

**Semestrální projekt do předmětu
Směrované a přepínané sítě**

**Vysílání a příjem multicastů v Javě.
Návaznost volání jednotlivých metod na
zprávy protokolu IGMP**

1. Úvod

Protokol IP umožňuje komunikaci nejen mezi jednotlivými členy, ale také, kromě jiného, komunikaci v rámci skupiny (multicasting). Skupina může existovat v rámci jednoho síťového segmentu, nebo může být libovolně geograficky rozptýlena.

Skupinové vysílání v IP sítích se zrodilo na Stanfordské univerzitě při vývoji distribuovaného operačního systému VSystem (Steve Deering).

Pozn.: Paradoxně ve světě multicastu je tradiční úloha klient/server změněna. Server zde nečeká na spojení od klienta (žádost), ale asynchronně posílá data do sítě. Naopak klient neinicuje žádné spojení, jen čeká na příchozí data. Této terminologie se budeme držet i v tomto textu.

2. Komunikace ve skupině přes IP a UDP

Důvodem k zavedení skupin byla snaha o snížení zatížení síťového provozu. V případě multicastového vysílání je totiž paket přijímán všemi členy skupiny, aniž by bylo nutné jej vysílat každému členu zvlášť. Tato optimalizace ještě více nabývá na významu v případě vysílání objemnějších dat, která musí být doručena "v reálném čase" (např. on-line videokonference). Dalším pěkným příkladem využití skupinového vysílání je časová synchronizace pomocí služby NTP.

Skupinové vysílání probíhá přes IP síť probíhá pomocí protokolu UDP. Důvod je jednoduchý. V případě spojové orientovaného TCP nelze navázat spojení od jednoho uzlu k mnoha v jedné relaci. Datagramy UDP jsou však vyslány do sítě bez navazování spojení a je jen na členech skupiny, aby je vyzvedli. Výhodou multicastingu je tedy snížení zatížení sítě. Naopak jeho největší slabina tkví právě v použití UDP, přenos dat je tudíž nespolehlivý (podobně jako IP - "pouze" Best Effort)

3. Adresní rozsah pro skupinové vysílání

Pro skupinové vysílání dat se používá speciální vyhrazený adresový prostor ve třídě D (**224.0.0.0 - 239.255.255.255**). První binární oktet skupinové adresy začíná **1110**. Jinak se multicastový IP paket nijak neliší od unicastu. Rozdíl je jen v uvedené cílové adrese. Uvádím menší přehled o použití jednotlivých adres a jejich skupin.

- Lokální linkové (Link-Local) adresy jsou z rozsahu **224.0.0.0 - 224.0.0.255**. Pakety posílané na adresy z tohoto rozsahu nesmí směrovače forwardovat dále a slouží pro adresování strojů v lokální síti. Obvykle mají specifický význam, který přiděluje IANA. Uvádím několik příkladů:
 - **224.0.0.1** - všechny počítače na lokálním segmentu používající multicasting
 - **224.0.0.2** - směrovače připojené k segmentu podporující multicasting
 - **224.0.0.22** - všechny směrovače v lokální síti podporující IGMPv3
- Zvláštní rezervované adresy jsou z rozsahu **224.0.1.0 - 224.0.1.255**. IANA je obvykle přiděluje významným síťovým službám, jako je třeba 224.0.1.1 pro NTP. Tyto adresy se forwardují běžně.
- Adresy s administrativně omezeným rozsahem (Administratively Scoped) patří do rozsahu **239.0.0.0 - 239.255.255.255** a jejich použití se doporučuje pro aplikace s čistě soukromým účelem, pro testování a také pro sítě, které nejsou přímo připojeny do Internetu. Jejich použití je tedy obdobné jako např. u adres **10.0.0.0/8** a podobných (viz RFC1918).

4. Internet Group Management Protocol

Ke správě výše zmíněných skupin slouží protokol IGMP. Pomocí něj jednotliví členové propagují své členství v dané skupině nebo naopak oznamují, že už o data, vysílaná v rámci skupiny, nemají zájem.

Protokol prošel několika verzemi (v0 **RFC988**, v1 **RFC1112**, v2 **RFC2236** a v3 **RFC3376**). Nejnovější třetí verze přináší především možnost selektivního příjmu multicastových zpráv jen z určitých zdrojových IP adres a dále snížení časové prodlevy při opouštění skupin. IGMP protokol používají nejen klienti multicastového vysílání (multicastové servery nemusí být členy skupiny) a směrovače ke vzájemné komunikaci, ale také protokol **DVMRP** (Distance Vector Multicast Routing Protocol - **RFC1075**), který slouží ke komunikaci mezi směrovači a propagaci údajů o registrovaných přijímačích.

Podstatným rysem multicastového vysílání je to, že se šíří po celé intersíti, tedy směrovače je forwardují. A právě výběr rozhraní, za kterými leží členové skupiny, místo prostého floodingu lze zajistit s pomocí **IGMP** (a dalších směrovacích protokolů pro Multicast Routing). Router totiž nemá adresy z multicastového rozsahu (D) ve svých směrovacích tabulkách, ani by to nemělo smysl.

4.1 IGMP v1

Hlavním rysem první verze tohoto protokolu je pracovní schéma na principu Query - Report. Klient, registrující se do skupiny tedy pošle zprávu na její IP adresu (**Membership Report**). O zpracování se stará směrovač, připojený k lokální síti a podporující správu skupinového vysílání.

Směrovač také průběžně kontroluje stav daného segmentu sítě vysláním dotazu (**Membership Query**) na adresu **224.0.0.1** cca každých 60 sekund. Všechny stanice, které jsou členem dané skupiny, čekají náhodnou dobu ze zvoleného časového intervalu a pak vyšlou odpověď (Membership Report). Pokud během čekání pošle zprávu jiná stanice, která je také členem skupiny, ostatní už nic nevysílají. Směrovači stačí jedna zpráva (principiálně je jedno, kolik stanic dané skupiny je na daném segmentu, podstatné je jen to zda tam je aspoň jedna nebo žádná).

Pokud tedy stanice už nemá zájem být členem skupiny, neodpovídá na výzvy od směrovače (každých 60 sekund). Pokud směrovači ani na třetí výzvu (po 3 minutách) nikdo neodpoví, dále už nepředává vysílání do dané skupiny na tento síťový segment.

Právě vypršení časovače je slabinou tohoto řešení. Pokud totiž více stanic rychle mění skupiny, síť bude zahlcena zprávami typu Membership Report, které se vysílají pro každou skupinu zvlášť.

4.2 IGMP v2

Druhá verze protokolu odstraňuje problém první verze protokolu IGMP, protože přináší zprávu typu **LeaveGroup**, kterou klient signalizuje opuštění skupiny. Směrovač na ni reaguje zprávou Membership Query. Je-li na segmentu ještě aspoň jeden klient, ohlásí se směrovači. Tím se zajistí, že zbývající členové skupiny na segmentu nebudou "odstaveni" od datového toku, o který mají zájem. Pokud se však

odhlásí poslední klient, směrovač už nebude na segment vysílat žádná data pro danou skupinu (u IGMPv1 by vysílal ještě 3 minuty).

IGMP verze 2 je zpětně kompatibilní s verzí 1. Pokud klienti multicastového vysílání detekují směrovač s podporou verze 1 (podle **Membership Query**), přejdou na první verzi protokolu. Současně si nastaví časovač na 8 minut. Pokud po uplynutí této doby nezachytí zprávu protokolu IGMPv1, začnou používat verzi 2.

4.3 IGMP v3

Třetí a v současné době poslední verze protokolu pro správu skupin s sebou přináší další významné vylepšení. Jedná se o tzv. filtrování podle zdroje (**Source Filtering**). Je založeno na myšlence, že stanice, která je členem skupiny, může mít zájem o příjem dat jen od některých členů této skupiny. Toto vylepšení se nazývá **Source-Specific Multicasting** (SSM). **IGMPv3** je zpětně kompatibilní se staršími verzemi protokolu.

Pokud se klient připojuje do skupiny zprávou protokolu IGMPv3, vyšle IGMP paket na adresu **224.0.0.22** (adresa směrovačů na segmentu, které podporují IGMP multicasting). Zpráva obsahuje adresu skupiny a seznam zdrojových adres hostů.

S možností filtrování podle zdrojové adresy souvisí se dvěma pracovními módy, které jsou nastaveny jako příznaky v paketu IGMPv3.

- **INCLUDE**
- **EXCLUDE**

Tyto módy jsou ve zprávě nastaveny jako příznak a za nimi následuje seznam zdrojových adres, od kterých klient má/nemá zájem přijímat vysílání pro danou skupinu.

5. Generování multicastových zpráv pomocí Javy (JDK1.4_2)

Jazyk Java poskytuje ke komunikaci nad IP rozhraní Sockets (součást java.net.*). Část tohoto rozhraní slouží i k řízení multicastingu na koncových stanicích. Pomocí rozhraní Sockets lze provádět soketovou komunikaci jak UDP tak TCP. Pro potřeby skupinového vysílání má Java speciální třídu MulticastSocket.

MulticastSocket multicastSocket = new MulticastSocket (port);

Pokud máme na stroji více zařízení, lze soketu explicitně přiřadit jeho adresu pomocí následující konstrukce:

***multicastSocket.setInterface(
InetAddress.getBy_name(String adresaDekadicky));***

Tím jsme vytvořili soket, do kterého lze zapisovat, nebo na něm čekat na příchozí datagramy (metodou **accept()**). Pokud má náš program sloužit jako multicastový server (vysílač dat), lze do soketu rovnou posílat data metodou:

multicastSocket.send(DatagramPacket datagramPacket);

Jak bylo zmíněno výše, datová komunikace ve skupině probíhá pomocí UDP datagramů, protože při tomto typu komunikace nelze efektivně navazovat spojení s

jednotlivými příjemci dat. Pro potřeby přenosu dat před UDP datagramy poskytuje Java třídu DatagramPacket:

***DatagramPacket datagramPacket =
new DatagramPacket(byte[] buffer, int delkaBufferu)***

Vytvoříme tedy objekt této třídy s odpovídajícími daty (binární data) a pak celý objekt předáme metodě send(). Není vůbec nutné aby multicastový server byl členem dané skupiny.

Pokud však náš program má sloužit jako klient, musíme se nejdříve přihlásit do příslušné multicastové skupiny a pak teprve můžeme čekat na příchozí data.

Pokud se tedy se klient chce připojit do skupiny, vytvoří multicastový soket podobně jako server (viz výše) a poté zavolá na soket přihlašovací metodu:

***multicastSocket.joinGroup(
InetAddress.getBy_name(String adresaDekadicky));***

Je vyslán IGMPv3 paket na adresu 224.0.0.22 a informován směrovač, připojený na lokální segment sítě. Ten pak předává všechny skupinové UDP datagramy příslušné skupiny na tento segment a klientovi se dostávají potřebná data.

Pokud už klient nemá zájem o členství ve skupině, zavolá na multicastový soket metodu:

***multicastSocket.leaveGroup(
InetAddress.getBy_name(String adresaDekadicky));***

Opět je informován směrovač, který provede kroky popsané v úvodu tohoto textu a zjistí, zda na segmentu ještě není další klient dané skupiny. Pokud, ne, další datový provoz pro tuto skupinu už na daný segment neforwarduje.

6. Praktické ověření

Pro praktické ověření jsem použil následující techniku:

- desktop AMD Athlon x86
 - Linux Mandrake 10.0 kernel 2.6.3-4 - rekompileováno
 - integrovaná síťová karta VIA 6102 Rhine 2 10/100 (Ethernet)
- notebook AmiloPro Intel Pentium M
 - Microsoft Windows XP SP1
 - integrovaná karta Realtek RTL8139/810x Family Fast Ethernet NIC

Z důvodu nedostatku použitelné techniky jsem se rozhodl ukázat použití IGMP a multicastu pouze na jednom segmentu (viz obr.1). Původně jsem se sice pokoušel nastavit druhý síťový segment pomocí loopback zařízení, ale testovací konfigurace nepracovala správně. Problém je jednak s tím, že multicastový routovací daemon pimd nepodporuje multicastování na loopback zařízeních a i po instalaci více síťových karet jsem narážel na problém s tím, že router i segment (další kartu) obsluhuje jedno linuxové jádro. Zde je podle mě i příčina nezdaru takové konfigurace. Proto zde uvádím pouze testovací příklad na jednom síťovém segmentu (obr.1).



obr.1: Topologie zapojení testovací sítě

6.1 Klient multicastového vysílání pomocí Javy ([MulticastClient](#))

Pro praktické ověření multicastingu jsem vytvořil jednoduchého klienta pomocí Java rozhraní sockets popsaného výše. Klient se přihlásí do skupiny a vypisuje posílané znaky. Po přijetí tečky se odhlásí. Projde tedy celým životním cyklem. Nejprve provede přihlášení do skupiny, pak přijímá data, po ukončení se ze skupiny odhlašuje.

Klientovi se předá adresa skupiny, do které se bude hlásit, a adresa síťového rozhraní, které se použije pro komunikaci. Typické užití vypadá takto:

```
java MulticastClient 239.1.1.1 10.0.0.3
```

V testovaném příkladě běžel klient na notebooku s Windows XP.

6.2 Server multicastového vysílání pomocí Javy ([MulticastServer](#))

Server se po svém spuštění nepřihlašuje do žádné skupiny, pouze vysílá text zapisovaný a potvrzený Enterem na konzoli do sítě na adresu zadané skupiny. Principiálně multicastový server vůbec nemusí být členem dané skupiny, proto se do ní nepřihlašuje.

Server běžel na linuxové stroji na rozhraní eth1. Použití tedy vypadá takto:

```
java MulticastServer 239.1.1.1 10.0.0.2
```

6.3 Příprava routeru

Router tvoří desktop s Linuxem a pracuje na rozhraní eth0 (10.0.0.2/8). Před samotnou instalací bylo nejdříve nutné překompilovat jádro.

6.3.1 Kompilace jádra

Použil jsem distribuci Mandrake 10.0 Community version a jádro k ní dodané s číslem 2.6.3-4mdk. Před samotnou kompilací bylo nutné nastavit několik parametrů, které nejsou standardní:

```
CONFIG_IP_MULTICAST           =y
CONFIG_IP_ADVANCED_ROUTER     =y
CONFIG_IP_MROUTE               =y
CONFIG_IP_PIMSM_V1            =y
CONFIG_IP_PIMSM_V2            =y
```

6.3.2 Nastavení síťových rozhraní

Pro konfiguraci sítě jsem použil programy z balíku *ip*. Podle výše uvedené topologie byla síťová rozhraní nastavena takto:

eth0:

<i>ip link set eth0 down</i>	(vypneme rozhraní)
<i>ip link set eth0 arp on</i>	(bude používat ARP)
<i>ip link set eth0 promisc off</i>	(vypneme promiskuitní mód)
<i>ip link set eth0 allmulti on</i>	(čte všechny multicast zprávy)
<i>ip link set eth0 multicast on</i>	(zapneme podporu multicastingu)
<i>ip link set eth0 up</i>	(zapneme rozhraní)
<i>ip add flush dev eth0</i>	(vymažeme všechny IP adresy)
<i>ip addr add 192.168.0.2/24 brd + dev eth0</i>	(přidáme adresu)

eth1:

<i>IP adresa:</i>	<i>10.0.0.3</i>
<i>maska podsítě:</i>	<i>255.0.0.0</i>
<i>výchozí brána:</i>	<i>10.0.0.2</i>

6.3.3 Nastavení směrování

I když jsem ve skutečnosti neprováděl žádné směrování paketů, multicastový routovací daemon pimd si žádá, aby běželo předávání paketů (***ip_forward***). Službu lze aktivovat následujícím způsobem:

echo 1 > /proc/sys/net/ipv4/ip_forward

Konfigurace směrovací tabulky pak byla jednoduchá. Je možné i ponechat nastavení jádra, která pochází z nastavení logických adres, protože síť je přímo připojená:

ip route flush all
ip route add 10.0.0.0/8 dev eth0

Dále je potřeba povolit směrování multicastů. Například následující dva řádky povolí směrování všech multicastových zpráv pro síť 224.0.0.0/4 a 239.0.0.0/8 do rozhraní eth0.

ip route add multicast 224/4 dev eth0
ip route add multicast 239/8 dev eth0

6.3.4 PIMD - instalace a nastavení

PIMD (Protocol Independent Multicast Daemon) je směrovací služba, která poskytuje podporu správy skupinového vysílání a předávání (forward) paketů v IP sítích. Existuje ve dvou verzích PIMDv1 podporuje IGMPv1 a novější verze PIMDv2, použitá i v tomto příkladě, podporující IGMPv2. Pro podporu nejnovější verze IGMP protokolu IGMPv3 je třeba použít některý jiný program, například mrouted, nebo některou verzi Gated s podporou multicastingu.

Zdrojová distribuce PIMD je určena nejen operačnímu systému Linux, ale především FreeBSD, Solaris a jiným. Proto je nutné před překladem upravit Makefile podle cílové distribuce (velice jednoduchým zrušením komentáře u řádku dané distribuce).

Po kompilaci nám stačí spustitelný soubor **pimd** a soubor s nastavením **pimd.conf**, který umístíme do adresáře **/etc**. Návod ke konfiguraci je přímo v něm.

6.4 Zprávy multicastového routeru

Ihned po spuštění začíná daemon pimd posílat do obou síťových segmentů zprávy protokolem PIM (Protocol Independent Multicast). Pomocí něj komunikuje se všemi PIM směrovači na stejném segmentu (obr.2).

Tyto zprávy slouží k dynamické výměně dat pro směrování multicastových zpráv. Detaily jsou patrné z následujícího obrázku. Všimněme si především hodnoty TTL IP paketu, která signalizuje, že paket je určen jen následujícímu směrovači a že nesmí být předáván (forward) dále.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.0.2	224.0.0.13	PIMv2	Bootstrap
2	24.992623	10.0.0.2	224.0.0.13	PIMv2	Hello
3	29.991141	10.0.0.2	224.0.0.13	PIMv2	Bootstrap
4	54.983766	10.0.0.2	224.0.0.13	PIMv2	Hello
5	59.982287	10.0.0.2	224.0.0.13	PIMv2	Bootstrap

⊞ Frame 1 (70 bytes on wire, 70 bytes captured)

⊞ Ethernet II, Src: 00:0c:76:3b:b5:b8, Dst: 01:00:5e:00:00:0d

⊞ Internet Protocol, Src Addr: 10.0.0.2 (10.0.0.2), Dst Addr: 224.0.0.13 (224.0.0.13)

⊞ Protocol Independent Multicast

- Version: 2
- Type: Bootstrap (4)
- Checksum: 0xcd6b (correct)
- ⊞ PIM parameters
 - Fragment tag: 0xe448
 - Hash mask len: 30
 - BSR priority: 5
 - BSR: 10.0.0.2
 - ⊞ Group 0: 224.0.0.0/4
 - RP count: 1
 - FRP count: 1
 - RP 0: 10.0.0.2
 - Holdtime: 60
 - Priority: 20

obr.2: Zprávy multicastového routovacího daemona protokolem PIMv2

Skupinová adresa **224.0.0.13** patří mezi vyhrazené adresy a patří všem multicastovým routerům na lokálním síťovém segmentu podporujícím PIM.

6.5 Přihlášení klienta do skupiny pomocí IGMPv2

Klient po svém spuštění vysílá na svůj síťový segment IGMP zprávu typu Membership Report (obr.3). Hodnota TTL je opět rovna 1, protože zprávu typu Membership Report mají slyšet pouze směrovače na lokálním segmentu a nepředávat je dál. Informace z těchto zpráv jsou určeny ke zpracování pouze jim. V tomto případě (obr.3) se klient hlásil ke skupině **239.1.1.1**. Nutno dodat, že verze zprávy IGMPv2 je vynucena směrovačem, přičemž klient jej rozpoznal ze dříve přijatých paketů typu PIMv2.

Kromě IGMP zprávy si povšimněme zejména položky **IP options**, která obsahuje nastavení **Router Alert**, tedy každý router, který zachytí tento paket, by jej měl zpracovat (předat vyšší vrstvě).

No. ↓	Time	Source	Destination	Protocol	Info
3	3.294331	10.0.0.3	239.1.1.1	IGMP	V2 Membership Report

☒ Frame 4 (46 bytes on wire, 46 bytes captured)					
☒ Ethernet II, Src: 00:02:3f:12:2f:bc, Dst: 01:00:5e:01:01:01					
☒ Internet Protocol, Src Addr: 10.0.0.3 (10.0.0.3), Dst Addr: 239.1.1.1 (239.1.1.1)					
Version: 4 Header length: 24 bytes					
☒ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)					
Total Length: 32 Identification: 0x7168 (29032)					
☒ Flags: 0x00 Fragment offset: 0 Time to live: 1 Protocol: IGMP (0x02) Header checksum: 0xb96a (correct) Source: 10.0.0.3 (10.0.0.3) Destination: 239.1.1.1 (239.1.1.1)					
☒ Options: (4 bytes)					
Router Alert: Every router examines packet					
☒ Internet Group Management Protocol					
IGMP Version: 2 Type: Membership Report (0x16) Max Response Time: 0,0 sec (0x00) Header checksum: 0xf9fc (correct) Multicast Address: 239.1.1.1 (239.1.1.1)					

obr.3: Přihlášení klienta do skupiny pomocí IGMPv2 zprávy typu Membership Report

6.6 Odhlášení klienta ze skupiny pomocí IGMPv2

Pokud už klient nemá zájem o příjem paketů multicastového vysílání a pokud podporuje IGMPv2 nebo IGMPv3, pošle do sítě zprávu typu **Leave Group** (obr.4). Tou dává směrovači najevo, že už nemá zájem o příjem paketů pro danou skupinu. Je už na směrovači, aby si ve vlastní režii zjistil, zda je na segmentu ještě nějaký jiný člen inkriminované skupiny.

No. ↓	Time	Source	Destination	Protocol	Info
11	36.426345	10.0.0.3	224.0.0.2	IGMP	V2 Leave Group

☒ Frame 11 (46 bytes on wire, 46 bytes captured)					
☒ Ethernet II, Src: 00:02:3f:12:2f:bc, Dst: 01:00:5e:00:00:02					
☒ Internet Protocol, Src Addr: 10.0.0.3 (10.0.0.3), Dst Addr: 224.0.0.2 (224.0.0.2)					
Version: 4 Header length: 24 bytes					
☒ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)					
Total Length: 32 Identification: 0x7169 (29033)					
☒ Flags: 0x00 Fragment offset: 0 Time to live: 1 Protocol: IGMP (0x02) Header checksum: 0xc969 (correct) Source: 10.0.0.3 (10.0.0.3) Destination: 224.0.0.2 (224.0.0.2)					
☒ Options: (4 bytes)					
☒ Internet Group Management Protocol					
IGMP Version: 2 Type: Leave Group (0x17) Max Response Time: 0,0 sec (0x00) Header checksum: 0xf8fc (correct) Multicast Address: 239.1.1.1 (239.1.1.1)					

obr.4: Odhlášení klienta ze skupiny pomocí IGMPv2 zprávy typu Leave Group

Uvedená činnost se realizuje tak, že po přijetí zprávy **Leave Group** posílá směrovač zpět zprávu **Membership Query**, aby se dotázal na další zbývající klienty (viz dále). Všichni klienti, kteří patří do této skupiny, zachytí zprávu a spustí si časovač. Po náhodné době z určitého maximálního intervalu (typicky 10 sekund) pošle každý klient odpověď zprávou typu IGMPv2 Membership Report. Klienti však během svého čekání poslouchají provoz a pokud některý jiný klient pošle zprávu, oni sami už zprávu neposílají.

Z principu totiž směrovači nezáleží na tom kolik je na segmentu členů dané skupiny, ale zda je tam aspoň jeden nebo žádný. Pokud tedy odpoví jeden klient, není třeba, aby odpovídali další klienti a zahlcovali tak provoz.

6.7 Router jako člen skupiny

Směrovač s podporou multicastového vysílání je sám o sobě také členem několika skupin. Jedná se především o skupinu **224.0.0.2**. Je to skupina všech směrovačů podporujících multicasting na daném segmentu. V testovaném příkladě je použit multicastový routovací daemon pimd, který se hlásí i do skupiny **224.0.0.13**, která je vyhrazena všem PIM směrovačům na daném síťovém segmentu. Ukázka zachycených zpráv Membership report je na obrázku 5.

41	195.216227	10.0.0.2	224.0.0.13	IGMP	V2 Membership Report
42	195.639094	10.0.0.2	224.0.0.2	IGMP	V2 Membership Report

obr.5: Směrovač resp. jeho rozhraní s adresou 10.0.0.2 se hlásí do uvedených skupin.

6.8 Časová synchronizace a NTP

Jedním z praktických příkladů použití multicastingu je komunikace za účelem synchronizace času pomocí **daemonu NTP**. Tato služba běží ve Windows na pozadí, aniž by o ní běžný uživatel věděl naslouchá na každém síťovém zařízení počítače a čeká na multicastové zprávy, které nesou informaci o čase. Na síti tak může existovat jeden centrální server, který rozesílá tyto data formou multicastových zpráv a všechny stanice na síti si upraví čas systému podle serveru. Služba NTP resp. její klient se hlásí do rezervovaná skupiny **239.255.255.0** (obr.6).

No. -	Time	Source	Destination	Protocol	Info
25	75.791217	10.0.0.3	239.255.255.250	IGMP	V2 Membership Report

[+] Frame 25 (46 bytes on wire (46 bytes captured) on interface 0)					
[+] Ethernet II, Src: 00:02:3f:12:2f:bc, Dst: 01:00:5e:7f:ff:fa					
[+] Internet Protocol, Src Addr: 10.0.0.3 (10.0.0.3), Dst Addr: 239.255.255.250 (239.255.255.250)					
Version: 4					
Header length: 24 bytes					
[+] Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)					
Total Length: 32					
Identification: 0x716e (29038)					
[+] Flags: 0x00					
Fragment offset: 0					
Time to live: 1					
Protocol: IGMP (0x02)					
Header checksum: 0xb96c (correct)					
Source: 10.0.0.3 (10.0.0.3)					
Destination: 239.255.255.250 (239.255.255.250)					
[+] Options: (4 bytes)					
Router Alert: Every router examines packet					
[+] Internet Group Management Protocol					
IGMP Version: 2					
Type: Membership Report (0x16)					
Max Response Time: 0,0 sec (0x00)					
Header checksum: 0xfa04 (correct)					
Multicast Address: 239.255.255.250 (239.255.255.250)					

obr.6: Touto zprávou se hlásí stanice ke skupině poskytující časovou synchronizaci

6.9 Výzvy routeru, odpovědi a timeout

Pokud se klient odhlásí ze skupiny, pošle zprávu IGMP **Leave Group**, pokud však klient selže nebo přestane reagovat, existuje už od dob IGMPv1 další mechanismus, který zajistí, že router po určité době přestane vysílat na daný segment data pro skupinu.

Jak bylo uvedeno v části 6.6, po přijetí zprávy **Leave Group** se router dotazuje na další členy. Navíc se však router dotazuje na členy každých 30 sekund (pokud není nastaveno jinak). Tedy každé půl minuty posílá na daný segment IGMP zprávu typu **Membership Query**. Pokud se mu po třikrát nedostane odpovědi zprávou **Membership Report**, přestane pro danou skupinu předávat data do tohoto segmentu. Prakticky to tedy znamená, že 90 sekund po poslední odpovědi klienta, přestane směrovač předávat datový provoz.

To je také hlavní slabina protokolu IGMPv1, který podporoval pouze tento způsob "odhlášení", tedy neobsahoval zprávy typu **Leave Group**. Pokud tedy více klientů na jedné síti rychle měnilo skupiny, došlo brzy k zahlcení sítě datovým provozem, o který už nikdo nestál.

V testované příkladě byla použita pro vytvoření klienta Java. Nepodařilo se mi vytvořit situaci, kdy by klient přestal odpovídat na výzvy **Membership Query**. Klient stihl vždy poslat odpověď, případně zprávu **Leave Group** a to i tehdy když jsem klienta ukončil na úrovni procesu! Příčinou je zpracování samotného jádra Windows, Java pouze volá jeho API.

6.10 Datový provoz v multicastové síti

Multicastový server posílá data ve formě zpráv protokolu **UDP** nad protokolem UDP. Pro multicastové vysílání nelze použít TCP resp. službu se spojením (viz teoretický úvod).

No. ↓	Time	Source	Destination	Protocol	Info
4	4.294298	10.0.0.3	239.1.1.1	IGMP	V2 Membership Report
5	13.240593	10.0.0.2	239.1.1.1	ICQ	

[-] Frame 5 (69 bytes on wire, 69 bytes captured)

[-] Ethernet II, Src: 00:05:1c:13:74:80, Dst: 01:00:5e:01:01:01

[-] Internet Protocol, Src Addr: 10.0.0.2 (10.0.0.2), Dst Addr: 239.1.1.1 (239.1.1.1)

Version: 4

Header length: 20 bytes

[-] Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)

Total Length: 55

Identification: 0x0000 (0)

[-] Flags: 0x04

Fragment offset: 0

Time to live: 1

Protocol: UDP (0x11)

Header checksum: 0x7fb2 (correct)

Source: 10.0.0.2 (10.0.0.2)

Destination: 239.1.1.1 (239.1.1.1)

[-] User Datagram Protocol, Src Port: 4000 (4000), Dst Port: 4001 (4001)

Source port: 4000 (4000)

Destination port: 4001 (4001)

Length: 35

Checksum: 0x8b86 (correct)

0000	01 00 5e 01 01 01 00 05 1c 13 74 80 08 00 45 00	..^.....t...E.
0010	00 37 00 00 40 00 01 11 7f b2 0a 00 00 02 ef 01	.7..@...
0020	01 01 0f a0 0f a1 00 23 8b 86 61 68 6f 6a 2c 20	#..ahoj,
0030	74 6f 68 6c 65 20 6a 65 20 6d 75 6c 74 69 63 61	tohle je multica
0040	73 74 69 6e 67	sting

obr.7 Datový paket přenášející multicastová data

Jak je vidět (obr.7), na rozdíl od IGMP zpráv zde není nastaven příznak **Router Alert**, tedy jedná se o běžný datový paket. Hodnota **TTL** je nastavena na 1, tedy směrovač musí rozhodnout, zda a kam forwardovat paket (specifický znak multicastu). Data jsou vysílána na skupinovou adresu **239.1.1.1**, což odpovídá privátnímu rozsahu multicastového vysílání. V dolní části obrázku jsou vidět textová data vysílaná pro skupinu.

6.11 Vysílání a příjem dat pro více skupin

Naprogramovaného klienta i server jsem vyzkoušel také pro provoz ve více skupinách. Klient (příjemce zpráv) poslouchá na portu 4001, server (vysílač) vysílá z portu 4000. Provoz se předává z portu relační vrstvy výš a o rozdělení se pak nejspíš stará aplikace (tedy **JVM**).

Provedl jsem tedy malý testovací příklad. Spustil jsem dva různé multicastové servery na linuxovém stroji:

```
java MulticastServer 239.1.1.1 10.0.0.2
java MulticastServer 239.1.1.2 10.0.0.2
```

Analogicky jsem pak spustil klienta na notebooku s Windows následujícím způsobem:

```
java MulticastClient 239.1.1.1 10.0.0.3
java MulticastClient 239.1.1.2 10.0.0.3
```

Servery i klienti běželi paralelně bez problémů jejich spouštění či ukončení vzájemně neovlivňovalo druhý běžící program. Na obrázcích 8 a 9 je uveden odchycený datový provoz mezi servery a klienty. Nejprve je spuštěn klient skupiny **239.1.1.1** pak druhý klient. Spouštění serverů klienty nijak neovlivňuje, navíc, servery se do skupin vůbec nepřihlašují (není to třeba). Servery jsou naprogramovány tak, aby při ukončení jejich vysílání se ukončili i klienti (rozpoznáním datového ICQ paketu obsahujícího tečku - ukončovací znak). Po přijetí takového paketu se klienti odhlašují z daných skupin.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.0.3	224.0.0.22	IGMP	V3 Membership Re
2	0.997312	10.0.0.3	224.0.0.22	IGMP	V3 Membership Re
3	3.343874	10.0.0.3	224.0.0.22	IGMP	V3 Membership Re
4	3.997138	10.0.0.3	224.0.0.22	IGMP	V3 Membership Re
5	17.716504	10.0.0.2	239.1.1.1	ICQ	
6	33.290621	10.0.0.2	239.1.1.2	ICQ	
7	36.741939	10.0.0.2	239.1.1.1	ICQ	[Malformed Packe
8	36.745120	10.0.0.3	224.0.0.22	IGMP	V3 Membership Re
9	37.495707	10.0.0.3	224.0.0.22	IGMP	V3 Membership Re
10	37.974402	10.0.0.2	239.1.1.2	ICQ	[Malformed Packe
11	37.977565	10.0.0.3	224.0.0.22	IGMP	V3 Membership Re
12	38.495673	10.0.0.3	224.0.0.22	IGMP	V3 Membership Re

Frame 1 (54 bytes on wire, 54 bytes captured)

Ethernet II, Src: 00:02:3f:12:2f:bc, Dst: 01:00:5e:00:00:16

Internet Protocol, Src Addr: 10.0.0.3 (10.0.0.3), Dst Addr: 224.0.0.22 (224.0.0.22)

Internet Group Management Protocol

IGMP Version: 3

Type: Membership Report (0x22)

Header checksum: 0xe9fb (correct)

Num Group Records: 1

Group Record : 239.1.1.1 Change To Exclude Mode

obr.8: přihlášení prvního klienta

1	0.000000	10.0.0.3	224.0.0.22	IGMP	V3 Membership Rep
2	0.997312	10.0.0.3	224.0.0.22	IGMP	V3 Membership Rep
3	3.343874	10.0.0.3	224.0.0.22	IGMP	V3 Membership Rep
4	3.997138	10.0.0.3	224.0.0.22	IGMP	V3 Membership Rep
5	17.716504	10.0.0.2	239.1.1.1	ICQ	
6	33.290621	10.0.0.2	239.1.1.2	ICQ	
7	36.741939	10.0.0.2	239.1.1.1	ICQ	[Malformed Packet
8	36.745120	10.0.0.3	224.0.0.22	IGMP	V3 Membership Rep
9	37.495707	10.0.0.3	224.0.0.22	IGMP	V3 Membership Rep
10	37.974402	10.0.0.2	239.1.1.2	ICQ	[Malformed Packet
11	37.977565	10.0.0.3	224.0.0.22	IGMP	V3 Membership Rep
12	38.495673	10.0.0.3	224.0.0.22	IGMP	V3 Membership Rep

+

Frame 3 (54 bytes on wire (54 bytes captured) on interface 0:00:00:00:00:00)

+

Ethernet II, Src: 00:02:3f:12:2f:bc, Dst: 01:00:5e:00:00:16

+

Internet Protocol, Src Addr: 10.0.0.3 (10.0.0.3), Dst Addr: 224.0.0.22 (224.0.0.22)

+

Internet Group Management Protocol

IGMP Version: 3

Type: Membership Report (0x22)

Header checksum: 0xe9fa (correct)

Num Group Records: 1

Group Record : 239.1.1.2 Change To Exclude Mode

obr.9: přihlášení druhého klienta

6.12 IGMPv3

Klient se typicky snaží používat co nejnovější verzi protokolu IGMP tedy verzi 3 (pokud ji sám podporuje). Pokud však směrovač podporuje pouze verzi starší, například IGMPv2 tak, jako je to v případě multicastového routovacího daemona PIMDv2, pak se klienti přizpůsobí směrovači.

Klient rozpozná používanou verzi protokolu podle zpráv **Membership Query**, které obsahují verzi protokolu, lepší klienti případně i podle zachycených zpráv multicastového routovacího protokolu. Pokud je požadována starší verze protokolu, klient ji začne používat a spustí si časovač. Po 480 sekundách se opět pokusí iniciovat novější verzi protokolu. Klienti se tedy přizpůsobují směrovačům.

Použitá verze protokolu IGMP samozřejmě nijak neovlivňuje datové pakety, které přenášejí data, pouze skupiny klientů, které je poslouchají.

Novější verze protokolu IGMPv3 přináší možnost filtrace zdrojů (**Source Filtering**), které umožňuje klientovi propagovat jeho zájem o příjem multicastových paketů jen z některých zdrojových adres (tedy jen z některých multicastových serverů). To snižuje zátěž sítě a navíc poskytuje další zabezpečovací prvek proti útokům typu **DoS** a **DDoS**.

Jak bylo uvedeno v části 4.3, **IGMPv3** zprávy typu **Membership Report** se liší od starších a přidávají dva módy: **INCLUDE** a **EXCLUDE**. Tyto módy jsou v paketech následovány seznamem adres, jednak zdrojových, jednak seznamem skupin, v závislosti na typu záznamu (**Record Type**). Podrobně je tato problematika popsána v **RFC2236** (IGMPv3).

Prakticky jsem ověřil zprávy IGMPv3 při přihlášení a odhlášení ze skupiny. Pro tento účel jsem na desktopu s Linuxem rebootoval do Windows XP, přičemž adresování zůstalo stejné. Linuxový routovací daemon totiž IGMPv3 nepodporoval. Na druhém stroji jsem pak rozběhl multicastový server:

java MulticastServer 239.1.1.1 10.0.0.2

Na druhém stroji jsem pak spustil klienta a zachytával jeho zprávy typu **Membership Report**. Ty se ve verzi 3 výrazně liší (viz obr.10):

No. ↓	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.0.3	224.0.0.22	IGMP	V3 Membership Rep

Frame 1 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 00:02:3f:12:2f:bc, Dst: 01:00:5e:00:00:16 Internet Protocol, Src Addr: 10.0.0.3 (10.0.0.3), Dst Addr: 224.0.0.22 (224.0.0.22) Internet Group Management Protocol IGMP Version: 3 Type: Membership Report (0x22) Header checksum: 0xe9fb (correct) Num Group Records: 1 Group Record : 239.1.1.1 Change To Exclude Mode Record Type: Change To Exclude Mode (4) Aux Data Len: 0 Num Src: 0 Multicast Address: 239.1.1.1 (239.1.1.1)					

obr.10: Zpráva typu Join Group multicastového klienta ve verzi IGMPv3

Jak vidíme, paket není adresován přímo na adresu skupiny, do které se klient hlásí, ale na adresu všech PIM směrovačů na lokální síti, tedy **224.0.0.22**. Samotná adresa skupiny resp. jejich seznam je obsažen až uvnitř IGMP paketu. Kromě počtu záznamů a jiných informací obsahuje především pole typ záznamu (**Record Type**). V našem případě má hodnotu **Change To Exclude Mode**, tedy avizuje, že klient má zájem o příjem adres z následujícího seznamu skupin. V našem případě následuje jen jedna skupinová adresa (klient se hlásí jen do skupiny **239.1.1.1**). V případě, že se klient hlásí do více skupin, nebo mění členství ve více skupinách, vše se provede vysláním jednoho paketu, což s sebou přináší další snížení zátěže sítě.

Pokud klient opouští nějakou skupinu nebo skupiny, pošle podobnou zprávu pouze s jiným typem záznamu **Change To Include Mode**. Tím dává klient najevo, že nemá už zájem o příjem paketů z následujícího seznamu skupin (viz obr.11).

No. ↓	Time	Source	Destination	Protocol	Info
18	65.725771	10.0.0.3	224.0.0.22	IGMP	V3 Membership Repo

Frame 18 (54 bytes on wire, 54 bytes captured) Ethernet II, Src: 00:02:3f:12:2f:bc, Dst: 01:00:5e:00:00:16 Internet Protocol, Src Addr: 10.0.0.3 (10.0.0.3), Dst Addr: 224.0.0.22 (224.0.0.22) Internet Group Management Protocol IGMP Version: 3 Type: Membership Report (0x22) Header checksum: 0xea fa (correct) Num Group Records: 1 Group Record : 239.1.1.2 Change To Include Mode Record Type: Change To Include Mode (3) Aux Data Len: 0 Num Src: 0 Multicast Address: 239.1.1.2 (239.1.1.2)					

obr.11: Zpráva typu Leave Group při použití IGMPv3

7. Závěr

Multicastové vysílání přináší především snížení zátěže síťového provozu, směrovačů a prepínačů. Umožňuje rozvoj a aplikaci nových síťových služeb, ať už se jedná o Internetová rádia, streamované video, nebo třeba on-line videokonference.

Na druhou stranu s sebou přináší zvýšení režie směrovačů v tom smyslu, že musí spravovat mechanismus, který zajistí správné směrování multicastových zpráv. Ideální pomocí pro tento problém je využití protokolu IGMPv3, který poskytuje směrovacím protokolům dobrou podporu k vytváření jejich multicastových směrovacích tabulek. Další problém je výměna multicastových směrovacích dat. Podporu pro ni zajišťují specializované směrovací protokoly PIM, DVMRP a jiné.

Použité zdroje:

- RFC 3376 (Internet Group Management Protocol version 3)
- <http://lupa.cz> - seriál Úvod do IP multicastu (díly 1.-5.)
- <http://cs.vsb.cz/grygarek> (Java a rozhraní Sockets)
- <http://xerox.com> - multicast routing daemon mrouted
- <http://netweb.usc.edu/pim/> - PIMD mc routing daemon
- <http://cisco.com> - informace o multicastování a konfiguraci
- <http://root.cz> - seriál článků Linux jako internetová gateway