

**Sledování provozu protokolu
PIM
pro směrování multicastů**

Michal Sehnal
SEH016

Obsah

1	Úvod	2
2	Multicasting	2
2.1	Základní vlastnosti skupinového vysílání	2
2.2	Skupinové vysílání v lokální síti	3
2.3	Přenos skupinového vysílání mezi sítěmi	4
2.3.1	IGMP v.1	4
2.3.2	IGMP v.2	5
2.3.3	IGMP v.3	6
2.3.4	IGMP Snooping	6
2.4	Distribuční stromy	7
2.4.1	Shortest-Path Tree (SPT), Source Tree	7
2.4.2	Shared tree	8
2.5	Směrování skupinového vysílání	8
2.5.1	Hustý režim (Dense Mode)	9
2.5.2	Řídký mód (Sparse Mode)	9
2.6	Protocol Independent Multicast (PIM)	10
2.6.1	PIM Dense Mode	10
2.6.2	PIM Sparse Mode	10
3	Sledování provozu protokolu PIM	11
3.1	Nastavení PIM Dense Mode	11
3.2	Nastavení PIM Sparse Mode	16
3.3	Další výsledky	20

1 Úvod

Technologie skupinového vysílání (*multicast*) byla vyvinuta především pro podporu aplikací přirozeně obsahujících komunikaci jednoho zdroje s velkým počtem příjemců stejných dat. Velmi příhodné vlastnosti mají například multimediální aplikace, kdy jeden zdroj (vysílač) v reálném čase posílá řadě příjemců zvuková či obrazová data. Lze si ovšem představit i poměrně konvenční aplikace, které tomuto základnímu kritériu vyhovují, např. posílání oběžníku všem zaměstnancům organizace nebo oprava tisícídvoústedmapadesáté chyby v jednom velmi rozšířeném operačním systému. Jak z dalšího textu vyplyne, jsou multimediální aplikace, vzhledem k jisté tolerantnosti vůči nedokonalostem přenosu, zvláště výhodné a také byly jako první implementovány. Typické použití multicastů teda je v:

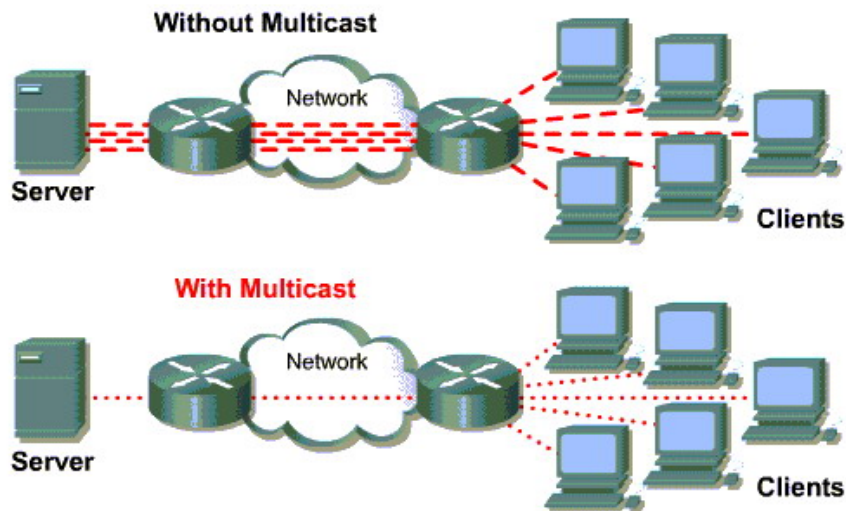
- distribuce vysílání videa, hlasu;
- videokonference;
- vyhledávání služeb;
- distribuované simulace (včetně her).

2 Multicasting

2.1 Základní vlastnosti skupinového vysílání

Klíčovým cílem této technologie je zásadní odlehčení zátěže vysílajícího uzlu a přenosové soustavy při přenosech typu jeden zdroj – mnoho příjemců (viz obr. 1). Zdroj tedy vysílá data, určená neznámému, potenciálně velmi velkému počtu příjemců (skupině), pouze jednou a veškerá režie spojená s distribucí příjemcům je ponechána na přenosové soustavě, v prostředí Internetu tedy (v ideálním stavu) na směrovačích (routerech). Na nich také je, aby zajistily efektivní přenos dat od zdroje k příjemcům, tedy aby vysílaná data poslaly po každém spoji nejvýše jedenkrát, a to pouze tehdy, je-li daným směrem skutečně nějaký příjemce. Na rozdíl od klasického přímého vysílání (*unicast*), kdy přenos paketu dat od zdroje k cíli je iniciován zdrojem, je tok paketů skupinového vysílání určován příjemci.

K identifikaci skupin příjemců se používá speciální třída adres IP (třída D), zahrnující adresy z množiny 224.0.0.0 až 239.255.255.255. Vysílající uzel odesílá pakety dat s cílovou adresou skupiny (a svou vlastní obyčejnou zdrojovou adresou). Další šíření přes směrovače by mělo (viz RFC 1112) probíhat



Obrázek 1: Rozdíl mezi unicastem a multicastem

stejnou metodou best effort (aneb dělám, co můžu) jako šíření běžných paketů přímého vysílání. V případě skupinového vysílání ovšem může směrovač provést replikaci paketu a jeho vysílání do více směrů.

2.2 Skupinové vysílání v lokální síti

Protokoly na 2. vrstvě síťové hierarchie (v našich podmínkách je z nich daleko nejrozšířenější ethernet) obsahují ve svých specifikacích podporu skupinového vysílání v podobě speciálních MAC adres. Běžné síťové karty pracovních stanic (včetně PC) pak mají schopnost podle svého okamžitého nastavení (na základě požadavků programu) filtrovat pakety skupinového vysílání a nejbližším vrstvám programového vybavení již předávat jen relevantní část paketů skupinového vysílání, které se v lokální síti pohybují, tedy pouze skupiny, jež jsou předmětem momentálního zájmu dané stanice. Nedochozí tedy k zatěžování stanic lokální sítě, jichž se dané skupinové vysílání netýká. Z výše řečeného vyplývá, že například k experimentu se skupinovým vysíláním v rámci lokální sítě může postačit běžné technické vybavení a příslušný aplikační program (a samozřejmě případné další technické prostředky, které jsou pro uvažovanou aplikaci potřebné, např. zvuková karta a reproduktory).

Link Local IP Address	Usage
224.0.0.1	All systems on this subnet
224.0.0.2	All routers on this subnet
224.0.0.5	OSPF routers
224.0.0.6	OSPF designated routers
224.0.0.9	RIP Version 2 routers
224.0.0.10	EIGRP routers
224.0.0.12	DHCP server/relay agent
224.0.0.13	All P1M routers
224.0.0.22	IGMP
224.0.0.25	Router-to-switch (such as RGMP)

Obrázek 2: Některé přednastavené IP adresy pro multicasty

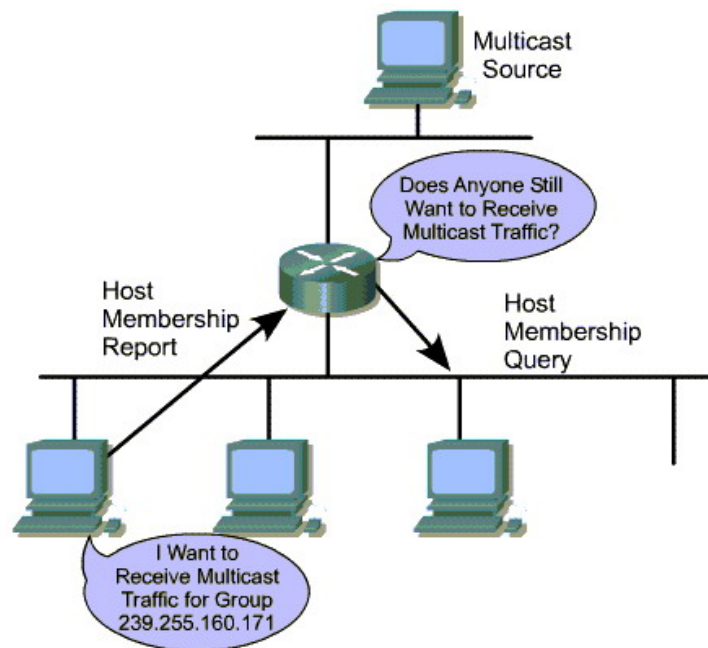
2.3 Přenos skupinového vysílání mezi sítěmi

Snadnost implementace skupinového vysílání v rámci lokální sítě se vytrácí, jakmile chceme dosáhnout přenosu v rámci propojených sítí. Do hry vstupují směrovače s jejich primárním úkolem získat informace o tom, které skupiny mají být vysílány do sítí, jež jsou ke směrovači bezprostředně připojeny. K tomuto účelu byl vyvinut speciální protokol **IGMP, Internet Group Management Protocol**. Jeho pomocí směrovač periodicky zjišťuje zájem stanic v připojených sítích o jednotlivé proudy skupinového vysílání. Směrovač vyšle do připojené sítě dotaz (paket se speciální skupinovou adresou 224.0.0.1) a jednotlivé stanice odpovídají (s náhodně zvoleným zpožděním, aby nedocházelo k zahlcení sítě při současné odpovědi všech najednou) informací o adresách skupinového vysílání, o něž mají zájem. Odpovědi jsou rovněž vysílány na adresu 224.0.0.1 a odposlouchávány ostatními stanicemi. Tím se zamezí duplicitnímu vysílání požadavků na stejnou skupinu. Programové vybavení koncové stanice tedy musí navíc podporovat protokol IGMP. Směrovače tak pomocí protokolu IGMP sledují zájem o příjem konkrétních skupin ve svém bezprostředním okolí. IGMP existuje ve třech verzích, a to:

2.3.1 IGMP v.1

Obsahuje pouze dvě zprávy:

- **MEMBERSHIP REPORT** – zasílá stanice při přihlášení do skupiny a jako pozitivní odpověď na dotaz směrovače, zda je na segmentu



Obrázek 3: Šíření multicastů v síti

zájemce o danou skupinu. Zasílá se na adresu požadované multicast skupiny.

- **MEMBERSHIP QUERY** – periodicky zasílá směrovač na každém rozhraní pro zjištění, zda je na segmentu nějaká stanice se zájmem o některou multicastovou skupinu¹.

Pokud stanice přestane mít zájem o multicast skupinu, přestane na dotaz směrovače odpovídat zprávou MEMBERSHIP REPORT.

2.3.2 IGMP v.2

Přináší novou zprávu **LEAVE GROUP**, kterou se stanice může explicitně odhlásit z multicastové skupiny. Výhodou je zkrácení latence odhlašování,

¹Na segmentu sítě s velkým množstvím příjemců multicastové skupiny by dotaz směrovače zprávou MEMBERSHIP QUERY vygeneroval smršť odpovědí MEMBERSHIP REPORT. Proto je do protokolu vnesena optimalizace: stanice neodpovídá na zprávu MEMBERSHIP QUERY ihned, ale jistou náhodnou dobu s odpovědí posečká. Pokud uslyší, že mezitím na dotaz odpověděla některá jiná stanice, zprávu u MEMBERSHIP REPORT sama generovat nebude.

tedy doby, po kterou je segment zbytečně zahlcován provozem multicastové skupiny, kterou již nikdo neposlouchá.

Dalším rozšířením je možnost specifického dotazu na zájemce o jednu konkrétní multicast skupinu ve zprávě MEMBERSHIP QUERY (nikoli jen na zájemce o jakoukoli skupinu, jako v IGMP v.1). To je užitečné zejména když router přijme zprávu LEAVE GROUP pro nějakou multicastovou skupinu a chce bezprostředně poté ověřit, zda má ještě stále smysl na segment provoz dané skupiny vysílat.

Poznámka:

- Kvůli možnosti havárie stanic bez odhlášení ze skupiny a také kvůli optimalizaci ve vysílání odpovědí na MEMBERSHIP QUERY pouze jedinou stanicí není možné, aby směrovač počítal počet příjemců na segmentu pouze na základě zvyšování, resp. snižování čítače při příchodu zpráv MEMBERSHIP REPORT a LEAVE GROUP pro danou skupinu. Proto je nezbytné, aby nepřítomnost příjemců pro danou skupinu zjišťoval dotazem pomocí zprávy MEMBERSHIP QUERY.

2.3.3 IGMP v.3

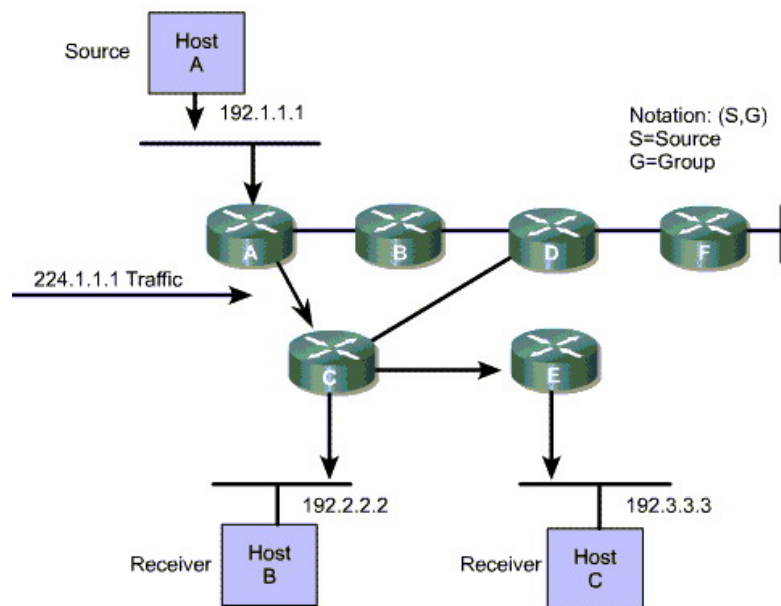
Obohacuje protokol o možnost filtrování požadovaného provozu na základě zdrojových adres. Tím se je možné bránit před nekorektně se chovajícími stanicemi, které multicastovou skupinu nežádoucím způsobem zahlcují. Při žádosti o provoz multicastové skupiny je potom možné explicitně zadat buďto zadat seznam zdrojů, ze kterých jediné mají být zprávy přebírány nebo naopak seznam zdrojů, od nichž mají být zprávy zaslané do multicastové skupiny filtrovány.

2.3.4 IGMP Snooping

IGMP Snooping spočívá v tom, že přepínač nahlíží do dat 3. vrstvy v přenášených rámcích a pokud je v ní obsažená zpráva IGMP (MEMBERSHIP REPORT, LEAVE GROUP), získá z ní potřebnou informaci o příslušnosti MAC adres stanic do jednotlivých multicastových skupin. Tato metoda samozřejmě přepínač zatěžuje a zpravidla má smysl jen v případě, že je realizována hardwarově.

Poznámka:

- Zprávy MEMBERSHIP REPORT a LEAVE GROUP se podle protokolu IGMP zasílají na adresu příslušné IP multicastové skupiny a tedy



Obrázek 4: Příklad stromu SPT $\langle 192.2.2.2, 224.1.1.1 \rangle$

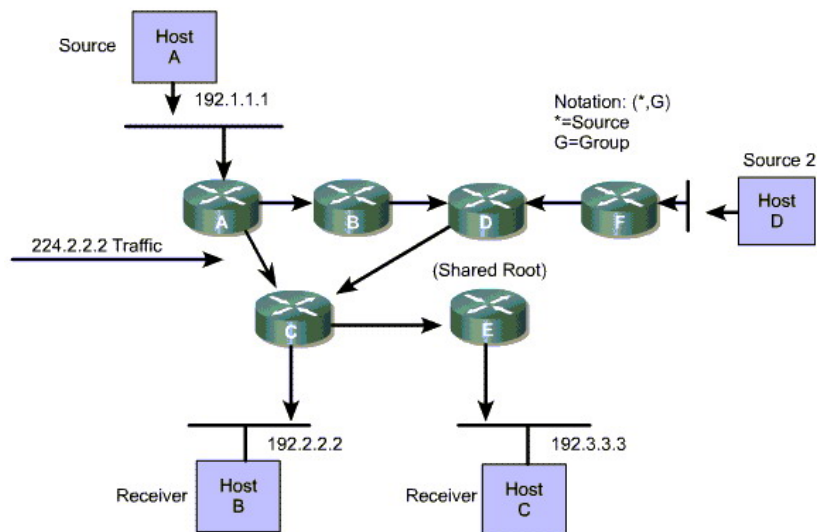
na 2. vrstvě na multicastovou MAC adresu, na kterou se daná IP multicastová adresa mapuje. Postačí tedy, aby přepínač zkoumal 3. vrstvu jen u rámců zasílaných na multicastové MAC adresy.

2.4 Distribuční stromy

Distribuční strom tvoří acyklický podgraf grafu topologie sítě a spojuje všechny sítě, na nichž jsou příjemce dané multicastové skupiny. Jak se do skupiny přihlašují nové příjemce a odhlašují existující, musí se do stromu připojovat nové větve a odstraňovat („prořezávat“, angl. „prune“) staré.

2.4.1 Shortest-Path Tree (SPT), Source Tree

Strom nejkratších cest ze zdroje ke všem sítím s příjemci. Značí se: $\langle S, G \rangle$, kde S je zdrojová adresa, G je adresa multicastové skupiny. Existuje samostatný strom pro každý zdroj vysílání do každé multicastové skupiny \Rightarrow optimální, ale málo škálovatelné řešení.



Obrázek 5: Příklad sdíleného stromu $\langle *, 224.2.2.2 \rangle$

2.4.2 Shared tree

Sdílený strom společný pro všechny zdroje ve skupině. Kořenem je vhodně zvolený směrovač (Rendezvous Point – RP). Zdroj musí zasílat každý paket na kořen. Značení $\langle *, G \rangle$, kde * označuje všechny zdrojové adresy vysílající do skupiny G \Rightarrow poněkud delší cesta paketů (navíc cesta ke kořeni), ale jen jediný strom pro skupinu.

2.5 Směrování skupinového vysílání

Směrovače musejí – kromě trvalého mapování svého bezprostředního okolí – zajistit tok paketů skupinového vysílání i do vzdálených oblastí sítě, a to pokud možno optimálním způsobem. K tomu slouží tzv. *směrovací protokoly*. Jejich pomocí směrovače hledají minimální strom spojů pokrývající cestu od zdroje skupinového vysílání k momentálním zájemcům o příjem. Je zřejmé, že na rozdíl od klasického směrování přímého vysílání půjde o proces velmi dynamický. Cesta od daného zdroje k danému cíli je totiž stálá, pokud nedojde k nějaké vnější události měnící topologii sítě, např. poruše linky. Naproti tomu zájemci o příjem daného skupinového vysílání mohou vznikat a zanikat trvale a tento proces průběžných změn musejí směrovací protokoly vhodně reflektovat. Směrovací protokoly skupinového vysílání jsou dosud předmětem intenzivního výzkumu a vývoje. V současné době se nejvíce používají

protokoly *DVMRP* (*Distance Vector Multicast Routing Protocol*) a dvě varianty protokolu *PIM* (*Protocol Independent Multicast*). Směrovací protokoly dělíme podle jejich funkce do dvou skupin, a to:

2.5.1 Hustý režim (Dense Mode)

V hustém režimu se předpokládá, že zájemci o multicastovou skupinu jsou skoro na všech segmentech sítě. Proto je provoz implicitně směrován do všech segmentů. Pokud směrovač časem (na základě protokolu IGMP) zjistí, že na žádném svém rozhraní nemá zájemce o multicastovou skupinu, pošle směrovači ve vyšší úrovni distribučního stromu žádost o „prořezání“ (prune). Směrovač ve vyšší úrovni stromu na jejím základě přestane do větve multicastový provoz dané skupiny vysílat. Pokud se ve větvi časem objeví zájemce o multicastovou skupinu, může lokální směrovač segmentu větev do distribučního stromu opětovně přihlásit.

Používané protokoly:

- DVMRP
- PIM-DM
- MOSPF

2.5.2 Řídký mód (Sparse Mode)

Na rozdíl od hustého režimu nejsou v řídkém režimu implicitně multicast pakety zasílány nikam. Většina větví by totiž z důvodu řídkého výskytu příjemců byla multicasty zaplavována zbytečně. Až když se na segmentu objeví zájemce o danou skupinu, pošle se směrem ke kořeni žádost o připojení nové větve distribučního stromu. Po této větvi pak k novému zájemci poteče provoz požadované multicastové skupiny.

Připojení větve do distribučního stromu v řídkém režimu nebo její odpojení v režimu hustém není trvalé. Každý směrovač distribučního stromu si totiž žádost o připojení, resp. odpojení pamatuje pouze po jistou omezenou dobu a po jejím vypršení přejde k původnímu chování. Proto se musí žádost o připojení a odpojení větve distribučního stromu periodicky opakovat.

Žádosti o připojení a odpojení větve stromu se mezi směrovači zpravidla zasílají prostřednictvím zpráv protokolu IGMP. Z hlediska směrovače tak není rozdílu, jestli multicastový provoz na rozhraní vyžaduje na segmentu připojená stanice nebo jiný směrovač, který multicastový provoz požaduje pro segmenty na jeho rozhraní připojené větve distribučního stromu.

V řídkém režimu se na řízení směrování účastní méně směrovačů. Pouze ty, které vytvářejí ne příliš rozvětvený distribuční strom. Proto jsou protokoly pracující v řídkém režimu vhodnější pro rozlehlé WAN sítě.

Používané protokoly:

- PIM-SM
- CBT

2.6 Protocol Independent Multicast (PIM)

V dnešní době se nejvíce používá pro směrování multicastů. Je nezávislý na specifickém unicastovém směrovacím protokolu použitým v síti². Multicasty směruje na základě RPF check. Ve skutečnosti není PIM směrovacím protokolem (neposílá a nepřijímá aktualizace o směrování – routing updates). Pro některé skupiny může pracovat v dense módu a pro některé ve sparse módu.

2.6.1 PIM Dense Mode

Flooduje provoz do všech větví; větev může požádat o prořezání, pokud neobsahuje příjemce multicast skupiny (refresh každé 3 minuty).

Podmínky pro efektivní funkci:

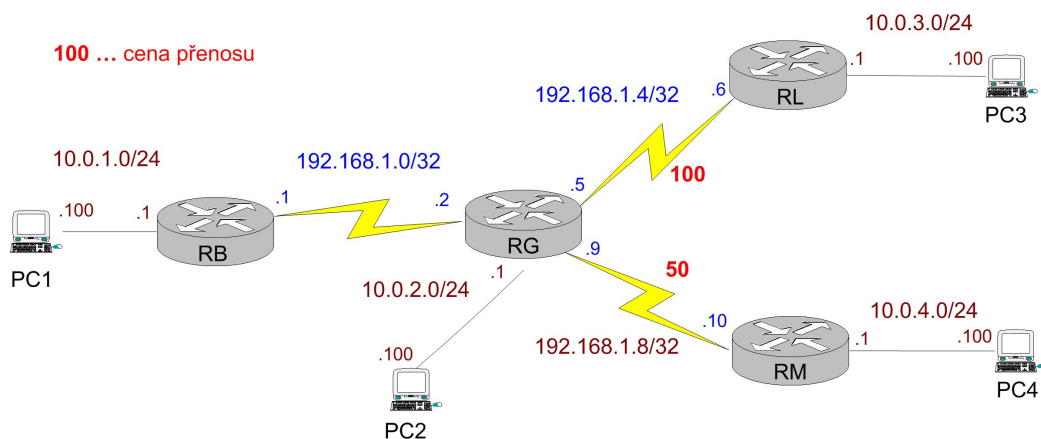
- příjemče a vysílače blízko;
- málo vysílačů a mnoho příjemců;
- intenzivní multicastový tok;
- konstantní proud multicast dat;

2.6.2 PIM Sparse Mode

Vhodný pro malý počet příjemců ve skupině a pro nepravidelné datové toky. Odesílatelé zasílají multicast pakety na RP. Příjemci se registrují u RP. Směrovače na cestě mohou optimalizovat trasu datového toku od zdroje k příjemci.

Rendezvous point (RP) pro jednotlivé multicast skupiny musí být nakonfigurován ve všech směrovačích. Existují také (zatím nestandardizované) protokoly, které šíří informaci o aktivních RP pomocí multicastingu.

²Ale používá jeho (unicastovou) směrovací tabulku.



Obrázek 6: Plán sítě

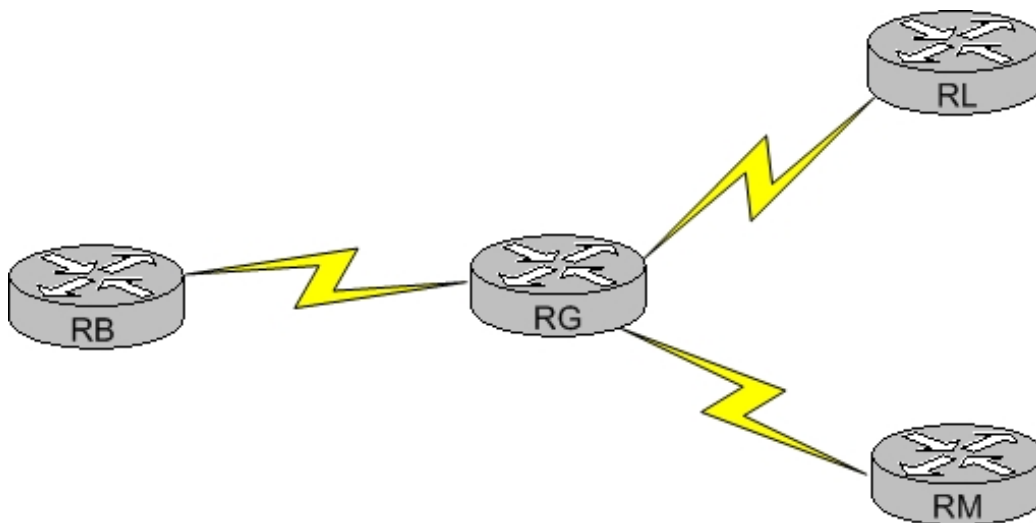
3 Sledování provozu protokolu PIM

Zapojovali jsme síť podle obrázku 6. K tomu jsme použili čtyři vhodné routery s patřičným počtem seriových linek a čtyři počítače. O komunikaci mezi routery se stará protokol OSPF. Dále jsme nastavili ceny spojení mezi RG a RM na 50 a mezi RG a RL na 100. Po zapojení a nastavení jsme pro jistotu vyzkoušeli spojení mezi pracovními stanicemi a směrovači pomocí příkazu *ping*.

3.1 Nastavení PIM Dense Mode

Na všech routerech jsme nastavili tento protokol na všech seriových rozhraních. Pomocí příkazu *ip pim dense-mode*. Protokol se bude šířit podle stromu na obrázku 7. Na počítači PC3 jsme spustili program *MListener* s parametrem IP adresy 226.1.1.1. Před spuštěním jsme nastavili na směrovači RL debug režim pro zachytávání paketů protokolů IGMP. Zjistili jsme následující údaje:

1. Přijat IGMP Report v2 z rozhraní FastEthernet 0/0 10.0.3.100 (PC3) na multicast 226.1.1.1.
2. Přijat Group record (mód 2) na skupinu 226.1.1.1 z 10.0.3.100 pro 0 zdrojů.
3. Přepnutí do EXCLUDE módu na FastEthernet 0/0 pro 226.1.1.1.
4. Přidání nebo aktualizace MRT FastEthernet 0/0 pro (*, 226.1.1.1)



Obrázek 7: Strom pro PIM-Dense Mode

5. Aktualizace EXCLUDE skupinového časovače pro 226.1.1.1.

IGMP pracuje ve dvou módech, a to INCLUDE a EXCLUDE. V prvním přijímač oznamuje členství hostitelské skupině a poskytuje seznam IP adres (INCLUDE list), ze kterého chce přijímat zprávy. Ve druhém módu přijímač oznamuje členství hostitelské skupině a poskytuje seznam IP adres (EXCLUDE list), ze kterého nechce přijímat zprávy. Indikuje, že host chce přijímat zprávy pouze ze zdrojů, jenž nejsou na seznamu EXCLUDE listu. Aby se mohlo přijímat zprávy ze všech zdrojů, jako například Internet Standard Multicast (ISM) servisní model, host vyjadřuje členství v EXCLUDE módu prázdným seznamem EXCLUDE.

Při zadání příkazu na směrovači RL *show ip igmp group* se zobrazilo:

```

IGMP Connected Group Membership
Group Address  Interface      Uptime    Expires    Last Reporter
224.0.1.40     Serial0/0      01:03:29 stopped    0.0.0.0
226.1.1.1      FastEthernet0/0 00:00:12 00:02:47 10.0.3.100
  
```

Po zadání příkazu *show ip pim* na RL neighbor se zobrazí:

```

PIM Neighbor Table
Neighbor      Interface      Uptime/Expires    Ver    DR
Address
192.168.1.5   Serial0/0      01:03:55/00:01:20 v2     None
  
```

U RG stejný příkaz vypadá následovně:

PIM Neighbor Table

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority
192.168.1.1	Serial1/0	01:03:55/00:01:20	v2	None
192.168.1.6	Serial1/1	01:03:55/00:01:20	v2	None
192.168.1.10	Serial1/2	01:03:55/00:01:20	v2	None

A po zadání *show 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 - Candidate for MSDP Advertisement, 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

```
(*, 226.1.1.1), 00:01:12/00:02:40, RP 0.0.0.0, flags: DC
Incoming interface: Null, RPF nbr 0.0.0.0
Outgoing interface list:
  Serial0/0, Forward/Dense, 00:01:12/00:00:00
  FastEthernet0/0, Forward/Dense, 00:01:12/00:00:00
```

Při ukončení programu *MListener* se na směrovači RL zobrazí:

1. Přijat IGMP Leave z 10.0.3.100 (FastEthernet 0/0) na 226.1.1.1.
2. Přijat Group record (mód 3) na skupinu 226.1.1.1 z 10.0.3.100 pro 0 zdrojů.
3. Nižší časovač vypršení na 1 sekundu pro 226.1.1.1 na FastEthernetu 0/0.
4. Poslán 2x IGMP Query v2 na FastEthernet 0/0 pro skupinu 226.1.1.1.
5. Přepnutí do INCLUDE módu pro 226.1.1.1 na FastEthernetu 0/0.
6. Smazání MRT FastEthernet 0/0 pro (*, 226.1.1.1).

Z programu *Ethereal* jsme našli zdrojové a cílové IP adresy pro zprávy IGMP. Údaje jsou zobrazeny v tabulce 1.

Při nastavení debug režimu pro protokol PIM jsme dostali následující údaje:

Název zprávy	Zdrojová IP	Cílová IP
Leave	10.0.3.100	224.0.0.2
Query	10.0.3.1	226.1.1.1
Report	10.0.3.100	226.1.1.1

Tabulka 1: Zprávy IGMP

```

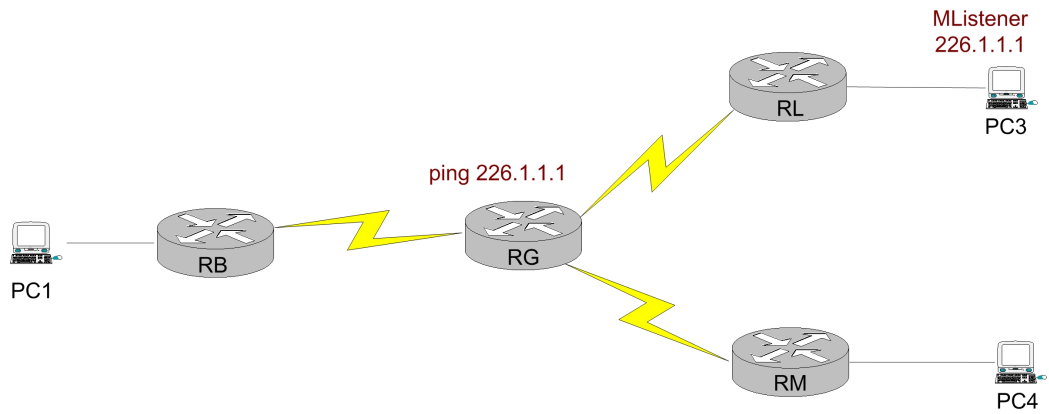
PIM: Building Graft message for 226.1.1.1, FastEthernet0/0:
no entries
PIM: Building Graft message for 226.1.1.1, Serial0/0:
no entries
PIM: Received v2 Hello on Serial0/0 from 192.168.1.5
PIM: Received deprecated PIM Bidir TLV 19 from 192.168.1.5
(Serial0/0)
PIM: Received deprecated PIM DR Priority TLV 18 from
192.168.1.5 (Serial 0/0)
PIM: Send v2 Hello on Serial0/0
PIM: Send v2 Hello on FastEthernet0/0
%PIM-4-DEPRECATED_HELLO_TLV: Deprecated PIM Hello Option
TLV 19 (Bidir TLV) from 192.168.1.5 (Serial0/0)
PIM: Received deprecated PIM Bidir TLV 19 from 192.168.1.5
(Serial0/0)
PIM: Received deprecated PIM DR Priority TLV 18 from
192.168.1.5 (Serial0/0)

```

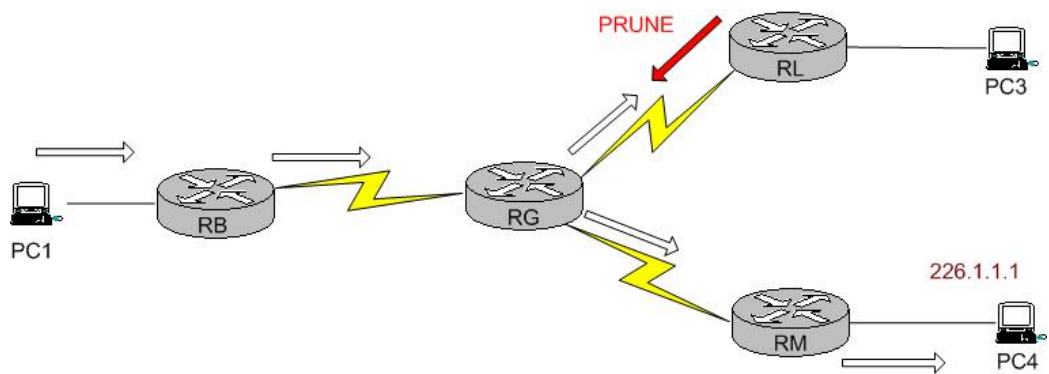
Zjistili jsme, že Hello zprávy se šíří sítí co půl minuty. Dále ze záznamů z programu *Ethereal* našli zdrojovou IP Hello zprávy (10.0.3.1) a cílovou IP (224.0.0.13 – všechny PIM směrovače). Dále zpráva PIM Graft se šířila když se *MListener* spustil.

Zkoušeli jsme poslat *ping* na 226.1.1.1 ze směrovače RG, když jsme měli spuštěný *MListener* na PC3 (obr. č. 8. Na PC2 a PC3 jsme měli aktivovaný program *Ethereal* pro zachytávání paketů. Ve výpisech na PC2 jsme našli ICMP protokol (dotaz ping) z 10.0.2.1 na 226.1.1.1. U PC3 jsme našli taky ICMP protokol (dotaz ping) z 192.168.1.5 na 226.1.1.1.

Typicky modelový příklad by vypadal podle obrázku č. 9. Z PC1 bychom poslali multicast pro skupinu 226.1.1.1 přes naši síť a na PC4. Paket by se postupně šířil přes směrovače RB, RG na RL a RM. RL zjistí, že nemá za sebou žádné příjemce skupiny, tak pošle zprávu RG Prune, aby neposílal tyto pakety. Ten bude zprávy šířit pouze na RM a ten následně na PC4.



Obrázek 8: Ping z RG na 226.1.1.1



Obrázek 9: Správné šíření multicastových zpráv

3.2 Nastavení PIM Sparse Mode

Opět vycházíme ze zapojení na obrázku 6. Ze všech směrovačů jsme zrušili protokol PIM-DM a nastavíme PIM-SM. Nejprve si zvolíme Rendezvous Point (RP). Z naší topologie sítě se nejlépe hodí RG. Na ostatních směrovačích nastavíme příkazem `ip pim rp-address 192.168.1.5`.

Nejprve jsme na PC3 spustili MListener s adresou 226.1.1.1 a na RL debug režim pro protokol IGMP. Zobrazily se následující zprávy:

```
IGMP: Received Group record for group 226.1.1.1, mode 2 from
10.0.3.100 for 0 sources
IGMP: Switching to EXCLUDE mode for 226.1.1.1
      on FastEthernet0/0
IGMP: MRT Add/Update FastEthernet0/0 for (*,226.1.1.1) by 0
IGMP: Updating EXCLUDE group timer for 226.1.1.1
```

Po ukončení MListeneru se na směrovači RL zobrazilo:

```
IGMP: Received Leave from 10.0.3.100 (FastEthernet0/0) for
226.1.1.1
IGMP: Received Group record for group 226.1.1.1, mode 3 from
10.0.3.100 for 0 sources
IGMP: Lower expiration timer to 1 seconds for 226.1.1.1 on
FastEthernet0/0
IGMP: Send v2 Query on FastEthernet0/0 for group 226.1.1.1
IGMP: Send v2 Query on FastEthernet0/0 for group 226.1.1.1
IGMP: Switching to INCLUDE mode for 226.1.1.1
      on FastEthernet0/0
IGMP: MRT delete FastEthernet0/0 for (*,226.1.1.1) by 0
```

Když porovnáme IGMP zprávy u protokolů PIM-Dense Mode a Sparse mode zjistíme, že jsou stejné. Při spuštění MListeneru jsme pak zadávali příkazy a nechali si zobrazit následující údaje. Nejprve jsme zadali `show igmp groups`:

```
IGMP Connected Group Membership
Group Address Interface      Uptime   Expires  Last Reporter
224.0.1.40   FastEthernet0/0  00:08:10 00:02:42 10.0.3.1
226.1.1.1    FastEthernet0/0  00:00:16 00:02:43 10.0.3.100
```

a pak příkaz `show 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 - Candidate for MSDP Advertisement, 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

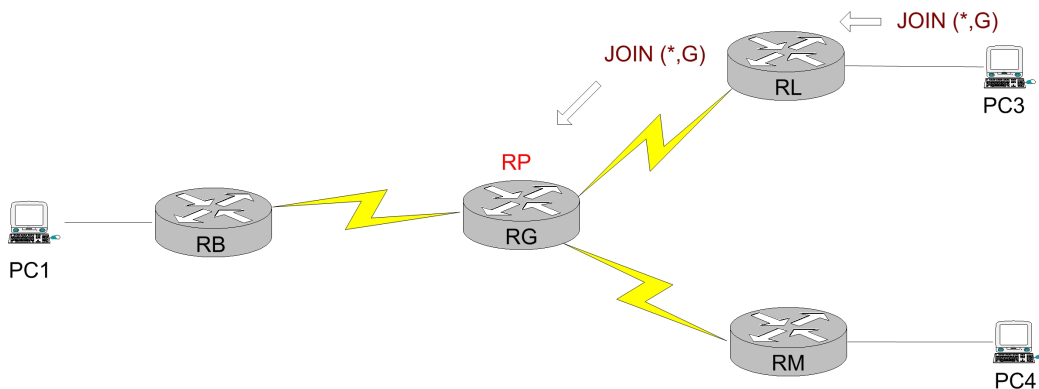
(*, 224.0.1.40), 00:07:25/00:00:00, RP 192.168.1.5, flags: SJCL
  Incoming interface: Serial0/0, RPF nbr 192.168.1.5
  Outgoing interface list:
    FastEthernet0/0, Forward/Sparse, 00:07:25/00:02:18

(*, 226.1.1.1), 00:06:40/00:02:18, RP 192.168.1.5, flags: SJC
  Incoming interface: Serial0/0, RPF nbr 192.168.1.5
  Outgoing interface list:
    FastEthernet0/0, Forward/Sparse, 00:00:41/00:02:18

Následně jsme se snažili zachytit PIM zprávy. Následující výpis ukazuje, jaké
typy se nám podařilo zjistit.

PIM: Building Join/Prune message for 224.0.1.40
PIM: v2, for RP, Join-list: 192.168.1.5/32, RP-bit, WC-bit,
      S-bit
PIM: Send v2 periodic Join/Prune to RP via 192.168.1.5
      (Serial0/0)
PIM: Received v2 Hello on Serial0/0 from 192.168.1.5
PIM: Received deprecated PIM Bidir TLV 19 from 192.168.1.5
      (Serial0/0)
PIM: Received deprecated PIM DR Priority TLV 18 from
      192.168.1.5 (Serial0/0)
PIM: Send v2 Hello on Serial0/0
PIM: Building Join/Prune message for 226.1.1.1
PIM: Received v2 Join/Prune on Serial0/0 from 192.168.1.5,
      to us
PIM: Join-list: (192.168.1.5/32, 226.1.1.1), S-bit set
PIM: Join received on RPF interface, do RPF check for
      (192.168.1.5, 226.1.1.1)
PIM: Received RP-Reachable on Serial0/0 from 192.168.1.5
      for group 224.0.1.40
PIM: Update RP expiration timer (270 sec) for 224.0.1.40
PIM: Send v2 Hello on FastEthernet0/0

```



Obrázek 10: Šíření Join zprávy k Rendezvous Pointu

```

PIM: Received RP-Reachable on Serial0/0 from 192.168.1.5
      for group 226.1.1.1
PIM: Update RP expiration timer (270 sec) for 226.1.1.1
%PIM-4-DEPRECATED_HELLO_TLV: Deprecated PIM Hello Option
      TLV 19 Bidir TLV) from 192.168.1.5 (Serial0/0)
PIM: Send v2 Hello on Serial0/0
PIM: Send v2 Null Register to 192.168.1.5
PIM: Received v2 Register-Stop on Serial0/0 from 192.168.1.5
      for source 0.0.0.0, group 0.0.0.0
PIM: Send v2 Hello on FastEthernet0/0
PIM: Send v2 Data-header Register to 192.168.1.5 for
      192.168.1.5, group 226.1.1.1
PIM: Received v2 Register-Stop on Serial0/0 from 192.168.1.5
      for source 192.168.1.5, group 226.1.1.1
PIM: Clear register flag to 192.168.1.5 for
      (192.168.1.5/32, 226.1.1.1)
PIM: Send v2 Prune on Serial0/0 to 192.168.1.5 for
      (192.168.1.5/32, 226.1.1.1), WC-bit, RPT-bit, S-bit
  
```

Z výpisu jsou asi nejdůležitější zprávy Join a Prune. Join se používá pro přihlášení dané skupiny k Rendezvous Pointu (RP). Obrázek č. 10 ukazuje tuto situaci. Prune zase naopak pro odhlášení. Další zprávy jsou Hello, které pravidelně (co 30 sekund) informují okolní směrovače zda jsou v dosahu, periodické zasílání a přijímání Join/Prune zpráv s RP, apod.

Na směrovači RG jsme zjistili tyto zprávy:

```

PIM: Building Join/Prune message for 224.0.1.40
  
```

PIM: Received v2 Hello on Serial1/1 from 192.168.1.6
PIM: Hello packet has unknown options, ignored
PIM: Send v2 Hello on Serial1/1
PIM: Send v2 Hello on Serial1/2
PIM: Received v2 Join/Prune on Serial1/1 from 192.168.1.6,
to us
PIM: Join-list: (*, 226.1.1.1) RP 192.168.1.5
PIM: Check RP 192.168.1.5 into the (*, 226.1.1.1) entry,
RPT-bit set, WC-bit set, S-bit set
PIM: Add Serial1/1/192.168.1.6 to (*, 226.1.1.1),
Forward state
PIM: Building Join/Prune message for 226.1.1.1
PIM: Received v2 Join/Prune on Serial1/1 from 192.168.1.6,
to us
PIM: Join-list: (*, 224.0.1.40) RP 192.168.1.5, RPT-bit set,
WC-bit set, S-bit set
PIM: Add Serial1/1/192.168.1.6 to (*, 224.0.1.40),
Forward state
PIM: Received v2 Register on Serial1/1 from 192.168.1.6
for 192.168.1.5, group 226.1.1.1.
PIM: Send RP-reachability for 224.0.1.40 on Serial1/1
PIM: Received v2 Hello on Serial1/1 from 192.168.1.6
PIM: Received v2 Register on Serial1/1 from 192.168.1.6
PIM: Received v2 Register on Serial1/2 from 192.168.1.10
for 192.168.1.5, group 226.1.1.1
PIM: Send v2 Register-Stop to 192.168.1.6 for 192.168.1.5,
group 226.1.1.1.
PIM: Building Join/Prune message for 224.0.1.40
PIM: Join-list: (*, 226.1.1.1) RP 192.168.1.5, RPT-bit set,
WC-bit set, S-bit set
PIM: Add Serial1/1/192.168.1.6 to (*, 226.1.1.1), Forward state
PIM: Add Serial1/1/192.168.1.6 to (192.168.1.5/32, 226.1.1.1)
PIM: Join-list: (192.168.1.5/32, 226.1.1.1), S-bit set
PIM: Building Join/Prune message for 226.1.1.1
PIM: For 192.168.1.6, Join-list: 192.168.1.5/32
PIM: Send v2 periodic Join/Prune to 192.168.1.6 (Serial1/1)
PIM: Add Serial1/1/192.168.1.6 to (*, 224.0.1.40), Forward state
PIM: Send RP-reachability for 226.1.1.1 on Serial1/1
PIM: Received v2 Register on Serial1/1 from 192.168.1.6
PIM: Send v2 Register-Stop to 192.168.1.6 for 0.0.0.0, group
0.0.0.0

Kromě zpráv popsaných výše, se zde objevily zprávy Add-Serial (přidání rozhraní do seznamu), Send Register-Stop (ukončení vysílání pro skupinu). Na směrovači RM a RB jsme pak zaznamenali jeden typ zprávy, a to:

```
PIM: No sources in join or prune list
```

Znamená, že tento směrovač nemá za sebou žádné příjemce multicastových zpráv.

3.3 Další výsledky

Bohužel přesnějšího měření se nám nepodařilo dosáhnout. Neměli jsme k dispozici program, který by šířil multicastové pakety celou sítí. K dispozici jsme měli programy MSender a Nemesis a oba nedokázaly přeposlat pakety přes směrovače. V lokální síti se pakety zjistit daly, ale pro náš problém to bylo nedostačující. Jen pro zajímavost, Hello pakety u protokolu OSPF se šíří sítí co 10 sekund. Jako příjemce zprávy se opět používá multicastová adresa, a to 224.0.0.5 (všechny směrovače s protokolem OSPF).

Reference

- [1] Grygárek Petr, IP Multicast – přednášky a studijní materiál
- [2] Microsoft Tech Info – PIM-SM Multicast Routing Protocol
- [3] Network Working Group – Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification