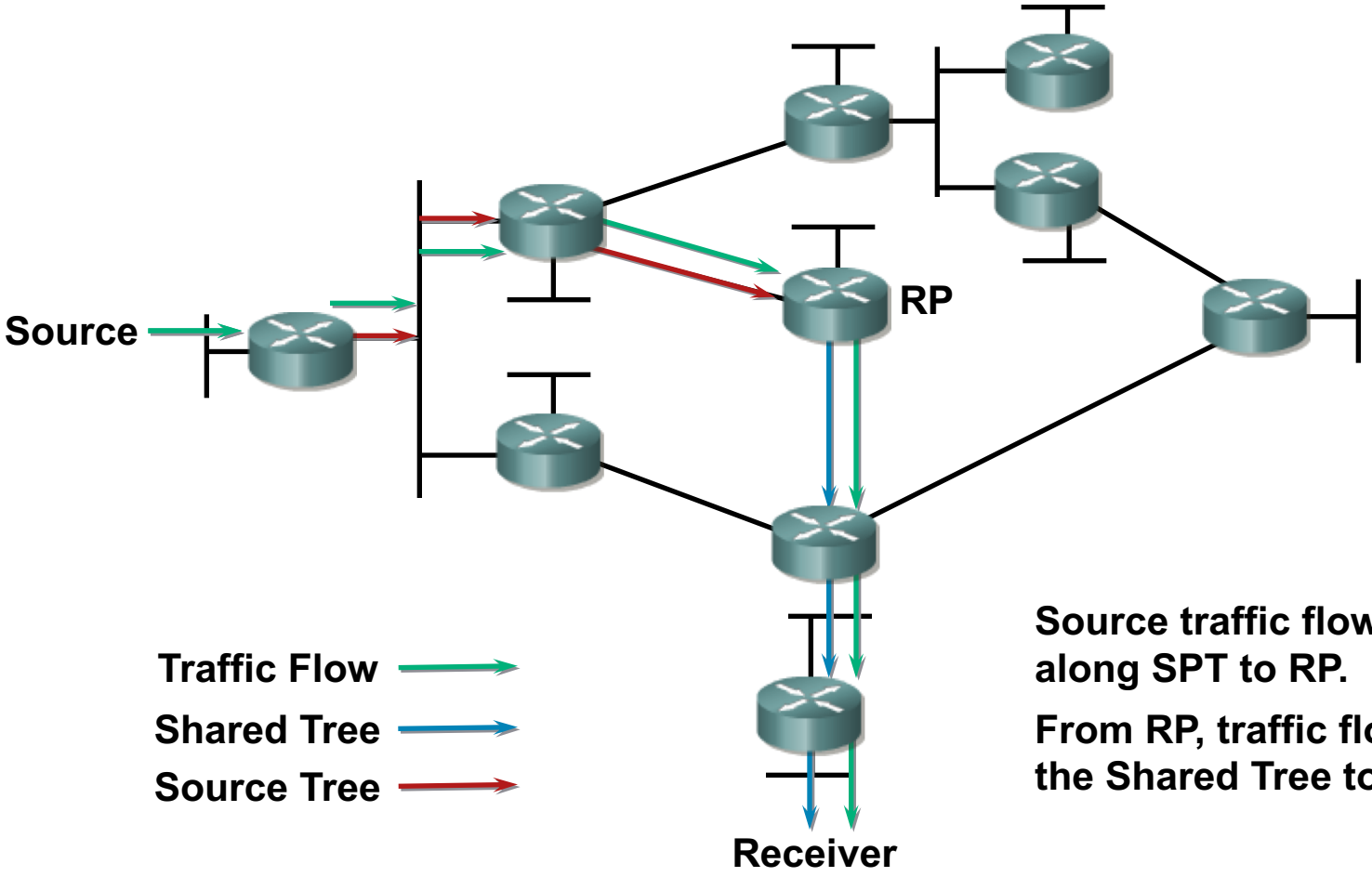
# PIM-SM Sender Registration




(S, G) traffic begins arriving at the RP through the Source tree.

RP sends a Register-Stop back to the first-hop router to stop the Register process.

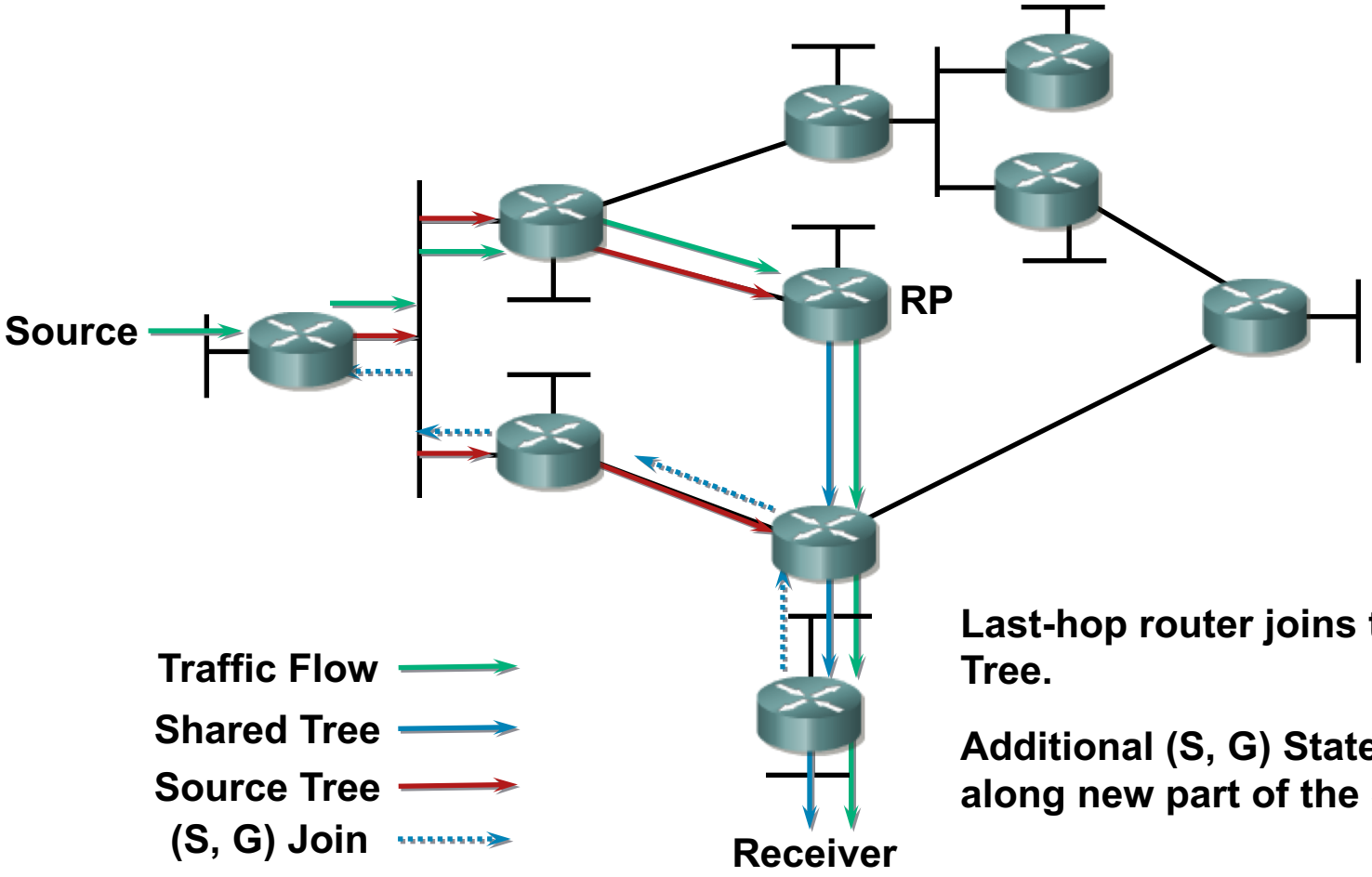
# PIM-SM Sender Registration




Source traffic flows natively along SPT to RP.

From RP, traffic flows down the Shared Tree to Receivers.

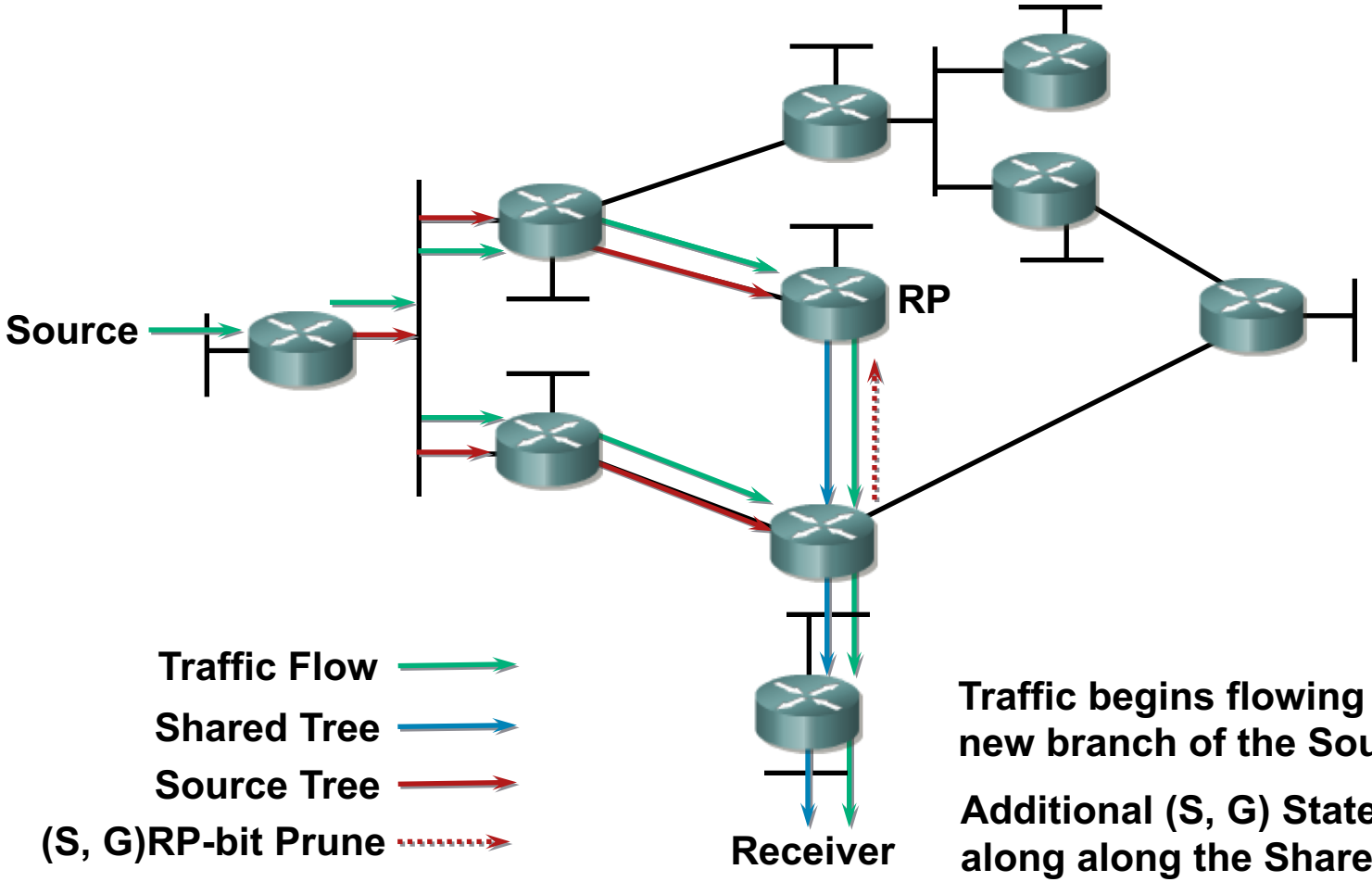
# PIM-SM SPT Switchover




Last-hop router joins the Source Tree.

Additional (S, G) State is created along new part of the Source Tree.

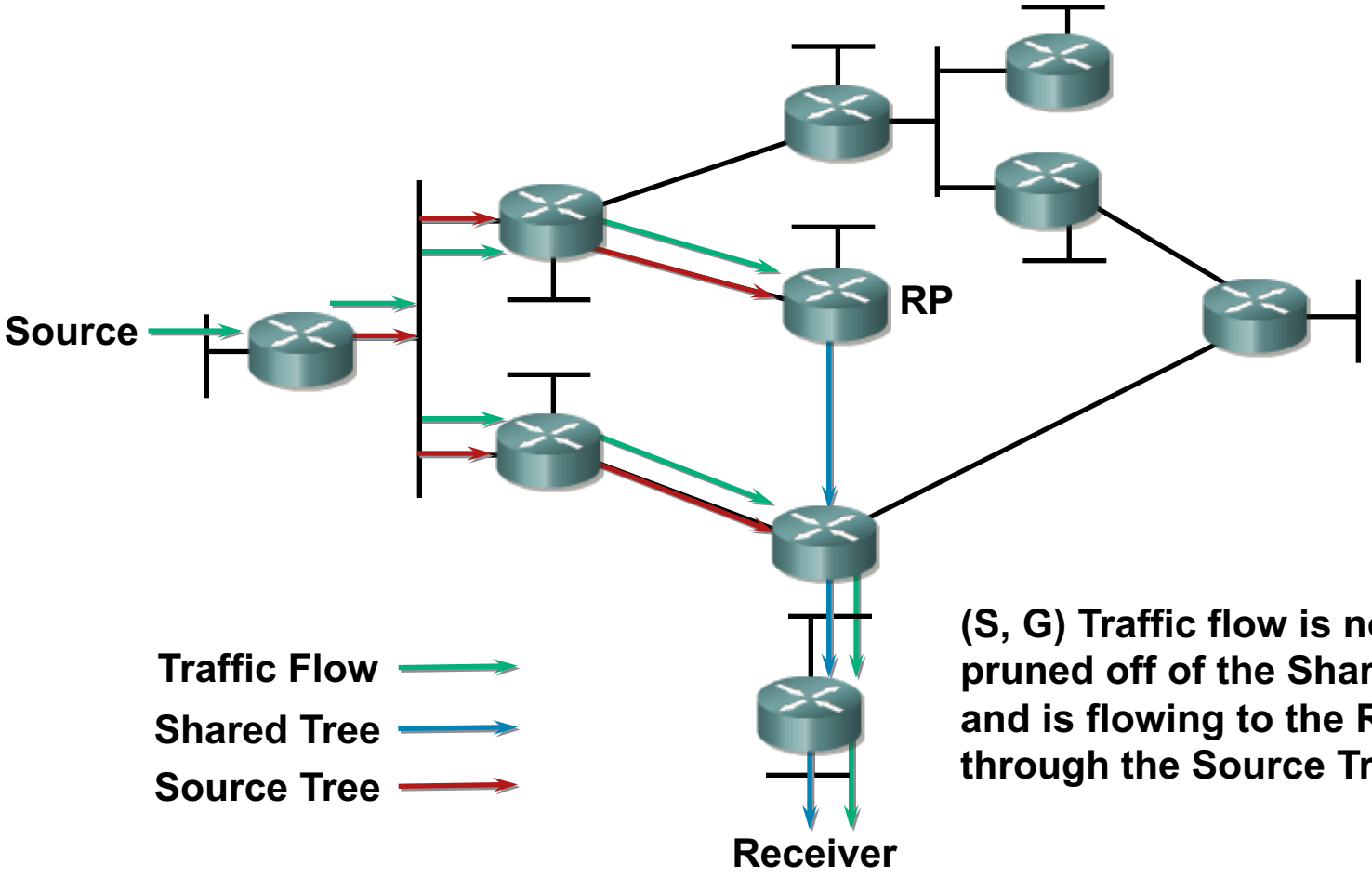
# PIM-SM SPT Switchover



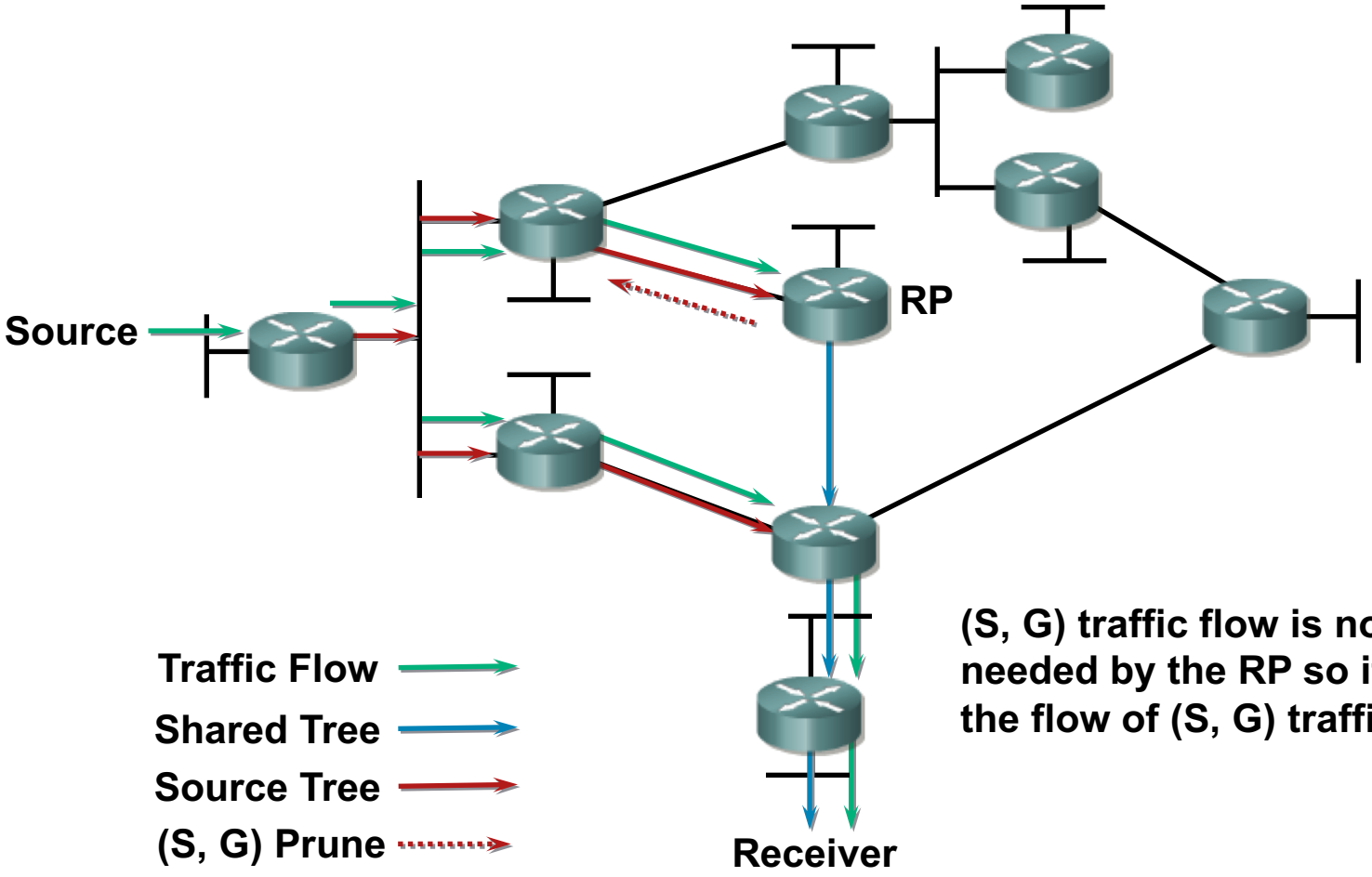

Traffic begins flowing down the new branch of the Source Tree.

Additional (S, G) State is created along along the Shared Tree to prune off (S, G) traffic.

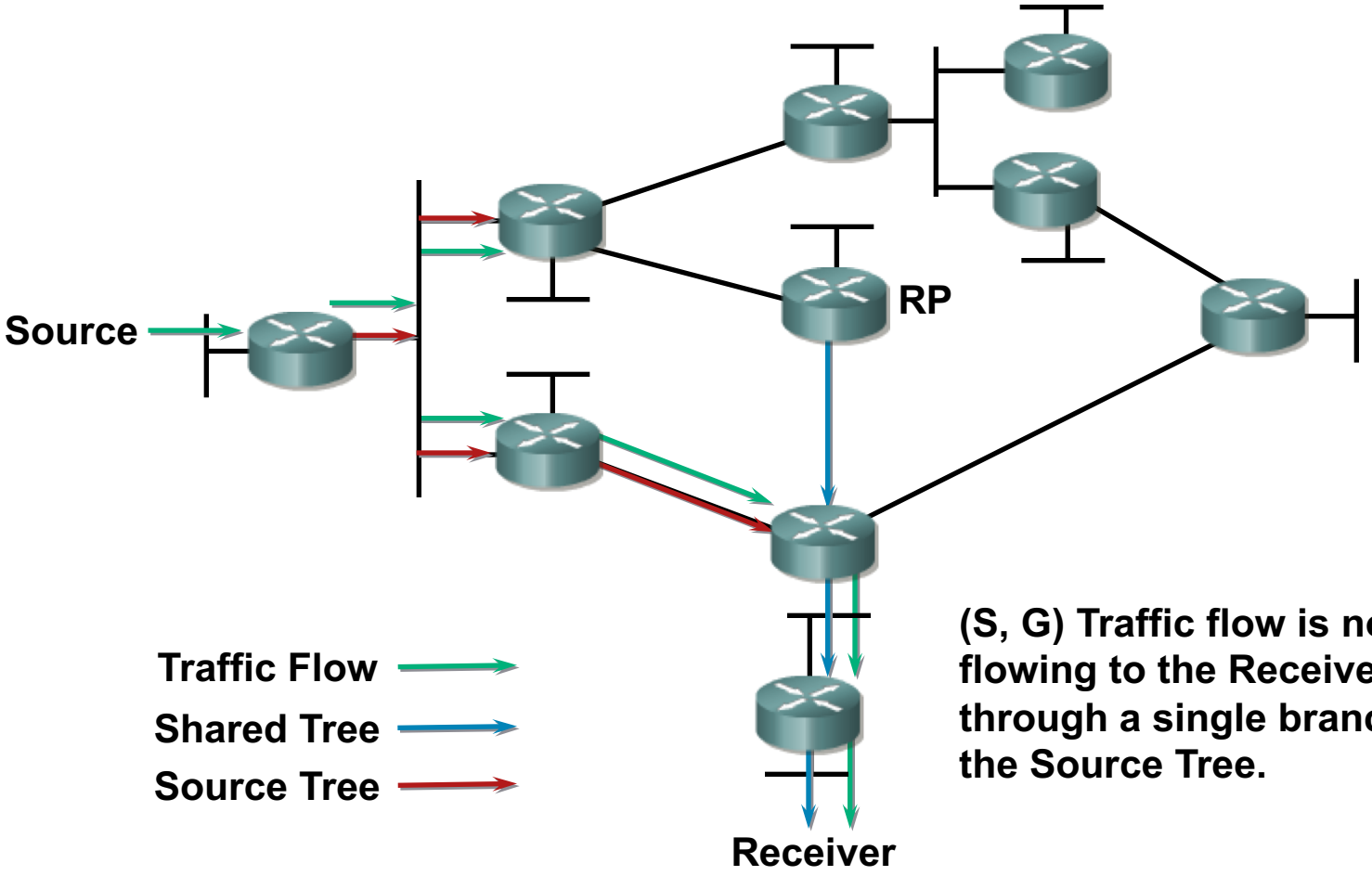
# PIM-SM SPT Switchover



# PIM-SM SPT Switchover



# PIM-SM SPT Switchover



“Implicitné správanie PIM-SM je, že smerovače s priamo pripojenými koncovými príjemcami multicast trafficu sa včlenia do Shortest Path Tree hneď, ako objavia nový zdroj v danej skupine.”

Často prehliadnutý fakt o PIM-SM

# Konfigurácia

# Aktivácia smerovania multicastov

```
Router(config)#
```

```
ip multicast-routing
```

- Aktivuje smerovanie multicastov
- Príkaz je potrebné zadať na každom routeri, implicitne je smerovanie multicastov vypnuté

# Aktivovanie PIM na rozhraní

```
Router(config-if)#
```

```
ip pim { sparse-mode | dense-mode | sparse-dense-mode }
```

- Aktivuje PIM na rozhraní a zvolí formu (sparse-dense dovoľuje kombináciu SM a DM; DM bude použité, ak pre danú skupinu nie je známy RP)
  - Odporúča sa sparse-dense-mode
  - Príkaz je potrebné použiť na všetkých rozhraniach, ktoré majú prenášať multicastový traffic
- Aktivácia PIM na rozhraní zároveň aktivuje aj podporu IGMP na ňom

# Statická konfigurácia RP

```
Router(config)#
```

```
ip pim rp-address address [ access-list ]
```

- Pri statickej konfigurácii RP je potrebné na každom smerovači vrátane RP zadať tento príkaz
  - Smerovač, ktorý má byť RP, sa vlastne odkáže sám na seba
  - Ostatné smerovače sa odkážu na RP
  - Voliteľným access listom je možné limitovať, pre ktoré multicastové skupiny je uvedený router považovaný za RP
- Evidentne, pri veľkej sieti a mnohých odosielateľoch je toto nepríliš škálovateľný spôsob konfigurácie

# Automatické ohlásenie RP a zoznamu obsluhovaných skupín

**Router(config)#**

```
ip pim send-rp-announce {interface type} scope {ttl} group-list {acl}
```

- Nakonfiguruje router ako RP pre skupiny povolené uvedeným ACL
  - Tento mechanizmus je Cisco proprietárny a nazýva sa Auto-RP
  - Informácia o RP sa šíri do hĺbky siete uvedenej parametrom `ttl`
  - Auto-RP announcement správy sa posielajú na IP 224.0.1.39 (skupina CISCO-RP-ANNOUNCE), na tejto adrese načúvajú tzv. RP mapping agent routery

- Nasledujúci príklad ohlási router s jeho IP adresou z rozhrania E0 ako RP pre administratively scoped skupiny:

**Router(config)#**

```
ip pim send-rp-announce ethernet0 scope 16 group-list 1
access-list 1 permit 239.0.0.0 0.255.255.255
```

# RP Mapping Agent

```
Router(config)#
ip pim send-rp-discovery {interface type} scope {ttl}
```

- RP mapping agent je router, ktorý zbiera announcementy od potenciálnych RP posielaných na IP 224.0.1.39 a ostatným routerom rozpošle zoznam RP a príslušných skupín, ktoré obsluhujú
  - Auto-RP discovery správy sa posielajú na IP 224.0.1.40 (CISCO-RP-DISCOVERY), na ktorej počúvajú všetky ostatné PIM routery
- Celý postup v Auto-RP je nasledujúci:
  - Routery nakonfigurované príkazom **ip pim send-rp-announce** sa ohlasujú v skupine 224.0.1.39 a inzerujú svoju ochotu byť RP pre nejaký zoznam skupín
  - RP mapping agent routery konfigurované príkazom **ip pim send-rp-discovery** počúvajú na announcementy v skupine 224.0.1.39, vytvoria výsledný zoznam RP, nimi obsluhovaných skupín a rozpošlú ho na adresu 224.0.1.40
  - Na tejto adrese počúvajú všetky Auto-RP PIM routery a naučia sa RP

# Auto-RP a obmedzenia

- Auto-RP je Cisco proprietárny mechanizmus na automatickú distribúciu RP
  - Nespolupracuje so zariadeniami iných výrobcov
  - Pre správnu činnosť je potrebné, aby rozhrania boli v režime sparse-dense-mode, inak vzniká problém sliepka-vajce, ktorý je možné riešiť dodatočnou (ale nadbytočnou) konfiguráciou
- Od verzie PIMv2 existuje otvorený variant Auto-RP, ktorý sa nazýva BootStrap Router (BSR) a konfiguruje sa podobne
  - Namiesto ip pim send-rp-announce: **`ip pim rp-candidate`**
  - Namiesto ip pim send-rp-discovery: **`ip pim bsr-candidate`**

# Kontrola a troubleshooting

# Zobrazenie multicastovej smerovacej tabuľky

```
Router#
show ip mroute [group-address] [summary] [count] [active kbps]
```

- Zobrazí obsah m-castovej smerovacej tabuľky
  - **summary**: Zostručnený výpis, jeden riadok pre každú položku
  - **count**: Zobrazí štatistiky o skupinách a zdrojoch, vrátane počtov paketov, paketov za sekundu, veľkosti paketov
  - **active**: Zobrazí prenosové objemy od jednotlivých aktívnych zdrojov (aktívny zdroj je taký, ktorý posiela dáta na rýchlosti podľa argumentu *kbps* alebo viac. Štandardne sa berú 4 kbps.)

# show ip mroute

```
NA-1#sh ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Advertised via MSDP, U - URD,
       I - Received Source Specific Host Report
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.1.1.1), 00:07:54/00:02:59, RP 10.127.0.7, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Serial1/3, Forward/Sparse, 00:07:54/00:02:32

(172.16.8.1, 224.1.1.1), 00:01:29/00:02:08, flags: TA
  Incoming interface: Serial1/4, RPF nbr 10.139.16.130
  Outgoing interface list:
    Serial1/3, Forward/Sparse, 00:00:57/00:02:02
```

# Zobrazenie PIM susedov

```
Router#
show ip pim interface [type number] [count]
```

- Zobrazí informácie o PIM rozhraniach

```
Router#
show ip pim neighbor [type number]
```

- Zobrazí zoznam PIM susedov

```
Router#
mrinfo [hostname | address]
```

- Zobrazí zoznam susedných routerov s podporou multicast routingu

# show ip pim interface

```
NA-2#show ip pim interface
Address          Interface            Ver/   Nbr    Query  DR     DR
                                      Mode   Count  Intvl  Prior
10.139.16.133    Serial0/0            v2/S   1      30     1      0.0.0.0
10.127.0.170     Serial1/2            v2/S   1      30     1      0.0.0.0
10.127.0.242     Serial1/3            v2/S   1      30     1      0.0.0.0
```

# show ip pim neighbor

```
NA-2#show ip pim neighbor
PIM Neighbor Table
Neighbor          Interface          Uptime/Expires    Ver   DR
Address                                                    Priority
10.139.16.134     Serial0/0          00:01:46/00:01:28 v2    None
10.127.0.169      Serial1/2          00:01:05/00:01:40 v2    1          (BD)
10.127.0.241      Serial1/3          00:01:56/00:01:18 v2    1          (BD)
```

# Kontrola RP nastavení

```
Router(config)#
```

```
show ip pim rp [group-name | group-address | mapping]
```

- Zobrazí aktívne RP
  - Mapping: zobrazí všetky group-to-RP mapovania, o ktorých router vie

```
Router(config)#
```

```
show ip rpf {source address | name }
```

- Zobrazí informácie o RPF pre danú adresu zdroja alebo pre RP

# show ip pim rp

```
P4-2#show ip pim rp
Group: 224.1.2.3, RP: 10.127.0.7, uptime 00:00:20, expires never

P4-2#show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s) 224.0.1.39/32
  RP 10.127.0.7 (NA-1), v1
    Info source: local, via Auto-RP
         Uptime: 00:00:21, expires: never
Group(s) 224.0.1.40/32
  RP 10.127.0.7 (NA-1), v1
    Info source: local, via Auto-RP
         Uptime: 00:00:21, expires: never
Group(s): 224.0.0.0/4, Static
    RP: 10.127.0.7 (NA-1)
```

# show ip rpf

```
 (voči RP)
NA-2#show ip rpf 10.127.0.7
RPF information for NA-1 (10.127.0.7)
  RPF interface: Serial1/3
  RPF neighbor: ? (10.127.0.241)
  RPF route/mask: 10.127.0.7/32
  RPF type: unicast (ospf 1)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables

 (voči zdroju)
NA-2#show ip rpf 10.139.17.126
RPF information for ? (10.139.17.126)
  RPF interface: Serial0/0
  RPF neighbor: ? (10.139.16.134)
  RPF route/mask: 10.139.17.0/25
  RPF type: unicast (ospf 1)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
```

# Kontrola stavu o skupinách

```
Router#
```

```
show ip igmp interface [type number]
```

- Zobrazí informácie týkajúce sa multicastov o danom zariadení

```
Router#
```

```
show ip igmp groups [group-address | type number]
```

- Zobrazí info o skupinách, ktorých členovia sú k routeru priamo pripojení a zapísali sa do nich pomocou IGMP

# Konfigurácia routera ako člena skupiny

```
Router (config-if)#
ip igmp join-group group-address
```

- Nakonfiguruje router, aby sám bol členom danej skupiny, a aktivuje IGMP na danom rozhraní
  - Router na danom rozhraní pošle IGMP Join (Report) správu a stane sa členom skupiny
  - Dôsledkom je, že IP driver na samotnom routeri bude spracovávať všetky multicasty posielané do tejto skupiny, ako keby boli určené aj pre router

```
Router (config-if)#
ip igmp static-group group-address
```

- Rozhranie sa staticky zaradí do danej IGMP skupiny

# show ip igmp interface

```
rtr-a>show ip igmp interface e0
Ethernet0 is up, line protocol is up
  Internet address is 1.1.1.1, subnet mask is 255.255.255.0
  IGMP is enabled on interface
  Current IGMP version is 2
  CGMP is disabled on interface
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 1.1.1.1 (this system)
  IGMP querying router is 1.1.1.1 (this system)
  Multicast groups joined: 224.0.1.40 224.2.127.254
```

# show ip igmp groups

```
rtr-a>sh ip igmp groups
IGMP Connected Group Membership
Group Address    Interface       Uptime    Expires   Last Reporter
224.1.1.1        Ethernet0       6d17h     00:01:47  1.1.1.12
224.0.1.40       Ethernet0       6d17h     never     1.1.1.17
```

# Kontrola IGMP Snoopingu na switchi

```
Switch#
show ip igmp snooping
show ip igmp snooping multicast
show ip igmp snooping multicast vlan vlan-id
show ip igmp snooping mrouter
```