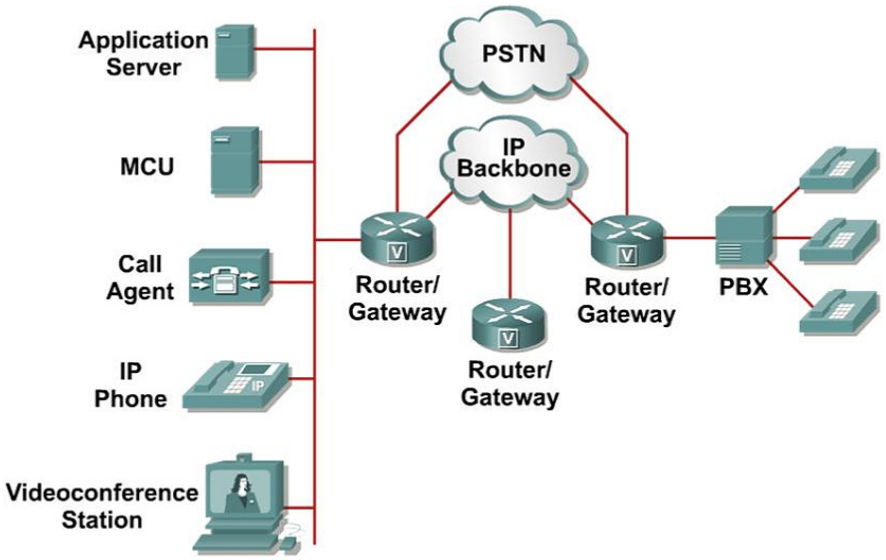
Voice over IP
v prepínaných sieťach

Základy Voice over IP

- VoIP je rodina služieb pre obojsmerný prenos hlasu s využitím sietí pracujúcich na báze protokolu IP
- Prvá lastovička VoIP sa objavila v roku 1995
  - Softvérový produkt izraelskej firmy Vocaltec na prenos hlasu cez dial-up pripojenie
- VoIP dospelo vývojom do IP telefónie – poskytovania telefónnych služieb pomocou telefónov využívajúcich IP protokol ako transport pre hlasové dáta

Zariadenia vo VoIP sieťach – architektúra podľa Cisca



Protokoly vo VoIP

- V súvislosti s VoIP sa veľmi často spomína celá séria najrôznejších komunikačných protokolov
- Vo všeobecnosti VoIP využíva dva druhy protokolov
  - Signalizačné protokoly
    - Call Control – riadenie hovoru
    - Device control – riadenie zariadení
  - Media protokoly
    - RTP

Signalizačné protokoly

- Signalizačné protokoly zabezpečujú riadiace funkcie pre VoIP sieť
  - Prenášajú sa v TCP alebo v UDP segmentoch
- Call Control
  - H.323 a mnohé ďalšie podprotokoly (H.225, H.245)
  - SIP (Session Initiation Protocol)
  - Skinny Call Control Protocol (Skinny)
- Device Control
  - H.248/Megaco (Media Gateway Control)
  - SIGTRAN

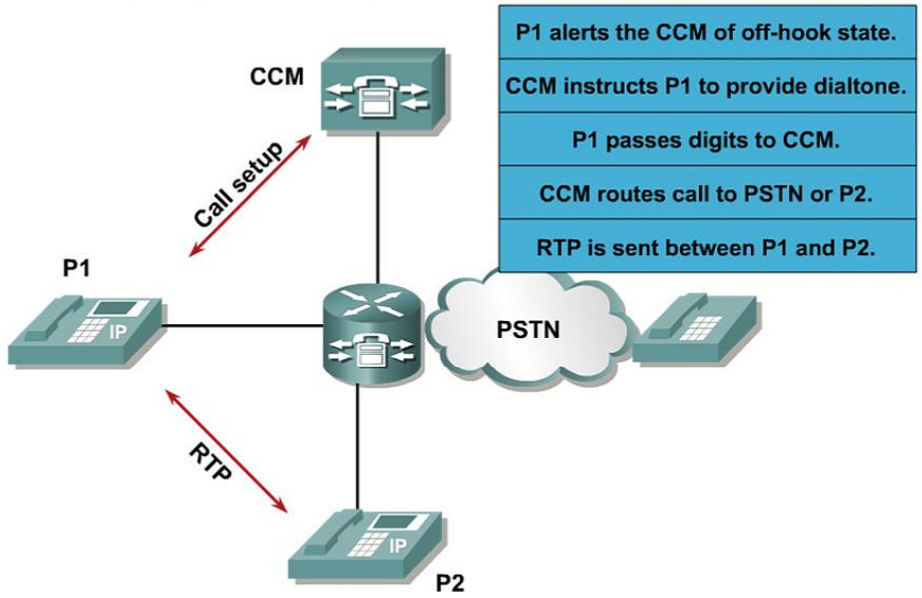
Media protokoly

- Media protokoly prenášajú digitalizovaný hlas, prípadne video, DTMF tóny a iný informačný obsah
- Prakticky jediným v súčasnosti používaným media protokolom je Real-time Transport Protocol (RTP)
  - RTP sa vkladá do UDP segmentov
  - Umožňuje očíslovať segmenty, identifikovať formát prenášaných dát, časovo synchronizovať viaceré toky
- Prenášaný hlas sa digitalizuje pomocou tzv. kodekov
  - Algoritmy pre digitalizáciu a spracovanie hlasu
  - Rôzne kodeky majú rozličné nároky na prenosové pásmo
  - Vo všeobecnosti, čím nižšie nároky, tým horšia kvalita hlasu

Hlasové kodeky

Codec	G.711	G.726 r32	G.726 r24	G.726 r16	G.728	G.729	G.723 r63	G.723 r53
Bandwidth	64 kbps	32 kbps	24 kbps	16 kbps	16 kbps	8 kbps	6.3 kbps	5.3 kbps

Tok dát vo VoIP sieti – Cisco Call Manager - Out of Band signalizácia



Kvalita služby vo VoIP sieťach

IP siete – trend

- Zmena paradigmy „IP over everything“ na „Everything over IP“
- Súčasný trend
  - Integrovaná sieť s mnohými službami (integrácia dát, hlasu, videa a pod.) založená na paketovej IP infraštruktúre
- Trend – výzva pre IP:
  - Nárast zaťaženia
  - Zmena charakteru internetovej prevádzky
    - Integrovaná sieť prenáša dáta rôznych typov rôznorodých aplikácií
    - Nové, rôznorodé požiadavky na spracovávanie dát aplikácií sieťou (sieťové parametre)

Charakteristiky multimediálneho prenosu

- Dáta sú generované v reálnom čase a musia byť doručené načas
- Vysoké a striktné požiadavky na oneskorenie a čas
- Relatívne netolerantné na straty
  - V závislosti od kodeku a pomere strát
- Rozdielne požiadavky na prenos
  - Podľa služby, t.j. video, audio

- Konštantné pásmo
- Citlivý na straty
- Citlivý na oneskorenie

Klasifikácia

- Prvý z QoS nástrojov
- Typicky na access a distro vrstve
  - Ideálne čo najbližšie k zdroju
- Založené na:
  - Layer 2 parametroch
    - MAC adresa, 802.1p CoS, Multiprotocol Label Switching (MPLS) TC, ATM Cell Loss Priority (CLP) bit, Frame Relay Discard Eligible (DE) bit, vstupné rozhranie
  - Layer 3 parametre
    - IP precedencia, Differentiated Services Code Point (DSCP), IP addresa, vstupné rozhranie
  - Layer 4 parametre
    - TCP/UDP porty, transportný protokol
  - Layer 7 parametere
    - Podľa aplikácie

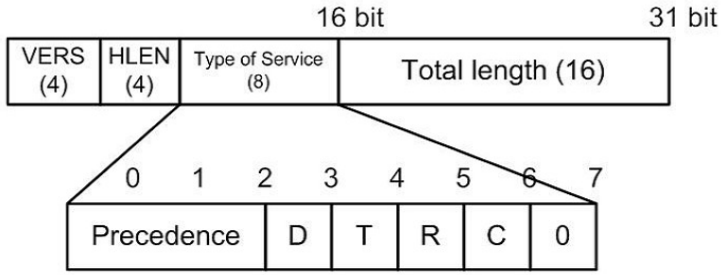
Značkovanie

- Ako následok klasifikácie
  - L2 využíva 802.1p (čo je súčasť 802.1q)
  - L3 IP Precedence (Type of Service pole)
  - DSCP (Differentiated Services Code Point)
- Priradenie k určitému obslužnému správaniu
  - Rámce rovnako označkované sú rovnako obslúžené
    - Input queue scheduling
    - Policing
    - Output queue scheduling

IEEE 802.1p

- IEEE 802.1p
  - Rozšírenie IEEE 802.1q štandardu týkajúce sa Quality of Service
  - 3 bity v 802.1q hlavičke
  - Umožňuje deliť LAN prevádzku podľa stupňov priorít
    - 8 stupňov delenia priorít
- Implementácia
  - Mechanizmy riadenia front

ToS / IP precedence – RFC1349



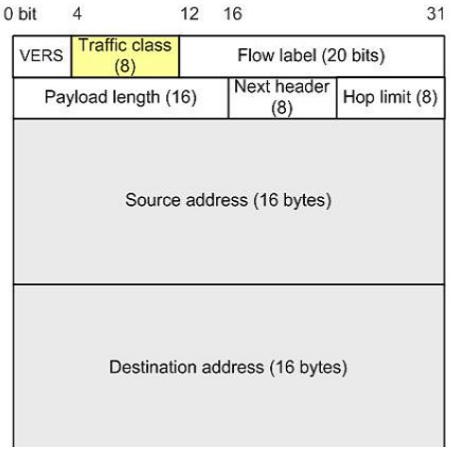
- Precedence
  - 111 - Network Control
  - 110 - Internetwork Control
  - 101 - CRITIC/ECP
  - 100 - Flash Override
  - 011 - Flash
  - 010 - Immediate
  - 001 - Priority
  - 000 - Routine (BE)
- D - Delay,
- T – Throughput
- R – Reliability
- C – Cost

0000 – All normal (Default)
1000 – Minimize delay
0100 – Maximize throughput
0010 – Maximize reliability
0001 – Minimize monetary cost

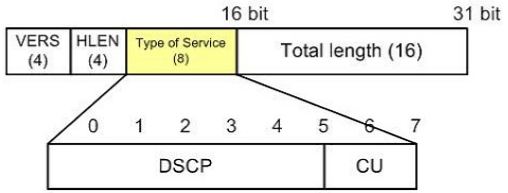
DiffServ Code Point – DSCP

- Tok patriaci do triedy je identifikovaný jedinečnou značkou
  - ***Differentiated Services Code Point – DSCP***
    - IPv4 – Type of Service, IPv6 – Traffic class

IPv6 header



IPv4 Header

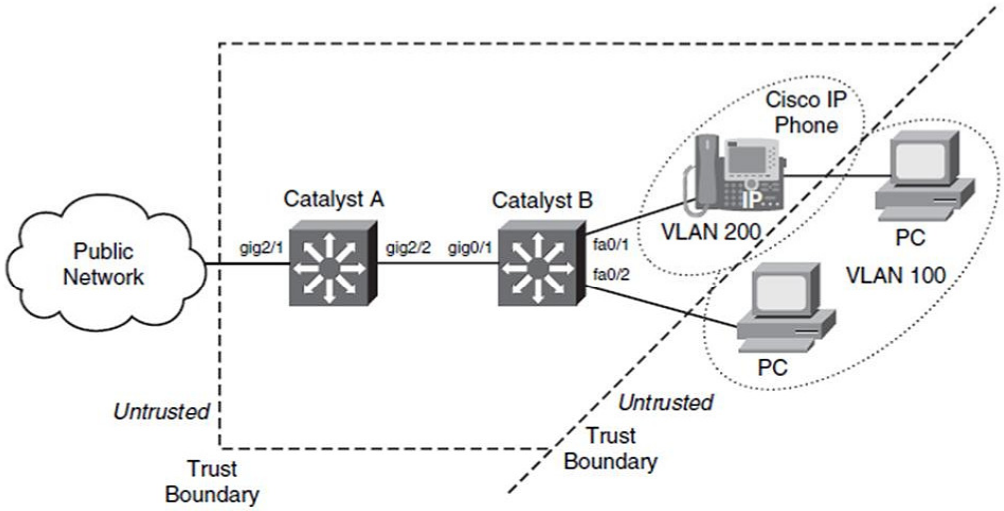


DSCP – DiffServ Code Point
CU – Currently unused

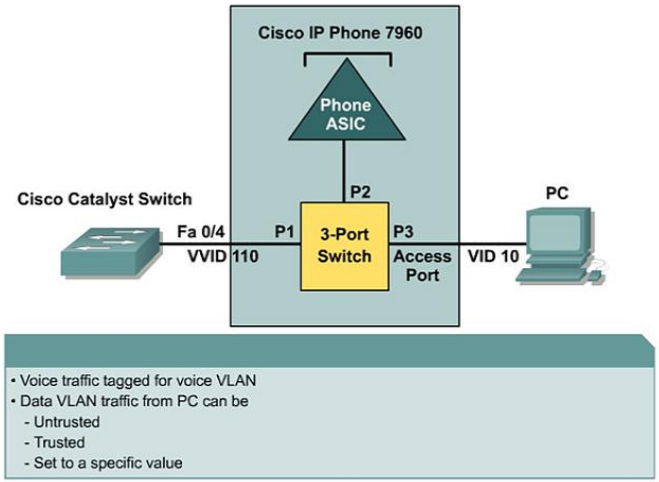
Konfigurácia prepínačov pre VoIP a QoS

Trust boundaries

- Podľa časti siete, ktorú spravujeme



Oddelenie hlasových a dátových tokov Cisco IP telefón



- IP telefón má obvykle 2 ethernetové zásuvky
  - Pre pripojenie do siete
  - Pre pripojenie počítača
- IP telefón prenáša dáta
  - Svoje hlasové pakety
  - Dátové PC pakety

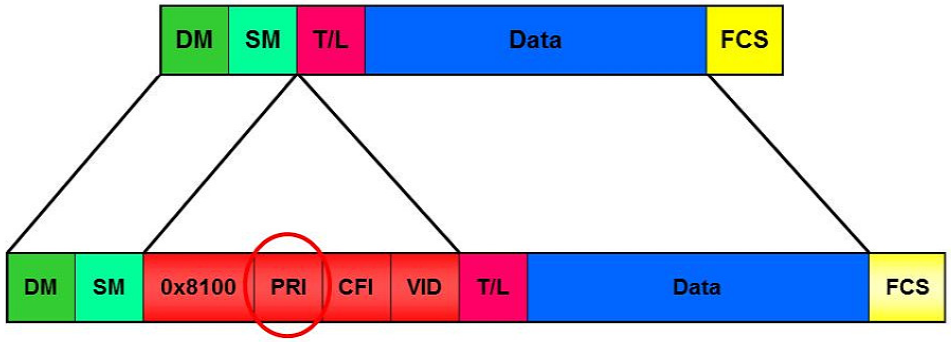
Voice VLAN (Auxiliary)

- Cisco switche umožňujú na access portoch definovať **doplnkovú hlasovú VLAN (Auxiliary VLAN)**
  - Dátová prevádzka nepoužíva 802.1Q značky
  - Hlasová prevádzka bude označkovaná podľa konfigurácie
    - Voice Vlan ID - VVID
- Cisco IP telefón sa o hlasovej VLAN dozvie pri štarte automaticky pomocou **CDP**
  - Na access portoch s voice VLAN **je potrebné mať aktívne** CDP
  - IP telefón začne automaticky značkovať Voice rámce tagom *Voice VLAN ID*

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# switchport voice vlan 200
```

Class of Service

- Na čo je dobré mať hlasovú prevádzku označkovanú?
  - Môžem ju spracovávať v samostatnej VLAN
  - Mám kde vyjadriť prioritu rámca (jeho prednosť v spracovaní)
  - V 802.1Q tagu sú 3 bity pre vyjadrenie priority



Voice VLAN – Konfigurácia VoIP Uplink – možnosti cmd

- Možnosti príkazu

```
Switch(config-if)# switchport voice vlan {vlan-id | dot1p | untagged | none}
```

Keyword	In figure	Native VLAN (untagged)	Voice VLAN	Voice QoS (CoS)
vlan-id	A	PCdata	VLAN vlan-id	802.1p
dot1p	B	PCdata	VLAN 0	802.1p
untagged	C	PCdata/voice	—	—
none (default)	D	PCdata/voice	—	—

Konfigurácia QoS

- Spustenie QoS na prepínači
  - Na niektorých typoch je globálne zakázané

```
Switch(config)# mls qos
```

Class of Service

- Pomocou hodnoty CoS poľa v 802.1Q značke si switch roztriedi pakety medzi fronty na výstupnom rozhraní
  - Je možné nastaviť, aby sa jeden front vyprázdňoval prednostne, alebo aby mal väčší podiel na celkovej kapacite
  - Pre hlas je odporúčaná hodnota **CoS 5**
  - Cisco IP telefóny **automaticky značkujú** hlasové pakety na CoS 5
- Switch je však implicitne nedôverčivý a neverí prioritám v prichádzajúcich rámcoch na danom porte
  - Treba mu preto prikázať, aby dôveroval nastaveným prioritným CoS bitom v prichádzajúcich rámcoch

```
Switch(config-if)# mls qos trust cos
```

  - ... alebo aby im dôveroval iba vtedy, keď je pripojený Cisco IP telefón

```
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos trust device cisco-phone
```

CoS dátových rámcov

- Čo robiť, ak zlomyseľný používateľ na svojom počítači začne svoje dátové pakety značkovať a nastavovať im nežiaducu prioritu?
  - Treba prikázať IP telefónu, aby kontroloval prechádzajúce dátové rámce
  - Ak v nich telefón nájde vyznačenú prioritu, prepíše ju na **prednastavenú hodnotu**
  - Informácia je telefónu opäť odovzdaná cez CDP

```
Switch(config-if)# switchport priority extend cos 2
```

- Ale ak dôverujem PC
  - Predĺžim trust boundaries až na PC

```
Switch(config-if)# switchport priority extend trust
```

CoS dátových rámcov

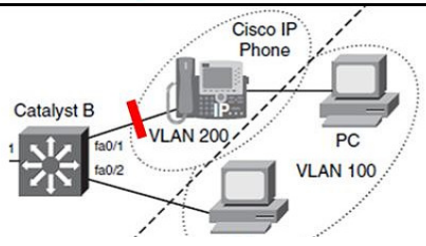
- Čo robiť, ak potrebujeme prideliť prioritu dátovým rámcom prijatým na porte, ktoré nemajú vyznačenú prioritu?
  - Nastavím im definovanú

```
Switch(config-if)# mls qos cos 1
```

Kompletná konfigurácia rozhrania voči hardvérovému IP telefónu

- Kompletná konfigurácia rozhrania voči hardvérovému IP telefónu môže vyzerať takto:

```
Switch(config)# mls qos ! Netreba na 2950
Switch(config)# interface Fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# switchport voice vlan 200
Switch(config-if)# switchport priority extend cos 2
Switch(config-if)# mls qos cos 1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos trust device cisco-phone
```



Kompletná konfigurácia rozhrania voči softvérovému IP telefónu

- Konfigurácia portu voči počítaču so softvérovým IP telefónom je o niečo inakšia
  - Počítač nevie využívať Voice VLAN
  - Cisco IP Communicator neposiela prioritne označkované rámce
  - Dôvera sa musí realizovať voči DSCP v záhlaví IP paketu

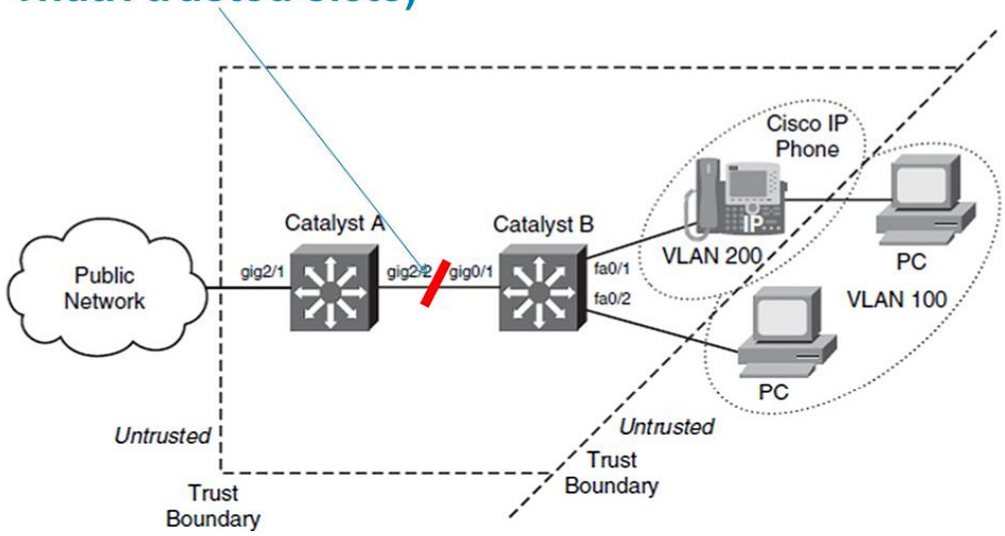
```
Switch(config)# mls qos ! Netreba na 2950
Switch(config)# interface Fa0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos trust device cisco-phone

!!! Namiesto posledného príkazu niekedy bolo aj:
!!! mls qos trust device cisco-softphone
```

Overenie QoS

```
show mls qos interface
```

```
Switch# show mls qos interface fastethernet
0/1
FastEthernet0/1
trust state: trust cos
trust mode: trust cos
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
```

Prepojenie prepínača a prepínača = Uplink (vo vnútri trusted siete)



Prepojenie prepínača a prepínača

- Voči iným trusted switchom je potrebné zapnúť dôveru voči CoS

```
Switch(config)# interface type mod/num
Switch(config-if)# switchport mode trunk
Switch(config-if)# mls qos trust cos
```

Prepojenie routera a switcha

- CoS značky sú použiteľné iba na trunkoch...
  - Dajú sa zapísať iba do 802.1Q tagov, obyčajný Ethernet rámec neobsahuje prioritné bity
- ... a platia iba vo vnútri jednej broadcastovej domény
  - Paket po prechode routerom získava nový rámec, do ktorého sa hodnota starých CoS bitov neprenáša (ak vôbec je do čoho)
- Voči routerom sa teda dôvera na CoS bity vo všeobecnosti nedá na switchoch použiť
- Ako potom realizovať prioritu na uplinkoch medzi switchom a routerom?
  - Využiť DSCP bity v hlavičke IP paketu

Auto-QoS

- Nastavovanie QoS prostriedkov je netriviálna záležitosť
- Cisco pripravilo pre smerovače a prepínače niekoľko makier, ktoré po spustení vygenerujú automagickú konfiguráciu dôležitých QoS prostriedkov
- Na porte switcha smerom k telefónu:
  - Pre HW phone, trust CoS

```
Switch(config-if)# auto qos voip cisco-phone
```

  - Pre SW phone, trust DSCP

```
Switch(config-if)# auto qos voip cisco-softphone
```

  - Ak verím PC

```
Switch(config-if)# auto qos voip trust
```

  - Na porte switcha smerom k routeru (uplink):

```
Switch(config-if)# auto qos voip trust
```

Auto-QoS

- Vygenerovanú konfiguráciu je samozrejme možné neskôr ľubovoľne upraviť
- Príkaz **show auto qos** zobrazí pôvodné nastavenia, ktoré boli pomocou Auto-QoS vygenerované
  - Nezobrazí prípadné používateľské úpravy

Power Over Ethernet (PoE)

Power over Ethernet

- Technológia napájania IP zariadení po Ethernet médiu
  - Efektívne, dosiahnutie vyššej dostupnosti
- Dve metódy napájania
  - Cisco Inline Power (ILP)
    - Cisco proprietárny, vyvinutý pred 802.3af
  - IEEE 802.3af
    - IEEE štandard, 15.4W na port
  - IEEE 802.3at
    - IEEE štandard, 25.5W na port
- Napájanie
  - 48V DC
  - Piny 1-3, 2-6 (ILP, IEEE)
  - Alebo piny 4,5 a 7,8 (len IEEE)

Konfigurácia PoE

- Cat prepínače defaultne zapnutú podporu PoE
  - Dá sa vypnúť, nastaviť

```
Switch(config)# interface type mod/num
Switch(config-if)# power inline {auto [max milli-watts] | static [max milli-watts] | never}
```

- Overenie

```
Switch# show power inline [ type mod/num ]
```

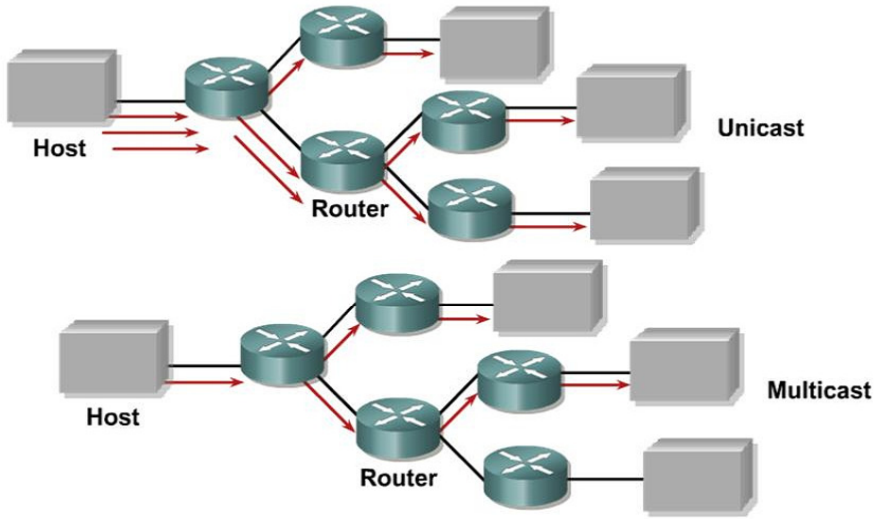
cisco

IP Multicasting

Načo multicast?

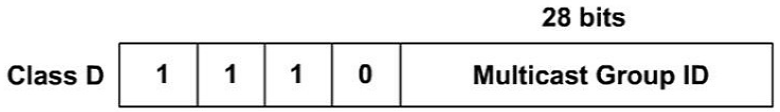
- Mnohé sieťové aplikácie požadujú príjem istého dátového toku mnohými príjemcami súčasne
  - Internetové analógy rozhlasu, televízie, konferenčných spojení
  - Music-on-hold v IP telefónii
  - Distribúcia informácií mnohým (potenciálne neznámym) príjemcom naraz (presný čas, konfiguračné parametre alebo 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

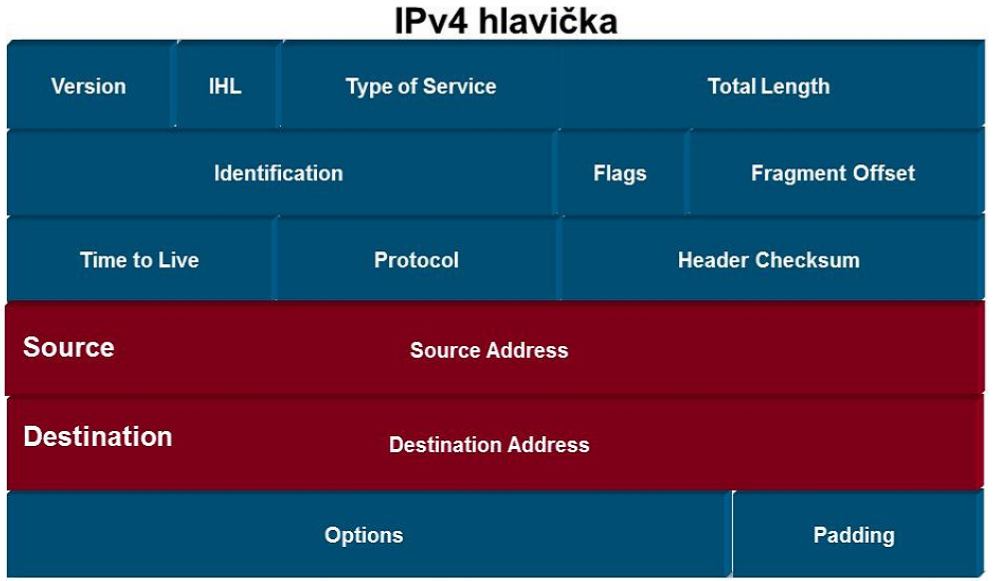


Štruktúra multicastovej IP adresy

- 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



IP adresovanie v multicastoch

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)

Multicastové adresovanie na L2

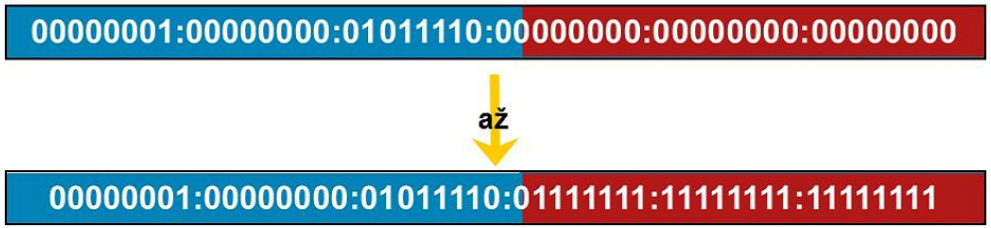
- Doposiaľ sme predpokladali, že MAC adresa v ethernetovom rámci označuje jedno konkrétne sieťové rozhranie
- V skutočnosti existujú MAC adresy, ktoré označujú nejakú skupinu počítačov (v broadcastovej doméne)
- MAC adresa: 6B, prvé 3B: OUI, druhé 3B: S/N
- Tvar prvého bajtu MAC adresy:

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

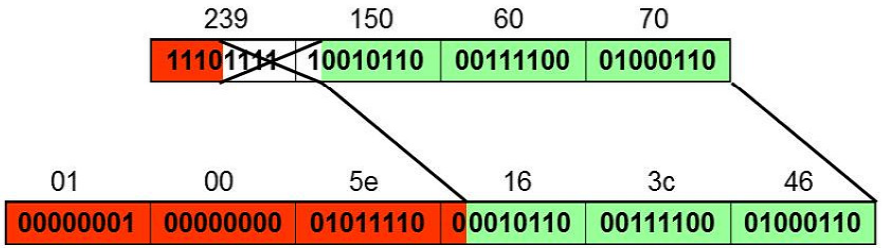
IANA vyčlenila pre IPv4 multicasting rozsah MAC **01:00:5e:00:00:00 až 01:00:5e:7f:ff:ff**



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

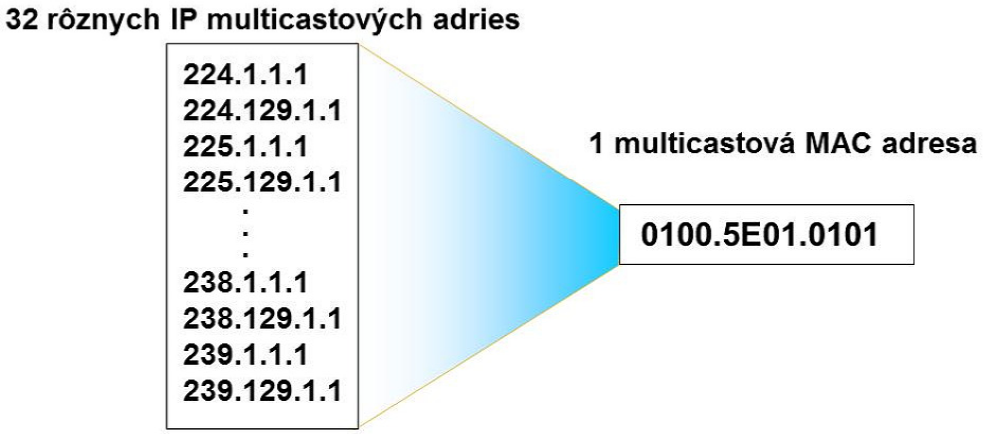
Mapovanie multicastových IP adries na multicastové MAC adresy

- 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 (routerom)
- Existujú v súčasnosti 3 verzie:
  - IGMPv1 definované v RFC 1112 a IGMPv2 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

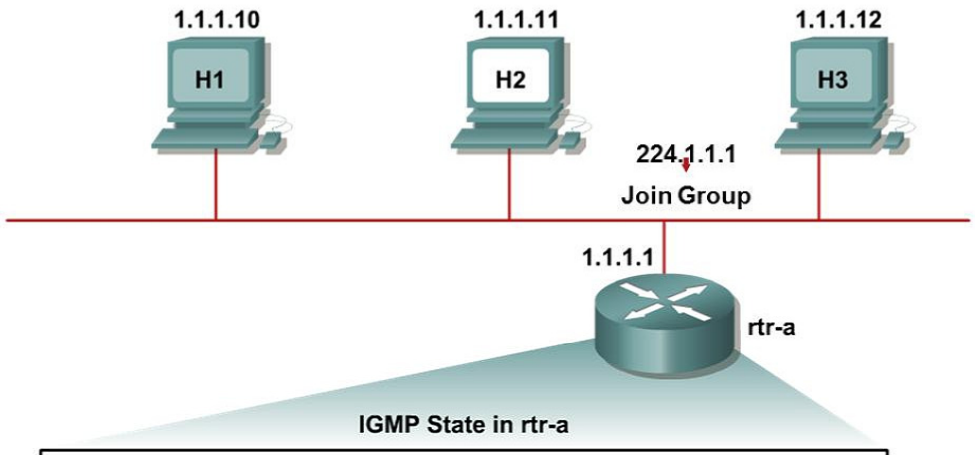
IGMPv2

- 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, rovnako ako v IGMPv1
  - **Leave group**
    - Stanica touto správou ohlasuje opustenie skupiny, posielaná na 224.0.0.2
    - Správu netreba poslať, ak na poslednú group-specific Query odpovedala iná stanica než tá, ktorá sa odhlasuje
- 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

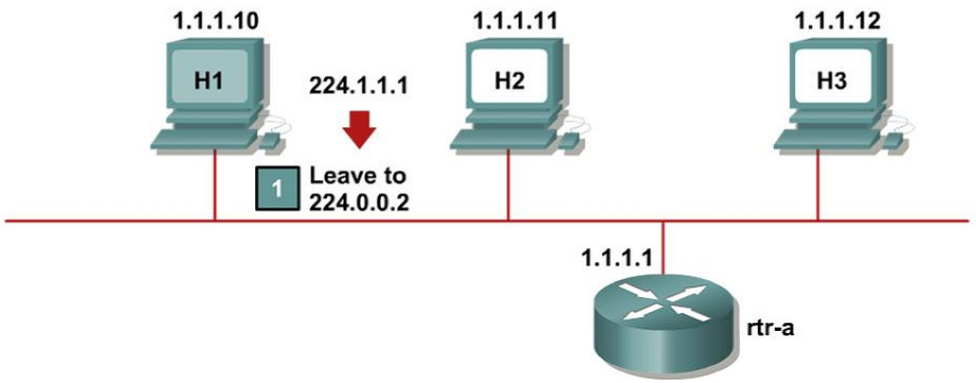
- Dva základné druhy správ:
  - **Membership query**
    - General query, posielané na 224.0.0.1
    - Group-specific query (*,G), posielané na skupinu
    - Group-and-source specific (S,G), posielané na skupinu
  - **Membership report**
    - Odosielané na adresu 224.0.0.22
- IGMPv3 má podstatne zložitejšiu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

IGMPv2: Prihlásenie sa do skupiny




```
rtr-a>show ip igmp group
IGMP Connected Group Membership
Group Address   Interface   Uptime   Expires    Last Reporter
224.1.1.1       Ethernet0   0d1h3m   00:02:31   1.1.1.11
```

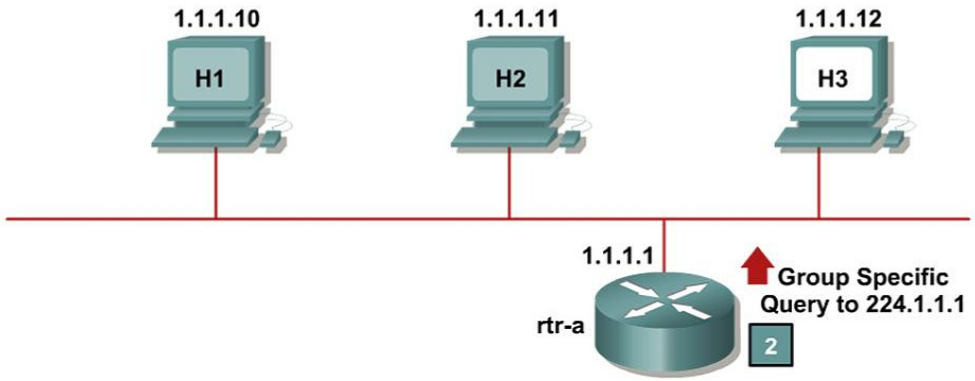
IGMPv2: Opustenie skupiny



Stanice H2 a H3 sú členmi skupiny 224.1.1.1

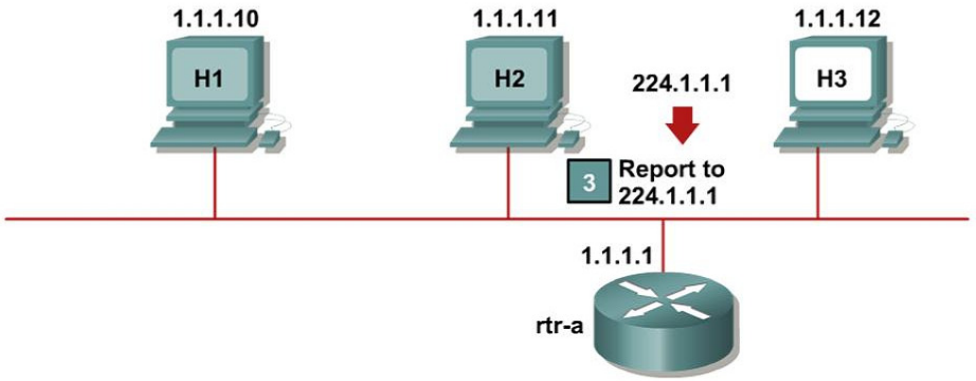
1. H2 pošle správu Leave group

IGMPv2: Opustenie skupiny



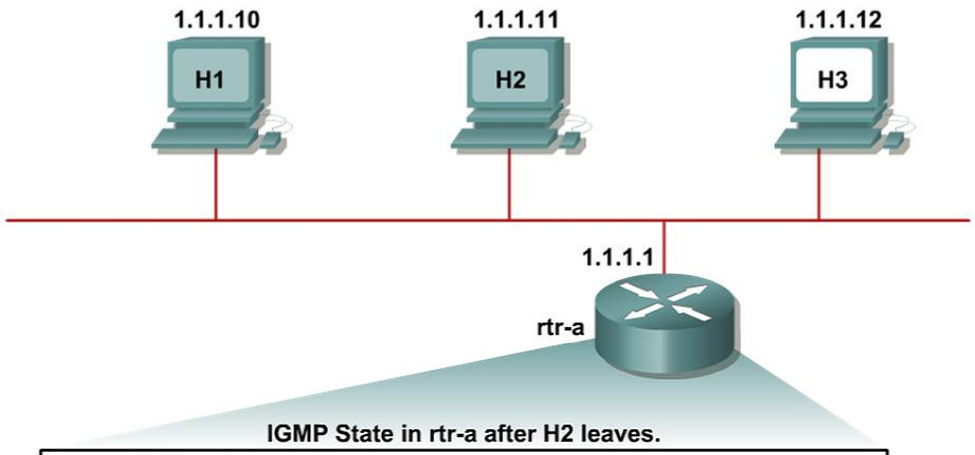
2. Router pošle group-specific query

IGMPv2: Opustenie skupiny



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

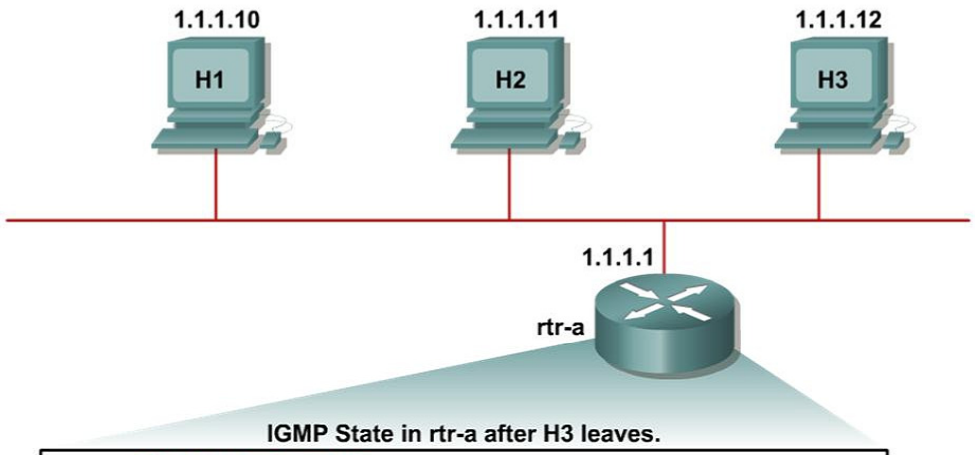
IGMPv2: Opustenie skupiny



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.

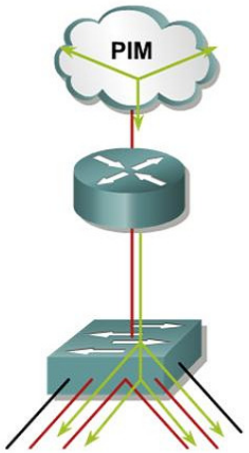
```
rtr-a>sh ip igmp group
IGMP Connected Group Membership
Group Address  Interface  Uptime  Expires   Last Reporter
```

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
- Bolo by vhodné, aby switch posielal multicasty len tým staniciam, ktoré sa do zvolenej skupiny zapísali

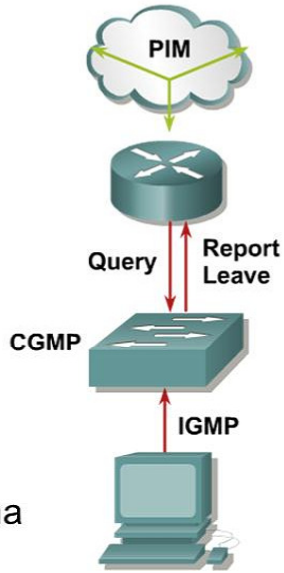


Efektívne doručovanie multicastov na L2

- 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

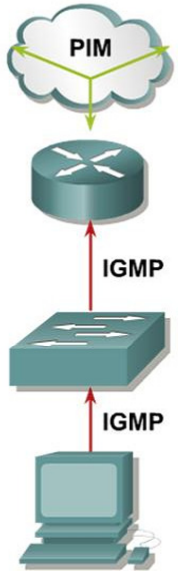
CGMP

- 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

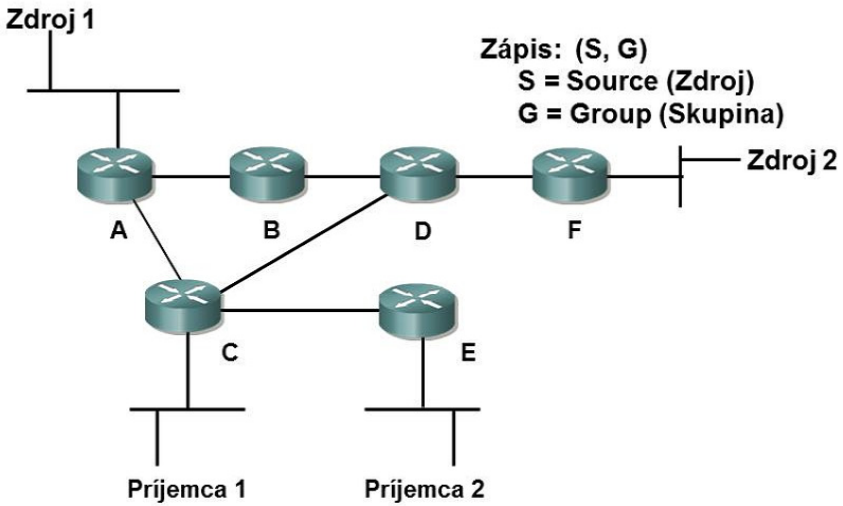
- Cesta, ktorou tečie multicastový tok dát od odosielateľa cez medziľahlé routery až po koncových príjemcov v jednej konkrétnej skupine, vytvára strom, ktorý sa nazýva multicastový distribučný strom
- Dva druhy stromov:
  - Zdrojové distribučné stromy čiže stromy najkratších vzdialeností (shortest path 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 najkratšie 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

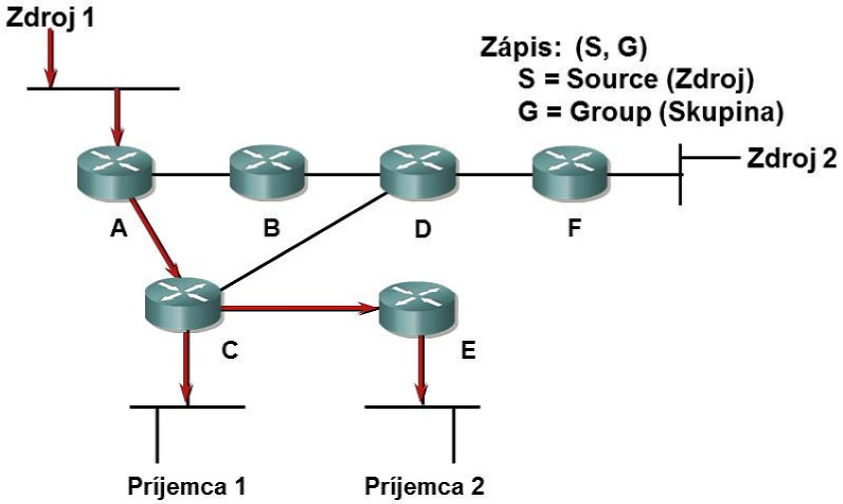
Multicastové distribučné stromy

Shortest Path Tree (Zdrojový strom)



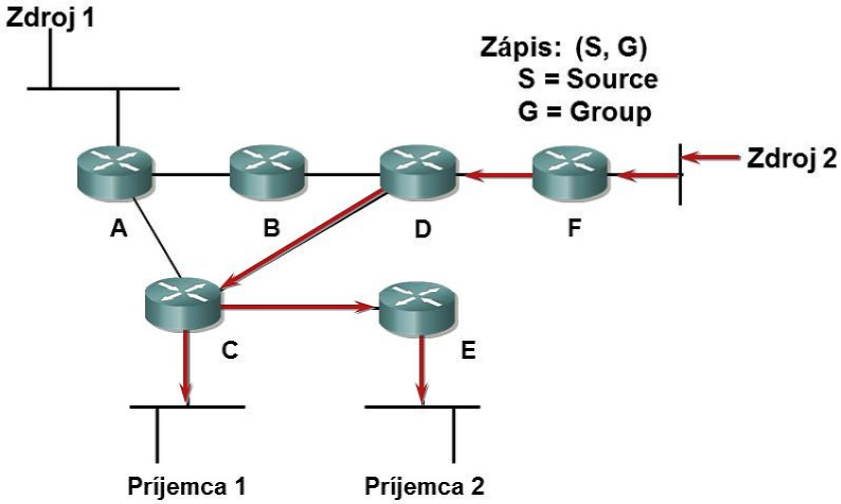
Multicastové distribučné stromy

Shortest Path Tree (Zdrojový strom)



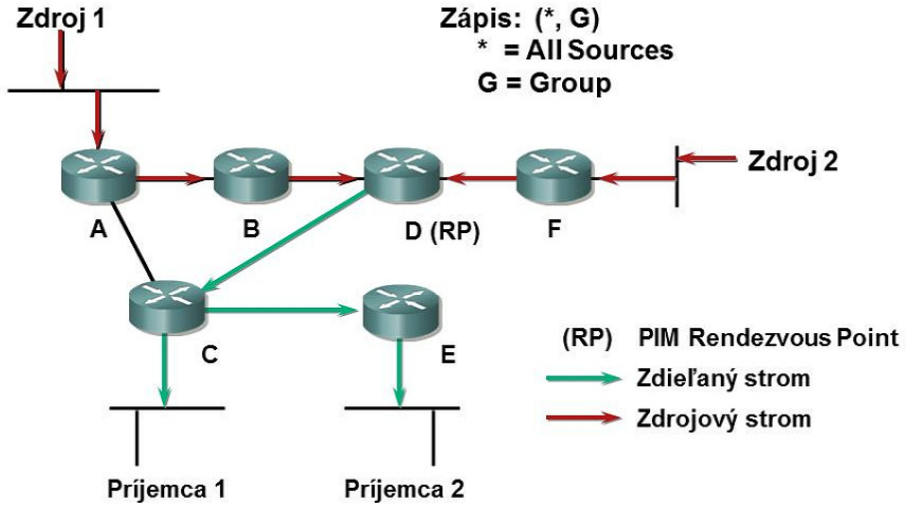
Multicastové distribučné stromy

Shortest Path Tree (Zdrojový strom)



Multicastové distribučné stromy

Shared Distribution Tree (Zdieľaný strom)



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

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
    - Spätná cesta k odosielateľovi alebo k RP slúži práve na vytvorenie distribučného stromu
- Multicastové smerovanie používa tzv. Reverse Path Forwarding (RPF) na elimináciu forwarding loops
  - Multicastový paket musí vojsť tým rozhraním, ktorým sa dá podľa unicastovej smerovacej tabuľky dostať po najkratšej ceste nazad **k odosielateľovi** multicastového paketu (pri SPT) **alebo k RP** (pri shared tree)

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 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 od príjemcov

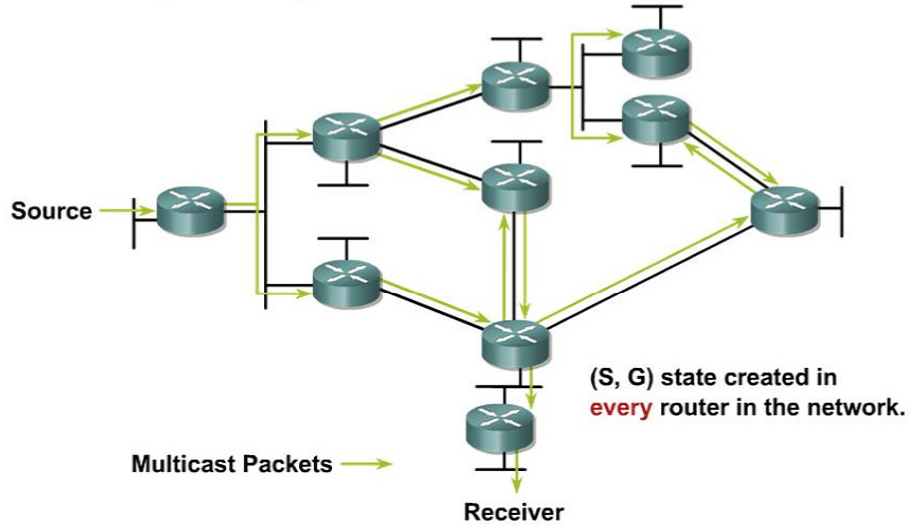
Vytvorenie multicastového distribučného stromu v PIM

- Ak má jeden segment siete viac smerovačov, len jeden z nich je zodpovedný za komunikáciu v PIM, tzv. DR
  - Vyššia priorita
  - Vyššia IP adresa na segmente
- 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)

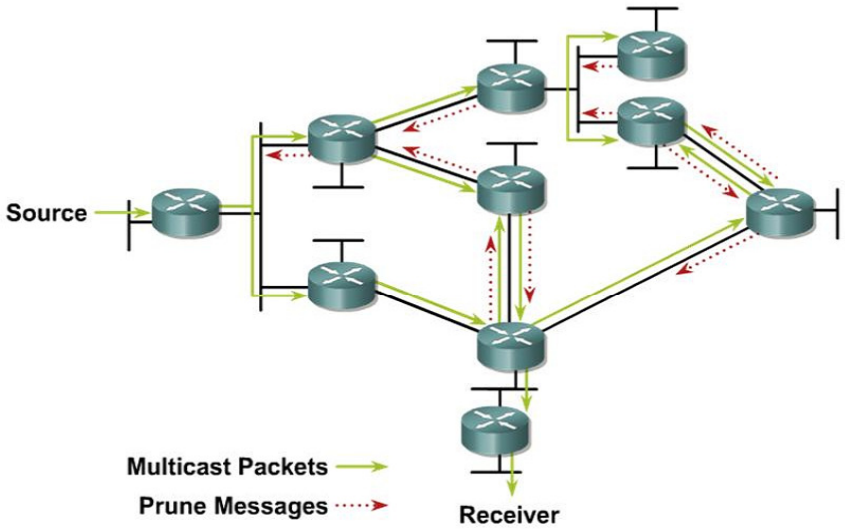
PIM Dense Mode

PIM-DM Flood and Prune

Počiatočný flooding

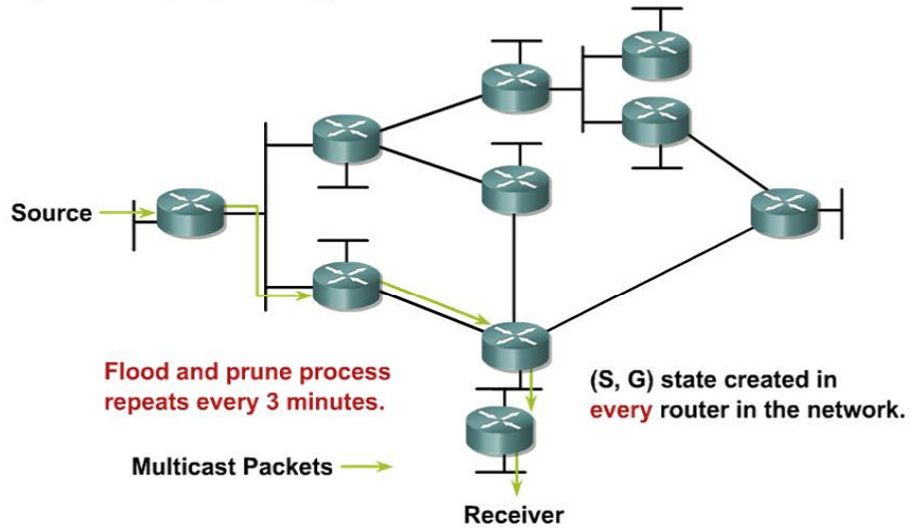


PIM-DM Flood and Prune



PIM-DM Flood and Prune

Výsledok po pruningu

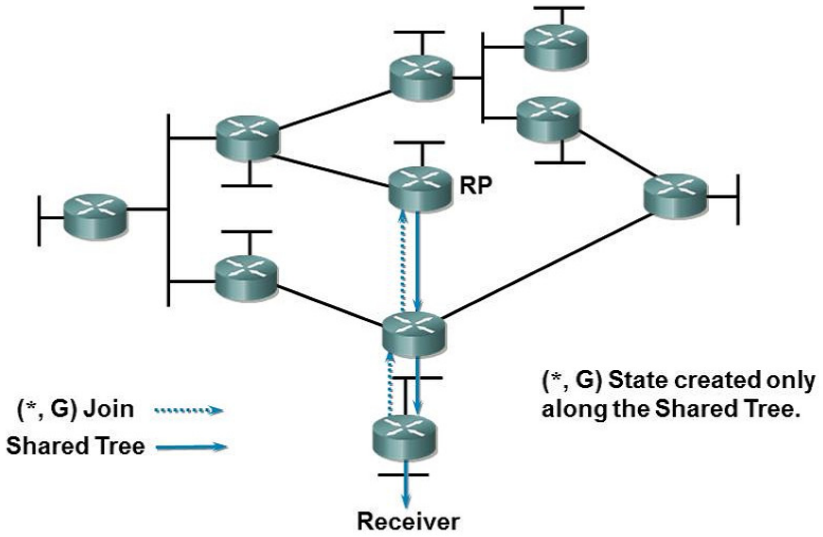


PIM Sparse Mode

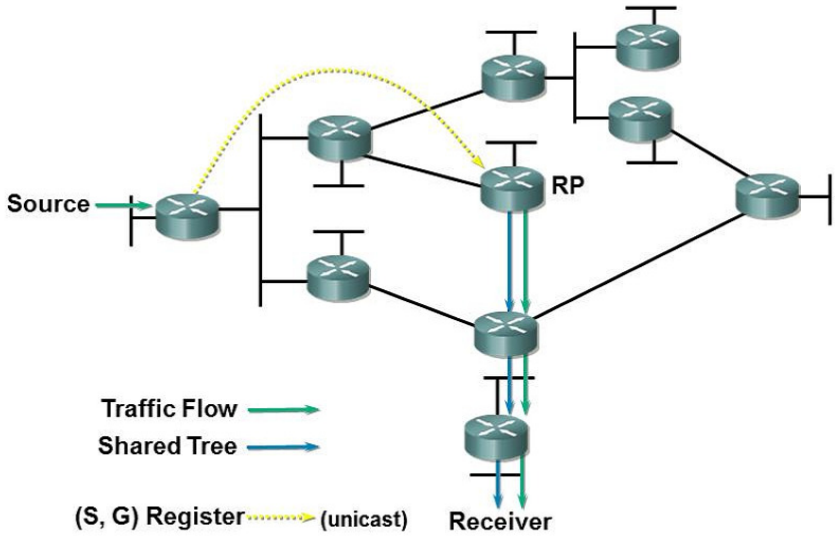
PIM Sparse Mode

- PIM-SM podporuje aj source, aj shared trees
  - PIM-DM principálne vytvára iba shortest path trees
- PIM-SM 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)

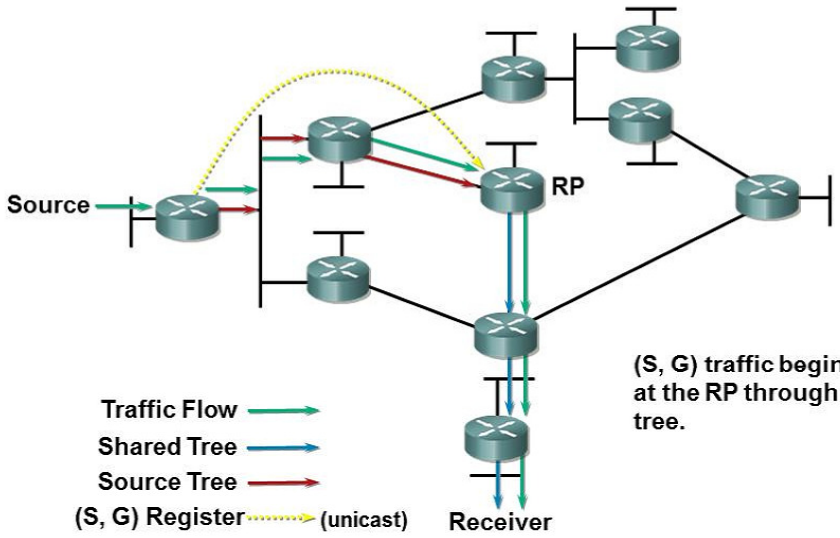
PIM-SM Shared Tree Join



PIM-SM Sender Registration

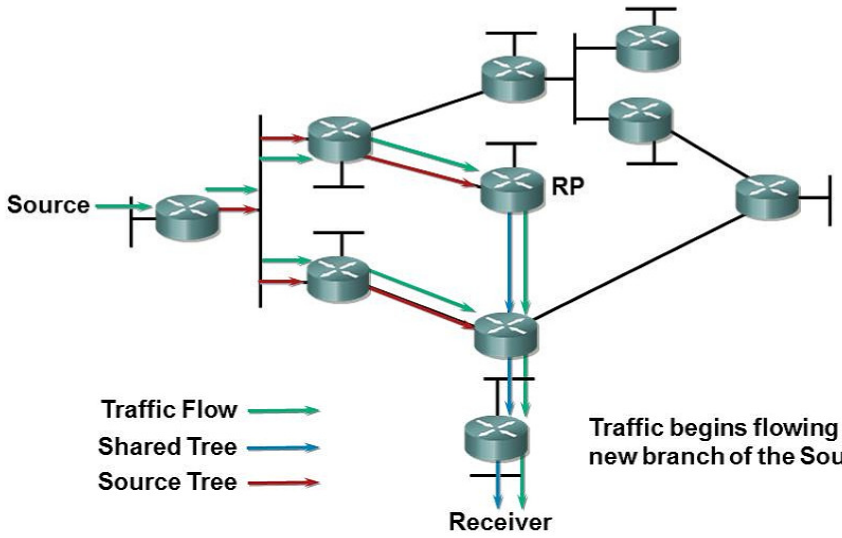


PIM-SM Sender Registration



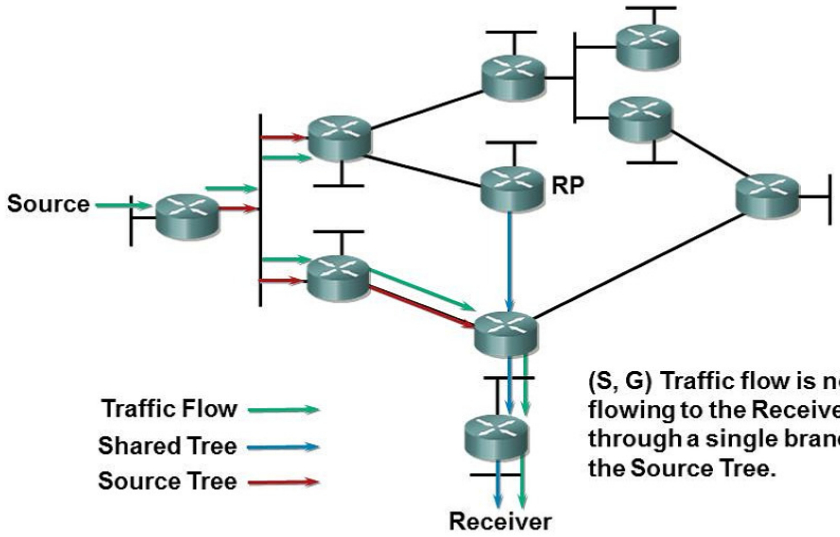
(S, G) traffic begins arriving at the RP through the Source tree.

PIM-SM SPT Switchover



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

PIM-SM SPT Switchover



(S, G) Traffic flow is now only flowing to the Receiver through a single branch of the Source Tree.

"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
  - Veľmi vhodné je používať adresu loopbacku
  - 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 neprílišškálovateľný spôsob konfigurácie

Auto-RP

- Cisco vytvorilo proprietárny spôsob automatického objavenia a voľby RP a nazýva ho Auto-RP
- Auto-RP má dva komponenty
  - Kandidáti na RP (RP Candidate)
    - Routery konfigurované príkazom **ip pim send-rp-announce**
    - Ohlasujú svoju ochotu byť RP pre zvolenú multicastovú skupinu
    - Kandidáti dávajú o sebe vedieť v skupine 224.0.1.39
  - Mapovací agenti (Mapping Agents)
    - Routery konfigurované príkazom **ip pim send-rp-discovery**
    - Ich úlohou je rozhodnúť, ktorí kandidáti sa stanú skutočnými RP
    - Rozhodnutie, kto bude RP pre zvolenú skupinu, rozposielajú na adresu 224.0.1.40
  - Na adrese 224.0.1.40 počúvajú všetky Auto-RP routery

Automatické ohlásenie RP a zoznamu obsluhovaných skupín

```
Router(config)#
ip pim send-rp-announce {interface} scope {ttl} [ group-list acl ]
```

- Nakonfiguruje router ako RP pre skupiny povolené uvedeným ACL
  - 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 Lo0 ako RP pre administratively scoped skupiny:

```
Router(config)#
ip pim send-rp-announce Loopback0 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 pre každú skupinu
  - Auto-RP discovery správy sa posielajú na IP 224.0.1.40 (CISCO-RP-DISCOVERY), na ktorej počúvajú všetky ostatné PIM routery

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

Porovnanie Auto-RP a BSR

Auto-RP (Cisco)

- Mapping agent:

```
ip pim send-rp-discovery
 lo0 scope 255
```

- RP kandidát:

```
ip pim send-rp-announce
 lo0 scope 255
```

BootStrap Router (RFC)

- Mapping agent:

```
ip pim bsr-candidate lo0
```

- RP kandidát:

```
ip pim rp-candidate lo0
```

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
```

- Zaradí rozhranie do outgoing interface zoznamu pre zvolenú skupinu

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
```